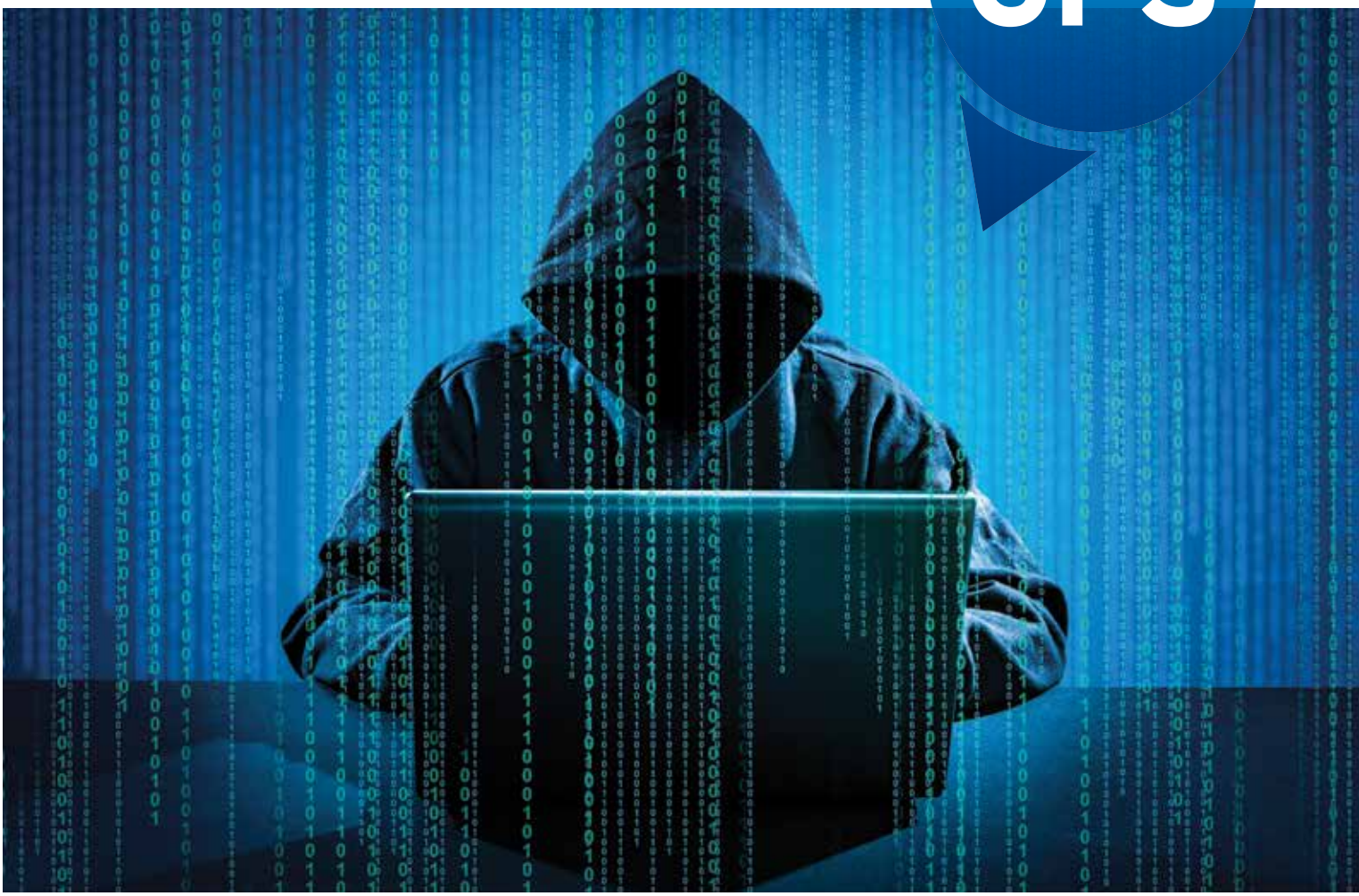
Citi GPS



MANAGING CYBER RISK WITH HUMAN INTELLIGENCE

A Practical Approach

Citi GPS: Global Perspectives & Solutions

May 2019

Elizabeth Petrie
Managing Director, Citi Technology & Cyber Risk
+1 (202) 776-1518
elizabeth.petrie@citi.com

Walter H Pritchard, CFA
U.S. Software Analyst, Citi Research
+1 (415) 951-1770
walter.h.pritchard@citi.com

Elizabeth Curmi
Global Thematic Analyst, Citi Research
+44-20-7986-6818
elizabeth.curmi@citi.com

Jeremy E Benatar, CFA
U.S. Software Team, Citi Research
+1 (212) 816-8916
jeremy.benatar@citi.com

Catherine T O'Neill
European Media Analyst, Citi Research
+44-20-7986-8053
catherine.oneill@citi.com

Dr. Andrew Coburn
Chief Scientist
Cambridge Centre for Risk Studies, Judge School of Business, University of Cambridge

Tamara Evans
Cambridge Centre for Risk Studies, Judge Business School, University of Cambridge

Arvind Purushotham
Global Head of Venture Investing, Citi Ventures
+1 (650) 798-8111
arvind.purushotham@citi.com

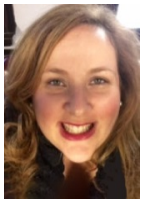
Charlotte Branfield
Head of Int'l Standards & Strategic External Engagement, Citi Global Information Security
+44 (20) 7986-8936
charlotte.thoms.branfield@citi.com

Teresa Chan
Cyber Risk Officer, Citi
+1 (202) 879-6824
teresa.chan@citi.com

Justin Deck
Senior Manager, Citi Technology & Cyber Operational Risk
+1 (202) 879-6802
justin.deck@citi.com

Nancy Glynn
Int'l Standards & Strategic External Engagement, Citi Global Information Security
+1 (212) 816-5535
nancy.glynn@citi.com

Brendan Goode
Global Head of Cyber Risk, Citi
+1 (212) 816-0079
brendan.goode@citi.com



Alyson Krause
Head of Cyber Risk Threat Management, Citi
+1 (212) 816-4472
alyson.krause@citi.com

Steven Landes
Outreach & Synchronization Lead, Citi Information Security
+1 (937) 540-0220
steven.landes@citi.com

Danielle J Meah
Chief of Analysis, Citi Cyber Intelligence Center
+1 (908) 563- 1065
danielle.j.meah@citi.com

Yogesh Mudgal
Director of Emerging Technology Risk, Citi
+1 (212) 816-8632
yogesh.mudgal@citi.com

Lauren Podber
Cyber Risk Officer, Citi
+1 (212) 816-9279
lauren.podber@citi.com

Michael Polscer
Cyber Risk Communications & Awareness, Citi
+1 (212) 816-9041
michael.polscer@citi.com

David Rose
EMEA Head of Digital Security, Citi TTS
+44 (20) 7500-9005
david.rose@citi.com

Rajesh Shenoy
Global Head of Digital Security, Citi TTS
+1 (908) 563-6485
rajesh.a.shenoy@citi.com

University of Cambridge
James Bourdeau **Jennifer Copic** **Dr Jennifer Daffron**
Dr Scott Kelly **Eireann Leverett** **Kelly Quantrill** **Simon Ruffle**

Citi Research
Michael Bilerman **Michael Rollins, CFA**

MANAGING CYBER RISK WITH HUMAN INTELLIGENCE

A Practical Approach

Kathleen Boyle, CFA
Managing Editor, Citi GPS

For years we've been told stories about how technology was going to make our lives better. And for the most part, it has. Technology has increased our efficiency, has allowed us to work from remote locations, and facilitates business transactions across the globe with a few keystrokes on a computer. As an individual, we can video chat with our loved ones, track our heart rate and exercise goals on a wrist watch, and control the lights, the thermostat, and see who's ringing the doorbell at our home all from an app on our mobile device.

Sadly, as with most things that are good in life, there is also a downside to technology. For all the reasons technology is a positive – interconnectedness, access, increased speed and efficiency – it is also a negative. Specifically, the positive attributes of technology can be used as a tool for criminal behavior that puts individuals, corporations, and governments at risk of cyber breaches.

It is estimated that cyber breaches cost the global economy $1.5 trillion per year, and this is expected to increase, with some sources believing it could cost the global economy a staggering $6 trillion by 2021. The increasing scale of cyber breaches means it has now become necessary for organizations to mature beyond a basic reactive defensive approach on cyber, to an intelligence-led, proactive one. To be intelligence-led is to know both yourself and your enemy. This means knowing what your critical assets are and who may have the motivation and capability to threaten those assets.

How are governments, corporations, and individuals tackling such risks? Governments have started to take cyber attacks more seriously. In fact many countries such as the U.S. and U.K. have set up national agencies dedicated solely to protecting government assets from cyber attacks. One particular concern involves cyber attacks on critical infrastructure systems. On the corporate side, many organizations are now asking themselves *when* an attack will occur, not *if*. As such, it is critical for a company to analyze and understand all potential points of cyber impact. We argue that taking an intelligence-led approach is the solution. Corporates should evolve to an active defense strategy by understanding the key drivers of cyber and building an effective security program through strong partnerships between their business lines and risk management teams.

Technology can also form part of the solution. As the corporates shift their technology needs from on-premise to cloud, the security solutions market is being reinvented, with hyper-scale cloud providers potentially playing a larger role in addressing security challenges. We note virtual/cloud form-factors of traditional products, like firewalls, becoming more important, as are new technologies such as cloud-based security brokers (CASB). Emerging tech solutions such as artificial intelligence, machine learning, blockchain, behavioral biometrics, and others can also provide an enhanced ability to predict and analyze threats and detect and stop cyber attacks — all at a speed and scale that would not have been possible without their use.

The risk of cyber attacks is most likely growing versus subsiding and having an intelligence-led approach will be critical to getting ahead of new threats. As an FBI agent recently said at a conference "The goal is to avoid a massive loss either in a business line at a corporate or in a personal account because someone clicked on a dancing kitty." Human intelligence…

Intelligence is Key in Developing a Cyber Risk Strategy

THE RISE IN INTERNET USE PLUS AN INCREASE IN IOT DEVICES MEANS CYBERATTACKS ARE INCREASINGLY AN ISSUE

2008 >>> 2018

The number of Internet users worldwide has increased...

100%

...while the number of websites has grown

818%

FINANCIAL LOSSES FROM DISRUPTIVE NON-TARGETED CYBERATTACKS CAN BE MASSIVE

Data Exfiltration: Average cost of a data breach attack was...

$3.86 million

Average cost of a **supply-chain cyberattack** is $1.1 million and takes...

63 hrs to resolve

In 2018 **attacks on the e-Commerce industry** in the U.S....

rose by 93%

Average loss associated with Distributed Denial-of-Service attack is...

$2.5 million

Losses from a **3-6 day cloud outage** in a top-4 U.S. service could cost global economy...

$19 billion

THE OPTIMAL WAY FOR ORGANIZATIONS TO ENHANCE THEIR RESILIENCY AGAINST CYBERATTACKS IS ADDRESSING BOTH TECHNOLOGY AND CYBER RISK UNDER OPERATIONAL RISK INSTEAD OF AS SEPARATE COMPONENTS

Enables the business to **prevent**, **detect**, and **respond** to the threat to information Security assets

Information Security collaboratively works to operationalize controls

Conducts **operational analysis** of threats and defines appropriate counter measures to address the threats

Defines the **cyber risk appetite** for the firm and risk tolerance levels

Uses a risk framework to **categorize key information** assets based on how critical they are to business processes.

Assesses cyber risk to key information assets that may be impacted by current and emerging threats

ORGANIZATIONS NEED TO MOVE BEYOND A REACTIVE DEFENSIVE APPROACH TO CYBER TOWARDS AN INTELLIGENCE-LED RISK MANAGEMENT STRATEGY

Contents

Executive Summary

It is estimated that cyber breaches cost the global economy $1.5 trillion per year, and this is expected to increase — some sources believe it could cost the global economy a staggering $6 trillion by 2021. The increasing scale of cyber breaches means it has now become necessary for organizations to mature beyond a basic reactive defensive approach on cyber, to an intelligence-led, proactive one. To be intelligence-led is to know both yourself and your enemy. This means knowing what your critical assets are and who may have the motivation and capability to threaten those assets.

The Evolving Cyber Risk Landscape

Increasing cyber risk is driven by the exponential rise in digitization

The largest driver behind increasing cyber risk is the exponential rise in digitization since the advent of the global Internet in the 1990s. As a result of increased digitization, a company's attack surface now extends far beyond the bounds of its offices and native IT network. With physical and digital assets now interlinked through supply chains, modern businesses are increasingly reliant on the security of all systems linked to their networks.

In addition to vulnerable and lengthening digital supply networks, the rise of state-backed actors who abuse digital systems for political advantage is a cause of great concern within the business community. Cyber politics and physical politics are becoming increasingly intertwined, and the cyber espionage, theft, and disruption caused by these state-backed actors have led to marked real-world political and corporate impacts.

Cyber attacks occur in a number of different forms including: (1) data exfiltration, where an average single attack is estimated to cost $3.86 million; (2) contagious malware, which can take different forms including ransomware, (3) financial theft, where online fraud dominates the criminal volume landscape; in fact between 2017 and 2018 attacks on the e-commerce industry in the U.S. grew by 93%; (4) cloud outages; and (5) distributed denial-of service attacks, which are usually cited as disruptive attacks averaging an estimated associated loss of $2.5 million for each instance.

Threat from cyber spans across governments, corporates, and individuals

The threat from cyber spans across governments, corporates, and individuals. At a high level, these threats include attacks on critical infrastructure, the theft of data (including the theft of trade secrets), and financial loss.

Cyber and Governments

State-backed actors and criminal organizations are forcing governments to be on cyber offensive

The rise of state-backed actors and cyber as a political weapon, as well as highly organized and sophisticated criminals, increases the risk that governments and critical infrastructure are targeted. This, in turn, has forced governments to move from a more defensive position on cyber to one that is more focused on offensive capabilities. Collaboration between national governments on cyber issues have been formed and international bodies, such as the UN, have set up groups to develop a common approach to align governments' behavior in cyber space. These discussions are ongoing.

On a national level, digital connectivity has increased the threat of attacks on critical national infrastructure. Public utilities such as electric grids and transportation systems could prove to be valuable assets to bad actors, and such an attack on these assets could result in systemic damage leading to costly, far-reaching consequences. The key issue? Most critical national infrastructure was designed and installed at a time when cyber risk was either not known or not considered.

Critical national infrastructure is a particular concern due to its frequent use of software updates for cyber protection

Given their complexity and size, critical infrastructure is typically difficult and expensive to replace, and therefore software updates and patches are primarily used to provide the simplest measure of security against cyber attacks. This results in additional risks to key operational technology due to poor patching cadence, poor password security and unencrypted protocols, third-party vendor access, enterprise management systems, and network architecture.

An attack on the energy sector poses the highest risk for systemic damage to critical network infrastructure in a majority of countries given its importance and size. Power and energy facilities have an 'enabling function', meaning that they are vital to the continued operation for all other sectors. It is therefore essential to understand the vulnerability of this sector and the threat to it as a means of understanding overall vulnerability to a country's critical network infrastructure.

Critical infrastructure in the energy, healthcare, and manufacturing sectors are most susceptible to cyber attacks

Future plans to establish smart grids and smart plants built around automated technology that centralizes utility management, will help increase reliability by rolling out software updates more efficiently and neutralizing problems that arise before they spread. However, the process of connecting thousands of devices to a highly integrated network will likely create smart grids with further vulnerabilities, which may proliferate through systems and become embedded.

The healthcare sector has become a well-known target for disruptive cyber attacks, especially ransomware attacks, as attack demands are more likely to be met due to the high rate of access and time sensitivity of the sector. Hospitals and healthcare facilities are under great pressure to provide constant service continuity. Therefore, when a vulnerability is discovered, or a patch is published, the decision to modify unique and costly devices, potentially taking them offline and limiting patient care, can easily be pushed back. The onus, however, remains on the healthcare sector to property educate staff on cyber threats and train employees to recognize phishing emails and suspicious links and attachments.

The cyber threat to manufacturing is significant due to the latent power of industry control systems. An attack which can bypass the safety systems of production lines and furnaces may exploit latent fuel sources to create a devastating attack. Because of its complexity, it is difficult to estimate the number of vulnerabilities present in industrial systems, and therefore to present a solution based on the realities of potential compromise.

With the further digitization of industry control systems and significant portions of critical national infrastructure, governments and industry leaders must accept that vulnerabilities will become an inherent part of vital systems. More investment in security testing is required to resolve issues before they arise, and to safeguard users and companies in the event that an unseen vulnerability is leveraged against them.

Cyber and Corporates

As reports of breaches and high-value fraud cases continue to dominate the news, corporate boards, investors, and customers increasingly challenge organizations on their ability to protect assets. When an incident does occur, the market monitors how well corporates respond during the crisis event. Given the stakes, cybersecurity is increasingly becoming a critical factor in decision-making discussions when considering business relationships. This shift in conversation means corporates need to pivot their cyber security approach away from damage minimization and toward business differentiation.

Cyber attacks impact corporates through financial loss from business disruption and reputational risk

Due to the public nature of cyber breaches, corporates are acutely aware of the impact cyber attacks can have on business and are including accepting the importance of cybersecurity. Progressing from baseline recognition, the next step for corporates is figuring out how to manage the risk of cyber attacks. A review of current literature on cybersecurity reveals repeated messaging on ensuring cyber security is not just an IT function. Only through shared ownership across functional areas and shared responsibility up, down, and across an organization can cyber security evolve past a pure IT role.

Focus on cyber at the Board level plus inter- and intra- sector collaboration is critical as the cyber threat landscape evolves and risks to corporates increase

As threat actors improve their capabilities, the threat landscape evolves and the impact and risks to corporates increases. Board-level reporting on this topic is likely to become more detailed and more frequent. Further, involvement of corporate boards in decision-making related to the threat and corresponding risks of cyber may necessitate the inclusion of additional cyber subject matter experts on corporate boards in the future. Cyber security, cyber risks, and cyber resilience affect all layers of an organization, therefore requiring a broad and holistic view of an organization that only executive leadership is able to provide. Once the view is established, corporates benefit further from an ongoing dialogue between senior management and their corporate boards on strategic direction and daily operations.

Another key to combatting cyber risk is through a combination of inter- and intra-sector and country collaboration, as well as public-private partnerships. For this strategic approach to be developed, experts from product teams, risk and finance units, and franchise management across public and private sector organizations must come together to debate, define, and understand cyber risk. Two areas that are most effective for informing and helping to monitor the global architecture of the cyber regulatory system and good cyber security standards are information sharing models and cyber threat exercising.

Cyber strategy is increasingly a differentiator for corporates and investors

Corporates who differentiate themselves on cyber security likely display agility. The same trends which expose corporates to more risk, such as emerging technology adoption, can also serve as business differentiators based on how a corporate chooses to manage the associated risk. Corporates can use their culture of compliance to demonstrate dedication to security in a tangible way. Cyber security can also play a role in an investor's decision-making process given the rise of ESG funds as smart cyber practices and investment can lead to a sustainable business and therefore play a role in positive outcomes, like attracting investors. Finally, cyber security can also become a business lure and a competitive advantage.

Cyber and People

In addition to corporations and governments being interconnected through digitization, so too are people — in their personal and professional lives. The main risk to individuals from cyber relate to the theft of personal and financial data which criminals then use for things such as identity crime, financial loss, or blackmail. Increasingly, individuals are being targeted through phishing emails and tailored social engineering attacks to gain access to corporate systems and data.

Targeting human weaknesses is an easier route into corporate systems

Although many bad actors possess sophisticated technical abilities, it is easier for them to target a human weaknesses or vulnerability than it is to bypass a sophisticated technical system control. Phishing emails which are mistakenly opened can download malware onto a user's computer and begin a ransomware campaign or target corporate systems. The increasing adoption by consumers of machines enabled with the Internet-of-Things increases the opportunity to exploit the vulnerabilities created as the number of attack surfaces increases. Information on people's habits, locations, and physical conditions over time, could be stolen and misused, or be sold and used to make decisions regarding the provision of credit, insurance or employment.

Cyber and the Insurance Market

Demand for cyber insurance with specialized products is growing as reported data breaches rise

The growing cyber insurance market is one solution corporates can use to combat cyber risk. As the cyber threat becomes more tangible and publically understood, companies have become more aware of the risks that come with mandated digitalization, and insurers have brought more specialized products to the market in response. Demand for cyber data breach insurance rose through the 2010s as the number of publically-reported data breaches rose —today around five major insurers write more than half of all cyber insurance policies with 90% of volume applying to exposure in the U.S. alone.

Cyber insurance products are either “affirmative”, meaning they explicitly cover cyber risk and specific losses associated with it, or “non-affirmative”, meaning the coverage is non-explicit. Currently there are about 20 types of cyber insurance product coverage available.

The cyber insurance market is nascent and with no historical catalog to determine the size and shape of future threats

Crucially, the cyber insurance industry has yet to suffer a truly ‘catastrophic’ cyber event, which may trigger major claims in a broad swathe of policyholders resulting from the same attack. Cyber risk is nascent, and unlike typical insurance businesses, there is no long historical catalog by which to determine the size and shape of the threat in the future. Given the possibility that the rate of cyber ‘catastrophes’ in an average decade is liable to change given the development of the risk landscape, insurers have exhibited caution in entering the cyber insurance market. Those who have entered are using probable maximum loss (PML) assessments, which are hypothetical scenarios of massive loss, in order to explore the potential for future large-scale losses stemming from a cyber attack. Given the growing catalog of experience with cyber claims, insurers are becoming more familiar with, and confident in, cyber as a line of insurance. With this growing confidence comes the expectation that the cyber insurance market will continue to grow, at least for the time being, despite the unique obstacles the risk presents.

Managing Cyber Risk with Human Intelligence

Fundamentals of an Intelligence-led Approach

Cyber security strategies need to shift from defense in-depth networks to active defense strategies

As the speed and sophistication of the adversary continues to escalate, defense in-depth network security programs need to evolve to active defense strategies. Across sectors, a ‘three lines of defense’ model is critical to maintaining adherence to industry standards — the first line, who owns and manages the risks to the business as well as the controls necessary to mitigate these risks; the second line, who monitors the risk types and controls to ensure they are bringing inherent risk to a residual risk level with tolerance for the organization’s appetite; and the third line, who acts as an independent assurance function to audit both the first and second line to ensure effectiveness of risk and control management.

Understanding drivers and strong partnerships between business lines and risk management are critical to successful cyber security programs

Understanding the key drivers of cyber, such as geopolitical flashpoints, domestic issues, demographics, and economic states, and how they impact an organization will help proactively build a cyber security program that can quickly scale to meet demands over a one- to two-year period. Building an effective strategy requires a strong partnership between an organization’s business lines and risk management teams to customize a cyber security program that instills trust and confidence both within the organization as well as externally. A blend of technology and cyber risk programs under operational risk within an organization is optimal because the synergies between the programs naturally enhance an organizations’ resiliency.

An intelligence-led mindset is needed in integrating a cyber risk management approach

Integrating a risk management approach with the firm's business strategy to anticipate cyber risk early on is an example of successfully employing an intelligence-led mindset. Although an intelligence-led strategy can contain a variation of elements, a few are considered foundational: understanding the threat, integrating threat intelligence and analytics into decision-making; establishing a learning culture, building a foundation of information sharing, executing strong program management, and maximizing collaboration. Furthermore, within an industry, when corporations act as partners, they come together to fulfill a common mission to prevent attack activity. By doing so, they are not only defending themselves, but by extension, their clients, investors, and other key stakeholders through the application of sound cyber security practices.

Implementing a strong internal interaction model between business line and risk management professionals is key to sustaining success in cyber risk strategies

Sustaining the success of a cyber risk management strategy is crucial but given today's cyber environment with the constant flow of emerging issues, being successful over time is even more complex. We believe the most critical factor in defining an organization's success in reducing cyber risk will be its ability to implement a strong internal interaction model between its business lines and risk management professionals. While the business lines are responsible for identifying, assessing, monitoring, and managing its cyber risks, risk management must take a step back to challenge each of these areas without impeding cyber security efforts. Some of these efforts will be in parallel with what the business is doing to assess and manage its cyber risk, which results in a 'belt and suspenders' approach.

Cultivating cyber talent at an organization will drive successful cyber security

People, process, and technology are often the three pillars of any successful organization operating in the global economy. In a technology or cyber role, people are often the cornerstone of these three pillars as many organizations lack existing processes or technology; therefore they need talent to build these elements. It is critical when building a team in cyber that leaders have a strategy and vision to execute against and must be savvy in the processes that need to be performed to deliver against that strategy. They have to know their own organization and how to capitalize upon efficiencies and staff the components with employees of diverse backgrounds that can navigate often complex environments to deliver a result.

Driving a change in cultivating cyber talent will require that both private and public organizations move into the driver's seat to shape how the technology and cyber educational system is building future leaders. By advancing clarity around the career path in corporate entities, more diverse candidates will be increasingly likely to identify opportunities and be attracted to the work environment.

Securing the Platform with Technology

IT security and solutions has grown to an $80 billion market

Especially as the speed of technological innovation accelerated with the proliferation of personal computers and broad-based networks, security quickly became an afterthought in the development of these platforms. Because of this, large markets grew up around providing security as an add-on to these important technology components to counter vulnerabilities exploited in early attacks. One could say that as a result of the platforms not solving their own security problem, one of the more vibrant technology markets was created — an $80 billion IT security & solutions market.

A new security market, driven by cloud usage and SaaS is emerging

Two new areas that are currently changing the face of technology include 'hyper-scale' public cloud offerings and software-as-a-service (SaaS). The sheer size of the public cloud market and the adoption by enterprise customers suggests there will also be a significant 'add-on' security market. Public cloud services differ from on-premise architecture in that much or all of the technology components are resident in the data center of the service providers.

In this way, the end-customer (corporate/enterprise) in most cases cannot choose the security technologies that are used within the public cloud environment. This dynamic, at a minimum, changes how the cloud must be secured as compared to traditional on-premise networks.

Technology systems in the cloud are increasingly secured by virtual firewalls and cloud access security brokers

The first change we're seeing in technology security is the 'virtualization' of security. We are seeing significant growth in 'virtual firewalls' which can be deployed as a virtual machine on any cloud, including firewalls at the 'workload' level and 'firewalls' that apply policy using native public cloud capabilities. Next, we are seeing deeper inspection of web traffic with the focus of investigation shifting from network ports and protocols to understanding the application, what its behavior is, and how that compares to stated security policy. The cloud access security broker (CASB) market is increasingly extending outside the reach of the firewall and relying on native connections into a cloud service. Instead of monitoring traffic in and out of a network, the cloud application program interface is the key control point.

Lastly, identity is coming to the fore as having renewed importance in the public cloud. It is important to establish who a user is and what applications they can connect to. This security model is more relied upon inside organizations that have built their IT architectures in the last 10-15 years. Critical to this architecture is identity management technology.

Emerging security technologies look to be additive to traditional firewall technology

Despite the long-term view that cloud adoption will enable the emerging security technologies described above at the expense of firewall spend, a Citi survey found that firewall technology continues to anchor core enterprise security strategy and incremental cloud security areas are largely additive in the near-term.

Overall, we expect the security technology market to remain a 'short-cycle' sector meaning that product cycles are measured in duration of 3-5 years. This compares to other technology markets where refresh timelines are a decade or more. For this reason, to both understand how to mitigate new challenges as well as be an investor in the market, it is necessary to understand the evolving threat landscape. Combined with this, there is a once in a decade (or more) shift in technology architecture underway which is currently in its early phases. Beyond the constant shift in the threat landscape, this force has the most potential to drive change in the market.

Emerging Technology

Emerging tech, such as AI and biometrics, will increasingly be deployed to stop cyber attacks

The extreme growth in data volume, the continued increase in computing power, and the need to adapt and counter ever-evolving cyber threats has led to the emergence of new technologies (emerging tech) which provide new tools and techniques to support business needs. Emerging tech such as artificial intelligence, machine learning, blockchain, behavioral biometrics, biometric authentication tech and emerging cloud services can all be deployed to detect and stop cyber attacks — and notably at a speed and scale that wouldn't have been previously possible.

The successful application of emerging tech capabilities for cyber defense requires a robust, adaptable governance and risk mitigation strategy, including roles and responsibilities, an accounting of emerging tech products, testing and security, enhanced monitoring and anomaly detection, knowledge of sharing platforms and continuous risk identification and mitigation plans. As businesses adopt products that use emerging tech or use emerging tech to develop in-house products, a governance framework will manage both the adoption of the new technology as well as its potential risk.

Section 1: Introduction to Cyber Risk

What is Cyber Risk?

Today's world is one of increasingly networked systems and reliance on interdependence for social connection and business operations. These rapid communication channels span globally and are growing exponentially with a majority of the population now conducting interactions and transactions in cyberspace. From a business standpoint, cyber has created new possibilities including as mobile applications, behavioral credential validation, and artificial intelligence (AI) allow business transactions to occur with limited to no human interaction. Meanwhile the Internet of Things (IoT) allows everything from oil pipelines to toasters to be controlled remotely and send feedback. Connectivity via cyberspace has led to incredible gains in the application of technology within the last decade, but threat actors with malicious intent have learned to use this same connectivity as a tool to commit crimes.

Cyber has created new possibilities and incredible gains in the application of technology while also exposing exploitable vulnerabilities

While new technology has provided new communications pathways, it has also revealed exploitable vulnerabilities embedded in the hardware and software used to construct and operate these pathways and exposed the people who use them. These vulnerabilities open a wide range of entry points for malicious actors, creating a challenge for cyber security professionals who must defend targets across a diverse network and geographical area. Any individual connected to these pathways might be targeted for fraud. Sensitive data in their possession can also be targeted making them an unwitting, hosting accomplice for attacks more valuable targets like corporate networks.

Cyber security professionals face a daunting challenge — securing their organization's networks by keeping attackers away from the most valuable data and responding to threat actors who may have entered the perimeter. Cyber adversaries are determined — working long hours to achieve their goals and using creative means to obtain their objectives — to make it difficult for cyber professionals to attribute, detect, or mitigate threats. This creates an increasingly varied cyber threat landscape.

The Changing Cyber Threat Landscape

The profile of threat actors has evolved significantly — they are now more organized and sophisticated enterprises

The cyber threat landscape has changed significantly in the past decade. The frequency, speed, and effectiveness of cyber attacks continues to increase, meaning that organizations must be right all the time, while malicious actors only need to be lucky once. Threat actors have evolved from largely disconnected individuals using limited toolsets to a broad network of groups using highly sophisticated and customized toolsets. Today, threat actors exist and operate within organized enterprises — and in some cases nation states — and increasingly leverage disruptive and destructive tactics to achieve financial gain.

The evolution of threat actors into more organized and sophisticated enterprises has increased the threat faced by any and every organization connected to the Internet. In 2018 alone, a multitude of global organizations encountered innovative and successful attacks, ranging from targeted campaigns against domestic and international payment systems, breaches of third party vendors and suppliers, and unprecedented intellectual property and sensitive data theft, to destructive attacks affecting the stability of business operations. Attacks need not be innovative to succeed. Simple attacks against trivially exploitable vulnerabilities, weak authentication, and poor access management — all of which are categorized as 'digital hygiene' — still represent substantial threats to even mature organizations.

Industry Targeting

Every industry connected to the Internet has concerns around the sophisticated attacks aimed specifically in their direction. However a significant portion of cyber attacks worldwide lack specific targets and largely automated. Driven in many cases by criminals looking for easy money, the constant 'background' threat environment requires organizations to build and maintain minimum-security standards.

Aside from the general threat environment, certain sectors — IT, manufacturing, and healthcare — face particular threats

Aside from the general threat environment, certain industries such as information technology, manufacturing, and healthcare, do experience threats crafted for their environment and the business they conduct. Information technology — the tech that facilitates all legitimate and threatening cyber activity — faces a high number of threats affecting its supply chain. Information technology compromises may create wide-ranging ripple effects, indirectly affecting much larger groups, as was seen with the Spectre and Meltdown vulnerabilities identified in 2018.[1]

Manufacturing and healthcare are both awash in confidential data, from patients and customers to intellectual property and treatment developments. Both industries face challenges due to the high value and sensitivity of their data. This prompts sophisticated threat actors to attempt intrusions to obtain the data for potential espionage gains as well as for their resale value. In dark web marketplaces (see box below), the sale of patient data typically garners a much higher premium because the data contained in health records is difficult to obtain – requiring far more sophisticated effort to exfiltrate out of a system.

The Dark Web

Many people have heard of the dark web, but what is it exactly? It is the part of the Internet that remains unindexed by most search engines, and requires special software to access it. The technology was created by military researchers in the U.S. for use by intelligence officers to share files anonymously.[2] The platform used was called 'Tor' ('The Onion Router)' which conceals the location and IP address of users who employ the software. Tor became a critical part of the dark web and hosts approximately 30,000 hidden sites. There are other platforms available such as I2P and Freenet, but it seems that Tor is the largest.[3] Tor provides two services — anonymous browsing and hosting of anonymous information exchanges. The anonymization provided by Tor is praised by many, including Google and Human Rights Watch, as it has helped many people to communicate freely despite repressive government measures. For example, the platform was used by opposition activists in Egypt to communicate and disseminate information in spite of a clampdown on the Internet by the Mubarak regime.

However, Tor also has a dark side in the form of a hidden service which allows anyone to create an untraceable server hosted within the network. This feature has given rise to hosting illicit content on the Tor darknet. Moore and Rid (2016) scanned 5,205 live websites on the Tor network, managing to classify 2,723 websites according to a number of different categories, and found that 1,547 of these were totally illicit. They concluded that the most common uses for websites on Tor hidden services are criminal, including drugs, illicit finance, and pornography.

[1] Spectre and Meltdown are terms used for hardware security vulnerabilities allowing threat actors to access a machine's data without permissions. With the attack targeting the machine's hardware as opposed to software, security teams have difficulty detecting or mitigating attacks using these vulnerabilities.
[2] Woollaston (2018)
[3] Moore & Rid (2016)

Many of the sites they visited offered services for laundering money through Bitcoin, and various websites offered cloned credit cards or financial information stolen via malware. There are, however, many non-illicit websites found on Tor such as hidden services run by newspapers, search engines, and blogs. The authors note the difference is that legitimate sites always choose to identify their operators, while illicit sites never do.

Cyber Threat Actors

There are five different types of threat actors — nation state, criminal, hacktivist, terrorist, and insider

There are five different types of threat actors — nation state, criminal, hacktivist, terrorist, and insider — each with different targets, methods, and objectives.

- **Nation state actors** conduct espionage to steal intellectual property and collect intelligence considered vital to advancing national interests. Challenging to detect and mitigate, these actors have substantial resources allocated to developing and sustaining sophisticated capabilities.
- **Organized criminals** are focused on monetary gains via methods such as spear phishing, social engineering, automated tools, ransomware/other extortion tools, and enhanced distributed denial-of-service attacks (DDoS) — sometimes forcing organizations to choose between criminal payouts or steep recovery costs. Monetary gain is not exclusive to stealing money from accounts; Personally Identifiable Information (PII) data is also stolen and then sold in dark web marketplaces for other criminal groups to further exploit.
- **Terrorists and hacktivists** share similarities in that they both push political agendas using cyber means. Both use fear and disruptive cyber attacks, though cyber terrorists are more likely part of a larger organization that may also have a physical component. Hacktivists have limited physical presence or direct ties to existing in-person protest groups. They prefer to protest many perceived slights while looking for targets of opportunity to draw attention to a cause and achieve notoriety. Historically, hacktivists launch distributed denial-of-service (DDoS) attacks and perform website defacements as a means of protest.
- **Insiders** provide a greater threat to an organization than most external actors. They use local tools and their knowledge of the internal network to steal, damage, or commit fraud. These operations are difficult to detect as intentions and methods are varied, ranging from monetary gain and inflicting damage to perceived whistleblowing acts.

Evolving Techniques

Despite historically having distinct roles, these five groups of actors are increasingly meshed adversary groups

Although we can classify five distinct types of cyber threat actors, these actors have evolved from their traditional roles into increasingly meshed adversary groups. The intentions of cyber threat actors are no longer as clear and may blur operational lines to obscure their identities and methods of attack. Nation state targeting is a prime example. While typically nation states are believed to advance national interests via espionage or simply adjusting public perception, cyber threat analysts have recently identified nation state-attributed campaigns used to secure financial gains by criminal means. This has been through the use of criminal tool sets to obtain financing potentially to fund regimes. Both criminal and nation state advanced persistent threat actors are increasingly interested in industry data and will attempt to steal it.

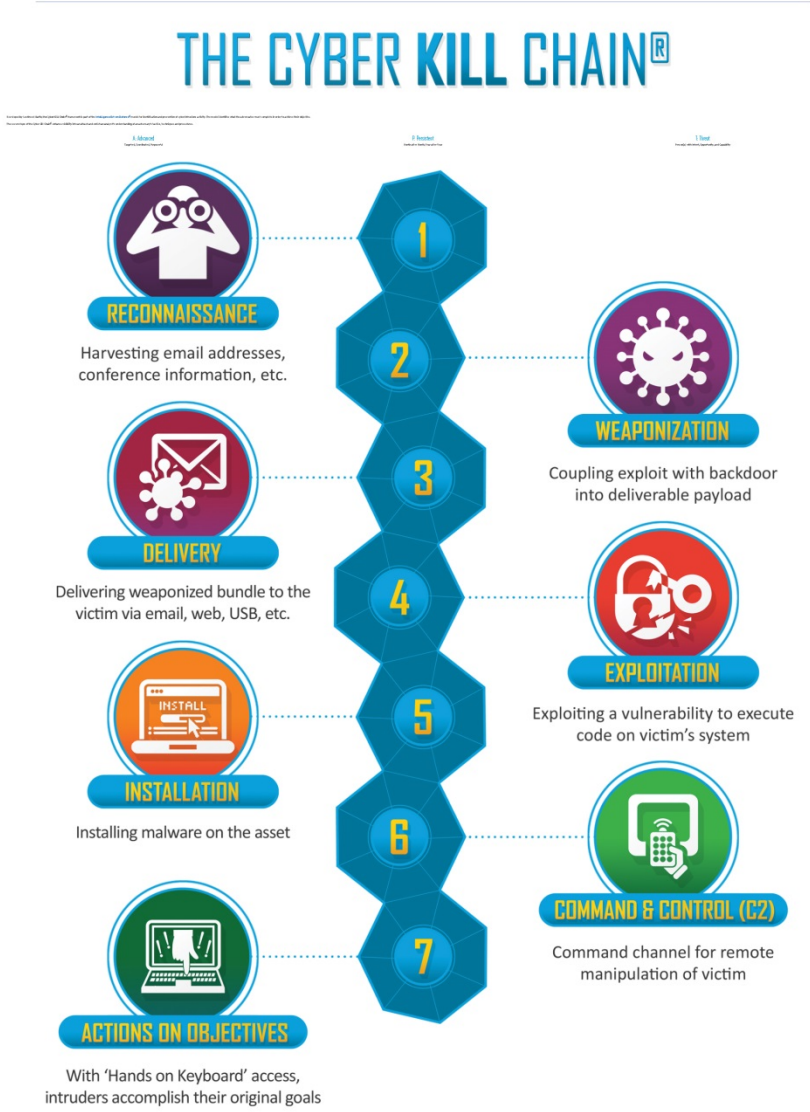
Additionally, there is mounting evidence that nation state threat actors have merged with or are reliant on criminal enterprises. Some have branched into service business models with specialized services offered solely to perform a particular function in the attack chain. For example, in some instances criminals purchase and set up attack infrastructure leveraged by nation state actors to conduct campaigns. This technique further blurs attribution and creates an easy, reliable method for nation state actors to gain illicit access to computer services.

The Cyber Kill Chain

The Cyber Kill Chain provides a framework for identifying where attackers are in a network and understanding their threat campaigns

One of the oldest means of describing the intrusion process of cyber threat actors is the Cyber Kill Chain. Developed by Lockheed Martin, the Cyber Kill Chain is adapted from military attack mapping concepts, intended to help analysts identify where attackers might be located on the network, or in other cases, reconstruct an attack in hindsight. It also provides a framework for understanding threat actor campaigns, giving defenders the chance to learn from and anticipate similar attacks in the future.

Figure 1. The Cyber Kill Chain



Source: Lockheed Martin-https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

In a Cyber Kill Chain, a threat actor campaign is broken into seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives

According to the model, a threat actor campaign is broken into seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. While some campaigns may skip over a single phase, the basic kill chain as a whole represents a complete compromise of the network. Examples of actions potentially required by the defenders is included below; however not all phases have available countermeasures.

- **Reconnaissance:** In the reconnaissance phase, threat actors are in the planning stage of operations, conducting research to better understand targets and determine which targets would most likely meet their objectives. Defense is difficult at this stage as much depends on the threat actor's intent. In many cases, reconnaissance activity is often discovered after the fact, such as when an Indicator of Compromise (IOC)[4] is discovered on the network, suggesting that a threat actor may have already breached the perimeter.

- **Weaponization:** Threat actors have found the victim's entry point and are looking to develop the tools that would likely lead to successful intrusion. Advanced actors expressly customize the payload and delivery mechanism to a target's network, thereby maximizing the chance of success.

- **Delivery:** Delivering the payload/malware is most often achieved through phishing, social media exploitation, and/or compromising or emulating websites used by the target. For defense, this is a key opportunity to stop threat actors from gaining further ground. If the malware never reaches the landing point, the attack will likely be unsuccessful.

- **Exploitation:** The malware has arrived at its intended location, but threat actors require a vulnerability to establish a foothold and gain access. Defenders with up-to-date patching are less likely to be compromised, however sophisticated actors may use 'zero-days', i.e., previously unknown vulnerabilities. Often after a zero-day is exposed, actors will attempt an attack immediately before the software provider can offer a patch and organizations can implement these security fixes in their environment.

- **Installation:** The malware is installed onto the network to further the operation. Some threat actors are looking for extended access while others are simply preparing to expedite the operation to achieve objectives quickly.

- **Command and Control (C2):** The malware opens communications to the threat actors, allowing them to remotely connect to the targeted systems. From this point, skilled threat actors can move laterally across the network, collecting data and information that is sent back to their C2 node. Defenders have the opportunity in this stage to eliminate or reduce the command and controls of threat actors.

- **Actions on Objectives:** Now that threat actors have established access on the system, they are able to conduct their operations and potentially achieve their goals. Skilled threat actors will make further gains than unsophisticated ones. Defenders in this stage are looking to identify anomalies created by the threat actor's presence and conduct damage control.

[4] IoCs are traces of activity found in a network revealing an intrusion. Viruses, malware, bots, and other threat actor activity can leave these IoCs behind, identifying evidence used for early detection of similar compromises in the future.

The kill chain offers advantages in understanding and recreating campaigns as part of an intelligence-led, defense in-depth strategy. The sooner threat actors are identified, the less potential damage they cause. The kill chain offers one of the best approaches to applying a reliable, analytical framework to the changing dynamics of the cyber threat landscape.

Success of an Attack

Disadvantages of the Cyber Kill Chain is consistency and resources – both of which increase the attacker's potential success

The disadvantages to the kill chain approach are twofold: consistency and resources. Attackers may shift their operation once inside of an organization's network — once they gain access, threat actors might customize or tailor refined approaches that maximize gains. This makes it harder for defenders to see the attack itself, much less identify the stage of the kill chain the threat actors have breached. According to the Verizon 2018 Breach Report, 68 percent of breaches took "months or longer" to discover, but it took attackers just minutes or less to compromise a system in 87 percent of breaches.

Resource constraints at an organization also help determine an attacker's potential for success. Hunting for sophisticated attackers requires extensive use of cyber security and intelligence resources. Does an organization wish to pursue those threat actors, although they make up a relatively small minority of threats faced? Would it be more productive to make sure areas such as cloud storage are not exposed and are properly configured, in order to prevent a multitude of less-sophisticated threat actors inside the victim's door? Finding the balance, especially when resources are inadequate to cover both sufficiently, is a challenge for many organizations. The kill chain is an effective tool for analyzing and countering actors and campaigns, but it is one small piece of a large and complex puzzle.

Citi's Role in Cyber Defense

The cyber threat landscape is constantly evolving — challenging organizations, vendors, and researchers to analyze and adapt to the shifting conditions set by threat actors. In the future, organizations will continue to mitigate to the best of their ability, with increased impacts to operations as new, advanced methods are used against networks. Eventually, the need to address concepts such as risk management, acceptable defensive posture, and measures of success within the cyber realm may lead to more proactive and collaborative approaches in dealing with threat actors.

At Citi, this customization of cyber defenses occurs at the Cyber Security Fusion Centers — intelligence-led organizations which house 13 Citi security teams including cyber intelligence, incident management, and vulnerability assessment. These centers constantly monitor for cyber attacks globally in an effort to better understand the methods and motivations of threat actors. Citi also works closely with external public and private partners and peer institutions to collect and share cyber threat-related information in real time. Only through this combined effort across the private and public sectors can we keep ahead of the ever changing cyber threat landscape.

The Evolving Cyber Risk Landscape

The threat of cyber attacks does not get better, it only gets worse. Attacks worldwide are growing in size, tenacity, and complexity. While 2018 saw few significant virulent cyber events in the vein of 2017's NotPetya and WannaCry, the disruption posed by smaller, more pedestrian cyber interference became ever more commonplace. A survey by the U.K. Department for Digital, Culture, Media & Sport demonstrated that four in ten U.K. businesses and two in ten charities had experienced a cyber security breach since the start of 2018.[5]

The cost to the global economy from cyber losses is over $1.5 trillion per year from lost revenues, payouts, and associated damages

The estimated cost to the global economy from cyber losses is over $1.5 trillion a year, including $65 billion in payouts and operational disruption from cyber attacks, $725 billion in lost revenues by enterprises that suffer a significant level of consequential business loss, and $825 billion in loss suffered by trading and business partners of the affected enterprise.[6] The average cost of a single successful cyber attack is estimated at $5 million,[7] primarily due to the long periods of system downtime and lost productivity that typically follow an attack.

The reputation of an organization is also at risk from a cyber attack

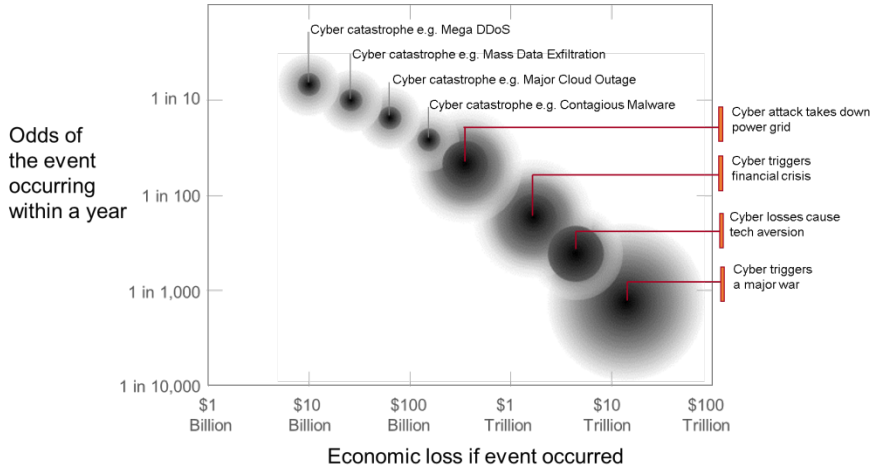
Organizations are also cognizant of the threat to reputation from cyber risk. A significant data loss may lead to a marked change in stock price valuation or massive customer flight. As business interruption impacts more people, fines and regulatory charges are growing more punitive.

In September 2018, after months of international scrutiny following the Cambridge Analytica scandal, Facebook experienced a breach affecting more than 50 million users.[8] Hackers exploited three vulnerabilities in Facebook's 'view as' feature to steal access tokens which permitted them to illegally take control of user profiles and gain access to third-party applications such as Pinterest and Spotify. Facebook's share price fell 3% on the day the breach was made public, resulting in a $13 billion drop in market capitalization.[9] Further litigation may find the platform is also in violation of recently enacted data protection regulations in Europe which could lead to a fine equal to 4% of the company's annual total turnover, or $1.63 billion in Facebook's case.[10]

Although many companies have suffered some sort of loss due to a cyber event, to date the global economy has not yet experienced one truly catastrophic event costing the economy hundreds of billions of dollars. Research into digitized attack surfaces, however, shows that attacks of this magnitude are possible, and that the capabilities and ambitions of threat actors are growing. A cyber catastrophe could send cascading impacts across multiple industries and geographies, potentially upsetting the status quo of modern politics.

[5] Cyber Security Breaches Survey 2018.
[6] Coburn et al. (2019).
[7] Fruhlinger (2018).
[8] Tynan (2018).
[9] Kelleher (2018).
[10] Schechner (2018); GDPR regulations are some of the most punitive in the world, stipulating that a company will be fined €20 million or 4% of annual turnover for significant data breaches. In the U.K., the maximum find that the Information Commissioner's Office (ICO) could issue previously was £500k.

Figure 2. Global Cyber Risk: Likelihood of Loss Occurring from Cyber Attacks



Source: Coburn et al. (2019)

This chapter will investigate the key drivers behind the growth in complexity of cyber attacks and the widening footprint of their effects. Chiefly, the drivers are the growth of digital integration, the shift in cyber as tool of political leverage, and the opening of cryptocurrency trade. The latter part of the chapter describes the trends in attacks which are driving industry losses to ever higher levels.

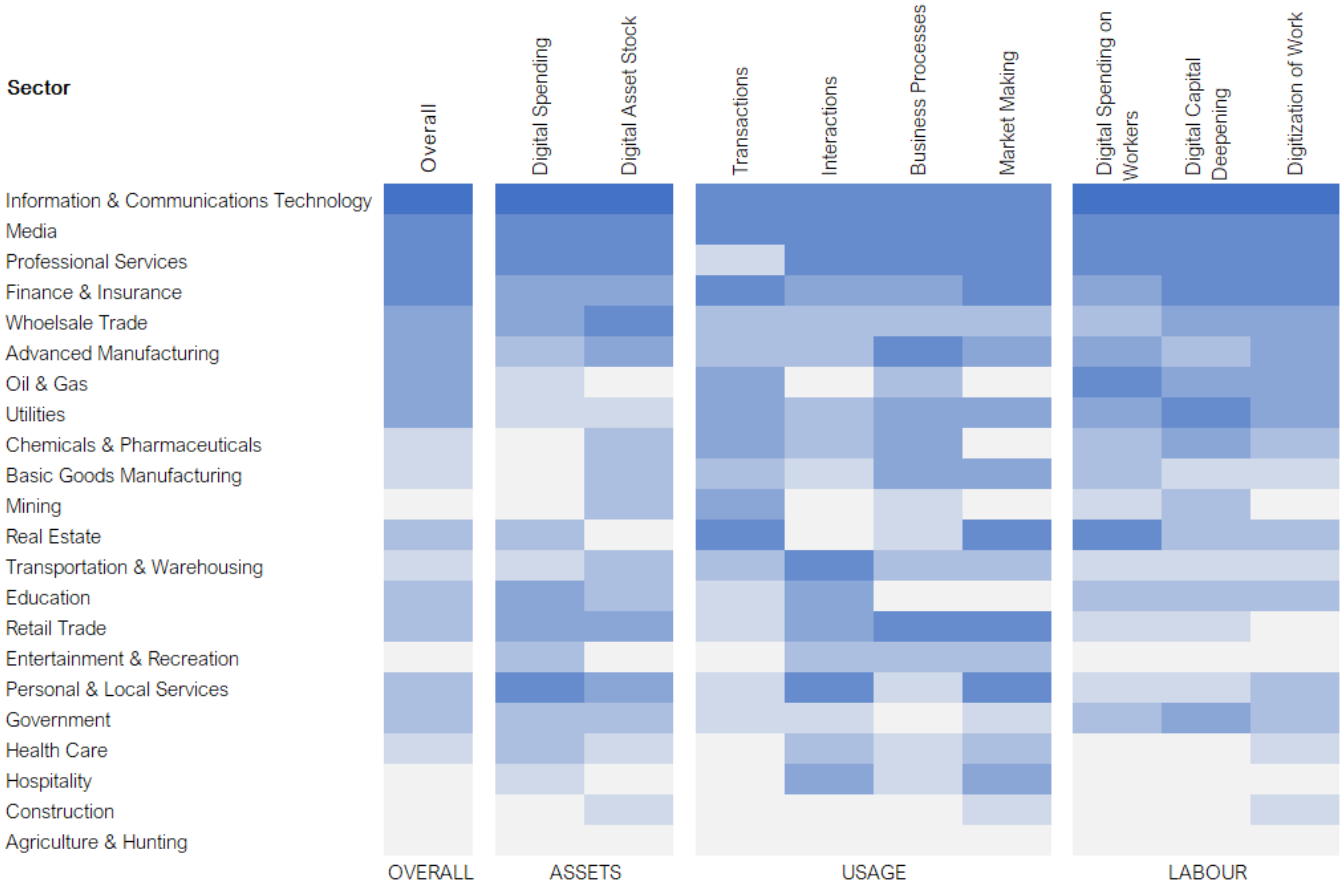
Growing Digital Integration

The number of Internet users has doubled in the past ten years while the number of website has increased over 800%

The rate of digitization has increased exponentially since the advent of the global Internet in the 1990s. In the past ten years, the number of Internet users worldwide has doubled, and the number of websites has grown by an extraordinary 818%.[11] Reliance on digital systems has become so integral to the conducti of global trade, business and finance that companies, industries, and whole economies now largely expect their continuous function. Knowledge-intensive sectors such as communications, media, and finance, are most likely to be highly digitized across all dimensions of the business, whereas labor-based sectors like construction and farming have been slower in the adoption of digitized assets to facilitate efficiency and ease of use (see Figure 3 below).

[11] Netcraft 2018.

Figure 3. Relative Digitization of Assets Across Sectors, as of 2016



**The variation across sectors is directly related to the dependence of each sector on connected devices for business revenue and management. Relative digitization is measured according to the level of hardware, software, data, and IT service investments, along with the digitization of physical assets such as big data systems in supply chains, connected vehicle fleets, smart buildings, etc.

Source: University Cambridge Centre for Risk Studies

Supply Chain Vulnerability

A company's attack surface is the sum of the different points in its technology environment through which an unauthorized user can enter data or extract data

As a result of increased digitization, a company's attack surface now extends far beyond the bounds of its offices and native IT network. Multiple unsecured devices may now be embedded in a network or connected to it intermittently. Services which were once maintained in-house may now be outsourced to third-party digital vendors. In addition, today's economy has physical and digital assets which are interlinked, as in the aviation and transport sectors.

The switch to digital means businesses need to worry about security of their own systems as well as all systems linked to their networks

The switch to digital has increased efficiency and ease of use but it also means that modern businesses are increasingly reliant on the security of not only their own systems, but all systems linked to their networks. The majority of private individuals and companies now operate within *"the context of multiple connections to third-party suppliers, technical support systems, and data flow controls that they do not necessarily have control over or even sight of."*[12] Vulnerabilities in less secure nodes in the system may offer a straightforward way for attackers to access the system as a whole and find backdoors into more sophisticated networks.

[12] Budd (2018), Cambridge Centre for Risk Studies.

The number of compromised or spurious software updates intended to access targeted systems grew throughout 2018.[13] A CrowdStrike survey of 1,300 companies across Europe, North America, Japan, and Singapore found that a majority of companies had experienced software attacks affecting their supply chains, with 90% of them leading to some degree of financial loss.[14] The average cost of these attacks was estimated at $1.1 million. Overall, the survey found a business community that was unprepared to mitigate cyber threats targeted at their supply chains. On average, disruptions were detected 10 hours after infection, the proper bodies were alerted after 13 hours, and the issues were resolved after a further 15 hours —a total of 63 hours, or two and a half business days, before the disruption ended.[15] Given that lack of productivity is a key driver of profit loss for a company, the growing rate of disruption stemming from vulnerable and lengthening digital supply networks is a great concern for the business community.

Cyber is Political

There has been a notable rise in publicly-attributed state-backed actors abusing digital systems for political advantage over the past four years

With a growing reliance on embedded networks, the threat posed by malicious cyber actors grows accordingly. Since 2015, there has been a notable rise in publicly-attributed state-backed actors abusing digital systems for political advantage. Cyber politics and physical politics are becoming increasingly intertwined, as state actors interfere with elections and manipulate perception on social media.

The same actors also pose a threat to corporations and business continuity. The NotPetya attack in 2017 (see box below) badly affected a number of corporates who were not intentionally targeted; Danish shipping company Maersk encountered ten days of business shutdown and losses of $300 million as a direct result of NotPetya, and had to replace its entire IT infrastructure after the infection.[16] Key organizations may be specifically targeted by aggressive states in order to steal intellectual property or security information, corrupt supply chains, raise funds, or cripple business through ransomware attacks or other disruptions. Given the substantial funding and expertise of the individuals involved in such state-sponsored teams, these attacks can be sophisticated and corrosive, and therefore devastating for the companies affected. They often lead to reputational ruin, frozen operations, clean-up costs, and punitive fines. State-backed cyber actors also pose a significant threat to economic continuity and critical national infrastructure.

NotPetya

On June 27, 2017, a virus that became known as ‘NotPetya’, to distinguish it from its antecedent versions of the ‘Petya’ virus, infected over 2,000 organizations across 65 countries. Disguised as ransomware, it was actually a destructive disk wiper that was hidden in the software update mechanism of M.E.Doc (U.K.), a Ukranian tax preparation program which is an industry standard for tax filing in Ukraine. As a result, 80% of the infections occurred in Russia and Ukraine, where more than 80 organizations initially reported being affected, including the National Bank of Ukraine, Kiev’s Boryspil International airport, and the radiation monitoring system at Ukraine’s Chernobyl Nuclear Power Plant. Nine percent of the infections occurred in Germany with the attack also reaching France, Italy, Poland, the United Kingdom and the United States.

[13] Ray et al. (2018).
[14] Larson (2018).
[15] Ibid.
[16] Greenberg (2018).

Similar to the WannaCry virus before it, NotPetya utilized an NSA exploit codenamed EternalBlue (made available the previous August by ShadowBrokers) but enhanced it with multiple techniques to propagate it throughout internal networks, while harvesting passwords, and running PSExec code on other local computers. The data encryption payload was irreversible, and the ransom demand was a hoax.

Because of the NotPetya attack, a number of large multinational organizations reported significant losses from business disruption. Maersk, one of the largest global shipping operators, reported that infections from the NotPetya virus caused it to suspend operations in parts of its organization, causing congestion in 76 ports that it operates worldwide. Resulting business losses reached up to $300 million in the initial three months after the attack. FedEx suspended its stock trading on the New York Stock Exchange after reporting $300 million in one-time costs from lost business and clean-up costs in its TNT Express division. Pharmaceutical giant Merck reported losses of $300 million for two successive quarters due to lost sales resulting from production shut-downs and the failure of internal IT systems. French construction materials company Saint Gobain reported a business impact of $393 million from the virus impacting its systems. Over a dozen multinational companies announced losses to quarterly earnings following the attack. There are additional reports of disruption to more than 30 international companies, and many Ukranian national organizations. The U.S. and U.K. governments attribute the NotPetya attack to Russia.

Influence on Real-World Politics

Cyber espionage, theft, and disruption caused by state-backed actors have led to marked real-world political and corporate implications

Cyber espionage, theft, and disruption caused by state-backed actors have real-world political and corporate implications. The WannaCry (see box below) and NotPetya attacks were both linked to state-backed groups, caused global disruption to corporates across a broad spectrum of industries, and threatened critical national infrastructure systems like the U.K.'s National Health Service and networks in the U.S.[17]

So far, malicious cyber behavior by nation states remains below the threshold of traditional war and is limited by international deterrence practices. Should the scope, scale, and seriousness of attacks persist, peacekeeping measures may erode and possibly lead to all-out cyber wars and traditional declarations of war. Diplomatic attempts may be pursued to ward off this eventuality, but without a clear means of enforcing rules and legitimate penalties, they are unlikely to represent a significant obstacle to escalating cyber attacks.

Wannacry

The WannaCry ransomware attack in May 2017 spread via file-sharing network protocols on computers using outdated Windows XP and version 8 operating systems (v8 OS). It resulted in 300,000 infections of computers across 150 countries. WannaCry used the same EternalBlue exploit as NotPetya and predominantly affected personal users, public sector organizations, and SME-scale companies by infecting unpatched boxes and equipment on dedicated older operating systems. Several dozen large companies also reported disruption and losses from infection of their systems. Of the roughly 400 million actively-used Windows computers running v8 or earlier operating system, approximately 0.1 percent were infected. The great majority of the Windows computers running v8 or earlier were protected by Microsoft patch MS17-010 which was issued two months earlier, in March 2017.

[17] Goldman (2017).

The event highlighted the issue of equipment software latency, in which machines and sub-networks within organizations rely on a specific version of an operating system that renders them vulnerable. In these cases, although the majority of systems within organizations ran more up-to-date systems, certain departments and activities were maintaining the older vulnerable versions. Devices such as medical MRI scanners and x-ray machines certified on XP and v8 and maintained on those operating systems, were among those crippled by the attack. Businesses reported substantial losses from system lock-outs around the world, in areas such as manufacturing processing, dispatch and ordering systems, gas pump payment applications, and telephone exchange equipment. We estimate the direct costs and indirect business disruption losses from WannaCry to be around half a billion dollars.

If the WannaCry malware was created to generate ransom payments then it was remarkably unsuccessful. The Bitcoin account where the ransomware was to be paid received less than $150,000 in payments, no company that paid a random got its data back and the funds may not have been claimed by the criminals. Instead, the motivation was more likely to sabotage some of the affected companies rather than generating funds for the hackers. It is also possible the widespread economic disruption was collateral damage to mask a separate, targeted destructive attack.

The propagation of WannaCry was stopped after four days by a researcher who found a kill-switch within the software. Without that discovery, the infection could have spread to many more machines and had a more severe impact. Counterfactual analysis by RMS suggests that if the kill-switch had not been triggered, and if the attack had occurred prior to the issuing of the MS17-010 patch for Windows 8, the infection rates and losses could have been an order of magnitude higher, perhaps reaching $3 to $6 billion. According to the U.S. government, North Korea was responsible for the WannaCry.

Cryptocurrencies Are Popular and Vulnerable

Lack of regulation and integrated dependency on a fully functioning network in cryptocurrency marketplaces makes them overwhelmingly vulnerable to attack and disruption

The rise of cryptocurrencies is also a significant driver of cyber crime and resulting losses. Since the introduction of Bitcoin in 2009, the cryptocurrency market has ballooned in value. In places like Japan, the trading volume of cryptocurrency has increased by 440,000% in three years.[18] The lack of regulation and integrated dependency on a fully functioning network in these marketplaces makes them profoundly vulnerable to attack and disruption. In June 2018, a dedicated denial-of-service attack on the major crypto-exchange Bitfinex overloaded the platform's server and took the exchange offline for an hour, during which Bitcoin prices fell by 2%.

Attacks on cryptocurrency trading platforms set new records for the largest digital financial thefts in 2018. Over the first six months of 2018, more than $1 billion was stolen from exchanges. In January, an attack on the Japanese exchange Coincheck resulted in the largest theft to date: a loss of $516 million worth of New Economy Movement (NEM)[19] cryptocurrency, affecting 260,000 users.[20] Blockchain reporting outlet CoinDesk estimates that $2.7 million is now stolen from exchanges every day.[21]

[18] Jonnie Emsley (2018).
[19] NEM is a highly adaptable peer-to-peer cryptocurrency supported by blockchain technology, introduced in 2015. It is used predominantly in Japan and SE Asia where it is used in partnership with the largest cryptocurrency exchanges and other traditional financial institutions.
[20] Spilotro (2018).
[21] Larcheveque (2018).

Insurers began offering cryptocurrency theft coverage in February 2018 as part of affirmative cyber insurance policies. Given the heightened risk in the space, insurers have limited the rollout so as to curtail potential exposure. Similar offerings include insurance for digital wallet theft caused by malicious interference, general policies for blockchain start-ups, and cyber-theft additions to specific policies.[22]

The Economic Threat to Industry

The themes described above establish the landscape in which cyber actors and their ambitions have flourished since 2010. While cyber losses to industries and corporates may be attributed to any of these trends, the growing availability of powerful digital tools on cyber criminal marketplaces also allows particular firms and industries to be specifically targeted for financial gain. In other cases, particularly virulent or disruptive non-targeted attacks may leave industries indiscriminately facing massive financial losses.

The majority of targeted cyber attacks, involve: (1) data exfiltration; (2) contagious malware; (3) financial theft; (4) cloud outage; and (5) distributed denial-of-service attacks

Targeted attacks, namely those involving: (1) data exfiltration; (2) contagious malware; (3) financial theft; (4) cloud outage; and (5) distributed denial-of-service, make up the majority of financial losses attributed to cyber, and are growing in popularity and frequency.

1. Data Exfiltration

Data exfiltration attacks were the most costly type of cyber attack to industry in 2018

Data exfiltration attacks were the most costly type of cyber attack to industry in 2018. Massive breaches regularly made headlines worldwide, leading to damaged brand reputations and hefty punitive fines. A breach of data from Indian database Aadhaar discovered in September 2018 was the second largest on record, with more than 1.1 billion records leaked. The average breach size continues to grow year over year.[23] In 2018, the average cost of a single data breach attack anywhere in the world was $3.86 million — a 6.4% increase from 2017. Mega-breaches where 1.5 million records are compromised can result in higher than average losses estimated between $40 and $350 million.

Figure 4. Selected Recent Large-scale Data Breaches

Company	Country	Number of Records	Date
Aadhaar	India	1,190,000,000	Jan-18
Exactis	United States	340,000,000	Jun-18
Twitter	United States	336,000,000	2018
Under Armour	United States	150,000,000	Mar-18
Huazhu Hotels Group	China	130,000,000	Aug-18
MindBody	United States	114,000,000	2018
Myheritage	Israel	92,300,000	Oct-18
T-Mobile	United States	74,000,000	Aug-18
Sungy Mobile Limited	China	50,600,000	May-18
Facebook	United States	50,000,000	Sep-18
MyEtherWallet	United States	50,000,000	Apr-18
Localbox	United States	48,000,000	Apr-18
Andhra Pradesh Government	India	45,000,000	2018
Panera Bread	United States	37,000,000	Apr-18
Ticketfly	United States	27,000,000	May-18
Comcast Xfinity	United States	26,500,000	May-18
Animoto	United States	22,000,000	Jul-18
Timehop	United States	21,000,000	Jul-18
Marriott	United States	500,000,000	Nov-18

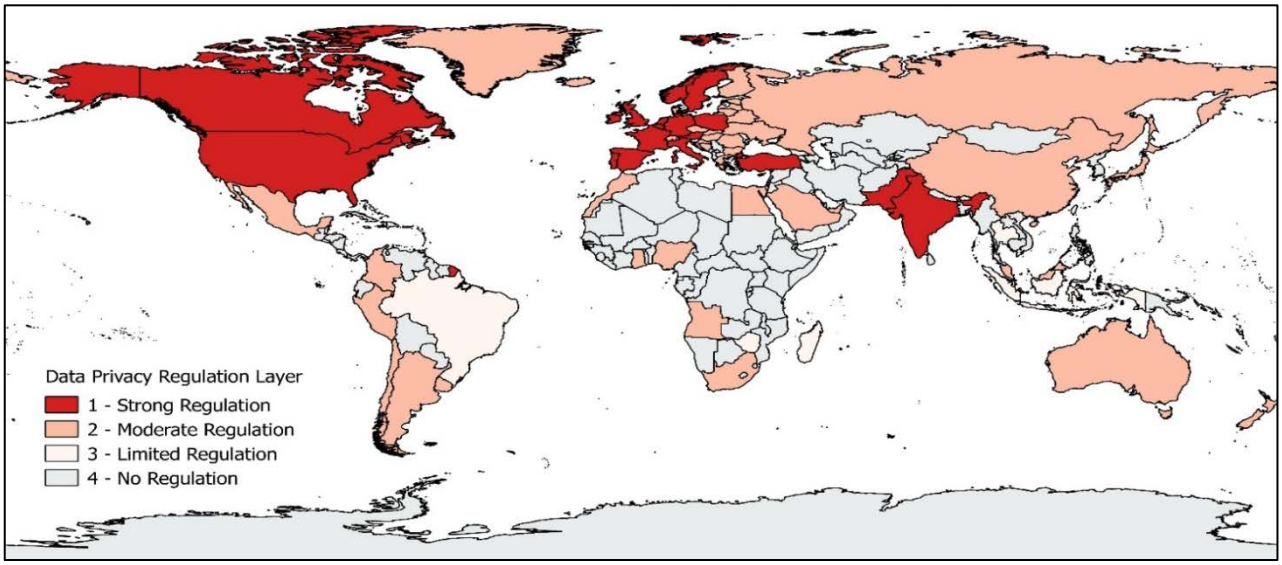
Note: Two Facebook breaches have been excluded from this list as the data was not exfiltrated.
Source: Cambridge Centre for Risk Studies, 2019, 'Cyber Risk Outlook, 2019

[22] Helms (2018)
[23] Saini (2018).

Indirect losses generated the greatest amount of economic damage in data exfiltration incidents. Impacts to brand reputation, customer churn, business interruption, and reactionary management strategies drive significant losses; incidence response costs also contribute, as more complex digital networks require longer clean-ups and securitization measures. *"Large-scale breaches (over 1 million records) cause high levels of customer churn due to a strong correlation between the severity and longevity of a breach and reputational damage caused to a company."*[24] Reputational damage is felt long after remediation and changes in security or business structure, and can be extremely difficult to mitigate.

As regulatory fines grow, breaches will likely become more costly. In May 2018, the introduction of General Data Protection and Regulation (GDPR) standards in Europe provided a centralized legal framework for reporting and addressing data breaches. Since May when GDPR came into application and end January 2019, there have been over 95,000 complaints made to the regulators, with three fines issued, the largest being €50 million to Google for the lack of consent on advertisements.[25] Decisions over Facebook's October 2018 violation are pending.

Figure 5. Global Data Privacy Regulations



Note: Data compiled and reviewed from the following sources to create this map: DLA Piper n.d.; CNIL (2018); Privacy International (2018); Hedrich, et al. (2017)
Source: Cambridge Centre for Risk Studies

With increased digitization, companies depend on the strength of the security throughout their operations to limit exposure to tail-risk data loss. Studies indicate that almost 60% of the data breaches reported in the last two years were ultimately traced back to a known, latent vulnerability which the organization had not yet patched.[26]

While the size and damage of breaches continues to climb, the overall number of data exfiltration incidents dropped in 2018, likely due to a flooded criminal market for stolen information. The abundance of personal data available for sale online inhibited demand and drove down the profitability of breach attacks. Effective anti-fraud measures also limit the value of stolen data. Because data on its own has lost value in the cyber economy, actors are instead wielding the potential damage breaches pose to company reputations as a means of extorting firms.[27]

[24] Ponemon (2018). Cambridge Centre for Risk Studies (2018).
[25] GDPR (2019).
[26] Higgins (2018).
[27] Armor (2018).

2. Contagious Malware

Ransomware is now the malware of choice for financially-motivated cyber attacks

Contagious malware and malicious software exploits pose a significant threat to the business world and its continuity. Ransomware is now the malware of choice for financially-motivated cyber attacks, overtaking Banking Trojan incidents in 2018. While a Banking Trojan, which disguises itself as a genuine app to access your banking details, requires a money laundering process susceptible to financial anti-fraud measures, ransomware involves straightforward transactions.

Demanding payment in an unregulated, difficult to trace cryptocurrency is one way that ransomware attacks negate these logistical burdens. In the past two years alone, cyber criminals have accrued more than $25 million in ransomware attacks.[28]

2017 was termed the "year of ransomware" following the NotPetya and WannaCry attacks.[29] Although ransomware attacks dropped in 2018, partly due to security advances and mitigations made during the previous year, the threat of a self-propagating malware attack causing vast systemic damage remains tangible.

Typically, contagious malware affects systems by taking advantage of human judgment and error. Spear phishing — or targeting specific individuals with personalized emails — is still the most successful means of gaining access to a network and was used by 71% of cyber criminal groups in 2017.[30] More frequently, however, malware is introduced into a system when attackers take advantage of poor patching rhythms or latent software vulnerabilities. These malwares are known as cryptoworms, due to their exploratory, self-propagating nature.

This was the case with WannaCry and NotPetya, which both used the EternalBlue exploit first published by the ShadowBrokers leaker in April 2017. The EternalBlue exploit was latent in Microsoft Windows operating systems. Systems patched following a security bulletin in March were safeguarded against the ransomware spread, but many older networks, such as those used by the U.K.'s National Health Service, were not properly safeguarded or surveyed. The WannaCry cryptoworm resulted in an estimated $4 billion loss worldwide; NotPetya's wiper cryptoworm led to a $10 billion loss.[31] No similar attacks occurred in 2018, but there is every possibility that cryptoworms will cause significant systemic damage again. In these cases, the losses are dependent on the rate at which the infection spreads to additional devices, causing higher clean-up costs and a wider footprint for business interruption.

Mobile malware attacks are on the rise in emerging economies, as attackers write Trojan, adware, and spyware variants for new mobile operating systems. China, Bangladesh, and Iran had the highest share of reported mobile malware attacks in early 2018, a fact that Kaspersky attributed to the density of unpatched devices in the network.[32] A recent report suggested that 87% of Android smartphones contained at least one latent software vulnerability and that 95% of Android devices were susceptible to ransomware, mobile Trojans, and botnets via simple text commands.[33]

In June 2018, research showed that, even in the U.S., Android users are exposed to a 'hidden patch gap', meaning that their security may be out of date by as many as four updates.[34]

[28] Europol (2018).
[29] Dean (2018).
[30] Symantec (2018).
[31] Galling (2018), Reinsurance (2018).
[32] Kaspersky Lab (2018).
[33] Thomas, et al. (2015)
[34] Ibid.

3. Financial Theft

Online fraud dominates the financial theft landscape by criminal volume

Financial transaction systems are exploited at multiple levels, and even the introduction of EMV (Europay, Mastercard, Visa), an authentication service on transactions to reduce point-of-sale fraud and smartcard data skimming, has not reduced the rate of innovation in cyber criminal financial theft.

Online fraud, dominates the financial theft landscape in terms of volume. Between 2017 and 2018, attacks on the e-commerce industry in the U.S. grew by 93%.[35] It is estimated that the cost of reimbursing fraud charges on e-commerce crimes could reach $31 billion if the growth of theft continues at the current rate to 2020. In the growing mobile commerce sector, where retailers are highly susceptible to fraud and identity theft, every $1 lost in fraud costs the vendor an average of $3.29.[36] As steps are taken to securitize vulnerable points in the transaction system, fraudsters adapt and compromise the system in new and damaging ways.

Cyber criminals have also embraced social engineering as a tool in financial theft heists. In the U.S., 'whaling', is a style of phishing campaign in which attackers pretend to be trusted colleagues or key suppliers in order to action large cash transfers from C-Suite and senior professionals. This form of fraud grew by 138% between 2016 and 2018. Whaling attacks have cost companies $12.5 billion since 2013.

Case Study: Cyber Crime and the SWIFT Network

One of the most significant cyber bank heists took place in 2016, when an extended campaign enacted by the Lazarus Group stole almost $1 billion from commercial banks by penetrating the SWIFT network's backend Alliance Access software. The largest individual theft saw $101 million stolen from the Central Bank of Bangladesh via its account with the U.S. Federal Reserve. The report of this loss led to the realization that several other banks had been hit by similar attacks in Vietnam, Ecuador, and Southeast Asia. In these incidents, malware issued SWIFT transfer notices for large funds and deleted the requests and confirmation messages from the SWIFT database after funds were received.

In 2018, attacks continued with a $10 million theft from Banco de Chile. In this instance, the attackers used a destructive wiper and ransomware as a misdirection tool while illicit transactions were made on the SWIFT network.[37] In May 2018, Banco de Mexico reported an attack against their domestic inter-banking payment system that resulted in a $15 million loss.[38]

The attacks threatened the international banking systems' trust in the SWIFT network. SWIFT announced they would review their security protocol and in 2017 issued updates. It was judged that the malware had accessed the network via exploitation of human error, and SWIFT introduced a mandatory 'Customer Security Control Framework', which required adherence to 16 mandatory security standards by all users.[39] Nineteen further security protocols will be introduced in 2019 to address the issues found in 2018 SWIFT heists.[40]

[35] ThreatMetrix (2018).
[36] LexisNexis (2018).
[37] Kirk (2018).
[38] O'Boyle (2018).
[39] SWIFT (2018).
[40] Koetsier, et al. (2018).

4. Cloud Outage

The growth of the IoT to 20 billion devices by 2020 is estimated to require 400 million servers for support, most of which will be cloud based, increasing the negative consequences of any cloud outage

Cloud computing services are now a vital pillar of digital business and economics, allowing for rapid sharing, streaming, and storage of data with minimal difficulty in about 60% of enterprises.[41] The growing reliance on these shared resources, however, creates a high risk in the event of an outage or network breach.

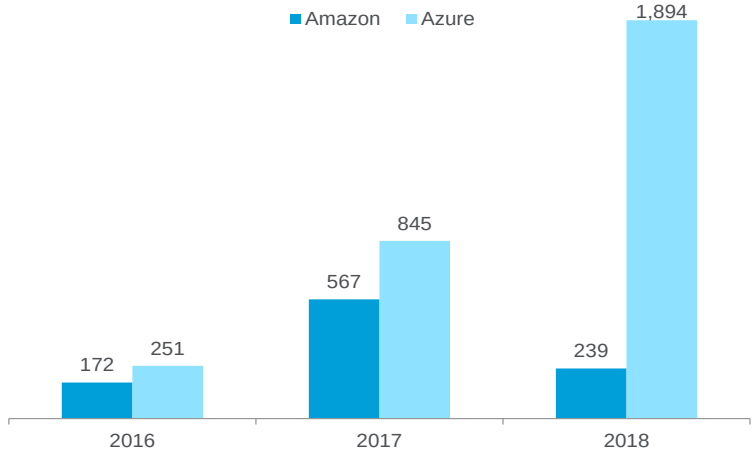
Cloud adoption has increased, and will continue to grow as the Internet-of-Things (IoT) builds an ever wider network and Asia-Pacific companies migrate their business to the cloud. It is estimated that the growth of the IoT to 20 billion devices by 2020 will require 400 million servers for support, most of which will be cloud based.[42] In this scenario, cloud spending is expected to surpass $500 billion within two years.[43]

The security of cloud computing services is a responsibility shared between its users. There is a presumption that cloud services offset the responsibility of data security to a dedicated team maintained by the services provider. At present, the public cloud market is dominated by four major providers: IBM, Microsoft (Azure), Google (Google Cloud Platform), and — the largest — Amazon Web Services (AWS). Due to an established relationship of trust in these giants, there is little indication that this dominance will change in the years to come, meaning that the largest part of the significant burden in cloud security will remain with four major companies.

Yet around half of organizations using the cloud experienced at least one breach of their hosted data between 2017 and 2018 and were quick to blame AWS, as in the cases of Dow Jones, Verizon, Tesla, and FedEx. In these cases less than a third of the compromises could be attributed to the cloud provider itself. Instead, poor data configurations, incorrect settings, and simple or non-existent passwords on AWS servers used by cloud clients were responsible for these failures.

As cloud dependency increases, so too does the cost of downtime for both clients and providers. Cloud outage hours rose on average in the through 2018. Although it is unlikely a provider will experience a complete outage, there is no doubt the effects of such an event would have a significant damaging impact on the global economy. Losses from a hypothetical three to six day cloud outage in one of the top four services in the U.S. could cost the global economy $19 billion.[44] Partial outages, affecting particular cloud services, could cumulatively be as costly over time.

Figure 6. Logged Hours of Server Downtime Between AWS and Microsoft Azure from 2016 to 2018



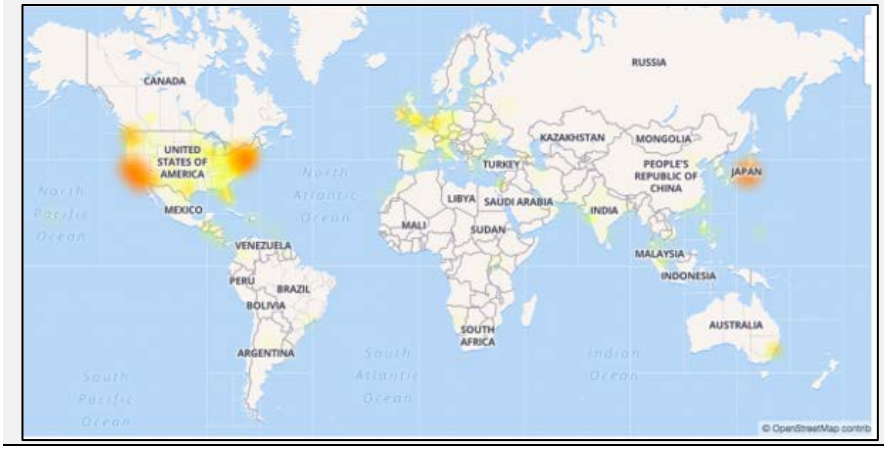
Source: Cambridge Centre for Risk Studies

[41] DeNisco (2018).
[42] Gartner (2017), Business Sweden.
[43] Rightscale (2018).
[44] Lloyd's and AIR (2018).

Case Study: Amazon Prime Day Outage

Amazon's 2018 'Prime Day' sale set the record as the biggest shopping day in the site's history, with over 100 million products purchased in a period of 36 hours. The massive surge of web traffic to the site shortly after the sales' launch overwhelmed servers and, without additional server power, customers primarily in the U.S. and Europe experienced scattered server issues, affecting website navigation, check out, and account services. The burden on servers led to cascading issues with internal storage and computation, which ultimately affected Amazon's Alexa, Prime Video, and music services. Amazon quickly adjusted its homepage settings to limit international usage and server workload. Although the event was highly profitable, an assessment by One Click Retail estimates that Amazon lost $1.2 million in sales per minute of downtime.

Figure 7. Map of Service Disruptions of AWS on Amazon Prime Day



Source: https://outage.report/

5. Distributed Denial-of-Service

DDoS attacks, which increase the traffic on a particular network to an extent that it overwhelms systems and makes them inaccessible to legitimate users, have grown markedly more aggressive in recent years

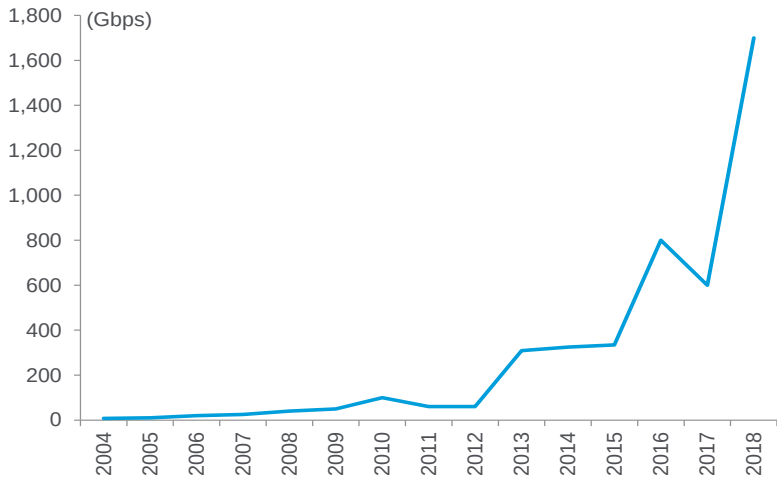
Distributed denial-of-service (DDoS) attacks involve increasing the traffic on a particular network until it overwhelms systems making them inaccessible to legitimate users.[45] DDoS attacks often exploit connected devices with low security in order to scale the severity of the attack. DDoS attacks have grown markedly more aggressive in recent years with the introduction of more devices to the Internet-of-Things. These unsecured devices can be used remotely to overwhelm connected systems. In 2018, the largest ever DDoS attack overwhelmed GitHub services for four minutes, with traffic reaching a peak of 1.35 terabits per second (Tbps). It is unknown what prompted the attack. (Foltyn 2018)

While attacks over ten Gigabits per second (Gbps) have doubled in recent years, the vast majority of DDoS attacks are still less than five Gbps in volume. Attacks of this low volume may not cause a complete outage of the site, but will still significantly slow down service. These low-and-slow attacks may be difficult to discern from regular traffic or expected spikes, making them very difficult to mitigate. While the frequency of DDoS attacks has increased, their duration, as in the case with GitHub, has decreased sharply. Over three-quarters of attacks now last for less than ten minutes.[46]

[45] Kohout n.d.
[46] Corero Network Security, Inc. (2018)

This change in qualities is connected to a new technique for amplifying attacks. Many threat actors enacting DDoS attacks have pivoted from targeting network layers to attacking application layers instead, which provide the interface between applications and the network, and can amplify an attack's impact. Disruptive attacks on this level are far more damaging to data structures, despite their shortened duration. Attackers have also begun to utilize Memcached systems and DNS protocols to enact reflected amplification DDoS (rDDoS). Two in five businesses who experience a DDoS attack, report the effects of rDDoS, which are far more difficult to mitigate.[47] The GitHub attack was one such incident where Memcached was weaponized to take a site offline.

Figure 8. Peak DDoS attack size from 2004 to 2018



Source: Citi Research, Cambridge Centre for Risk Studies

The main impact to a corporate from a DDoS attacks is the interruption of business, but brand and reputational damage also have a huge impact

DDoS attacks are typically cited as disruptive attacks — their main loss process is the interruption of business and forcing companies to recover from attacks in short periods, with no change to business procedures. Fifty-seven percent of organizations which suffer a DDoS attack report damage to reputation and brand as the primary business impact, with a rise in operational expenses a secondary issue. The cost of a site outage due to a DDoS attack varies from target to target. The BBC experienced a DDoS attack in 2015 which left users unable to access stories and content, but did not affect ad revenues, which the BBC does not acquire.[48] A 2016 DDoS attack on HSBC, however, left up to 17 million customers unable to complete transactions or bank online.[49] In 2018, a survey by Neustar suggested that the average loss associated with a DDoS attack was $2.5 million, with $2.2 billion lost in the course of 12 months across 849 respondents.

The operation costs of preventing and recovering from DDoS attacks can be high. In a third of instances, DDoS attacks mask the entry of malware or ransomware into, or the exfiltration of data from, a network.[50] Ninety percent of companies that undergo a DDoS attack also experience a significant data breach either simultaneously or shortly afterwards.[51]

[47] Cisco (2018)
[48] BBC (2015).
[49] Osborne (2016).
[50] Kaspersky (2015).
[51] Reo (2017).

Section 2: Who is at Risk?

Cyber and Governments

On the December 20, 2018, U.S. Deputy Attorney General Rod J. Rosenstein announced charges against two Chinese hackers. In his speech he stated that *"More than 90% of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China."* This speech was extraordinary as it showed just how nation states have become sophisticated players in the cyber world. Recently the U.S. Department of Justice charged China's Huawei with theft of trade secrets, wire fraud, and obstruction of justice. A 10-count indictment alleges China's Huawei stole trade secrets from U.S. carrier T-Mobile beginning in 2012.[52] However, it has been reported that the core issue with Huawei is its closeness with the Chinese government.

Multiple countries are accused of using cyber attacks for both espionage and competitive advantage

China is not the only country accused of using cyber attacks — North Korea, Iran and Russia have all been accused by the West. According to Oxford Analytica,[53] North Korea has caused considerable disruption since at least 2009 even though their offensive cyber capabilities are not on par with those of the U.S., Russia, or China. As with most nation states, North Korea's cyber operations reflect Pyongyang's strategic and geopolitics interests. It is thought most nation states deploy cyber capabilities for espionage or for competitive advantage, however it seems that North Korea is different, as they usually seek some sort of financial gain. Russia, on the other hand, completely denies being responsible for cyber attacks against other nation states despite the mountain of evidence that is growing against them. Russia has recently been accused of trying to trying to breach the WiFi network of the Organization for the Prohibition of Chemical Weapons in the Hague. In the U.S., 13 Russian nationals and three Russian companies were indicted on conspiracy charges, related to a Russian propaganda effort designed to interfere with the 2016 US election campaign. The companies involved include the Internet Research Agency (often described as a troll farm) and two other companies that helped finance the attack.[54] Iran started to invest more in its cyber capabilities following Stuxnet, a joint cyber attack by the U.S. and Israel to undermine Iran's nuclear capability.

Western countries are reported to have installed offensive cyber capabilities to respond effectively to hostile nation states and other cyber threat actors

It has been reported that Western countries such as the U.S. and the U.K. also have offensive cyber capabilities. The U.S. Department of Defense's 2018 cyber strategy, for example, stated overtly that it was expanding its offensive cyber capabilities in order to gain an edge in its long-running strategic competition with cyber teams in Russia and China.[55] The report also defined the U.S.'s choice to "defend forward" by actively addressing and pursuing cyber threats to national security before attacks can be triggered. Following the Russian poisonous attacks on U.K. soil, the U.K. government extraordinarily announced it will be spending £250 million on an offensive cyber-force comprised of 2,000 personnel to respond effectively to hostile nation states and other cyber threat actors.[56]

It is important to note that it is not only nation states that cause disruption to governments, but also other threat actors such as highly-organized and sophisticated criminals.

[52] Cnet (2019).
[53] Oxford Analytica (2019).
[54] Prokop (2019).
[55] Department of Defense (2018).
[56] Jay Jay (2018).

Threats to Governments

What particular threats do governments face? Threats to governments are much like threats to corporates and people. At a high level, these threats include:

1. Critical infrastructure;
2. Theft of data including the theft of trade secrets; and
3. Financial loss.

Each country addresses threats from cyber in their own way — with a significant number of countries not yet having a cyber strategy in place

Each country is addressing threat to its government in their own way. However, according to the UN's ITU 2017 Global Security Survey, 50% of countries have no cyber strategy in place.[57] This obviously could have changed in the two years since the survey, given the speed at which the world of cyber is changing. In the last few years many countries have set up national cyber centers, i.e., the National Cyber Security Centre (NSCS) in the U.K., which was set up in 2016 and brought expertise from the Communications-Electronics Security Group (CESG) — the information assurance arm of Government Communications HQ) and the Cyber Assessment, CERT-UK. The NSCS aims are to protect the U.K.'s critical services from cyber attacks, manage major cybersecurity incidents, and improve security of the U.K. Internet through technological improvement and advice to companies and citizens.[58] In the U.S., President Trump signed legislation creating the Cybersecurity and Infrastructure Agency (CISA) to help protect a variety of important infrastructure systems including the country's electricity grid and election infrastructure. The National Risk Management Center within CISA aims to identify and address the most significant risks to critical infrastructure systems within the U.S.

And there is limited collaboration between national governments on cyber

It is thought there is also collaboration between national governments on cyber. For example the Five Eyes Intelligence Partnership[59] issued a report detailing five publicly available tools used by threat actors, including advice on how to limit their effectiveness. The European Union has set up the European Union Agency for Network and Information and Security to better support member states with tackling cybersecurity threats and attacks. NATO has also adopted a new command structure, with two new commands focusing on the North Atlantic and logistics, together with a cyber operations center. These two command centers are rather small, but have scope to grow depending on the security environment in Europe.[60]

International Legislation

A starting point on international cyber legislation was started by the UN in 2004

Are cyber activities covered by any form of international legislation? In 2004, the UN Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was set up to develop a common approach to align governments behavior in cyberspace. The UN GGE process has been the primary avenue for countries to discuss the international regulation of cyberspace.[61] As a starting point, it was agreed that cyber was governed by the same international legal principles that govern the 'physical' world. However, as Henriksen notes in his 2019 paper, the question of how exactly these principles should apply to information & communications technology (ICT) proved to be very difficult to answer.

[57] ITU, Global Cybersecurity Index (GCI) 2017.
[58] McKinsey & Company (2018).
[59] The Five Eyes (FVEY) is an Anglophone intelligence alliance comprising Australia, Canada, New Zealand, the U.K., and the U.S.
[60] Oxford Analytica (2018), Cybersecurity and Geopolitics.
[61] Henriksen (2019)

Several reports and expert groups have been convened over the years but none of them have provided clarity or consensus outside of listing views on how international law applies to the use of ICT by different countries. With the collapse of the latest attempt in 2017 to find clarity, countries instead have sought bi-lateral agreements — i.e., China and Russia created the Shanghai Cooperation Organization, which submitted a code of Conduct for Information Security to the UN, while the U.S. said it would work with like-minded partners.

The discussion on how nation states should behave in cyberspace is ongoing

The discussion on the behavior of nation states in cyberspace is ongoing. The UN General Assembly has just adopted two separate resolutions — one sponsored by Russia and the other by the U.S. — on the action of nation states in cyberspace. The Russian resolution creates an open-ended working group to study the existing norms contained in the UN GGE reports, to develop new norms, and to determine whether there is a possibility of establishing regular institutional dialogue. The U.S.-sponsored resolution aims to create a new group of government experts to study how international law applies to nation state action in cyberspace. [62]

[62] Council of Foreign Affairs (2018).

Cyber and Critical Infrastructure Systems

As critical national infrastructure systems increasingly move from being 'air-gapped' to being connected, the threat from cyber increases

Digital connectivity is now an integral component of the global economy, vital for the operation of almost all elements of trade and business continuity. As this interconnectivity grows, these elements become ever more exposed to the vulnerabilities inherent in both new and intrinsic technologies. As recently as five years ago, many in the industry were certain that key operational technology (OT) vital to the sustainability of critical national infrastructure (CNI) was 'air-gapped', or impossible to access from the outside. Although historically, many CNI systems have been networked locally, more systems are now connected to the Internet in order to streamline the process of installing updates and improving system reliability. These systems include supervisory control and data acquisition (SCADA), Distributed Control Systems and Programmable Logic Controllers.

Recent events, however, have led governments worldwide to recognize CNI vulnerability and to investigate both the threat of cyber attacks on critical systems and the impact such attacks could have on both local and global economies. In cases affecting CNI, even cyber attacks which freeze or disrupt a limited number of systems may ultimately cause systemic damage, leading to costly, far-reaching consequences.[63]

Generally, the term national infrastructure refers to systems in the following subsectors:[64]

1. Energy & power; electricity, gas & fuel;
2. Communications: telecommunications (including digital communications), postal services, and broadcasting;
3. Transport: aviation, maritime, rail and land;
4. Emergency services: ambulance, fire & rescue, marine, and police;
5. Financial services: payment, clearing & settlement systems, markets & exchanges, public finances;
6. Food: production, processing, import, distribution, retail;
7. Government: central government, devolved administration/functions, regional and local government;
8. Health: healthcare, social care; and
9. Water supply: drinking water supply, waste water services, dams.

[63] https://www.dhs.gov/CISA.
[64] U.K. Government (2010).

Attacks on Critical National Infrastructure

As key sectors in utilities become more integrated, ensuring the security of the whole system becomes more reliant on the securitization of its total parts

As key utilities in the supply of power, water, healthcare, and transport become increasingly integrated with digital systems to permit ease and efficiency of use, the system as a whole becomes more reliant on the securitization of its total parts. A disruption in the power supply for a major city or population center, for example, could affect millions of electricity customers, as well as emergency services, telecoms, transportation, and access to fuel and water for an even greater number.

A number of deliberate, targeted cyber attacks on areas of CNI have already occurred in parts of Europe and the Middle East. In 2005, the success of the Stuxnet worm (see box below) in hamstringing Iran's nuclear program alerted global powers to the latent risk of cyber threats to major national facilities. In December 2015, a cyber attack against three power distribution companies caused a blackout in the Ivano-Frankivsk region of Ukraine. Almost a year later, an attack against the Ukrenergo transmission station led to an eight-hour blackout which affected 225,000 customers. In the latter case, the malware found was linked back to the Russian APT Sandworm. Malware was also used to try and take control over a petrochemical plant's safety instrument system in Saudi Arabia. This rogue code known as Triton was found to have the ability to disable safety systems designed to prevent industrial accidents (see box below).

Stuxnet and Triton

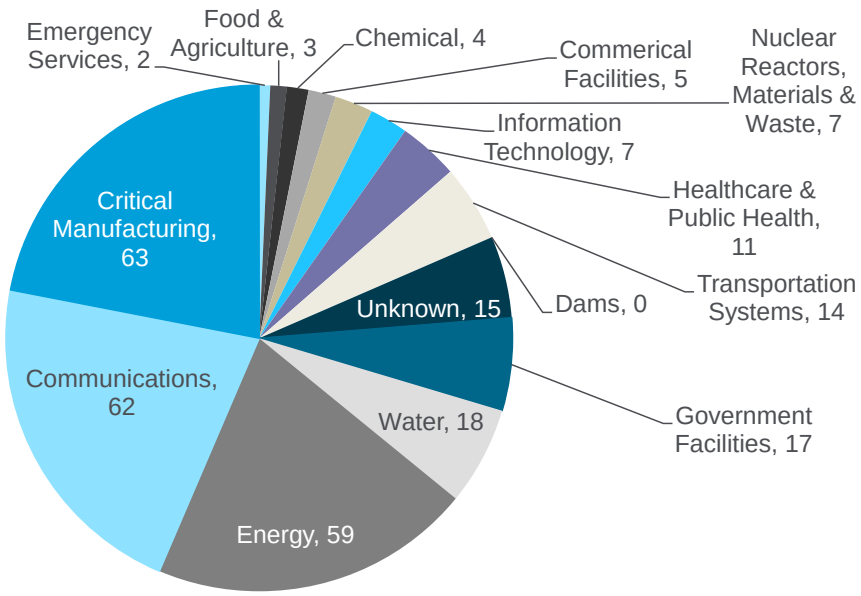
Stuxnet was a game changer — although losses were not large, it made headlines because malicious code was sent deliberately to target physical critical infrastructure. Stuxnet targeted industrial systems under control of the Siemens PCS7 SCADA (Supervisory Control and Data Acquisition) system. The specific target appeared to be the Natanz Nuclear Facility in Iran where the malicious code spun 1,000 nuclear centrifuges past their operating limits leading to their destruction. It also caused damage to other industrial systems controlled by the Siemens system, i.e., the oil industry. The perpetrators are generally considered to be the U.S. and Israel.[65]

Triton has been described by MIT Technology Review as 'the world's most murderous malware'.[66] Triton was discovered in summer 2017 in a petrochemical plant in Saudi Arabia. The malware made it possible to take over the plants safety systems remotely and potentially cause serious damage to the plant and to people's lives. Despite the attack not being successful due to a flaw in the code, a flaw in the code which was discovered before the hackers could do any damage, which made the attack unsuccessful, but the fact hackers could compromise or disable safety systems in critical infrastructure systems was terrifying. It is believed that a nation state is behind the attack with cybersecurity company FireEye, who was called at the very beginning of the attack, pointing a finger at Russia. The hackers had been inside the petrochemical company's corporate IT network since 2014 and managed to find a way from that network into the petrochemical's own network. It is also claimed that the hackers acquired an identical safety instrument machine and used it to test the malware they developed. They seem to have found a 'zero day vulnerability' in the machine's firmware which allowed them to inject code into the safety system and enabled access whenever they wanted. This example shows how some hackers will go to great lengths to ensure a successful cyber attack, including purchasing machines to test out malware applications and years of assessment to find ways to compromise systems and potentially put lives at risk.

[65] Schneier (2010)
[66] Giles (2019)

Even in instances of error and oversight, critical systems have been significantly compromised by digital means. In December 2018, the expiration of a transport layer security (TLS) certificate knocked out Telefonica UK Ltd's data network for 32 million O2 customers in the United Kingdom.[67] Airlines and airports commonly face expensive disruption stemming from glitches and outages in booking software and air traffic control systems.[68] In May 2017, the highly virulent WannaCry ransomware attack drew attention to the particular vulnerability of the National Health Service; a government audit in 2018 revealed that 200 NHS Trusts in England and Scotland still could not pass a cyber security assessment.[69]

Figure 9. Industrial Control System Cyber Incidents by Sector as Reported to the U.S. National Cybersecurity and Communications Integration Centre for 2016



Source: Centre for Risk Studies, Incident Response Pie Charts (YIR 2016 Addendum)

Key Vulnerabilities in Operational Technology

Aging operational technology in critical national infrastructure and their reliance on software patching for security increases the risk of cyber attack

Most OT systems used in CNI were designed and installed at a time when cyber risk was either not known or not considered. Such systems are typically difficult and expensive to replace and therefore software updates and patches are the simplest path to providing a measure of security.[70] The major trend vulnerabilities existing in OT systems and industrial control systems (ICS) have their roots chiefly in both unsecured technology and matters of human judgment:[71]

[67] Scroxton (2018).
[68] Yanofsky (2015).
[69] House of Commons (2017).
[70] For further information on the technical side of these vulnerabilities, see ICS-CERT, n.d.
[71] The following trend analysis was submitted by the Cambridge Centre for Risk Studies as written evidence on November 19, 2018 to 'Cyber Security of the U.K.'s Critical National Infrastructure – Joint Committee on the National Security Strategy – House of Commons'.

- **Industrial control system lifetime versus IT system lifetime:** Operational engineering systems are generally designed to last five times longer than the underlying IT systems.[72]

- **Testing costs:** – The security of many commercially successful off-the-shelf products has steadily improved over time due to mutually beneficial security testing by independent security professionals. The popularity of a product, such as a smartphone or a virtual assistant, and its level of availability may inspire a penetration tester to interrogate that product for system weaknesses, leading to a growth in the tester's reputation and a boon for the product vendor. The reverse is true of OT equipment, however, as widely-used systems rarely have any brand recognition outside of industrial engineering circles and equipment is expensive or cumbersome for a researcher to acquire for testing purposes. Many OT products are therefore under-examined because there is too little incentive for independent security testing.

- **Poor patching cadence:** Given the complexities of technology, it is challenging to patch operating systems and software to ensure the functionality of the entire system. A study by the Zero Day Initiative determined that in 2016, it took 143 days for human machine interface vulnerabilities to have a patch released by the vendor.[73] Both patching cadence standards within an organization and regular patch releases from vendors are susceptible to long delays and installation issues.

- **Poor password security and unencrypted protocols:** The recent Mirai botnet came about as a result of IoT devices being sold with easily hackable passwords and using unencrypted protocols.[74] Although the Mirai botnet cyber attack was not related to ICS, it highlights several security issues imbedded in it. Default passwords on installed ICS devices are not regularly changed.[75] This situation is gradually improving as industries become more conscious of it, but many older systems still in use are vulnerable to cyber attack.

- **Third-party vendor access:** Outside vendors are often employed to aid in various engineering support activities, from system improvement to training. This poses a further risk should the vendor (or the client organization) not adhere to a rigorous cyber security culture.

- **Enterprise management systems:** In order to enable real-time monitoring of production processes, a corporate office will have an uptime/downtime and production count reporting system. These systems are a potential entry point for attackers who are trying to pivot from a corporate environment into the control system.

- **Network architecture:** The use of firewalls, intrusion detection systems, and user privileges can increase or decrease an OT system security depending on the method of deployment.

- **Potential for physical damage:** It is possible to cause physical effects, even damaging expensive and equipment which is difficult to reach or replace, by exploiting OT systems.

[72] SecurityZap (2015).
[73] Gorenc and Sands (2017).
[74] Furhlinger (2018).
[75] Gorenc and Sands (2017).

Cyber and the Energy Sector

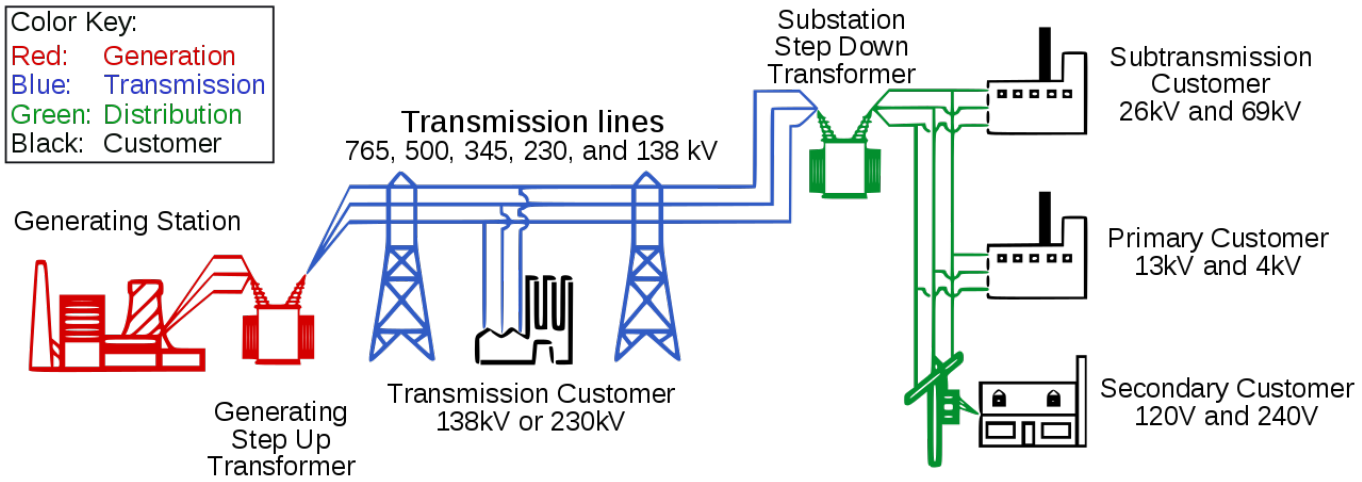
Given power and energy systems are 'enabling functions', an attack on either poses the highest risk for systemic damage to critical national infrastructure

An attack on the energy sector poses the highest risk for systemic damage to CNI in the majority of countries. Power and energy facilities have an 'enabling function', meaning that they are vital to the continued operation for all other sectors. It is therefore critical to understand the vulnerability of this sector and the threat to it as a means of understanding overall CNI vulnerability.

In the United Kingdom, a significant power outage would be followed by five days of recovery, using the "Black Start" system, which involves restarting generators without external supplies.[76] Given the complexity of the SCADA systems involved and the funding required to successfully compromise, test, and carry out an attack, cyber attacks affecting the power grid would likely only be plausible for groups with state funding and would therefore be considered acts of 'cyber war'.

There are three basic components to most electricity grids which have been demonstrated to be vulnerable to digital interference: generation, transmission, and distribution. Studies into generation and distribution hacks have highlighted the far-reaching impacts of a major attack against the energy sector.

Figure 10. Diagram of an Electric Power System



Source: US Department of Energy: U.S.-Canada Power System Outage Task Force (2014)

Generation Stations

The process of drawing power from primary energy sources has been digitized at multiple levels

The process of drawing power from primary energy sources has been digitized at multiple levels. For example, a generation plant may be connected to a control room via a corporate IT network, which in turn maintains a data connection to the internet.[77] As these networks were designed with efficiency and communication in mind rather than security, they may contain multiple points of vulnerability, through which a hacker can gain back door access to the key control systems of the plant.

[76] National ESO (2018)
[77] Cambridge Centre for Risk Studies (2015)

Future plans to establish smart grids and smart plants, built around automated technology that centralizes utility management, will help increase reliability by rolling out updates more efficiently and neutralizing problems that arise before they spread. However, the process of connecting thousands of devices to a highly integrated network will likely add smart grids with further vulnerabilities, which may then proliferate through systems and become embedded.

The Aurora Vulnerability

In 2007, researchers at Idaho National Laboratories carried out several experiments on a diesel generator to test whether cyber attacks could do physical damage to industrial power systems. The study demonstrated the existence of the 'Aurora vulnerability', found in unsecured protective relays used to isolate the generator from the grid. In cases where the vulnerability can be exploited, the circuit breakers on the generator were opened and closed out of phase with the grid, creating enough torque to cause parts of the generator to break and fly off. Video of the experiment test footage, later obtained by CNN, shows the generator being destroyed and catching fire in three minutes.[78]

The Business Blackout Scenario

2015 study by Lloyd's and the Cambridge Centre for Risk Studies, quantified the risk of a major cyber attack on the U.S. electricity generators for businesses and insurers

Using the Aurora experiment as a basis, a 2015 study by Lloyd's and the Cambridge Centre for Risk Studies, named the "Business Blackout" quantified the risk of a major cyber attack on the U.S. electricity generators for businesses and insurers.

Due to the structure of the U.S. generation grid, which contains redundancy and compensates for losses in power capacity, a disruption to the electricity delivery system cannot be achieved by disabling a single generator. The hypothetical scenario designed for the study assumes that a loss of 10% generating capacity during peak demand is required to trigger a cascading failure in the system. This is achieved by targeting multiple generators across two mutually-supporting reliability regions across the northeast. Using various means to access control rooms, the attackers are able to compromise a series of sites and damage 50 generators simultaneously on the day of the attack.

The attack triggers a blackout across 15 states and Washington DC, which affects 93 million people. Traffic systems, cell towers, rail and subway lines, Internet, television, and radio are all effected by the shutdown. Only those facilities, like hospitals, which maintain power generators are able to continue operating, though their ability to do so is hampered as time goes on and generators cannot be repowered.

The direct effects of the blackout scenario are based closely on the real-world consequences of the 2003 Northeast blackout (see box below), though the physical damage to generators in the scenario case means that the restoration of power is more complex and takes longer. The replacement of damaged generators costs tens of millions of dollars and several months are needed to transport them and bring them back on line.

[78] CNN.com (2007)

2003 Northeast Blackout

The 2003 Northeast blackout was a long-lasting and widespread cascading outage that effected parts of the Northeastern and Midwestern United States and the Canadian province of Ontario, including the cities of New York, Toronto, and Detroit. The blackout was caused when foliage fell into transmission lines, and a software bug in a FirstEnergy control room alarm system failed to inform operators of the need to adjust power load distribution. The blackout lasted for two days in most regions, but the ultimate length of the outage was more than a week in some places. There were fears that the cascading nature of the outage would cause rolling blackouts for weeks following the restoration of power due to the imbalance of load in the grid, but these did not ultimately occur.

In the study, the blackout lasts 2-4 weeks, causing an overall loss to the U.S. economy of $243 billion to $1.02 trillion across different scenarios

In the scenarios, though prioritized areas have their power quickly restored, the blackout lasts between two and four weeks, causing an overall loss to the U.S. economy of $243 billion to $1.02 trillion across scenario variants.[79] An independent probabilistic assessment of the scenario, carried out by Johns Hopkins Applied Physics Laboratory in 2018, reinforced the report's conclusions.[80]

Case Study: Transformer Manufacturing and Repair Lead Times

An attack which causes physical damage to transformers may have a significantly longer recovery time. The average lead time for a domestically-manufactured transformer to be built and delivered is 5 to 12 months due to the demand for large amounts of copper and electrical steel, which are expensive and in limited supply. Internationally, this wait time increases to 6 to 16 months. Eighty-five percent of U.S. transformers are manufactured overseas and highly liable to supply line breaks, though new production facilities have been opened in Georgia, Alabama, Tennessee, and Wisconsin. Overall, a new transformer can take over two years to build from scratch. In the U.K., the Royal Academy of Engineers estimates that it will take at least eight weeks to transport, install, and commission a spare transformer from storage.

An additional practical concern in the delivery of transformers is the stipulated procedure for transferal, requiring special roads or transports along a pre-approved route and requiring a civil engineer to ensure that all roads meet load requirements. Special permits must be approved and road closures may be required.

There have been developments to speed up the process of replacing transformers in recovery conditions. In 2006, U.S. Federal energy regulators approved the Spare Transformer Equipment Program, which stores stockpiled transformers and transformer parts for use in the wake of a terrorist attack. In 2014, the Recovery Transformer Project successfully transported three EHV transformers in 25 hours from St Louis to Houston and installed them within six days. Recoveries at this speed rely on surplus transformers and critical traffic closures at short notice.

[79] Cambridge Centre for Risk Studies (2015)
[80] Lee, et al. (2018).

Distribution Network

Following the release of the Business Blackout study, an additional report by Lockheed Martin U.K. and the Cambridge Centre for Risk Studies, examined the effects of a sophisticated cyber attack on the U.K. distribution network, centered on undermining substation security.

Substations function as nodes in the power network, transforming voltage for consumer delivery. They are located remotely and are generally unstaffed, monitored instead by SCADA control systems. As in the case of generators, substation networks generally contain redundancy and are therefore resilient to a point. Typically, substations are separated from power grid relay systems by a firewall; places where information needs to be transferred between the regional control center and substations are heavily screened. But all systems have vulnerabilities, and a sophisticated attack team may be able to devise a way to use the system's defenses for disruptive purposes.[81]

An attack would need to disable several substations in order to create a major blackout. Both attacks on the Ukrainian power network in 2015 and 2016 disabled power supply to electrical substations.[82]

Case Study: Ukrainian Substation Attacks

On December 23, 2015, an eight hour blackout in three regions of Ukraine, impacting 225,000 customers, was caused by a targeted malware attack. In the weeks after the blackout, malicious code was found in the networks of three energy companies, and firmware imaging revealed that 27 substations had been compromised by the attackers. Further forensics determined that the attackers had targeted energy companies in a spear phishing campaign and likely gained access to networks a full six months before the blackout was triggered. The attack remains unattributed, though, given Ukraine's geopolitical climate, suspicions have fallen on Russian state-sponsored groups.

The blackout was followed a year later by a very similar malware attack against power distribution firm Ukrenergo, which led to a short outage affecting Kiev and the surrounding area on December 17-18, 2016. In June 2017, computer forensics determined that the malware CRASHOVERRIDE found in Ukrenergo's systems shared features with the BlackEnergy and HAVEX malware, which had previously been linked to the Russian APT known as Sandworm. Further research on CRASHOVERRIDE has determined that it is a more sophisticated program than first thought, and that its presence on Ukrenergo's systems may have constituted a research gathering effort and testing phase by Sandworm.

The Substation Attack Scenario

An additional report by Lockheed Martin U.K. and the Cambridge Centre for Risk Studies, examined the effects of a sophisticated cyber attack on the U.K. distribution network, centered on undermining substation security

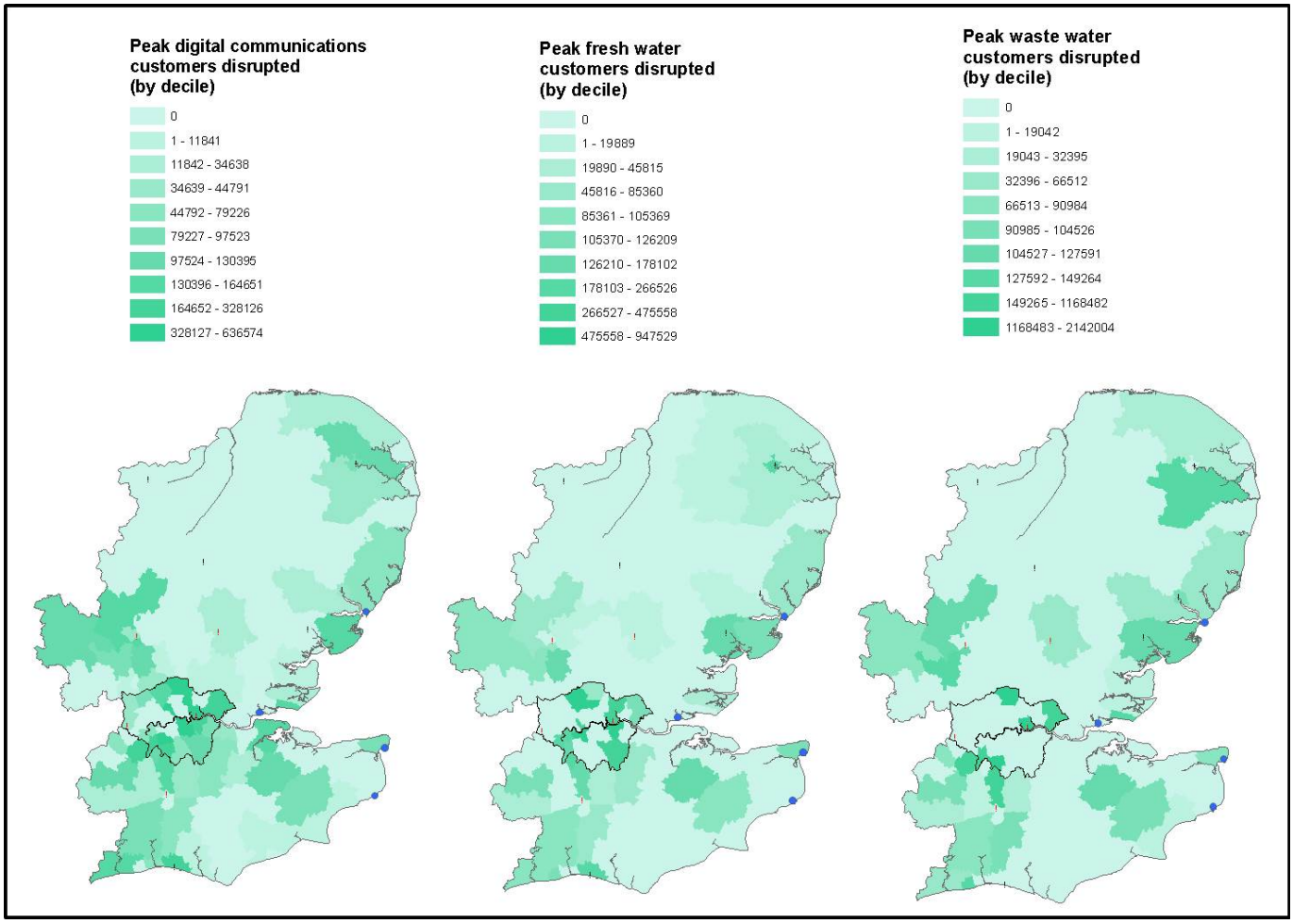
The scenario hypothesizes a well-funded and organized group of malicious cyber attackers are able to disrupt the power supply to at least 65 substations in the U.K. The process of accessing substations and testing the attack is timely and expensive, but due to a number of errors on the part of a substation supervisor, and the use of a disgruntled insider to aid attackers, the compromise is not detected.

[81] Cambridge Centre for Risk Studies (2016).
[82] Greenberg (2017).

Overall, the economic loss resulting from an attack on the U.K. power grid is estimated between £49 and £442 billion

The attack triggers a rolling blackout across the most populated parts of the U.K. Substations may be brought back online relatively quickly, and so the cyber team chooses to trigger outages at intervals around the infected area. Estimates vary on the time it will take to clear substations of malicious malware: between one and six weeks, during which blackouts will continue to plague the area. In the meantime, disruption travels along rail lines, affecting Northern industry and supply chains. Overall, the economic loss resulting from an attack on the U.K. power grid is estimated between £49 and £442 billion.[83]

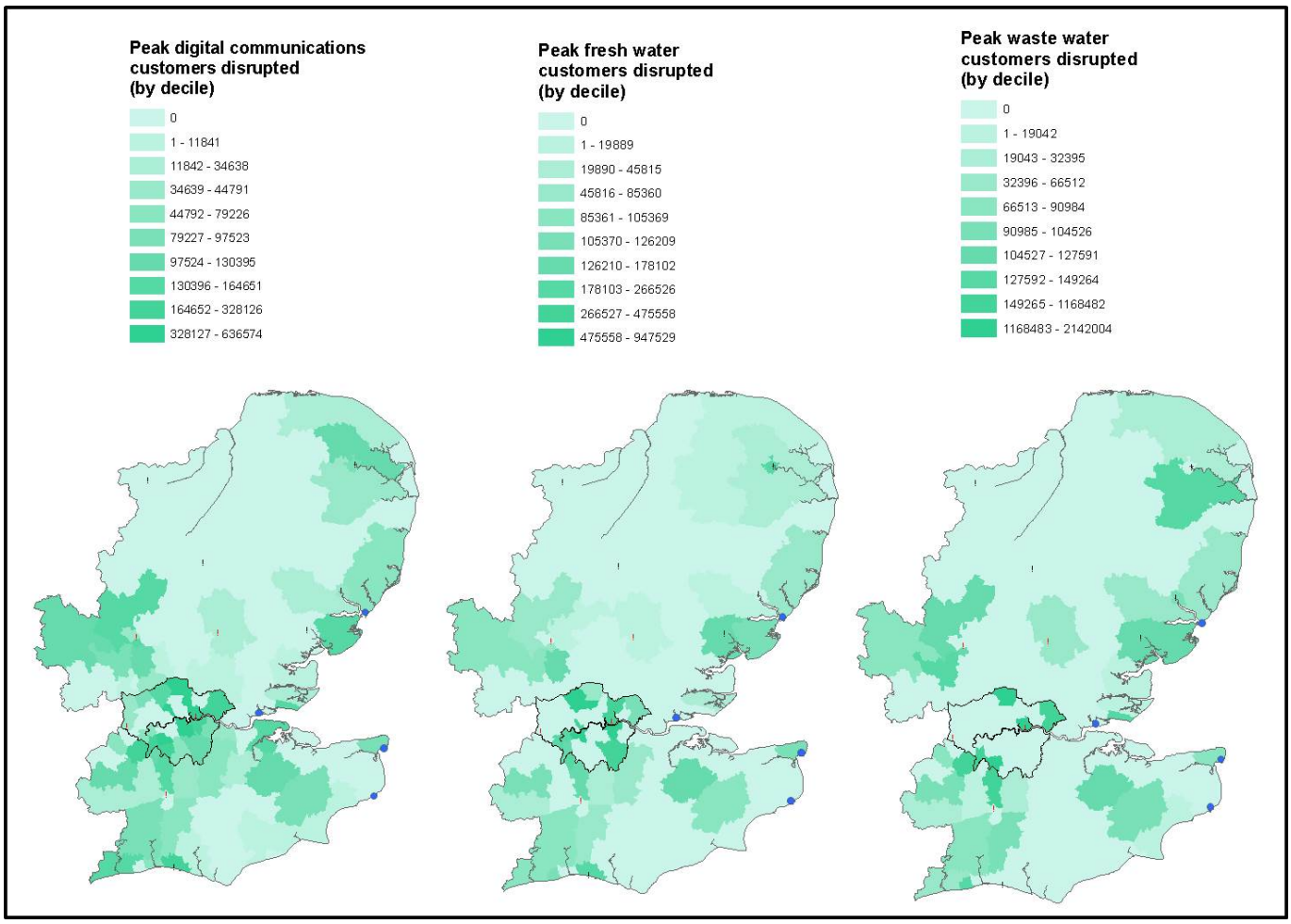
Figure 11. Peak Digital Communications, Fresh Water, and Waste Water Customers Disrupted Over the Course of the Hypothetical U.K. Blackout



Source: Cambridge Centre for Risk Studies

[83] Cambridge Centre for Risk Studies (2016).

Figure 12. Peak Rail Passenger Journeys Disrupted Over the Course of the Hypothetical UK Blackout



Source: Cambridge Centre for Risk Studies

Cyber and the Healthcare Sector

High rate of access and time sensitivity in healthcare means that ransomware demands are more likely to be met — a necessary loss compared with the restoration of access and the responsibility for care

The healthcare sector has become a well-known target for disruptive cyber attacks. News of ransomware attacks tying up hospital and trust systems became public in 2016, when around 20 hospitals were struck by various strains of malware in the space of eight months. The high rate of access and time sensitivity in healthcare means that ransomware demands are more likely to be met and the monetary loss is seen by many hospitals to be a necessary loss compared with the restoration of access and the responsibility for care. Although the rate of attacks against hospitals dropped sharply through 2017, incidents rose again by 47% through 2018.[84]

The 2017 WannaCry cyber attack was something of a watershed moment in the public awareness of the cyber threat in healthcare. Although the ransomware was indiscriminate in its infection, the NHS was badly impacted in the U.K., shedding light on both the virulence of the attack and the poor state of cyber security in a major public-facing service. It is estimated that 1,200 pieces of diagnostic equipment were struck by the attack, as well as the vast majority of computers and medical machinery running unpatched Microsoft Windows 7 operating systems.[85] According to the Department of Health and Social, the attack cost the NHS £92 million — £19 million from lost output during the attack, £0.5 million in IT costs during the attack and £72 million in IT costs after the attack.[86] U.S. hospitals were also affected by the WannaCry attack, though the damage was concentrated in MRI image enhancers, and Siemens and BD medical devices.[87]

The updating of operating technology used in hospitals carries its own risks as patching can be a lengthy process which strains the system and alters liabilities

The NHS received criticism for running unsecured, out-of-patch operating systems following the attack. However, it is crucial to understand that updating of operational technology used in hospitals and medical environments carries with it its own risks and hidden costs. Strict procedures are required for the modification of any medical device, including the installation of security patches. In many cases, medical care facilities are advised to restrict their purchase of stock to 'one type of device', in order to reduce complicated training times and limit operator confusion. Patching may be a lengthy process, with machines needing to be temporarily decommissioned and tested, placing a strain on the functioning system. Modified devices much be assessed for safety and changes must be approved by the Research Ethics Committee within the U.K. Health Department's Research Ethics Service, per the Medical Devices Regulations (2002).[88] Modifying a device alters its original liability, transferring it 'partly or wholly' to the modifier, increasing the exposure of hospitals and medical trusts.

Hospitals and healthcare facilities are under great pressure to provide constant service continuity. Therefore, when a vulnerability is discovered or a patch is published, the decision to modify unique and costly devices, potentially taking them offline and limiting patient care, can be easily pushed back.

Properly educating and training employees is required to avoid threat actors taking advantage of human vulnerabilities

The onus remains on the healthcare sector to properly educate staff on cyber threats and train employees to recognize phishing emails and suspicious links and attachments. Although WannaCry affected systems through a vulnerability in computer operating systems, hospitals and trusts are typically targeted specifically using traditional infection vectors.

[84] McAfee Labs Threats 2018.
[85] Hughes (2017)
[86] Department of Health and Social Care (2018)
[87] Seals (2017).
[88] The Medical Devices Regulations (2002).

Cyber and the Manufacturing Sector

Attacks that bypass the safety systems of an industrial plant could exploit latent fuel sources with devastating effects

The cyber threat to manufacturing is significant due to the latent power of industrial control systems used in the production of high powered machinery, computing, foodstuffs, and building materials. An attack which can bypass the safety systems of production lines and furnaces may exploit latent fuel sources to create devastating attacks. In 2014, a cyber attack against a German steel mill was the first attack to cause confirmed physical damage since 2007's Stuxnet.[89] Using social engineering and spear phishing emails, attackers were able to gain access to the mill's office network, which was connected to the industrial control system, and use the system to compromise production and cause a furnace blast and massive damage to the facility.

Attackers could also introduce long-term threat to the industry by altering manufacturing processes

Significant, too, is the long-term threat of cyber to the industry. Sophisticated attackers may be able to introduce faults into manufacturing materials, which would either render tonnes of product unusable, or potentially introduce new dangers into goods that are made with compromised material. In an extreme variant of this scenario, generations of aerospace parts, building materials, or automobiles may be made deliberately faulty, with little way to trace the error.

The rate of cyber attacks against the manufacturing sector is growing, limiting investment in digital methodologies. A 2018 study by EEF and AIG with the Royal United Service Institute (RUSI) reported that half of surveyed manufacturers had been victims of cyber crime or a cyber attack, and that a further 40% of companies did not feel that they had adequate access to the information needed to assess their cyber risk.[90] An IBM report from 2017 cites manufacturing as the third most attacked sector after Government and finance.[91]

The majority of these attacks have affected head offices and other services rather than industrial facilities. Manufacturing companies are also vulnerable to DDoS, malware, and ransomware attacks, which may lead to business interruption, lost production time, and slow communications with suppliers and vendors.

[89] Zetter (2015).
[90] EEF, AIG, and RUSI (2018)
[91] IBM (2018)

How Many Vulnerabilities Are There?

Estimating the number of vulnerabilities present in industrial systems is difficult and tracking vulnerabilities is an inexact science

It is difficult to estimate the number of vulnerabilities present in industrial systems, and thus to present a solution to the realities of potential compromise. Exploitable vulnerabilities can exist in hardware, software, network protocols, and programming languages such as Java, and can be present on both local and remote, or isolated or connected systems. Products and updates are rarely interrogated for an accurate count for new avenues of compromise, and, as in the case of WannaCry, patches and updates which reconcile pre-existing vulnerabilities may be difficult to roll out systematically and universally. If a programming language contains an exploitable fault, that fault is replicated across any code written in that language.

The number of vulnerabilities in digital and industrial products may be limited or infinite. Although vendors have a responsibility to adequately assess their products for user safety, compromises will inevitably be missed when economic demands and available knowledge limit the time spent to do so. As new technologies arrive with embedded system flaws, protocols may introduce additional faults which can be compromised, which are subsequently grandfathered in. As the cyber economy continues to grow and business becomes ever more reliant on digitization, vulnerabilities known and unknown will only proliferate further.

Vulnerability tracking is an inexact science and is subject to selection bias. Numbers published fluctuate heavily, between 5,000 and 15,000 per year. Companies that are able or willing to fund penetration testing or vulnerability research, or offer rewards for independent security testing, will see more exploits found and patched. There is little incentive for individual security experts to probe vital technologies for flaws on spec, however, for fear of punishment or being ignored by the technology's vendor, and thus many flaws will not be found.

Vulnerabilities which are found can be registered to databases, but there is no central standard hub for vulnerability data and oversight can be lacking. Naming schemes for exploits differ across industries and between security analysts, so lists undoubtedly contain duplicates.

As more vulnerabilities are registered, more money will be invested in security testing

Generally speaking, the number of vulnerabilities registered in a year will correlate with the amount of money invested in security testing. In 2014, the CERT Coordination Center automated the testing of more than 1 million mobile phone apps for SSL encryption, returning insight on 23,000 vulnerabilities in a year, all from a single test. This spike in registered vulnerabilities indicates that more vulnerabilities are found with dedicated security analysis. As the profession develops, more vulnerabilities will be found, though this is unlikely to ever accurately reflect the total number of vulnerabilities actually latent in the landscape. In the meantime, malicious actors will also be looking for and selling unregistered exploits through back channels. These vulnerabilities may be leveraged for significant damage or disruption, but may not become known or addressed until after they are used for malicious means.

As industrial control systems for critical national infrastructure increasingly become digitized, vulnerabilities will continue to increase

With the further digitization of industrial control systems and significant portions of critical national infrastructure, governments and industry leaders must accept that vulnerabilities will become an inherent part of vital systems. More investment in security testing is required to resolve issues before they arise, and to safeguard users and companies in the event that an unseen vulnerability is leveraged against them.

Figure 13. Catalog of Major ICS Cyber Events from 1999 Through 2017 with Primary Consequence or Harm

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
April 1999	Gazprom – Russian gas supplier[92]	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorized Access
July 1999	Bellingham[93]	Over 250,000 gallons of gasoline leaked into nearby creeks and caught fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb and April 2000	Maroochy Shire[94]	A recently fired civic employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers, and the grounds of a hotel.	Insider Attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001	California[95]	A hacking incident at CASO lasted two weeks, but did not cause any damage	External Attack	Unknown and Contained	Deliberate	Thwarted
August 2005	DaimlerChrysler[96]	Thirteen DaimlerChrysler U.S. auto manufacturing plants were taken offline for about an hour by an Internet worm. This resulted in an estimated $14 million in downtime costs.	Unknown	Spyware Installation	Zotob Worm and MS05-039 Plug-n-Play	Infection
Jan 2008	Kingsnorth[97]	Attacker broke into the EON Kingsnorth power station which caused a 500MW turbine to make an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Protest
Nov 2008	Pacific Energy[98]	A recently fired employee disarmed safety alarms on three offshore oil platforms.	Insider Attack	Disgruntled Employee	Disabling alarm systems	Revenge & Sabotage
June 2009 to 2010	Stuxnet	Malicious code targeted ICS at an Iranian nuclear plant.	Virus, Unknown Presumed Nation State	Sabotage	Destroying centrifuges and thwarting uranium enrichment	Revenge & Sabotage
2010 to Aug 2014	Dragonfly/Havex/ Energetic Bear campaign[99]	A campaign against defense, aviation, & energy companies	RAT, Espionage	Unknown	Malware infection and remote access	Malware Clean-up
August 2012	Shamoon/Wiper[100]	A Saudi Arabian oil company, Saudi Aramco, has over 30,000 workstations knocked out	Unknown, presumed Hacking group, RAT	Mischief	Wiping 30000 machines of their data	Unknown
2013	Bowman Avenue Dam	Iranian hackers breached the control system of a small dam outside New York City but were not able to remotely control the sluice gate	Targeted Attack	Revenge/ Sabotage	Penetration of computer systems via cellular modem	Thwarted, significant political attention paid to advancing cyber teams by foreign nations
April 2013	California Power Station	Snipers fired at a California substation, knocking out 17 transformers.	Unknown	Unknown	Destruction of substation oil tanks	Unknown
December 2014	German Steel Mill[101]	Experienced hackers used a spear phishing campaign to gain access firstly to the corporate and then to the wider plant control network.	Unknown, presumed hacking group	Unknown	Compromised plant control network, causing system components to fail	Physical Damage
December 2015	Ukrainian Blackout	Three energy companies in Ukraine were taken offline, causing an eight-hour blackout which affected 225,000. Malware was later found in the substations.	Presumed Nation State	Unknown	Infection of vulnerable power substations	Unknown
November 2016	Fidelix BMS Attack	A sustained DDoS attack against a vulnerable building management system (BMS) caused internal heating to shut down for 24 hours in two apartment buildings in eastern Finland during sub-zero temperatures	Unknown	Unknown	Sustained denial of service attacks caused system to restart every few minutes	Firewall Installed

[92] Milhorn (2007).
[93] National Transportation Safety Board (2009), Wilshusen (2012).
[94] Slay, et al. (2007).
[95] Committee on Homeland Security, (2005).
[96] Government Accountability Office (2007).
[97] Knapton (2008).
[98] Kravets (2019).
[99] Symantec (2014).
[100] Bronk, et al. (2013).
[101] Lee, et al. (2014).

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
December 2016	Ukrenergo Ukranian power outage[102]	A second attack on Ukraine's power distributor left Kiev and the surrounding area without power for several hours during the night of 17-18 December	Suspected APT	Unknown	Targeted CRASHOVERIDE malware attack	Unknown
May 2017	WannaCrypt/ WannaCry	A virulent strain of ransomware affected 300,000 computers in 150 countries, demanding $300 to release files per affected computer. An activated kill-switch stopped the malware from spreading further.	Suspected North Korean APT, Lazarus Group	Unknown; the malware did not accrue sufficient funds to suggest financial gain.	ETERNALBLUE and DOUBLEPULSAR exploits as released by ShadowBrokers in April 2017	Killswitch activated
June-July 2017	NotPetya	A second attack utilizing ShadowBrokers exploits affected 12,500 machines in 64 countries. The attack presented as a ransomware but functioned as a diskwiper Trojan.	Presumed Nation State	Unknown	ETERNALBLUE ShadowBrokers' exploit	Malware Clean up and Patch roll out
June-August 2017	Triton/TRISIS[103]	An infection of malware on a Saudi Arabia petrochemical plant caused several outages over the course of several months. The malware affected Triconex safety systems, potentially causing physical damage.	Presumed Nation State	Unknown, likely field testing	Malware Infection and Remote Access	Malware Clean up and System Repair

Source: Milhorn 2017, National Transportation Safety Board 2009, Wilshusen 2012, Slay et al. 2007 , Committee on Homeland Security, 2005, Government Accountability Office 2007, Knapton, 2008, Kravets 2019, Symantec 2014, Bronk et al. 2013, Lee et al. 2014, Greenberg 2017, Dragos 2018

[102] Greenberg (2017).
[103] Dragos (2018).

Cyber and Corporates

As news of breaches and high value fraud cases continue to dominate the news, Boards and customers increasingly challenge corporates on their ability to protect their assets. When an incident does occur, the market monitors how well corporates respond during crisis events. Given the stakes, cybersecurity is increasingly becoming a critical factor in decision-making discussions when considering business relationships. This shift in conversation means corporates need to pivot their cybersecurity approach away from damage minimization and toward business differentiation.

Cyber Security Risk Across Sectors

Although cyber risk overall is a collective challenge, specific threats to organizations may be targeted to specific sectors

While cyber threats are viewed as a collective challenge warranting cooperation from a variety of stakeholders, the specific threats organizations face tend to vary, based upon the capabilities and intentions of adversaries interested or engaged in targeting a particular sector.

Healthcare

The healthcare sector is targeted due to the value of its data, its intellectual property, and because as the sector's technology use is rapidly increasing, so are attack surfaces

Entities in the healthcare sector are frequently targeted by adversaries with a range of capabilities and objectives, likely due to *"the criticality of the services offered by healthcare providers, the high value of their assets, and the relative ease with which attackers have (historically) been able to compromise their infrastructure."*[104]

Data: Over time, pharmaceutical companies have been aggregating *"years of research and development data into medical databases, while payers and providers have digitized their patient records. Meanwhile, the U.S. federal government, and other public stakeholders have been opening their vast stores of healthcare knowledge, including data from clinical trials and information on patients covered under public insurance programs."*[105]

Personal Health Information (PHI) is valuable to actors looking to profit from a cyber-intrusion. In certain cases, hackers may 'borrow' a person's identity to obtain healthcare, leaving the victim financially responsible for the hacker's treatment.[106] Other adversaries may use data from a health record to open a new line of credit, or may use stolen information to blackmail or extort a victim.[107] Stolen health records are relatively more profitable for cyber criminals on the dark web: health records can sell for as much as $60 per record, compared to social security numbers ($15) and stolen credit card numbers ($1-$3).[108] While financially motivated cyber criminals may seek PHI to generate revenue, intelligence services could use this information to gather and analyze counterintelligence information on individuals of interest.[109]

Intellectual Property: Cyber enabled theft of intellectual property (IP) is a growing threat to companies, markets, and countries. Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create new and often complex challenges for organizations with trade secrets to protect.[110]

---

[104] Le Bris and El Asri (2016).
[105] Knott and Van Kuiken (2013).
[106] Roberts (2018).
[107] Ibid.
[108] Ibid.
[109] Homeland Security Committee (2018).
[110] Gelinne, et al. (2016).

Although not exclusively the purview of nation states, cyber-enabled IP theft has been used as a tool of statecraft by countries seeking to obtain IP to strengthen the competitive position of their national economies.[111] Information of interest in the healthcare sector includes but is not limited to, pharmaceutical research, imaging devices, biomedical research, and nanotechnology.[112]

In October 2018, the National Institute of Standards and Technology (NIST) issued a draft report, which examined cyber security and privacy risks posed by IoT devices, including healthcare IoT devices. These devices include connected and implanted devices such as cardiac pacemakers, drug administration devices, and defibrillators, among others. A successful cyber attack on this type of device could have serious repercussions for patients, many of whom depend upon their device for critical or lifesaving care. While both public and private sector entities acknowledge the importance of developing these devices in a secure and ethical way to minimize downside risks, securing increasingly complex IoT devices remains a challenge.

Opportunity: *"The increase in criminal activity over the past few years is underpinned by a relative lack of awareness among users of technology, substantial growth in the use of Internet-connected personal healthcare devices, ongoing digitization of patient health records and the increasing number of healthcare information systems connected to the internet."*[113] Further, as the health ecosystem expands and the number of access points within the healthcare supply chain increases, adversaries have a larger attack surface and the potential to inflict widespread damage, if an attack on one provider causes adverse, downstream effects.[114]

Telecommunications

The importance of telecom to business, public safety, and governments makes it attractive to attackers

The communications sector is an integral component of many economies, underlying the operations of all businesses, public safety organizations, and governments.[115] Because telecom companies build, control, and operate infrastructure used to communicate and to store sensitive data,[116] various actors continue to target the sector and its perimeter elements to achieve a range of objectives. Along these lines, as telecommunications infrastructure is critical for so many industries, even a minor or isolated incident could disrupt business operations on a broad scale and adversely impact capital markets.[117]

In the United States, U.S. PPD-21 — which affirms the federal government's responsibility to strengthen the resilience of critical infrastructure against threats — identifies *"energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors."*[118][119] For example, the banking system relies on the Internet for financial transactions, documents are transferred via Internet between businesses, and email is a primary means of communication. When the Internet is not available, commerce is directly affected and economic output is reduced.

[111] Grobman (2018).
[112] Universität Basel (2017).
[113] IEEE Access (2018).
[114] Roberts (2018).
[115] Department of Homeland Security (2017).
[116] Deloitte (2016).
[117] NIST (2014).
[118] Presidential Policy Directive (2013).
[119] Presidential Policy Directive (2015).

The telecommunications sector offers various actors a broad, interconnected attack surface, with multiple opportunities to steal data and trade secrets or disrupt operations.

Financial Services

Attacks on financial institutions are rising and range from pure financial gain to damaging data integrity and undermining the stability of the financial system and public confidence

Over the past decade, cyber attacks on financial institutions and financial market infrastructures have become *"more frequent, complex, and sophisticated."*[120] As such, a cyber attack on a target in the financial services sector could disrupt operations, damage the integrity of data, threaten the stability of the financial system, and/or undermine confidence in individual firms or capital markets altogether.[121] Financial institutions are attractive targets to adversaries looking to generate revenue. Criminal actors may attempt to directly wire funds without authorization or may steal other PII, trade secrets, or other sensitive information to facilitate fraudulent transactions. Nefarious actors can even disrupt and distort financial markets on an unprecedented scale by disseminating bad data, fake news, and faulty information into a marketplace that thrives on accurate information in order to generate a personal profit.[122] In the past, *"false data and unanticipated algorithm behaviors have caused significant fluctuations in the stock market because of the reliance on automated trading of financial instruments."*[123]

Actors looking to retaliate against a particular nation, with little regard for blowback, might be inclined to attempt to induce a failure of the global economy. Operational problems in a payment, clearing, and settlement system may impede the control of, or even exacerbate, other types of risk such as market, liquidity, or credit risk.[124] This could be done in an unanticipated way that could pose a systemic risk, resulting in participants incurring significant losses.[125] Payment and settlement related to operational risks could spill over into financial markets across a wide range of financial products with implications for global financial stability.[126]

[120] Healey, et al. (2018).
[121] Office of Financial Research (2017).
[122] Goshen & Parchomovsky (2006).
[123] Clapper (2016).
[124] Jayamaha (2005).
[125] Ibid.
[126] Ibid.

Thematic Ways Corporates Are Addressing Cyber Security

Cybersecurity as a Shared Responsibility

Shared ownership across functional areas and shared responsibility up, down, and across an organization will help manage the risk of cyber attacks

Due to the public nature of cyber breaches, corporates are acutely aware of the impact cyber attacks can have on business, and consequently, accept the importance of cybersecurity. Progressing from baseline recognition, the next step for corporates is figuring out how to manage the risk of cyber attacks. A literature review on cybersecurity reveals repeated messaging on ensuring cyber security is not just an IT function. Only through shared ownership across functional areas and shared responsibility up, down, and across an organization can cyber security evolve past a pure IT role.

Board-level executives worldwide are including cyber risk as an agenda item

In 2017, EY asserted that managing cyber risk should be included as an agenda item for European corporate boards. According to EY, cyber risk is of such profound importance that Boards should not view its oversight as a purely management function.[127] Although EY's report was written for a European audience, Board-level executives around the globe are increasingly including cyber risk as an agenda item. According to EY's survey, *"over [one] third of directors of U.S. public companies now discuss cybersecurity at every Board meeting."* And their concern is justified. Marsh[128] highlights the annual cost of cyber crime is estimated to top $1.5 trillion with only 15 percent of losses covered by existing insurance policies.[129]

Understanding the likelihood of a particular cyber event as well as the magnitude of impact to an organization is a must for corporate boards

To effectively steer and oversee their organizations, Board level executives must understand both the likelihood of particular cyber events as well as the potential magnitude of impact to their organization individually and more broadly to their sector, and the economy. Although the cost of malicious cyber activity continues to rise, insurance coverage does not appear to be growing at the same rate. As such, organizations face increased costs in both real and relative terms.

At the same time, Board discussions are expanding to cover concerns related to cyber resiliency. While growing costs of malicious cyber activity explain Boards' increased focus on risk, Board-level interest in cyber resilience is less clear.[130]

---

[127] EY (2018).
[128] Marsh McLellen (2018).
[129] EY (2018).
[130] EY defines resilience as "the organizational capability to sense, resist, and respond to disruptive cyber events, and to recover from them within an acceptable timeframe." (EY (2018) Cyber Resilience in the Digital Age Implications for the GCC Regions. Report no: EUG No: 03211-172GBL). Symantec further clarifies, "Cyber resilience is about managing security with a multi-layered approach that encompasses people, processes, and technology. As threats morph and organizational needs evolve, cyber resilience is by definition about continual refinement. The process can be best thought of as a framework with five pillars: prepare/identify, protect, detect, respond, and recover". (Symantec (2014): The Cyber Resilience Blueprint: A New Perspective on Security. Accessed February 3, 2019. https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf.

Companies are concentrating more today on *when* a cyber attack will occur vs. *if* it will occur

To ensure organizations are appropriately positioned to remain resilient in the face of an adverse cyber event, Board leaders should continue discussions related to cyber resiliency to improve their organizational postures. Previously, organizations may have considered whether or not a cyber attack would or could occur. However, that paradigm has shifted with many companies now asking themselves *when* an attack will occur, not *if*.[131] As such, it is critical for companies to analyze and understand all potential points of impact. Further, a company's development of a crisis response plan and its use of this plan for incident response are also critical.

Case Study: Cyber Crisis Response - A Citi TTS Perspective

A clear and robust recovery plan that is tested regularly is essential if companies are to meet the challenge of an increasing number and variety of cyber threats.

Cyber security threats are becoming increasingly frequent and sophisticated: WannaCry and NotPetya ransomware alone were responsible for billions of dollars of losses due to business disruption. For corporations, it is important to prepare and plan for when, not if, the next cyber attack happens.

Figure 14. Financial Losses Resulting from Petya/NotPetya Cyber Attack

Company	Losses
U.S. Pharmaceutical Company	$870 million
U.S. Shipping Firm	$400 million
French Construction Materials Manufacturer	$384 million
Danish Container Shipping Firm	$300 million
U.K. Consumer Goods Firm	$129 million

Source: Greenberg (2018)

Traditionally, cyber security takes a three layered approach — protect (in order to prevent access), detect (using technological tools and specialists to identify problems as early as possible), and respond. The third of these components — the response process — often receives less attention than protection and detection. However, having a robust and well thought out response process is critical to success in the event of a cyber attack where rapid and appropriate action is essential.

Managing cyber-related risks can be daunting given the technological jargon involved. However, conventional risk management principles can largely be applied. Just as every office has water sprinklers to prevent fire damage but still practices fire drills, so do all companies need to consider what will happen if their protection fails. To develop a strategic contingency plan, corporates need to follow best practices covering their planning, testing and recovery.

After speaking with a number of companies who experienced a catastrophic cyber crisis, a few common themes became apparent. These highlighted the difference between a crisis having limited impact or resulting in devastating paralysis.

Planning: Identifying General Principles

It is impossible to accurately predict every potential cyber threat. Therefore, an organization's preparation should be based on general principles and broad communications and governance guidelines along with potential response options that can be deployed in different ways depending on the severity of the cyber event.

One useful way to plan for cyber events is to consider the scale of possible compromise scenarios. For example, a small event may impact a limited number of desktop computers; a medium-sized event may affect enterprise resource planning or treasury management systems; a 'doomsday' event (of the type experienced as a result of NotPetya or WannaCry) may put all computers, networks and phones out of use.

[131] EY (2018).

Planning should identify critical functions and data, not just within the organization but also where there are vendor or supplier dependencies, including banks. Questions to be considered include:

- Who is empowered to make decisions?
- What are the priorities in terms of action?
- What alternative forms of communications should be used if there is no network or email?
- Who should be contacted at the bank or vendor?
- Should access to all bank services be restricted or should visibility be prioritized?
- Should clients or counterparties be contacted, and if so, by whom?

One also needs to ensure that the right tools are in place and appropriate subject matter expertise is available including technology, legal and others as appropriate from inside and outside the organization. Planning efforts should be undertaken together with broader corporate efforts with Treasurers highlighting the criticality of certain functions and systems so they can be prioritized appropriately.

Determining Acceptable Alternatives

A strategic contingency plan should identify alternative means of communication and interaction, with banks for example, in the event of a cyber attack. Almost inevitably, an emergency situation is likely to require the use of non-standard equipment or software. Risks associated with an organization's employee using a personal laptop using third-party instant messaging software to communicate needs to be balanced by the organization against an inability to access treasury workstations or use work telephones.

Recovering from a Cyber Crisis

A cyber event has many similarities with continuity of business planning for natural disasters or terrorism, including addressing how critical operations can be continued, the location of an alternative site, and how critical data is transferred.

However, because of the interconnectivity of cyber related threats, backup infrastructure may need to be isolated from regular networks and be regularly updated. Clearly, such contingency capacity is costly; a company must determine its minimum critical infrastructure in order to help limit losses and damage to its business and invest accordingly. Furthermore, a cyber attack has additional risks such as potential fraud or stolen data which can require additional expertise and considerations for a robust response plan.

Conclusion

While it is impossible to prepare for and have a detailed playbook for every possible scenario, basic response readiness preparedness can be of great benefit. For example: (1) A communications plan with key alternate contact information stored and available offline; (2) Governance principles on who is authorized and empowered to make prompt decisions; (3) Crisis management subject matter experts, insurance, and incident response on retainer; (4) Contingency infrastructure for critical systems/data and (5) Cyber simulation, training and practice for various scenarios.

To manage cyber risk, "*Directors must effectively corral a range of inputs to respond effectively: corporate crisis management, external parties' press and public opinion, regulators and even ministerial scrutiny in some cases. All of these aspects must form the backbone of an integrated plan to minimize the overall impact on the corporation and return to business as usual. Directors must also be prepared to look outside their organization to stay abreast of the latest developments. Nonexecutive Directors, potentially from a nontraditional background, should be of particular help here, bringing a broader industry perspective to how peer companies are handling this often sensitive risk.*"[132] Not only is the topic becoming a common point of discussion at Board meetings, but EY is also advocating for the addition of nonexecutive Directors to Boards to augment and improve organizations' respective abilities to understand and address this risk holistically.

Corporate Cyber and Culture

Similar to establishing a healthy corporate culture, good cybersecurity practices originate from a 'tone at the top', usually from the CEO. To motivate and track accountability, a tone at the top needs to be paired with tailored messaging at the local managerial level. The purpose is to convey functionally-specific information since threat actors tailor their tactics to specific targets. This level of manager-to-employee oversight also helps eliminate any sense of vague instruction. Putting an additional layer of responsibility at the local managerial level empowers mid-level managers and those they manage to feel a sense of ownership over protecting their work through better information security practices.

In addition to promoting a 'tone at the top' to encourage participation, it is equally important to carry out the mission from the ground up. Implementing the 'bottom up' concept acknowledges every single employee regardless of rank has an equal ability to help or harm an organization's security. Due to the evolving threat landscape, corporates benefit from taking a close look at how to constantly refresh security awareness training to improve effectiveness.

Corporates benefit from continued dialogue between their boards and senior management on strategic for cyber as well as daily operations

As threat actors' improve their capabilities, the threat landscape evolves, and the impact and risks to institutions increases, Board level reporting on this topic is likely to become more detailed and more frequent. Further, Board involvement in decision making related to the threat and corresponding risks may necessitate the inclusion of additional cyber subject matter experts on Boards going forward. Cyber security, cyber risks, and cyber resilience affect all layers of an organization, which require a broad and holistic view of an organization that only executive leadership is able to provide. Once the view is established, corporates further benefit from an ongoing dialogue between Boards and senior management on strategic direction and daily operations.

Critical Roles to Manage Cybersecurity

Information security, data privacy, human resources, legal, compliance, public affairs, and risk all play their part to strengthen cybersecurity

To go in-hand with spreading a consistent message across an organization, corporates draw on multiple departments to proactively and reactively manage cyber security. In addition to information security — data privacy, human resources, legal, compliance, public affairs, and risk — all play their part to strengthen information security at a corporation.

[132] EY (2018).

A corporation's response to a cyber breach demonstrates why each function needs to be involved in cyber security. In a simple example, after a breach, the information security function takes care of the immediate issue and aims to hinder or halt the actor before it moves further into the network or acts on its objectives. As soon as the information security function is aware of a possible breach, it should send — following the protocol of its cyber playbooks — a message to other functional stakeholders notifying them of the breach. Legal, compliance, and risk departments decide when the best time is to notify regulators of a breach.

Following incident response, information security works closely with data protection to figure out which areas of the business' data were impacted, if there was Personally Identifiable Information (PII) involved, and the best recourse given current data privacy regulations for notification. Public affairs contributes by managing the narrative of disclosing a breach to customers and the public through communicating what steps the corporation has and will take to mitigate the damage. Timeliness of reporting and notification to both regulators and the public is critical. Many other functional areas along the way provide guidance and support to manage an incident.

Public-Private Partnerships: Moving to the next Level to Better Manage Cyber Risk

As cyber is a borderless issue, a combination of inter- and intra-sector and country collaboration as well as public-private partnership is required to combat it

Cyber is a 'borderless' issue, requiring a combination of inter- and intra-sector and country collaboration as well as public-private partnership (PPP) to combat it. However, a strategic approach is required to move this collaboration beyond law enforcement, intelligence agency, and information security 'circles of trust' that exist today, which predominantly focus on operational and tactical threat information sharing. For this strategic approach to be developed, experts from product teams, risk and finance units, and franchise management across public and private sector organizations must come together to debate, define, and understand cyber risk. This is important not just for managing cyber risk. If private sector organizations do not understand their business' cyber risk, they will develop ineffective processes that need to be rectified at a later, more costly date. For the public sector, particularly regulators, ensuring a common understanding of cyber risk offers the opportunity to deepen the effectiveness and alignment of regulatory frameworks across borders, and avoid regulatory arbitrage, fragmentation, and diverging assessments of the same cyber risk management capabilities.

Information sharing and cyber threat exercising are two areas of public-private partnerships

There are two areas of PPPs which we highlight: (1) information sharing and (2) cyber threat exercising — both of which inform and help the maturing of the global architecture of the cyber regulatory system and good cyber security standards.

Information Sharing Models

Financial services firms created the first information sharing model in the U.S.

Information sharing models have existed for decades, most notably, the Financial Services-Intelligence Sharing System Analysis Center (FS-ISAC), which was created in 2001. In the U.S., these sector-specific 'ISACs' were created (including FS-ISAC – an ISAC dedicated to the financial services) in response to the 1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, which mandated that public and private sectors share information about physical and cyber security threats to help protect the U.S. Critical National Infrastructure (CNI). The cross-sector ISAC models are overseen by the National Council for ISAC.

Other countries have developed public and private partnerships over the years

Over the years, there has been great progress in developing awareness and increasing membership of these groups — a great example of how regulatory support has driven membership was a May 2014 report from American regulators, which highlighted the importance of public and private partnerships .This report, which specifically referenced the FS-ISAC, attracted 420 new members in the weeks following. Good examples of effective groups include The South African Banking Risk Information Center (SABRIC), the Dutch Electronic Crimes Task Force, the Dutch High Tech Crime Unit and Dutch ISACs, Brazil's Febraban Information Security Sub-Committee, which works with law enforcement and legislators to drive the adoption/creation of cyber best practices, and the Sao Paulo State Industry Federation (FIESP), which is looking to create an FS-ISAC-like cross-sector entity to share information on cyber attacks.

Industry is yet to create a single, mature capability where private sector firms can work together to develop comprehensive risk management strategies

Although several information sharing centers have been established, the industry is yet to create a single, mature capability where private sector firms can work together to develop comprehensive risk management strategies. In the U.S., a solution may be close cooperation between the FSARC and DHS' new National Risk Management Center, and in the U.K., the movement towards a risk management approach is seen in the National Cyber Security Centre and their Industry 100 program.

The Financial System Analysis and Resilience Centre (FSARC)

In August 2016 eight financial institutions (Bank of America, BNY Mellon, Citi, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo) established a select information sharing group — FSARC — to be affiliated with FS-ISAC and to proactively identify ways to enhance the resilience of the critical infrastructure underpinning much of the U.S. financial system.

FSARC's mission is a long-term strategic initiative to proactively identify, analyze and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber threats through: (1) Focused operations and enhanced collaboration between participating firms, industry partners, and government; (2) sharing of more sophisticated analysis techniques and information (via FS-ISAC controls); (3) building closer collaboration between large U.S. financial services firms and government agencies, including Treasury, the Department of Homeland Security (DHS) and FBI; (4) complementing established partnerships across the private and public sector, such as the Financial Services Sector Coordinating Council (FSSCC); (5) performing deep analysis of systemic cyber risk across financial products and practices; and (6) sharing findings and adaptable mitigation strategies across the financial sector through FS-ISAC's membership.

It is developing a risk registry to proactively identify, analyze, assess, and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. Government.

FSARC activities continue to enhance and improve the effectiveness of information exchange, sharing of greater sophisticated analysis techniques, and closer collaboration between large U.S. financial services firms and U.S. government agencies, including the Department of Treasury, the Department of Homeland Security, and the Federal Bureau of Investigation.

Cyber Threat Exercising

Cyber threat exercising ensures the safety and well-being of employees and markets

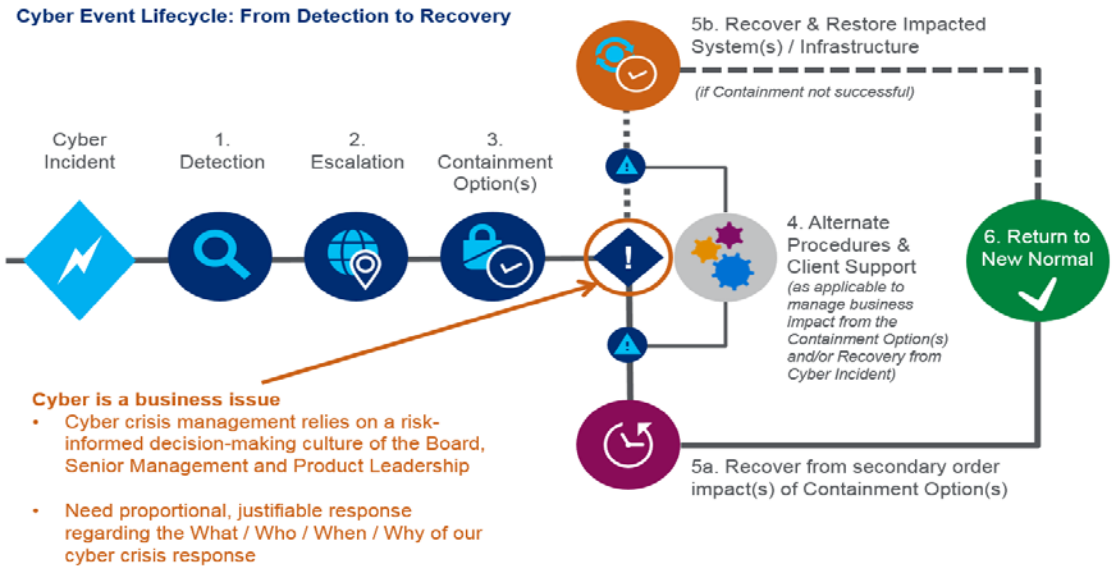
Cyber threat exercising is critical to ensuring the safety and well-being of the firm's employees and their dependents as well as the continued safety and sound operation of financial markets. It also helps to support clients in times of need should they experience an operational disruption and to provide clear and timely communication flows within the firm and between the firm and clients, third party partners, regulators etc.

Cyber Resilience and Crisis Management has been articulated by many regulators as being about the business, and the skills and capabilities the business has, and not about being owned and driven by the Chief Information Officer (CIO) or Chief Information Security Officer (CISO), where resilience is an outcome not a business function analogous to financial resilience. This makes it broader than preventing disruption.

Threat exercising should be led by business and franchise together as a firms leadership needs to understand the impact of decisions to ensure they make and take risk-informed decisions

As such, exercising needs to evolve to be business and franchise led — particularly as many firms can deploy containment or mitigation mechanisms during a cyber incident, such as disabling Internet access, disconnecting select business-to-business (B2B) connections, blocking remote access, undertaking a forced password rest and/or reboot, and blocking/quarantining inbound and/or outbound email. These decisions and their impacts need to be understood by the firm's leadership to ensure they make and take risk-informed decisions. It is vital for firms to do these exercises themselves and with key clients and third parties — it is also critical that these are done as a sector with regulators (non-supervisory side), governments, and law enforcement. This collaboration with the public sector on cyber threat exercising would aid the development of risk strategies for banks and corporates. For example, agreement on common sector and cross-sector communications protocols, understanding of shared risks, and agreement on what assurance from others looks like to show that they are not compromised and are functioning well (if other firms are having a "bad cyber day"). Deeper industry and public sector trust with regards to sharing exercising 'Lessons Learned' will lead to a common approach and culture to implementing and remediating After Action items from sector exercises, improving crisis management response.

Figure 15. Cyber Event Lifecycle: From Detection to Recovery



Source: Citi

Cyber Security Investment

Cyber Security Spend Relative to Overall Operating Budget

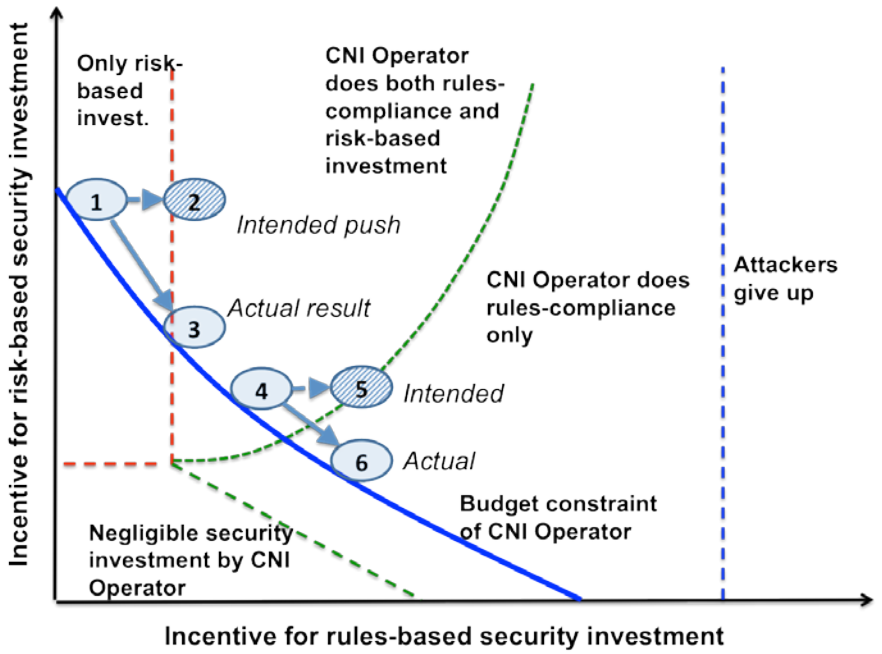
Information security spend is forecast to grow to $124 billion globally by end 2019

With shareholders, customers, regulators, and the general public holding corporates accountable for cyber security, corporate decision makers must consider what they intend to get out of financial investments in cyber security. Research firm Gartner predicts information security will increase 8.7% to $124 billion globally from 2018 to 2019.[133] Amongst this spending, the question remains on how money is being allocated and if indeed those investments are achieving the goals corporate decision makers intended for security, competitive advantage, consumer confidence, compliance, or other reasons.

Organizations should focus on risk-based versus. rules-based security measures

Research on cyber security budgets reveals a focus on 'check-the-box' compliance instead of thoroughly thinking through why spending is needed and for what, which might have unintended consequences. A study conducted by the European Network of Transmission System Operators for Electricity (ENTSO-E) cyber security group, the National Grid security leadership, national regulators, and other stakeholders, examined the impact of regulations on corporate cyber security spend. Researchers found, in lieu of increasing security, additional rules pushed some corporates to disinvest in the security measures identified by risk-based assessments as critical and move instead down the budgetary constraint curve toward the compliance only region.[134]

Figure 16. Incentive for Rules-Based Security Investment vs. Incentive for Risk-Based



Source: F. Massacci, R. Ruprai, M. Collison, J. Williams. Economic Impacts of Rules-based versus Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers). IEEE Security and Privacy Magazine 14(03):52-60, 2016.

[133] Gartner (2018).
[134] Massacci (2016).

Cyber security spending sometimes is decided without grasping cyber issues or without prioritization

Since most corporates are likely only trying to fulfill basic compliance requirements, deciding on cyber security spending remains a difficult exercise. Some corporates find themselves in a situation where they are investing in a range of cyber security services and tools without a full grasp of the issue dues to a shortage of cyber talent. Others take the route of purchasing a blanket of cyber security offerings in an attempt to cover all bases, but without prioritization. A 2017 Thales Data Threat Report notes, *"despite the higher spending (and planned spending) on security, 26% of respondents said their organizations experienced a breach in the last year, up from 21.7% in 2016, while 42% of respondents experienced a data breach at another time in the past, up from 39.3%."*[135]

Having a mature understanding of what security is really needed allows corporates to choose, prioritize, and justify security spend

The current predicament of recognizing the importance of cyber security investment, but still needing to mature an understanding of what security is really needed, leaves corporates in a rudimentary stage of how to choose, prioritize, and justify cyber security spend. Security is traditionally seen as a cost center to a firm. If corporates are dealing with constrained or declining IT budgets, simply spending more money is not a viable step towards security. Corporates may also be required to set aside capital in order to address future risk events. The capital set aside limits what they can presently invest back into people, technology, and the market.

These pressures lead to addressing how to improve a corporates cyber security posture relative to the amount spent. Answering this question requires taking full stock of the assets a corporate is securing through a valuation exercise, and determining how much more secure each asset will be through each cyber security investment. On a more granular level, this process involves identifying risks correlated with cyber events, the probability of the events occurring, and the projected losses associated with each risk.

The multitude of factors up for consideration emphasizes the importance of studying all methodologies and consistently while defining investment, return, security, and risk. Both quantitative and qualitative models have evolved to more accurately address the idea of 'putting a number' on cyber security spending.

Calculating the Value of Cybersecurity Spend

Valuing cybersecurity spend can be tricky as return on investment is not the main objective of network security

This section intends to provide a narrative on evolving schools of thought to address the cybersecurity spending question, and not as a comprehensive overview of all methodologies available.[136]

Business Finance Magazine advises against using return on investment (ROI) as a metric, stating *"ROI can be misleading as an indicator of which security product best suits a company's needs."*[137] The problem is with the word 'return' and how narrow or broad its definition is. In the traditional sense, return on investment is not the main objective of network security, and therefore a focus on ROI is mismatched. This does not mean cyber security investments have no return (which will be addressed later on in "Cybersecurity as a Business Differentiator"), but in the case of calculating a benefit of ROI, the formula requires an additional component.

[135] Bekker (2017)
[136] For an additional perspective, see https://www.csoonline.com/article/3010007/advanced-persistent-threats/how-to-calculate-roi-and-justify-your-cybersecurity-budget.html.
[137] Greengard (2003).

Return on Security investment (ROSI) Model[138]

Return on Security Investment is used to better capture what cyber security spending conversations are trying to achieve

Adding 'security' refines the established ROI model and further hones in on the question corporates are actually trying to answer on cyber security spend. The differentiation between ROI and ROSI — Return on Security Investment — is called out in research from economists' Bojanc and Jerman-Blazic:[139] Because there is no 'return' on security investments in the traditional revenue generation sense, the economists figured out a solution to better capture what cyber security spending conversations are trying to achieve. Benefit is measured as the level of loss prevention, or the difference in the annual loss expectancy (ALE) before and after the security investment.[140] As shown below, maximizing security through investment is reflected in the numerator of the ROSI equation: when the reduction in potential dollar losses exceeds the cost of the investment to achieve that reduction, the investment is worthwhile. A positive ROSI value indicates a worthwhile investment. If corporates build toward this model, applicability may make the most sense at the product as opposed to capability level (i.e., the ROSI on Splunk vs. the ROSI on a security monitoring capability, which is made up of many components).

$$\text{ROSI} = \frac{\text{ALE}_{\text{without investment}} - \text{ALE}_{\text{with investment}} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

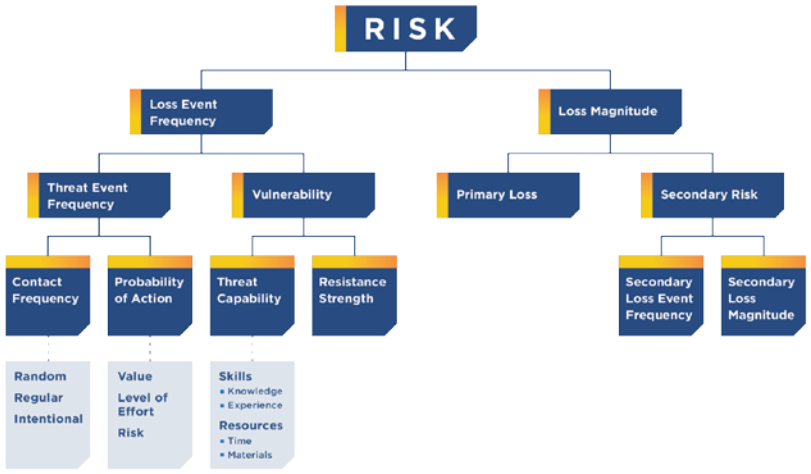
The FAIR Model

FAIR is a another model for understanding, analyzing and quantifying information risk in financial terms

Thinking specifically about quantifying cyber risk, the FAIR methodology below identifies the 'crown jewels' of an organization, determines the threat actors potentially interested in each asset, calculates the frequency of threat actor attempts as well as the probability the attackers will act against the organization's assets, and determines the potential aggregated annual losses in the event an attack is successful. The FAIR model is similar to widely accepted underwriting risk calculations used by investment banks, where underwriting risk is the product of the probability of default (PD) and the loss given default (LGD). In the model below, risk is the product of probability of loss 'loss event frequency' and loss for a given attack 'probable loss magnitude'.

[138] Bojanc and Jerman-Blazic (2008).
[139] Bojanc & Jerman-Blazic (2008).
[140] Pinto, et al. (2005).

Figure 17. The FAIR Model



Source: FAIR Institute, 2017.

One difficulty with the FAIR model is finding and tagging data inputs consistently

Although the FAIR model is the only model that meets the International Standards Organization's guidelines for risk analysis and evaluation, the model has limitations and critics. Primarily, even if the model is sound, the ability to find and tag data inputs consistently for the model is still in the developing stages. It also does not calculate ROSI, since it does not account for the cost of investment in cyber security. On a greater scale, these models demonstrate how risk plays a crucial role in answering the question of what corporates are trying to achieve when determining cyber security spend by separately breaking out the components of cyber security investment and cyber risk.

Alternative investments such as the use of cyber insurance can be also used to alleviate the cost of cyber security spend. However, there are many open questions about the utility of cyber insurance in its current form given the limited options for coverage and complex terms and conditions, which can lead to misaligned expectations. Because terms and conditions related to cyber insurance policies are largely untested, buyers' and sellers' expectations may not align.

Importance and Impact of Measuring Cyber Risk

Cyber risk is now business risk and there is no way to separate the two

Cyber risk is now business risk; there is no way to separate the two. RSA defines cyber risk as the potential of loss or harm related to technical infrastructure or the use of technology within an organization.[141] With consumer preferences gravitating toward adopting new technologies, the cyber risk associated with technology advances inherently links cyber security spend and corporates' ability to meet their bottom line.

Understanding risk plays a critical role in allocating resources for cyber security. Risk informs corporate leaders on where the most vulnerable areas of an organization are and measures how controls help mitigate those risks. Identified controls are often a basis for seeking out cyber security services that need to be put in place to mitigate inherent risk.

[141] RSA (2016).

Risk assessments can be used as an organized approach to prioritizing investment in cyber security service, tools, and/or insurance

Instead of being purely driven by compliance or purchasing a blanket of cyber security services, corporates can use risk assessments as an organized approach to think through prioritizing investment of cyber security services, tools, and/or insurance. Risk serves as a universal language throughout a corporation to ensure all functional areas are working off the same concepts to minimize negative outcomes.

Risk can also be used to measure change over a certain period of time to see if decisions should stay the course or change. As an example, *"an increasing number of CISOs have recently adopted maturity ratings, scoring mechanisms to assess the maturity of their organizations against a set of best practices (ex: NIST CSF), to show improvements on those scores based on new investments."*[142] Such ratings also contextualize the numbers and analysis to remind corporates of why they are investing in cyber security in the first place.

Ultimately, the goal of identifying and measuring risk is to decrease losses or damage to a corporation. Reputation damage, regulatory action, financial/operational loss, and impact on customers or even the overall financial market can be minimized if risk is managed properly. Risk is crucial for demonstrating transparency and responsibility of management to shareholders on how an organization is managing factors that can influence business performance.

Cyber Security Practices as a Business Differentiator

Corporate cyber security management and practice can be a differentiator with competitors

Corporates who differentiate themselves on cyber security likely practice agility. The same trends which expose corporates to more risk, such as emerging technology adoption, can also serve as business differentiators based on how a corporate chooses to manage the risk. Those that spent money earlier to fix legacy infrastructure issues, and who built security in by design, are far more capable today of handling digitization of channels and services, growth and innovation, and embracing emerging technology and markets. By doing so, corporates demonstrate the capability to correlate security spend to business growth and market capitalization. Corporates can use this evolved approach to distinguish themselves as conversations with potential clients continue to shift further towards effective cyber security approaches as a requirement for doing business.

- **Compliance as a Cyber Security Asset:** Earlier, this chapter warned against basing cyber security investments solely on compliance requirements, but compliance can still be a strong motivator in developing security products.

  By adopting an agile development cycle, corporates can ensure software coming down the pipeline is ready to meet new regulatory requirements as opposed to trying to meet requirements with a near-finished product.[143] By demonstrating the culture of compliance is applied all the way down to the way applications are developed, shareholders and customers can see a company's dedication to security in a tangible way.

[142] Bryant (2017).
[143] Wooton (2018).

- **Cyber Security for Responsible Investing:** Cyber security can play a role in an investor's decision calculus given the rising popularity of Environmental, Social, Governance (ESG) funds. Although ESG funds are rooted in environmental and social factors, cyber security is increasingly becoming a consideration for investors.[144] This is reasonable given cyber attacks have the ability to fundamentally harm corporations and investors want to be confident in the companies they are investing in. Smart cyber security practices and investment lead to a sustainable business and play a role in positive outcomes, like attracting investors.

- **Cyber Security as a Business Lure:** When a major cyber event occurs, this sometimes causes loyal customers of the affected party to search for 'greener pastures', or possibly delay continued business until the affected party improves its cyber security program. Customers and clients might choose to look for a service provider or third party offering a stronger cyber security program to protect their data, finances, and interests.[145][146][147] In this instance, cyber security at a company would not just be viewed as a cost center. Instead, it has the potential to retain or lose customers and possibly even attract new ones who were impacted from a cyber incident at another organization.

- **Cyber Security Culture as a Competitive Advantage:** A healthy corporate culture leads to overall benefits for an organization. Similarly, good information security practices throughout an organization feeding into a healthy corporate culture can produce energetic employees contributing to the competiveness of a corporation. By clearly messaging and providing recognition for good practices, corporate leaders can encourage a workforce culture that is both security-minded to prevent losses and motivated to produce results. Such a culture can also attract new cyber security talent at a time when the talent pool is limited. A healthy cyber security culture instills confidence in customers using a corporation's applications, services, and products.

[144] Baker (2017).
[145] Dugan (2017).
[146] Hadley (2014).
[147] Calzada, et al. (2016)

An Interview with Arvind Purushotham of Citi Ventures

About Arvind Purushotham

As Global Head of Venture Investing at Citi Ventures, Arvind leads Citi's efforts to invest in and partner with startups as a way to bring technology-based innovation to Citi's businesses. He focuses his investments on financial services, cybersecurity, and enterprise infrastructure. His investments in the cybersecurity space include Tanium, Pindrop Security, Cylance (acq: BlackBerry), Silver Tail Systems, Netskope and Verodin. Prior to Citi, Arvind spent nearly a decade as a Managing Director at Menlo Ventures, where he was an investor and Board member at several companies. Previously, Arvind was a Program Manager at Intel Corporation. Arvind obtained his BSEE from the Indian Institute of Technology, Madras, MSEE from Case Western Reserve University, and an MBA with Distinction from Harvard Business School.

About Citi Ventures

Citi Ventures' mission is to simplify and modernize financial services for our clients. The Venture Investing team within Citi Ventures makes strategic investments in startups developing solutions across five focus areas — Security & Enterprise IT, Commerce & Payments, Customer Experience & Marketing, Data Analytics & Machine Learning, and Financial Services & Technology — to identify and adopt best-in-class capabilities developed by these startups to benefit our clients.

The importance of cybersecurity has grown tremendously in the last few years. What do you see as the biggest change to the cyber landscape?

The biggest change in the cyber landscape is the advent of advanced persistent threats, or APTs, over the last five years.

What are APTs? It used to be that individual hackers mostly acted independently, sharing information on different types of attacks and methods on the dark web. Actors who hacked their way into an enterprise were mostly trying to cause trouble for companies they didn't like, create some news, or exfiltrate data or information they could then use for their own financial gain. This used to be the world of cybersecurity.

APTs are now well-coordinated hacker groups that are much more disciplined to cause harm to institutions based on financial, social, or political motives. They are patient, and are able to execute complicated hacks that can stretch over days or months to cause maximum damage. Many of these hacker organizations operate like corporations — i.e., with people working in shifts like in operating companies — and are extremely sophisticated.

The net effect is that APTs, who could be nation-state actors or organized gangs, are the highest level of cybersecurity threats. These actors have tremendous resources backing them, and when they get valuable assets, they monetize them through a vast supply chain in the dark web. For example, a person who harvests credit card information turns around and sells the portfolio on the dark web, and the buyer then could further filter that information and sell it to the ultimate criminal who victimizes the cardholder.

From an enterprise perspective, do these APT attacks look different than traditional hacking attacks?

Similar to a traditional hack, APT attackers initiate threats with the hope of successfully breaching an enterprise's defenses. Their ability to modify known attacks to evade protections makes them extra deadly. Once they breach, they are able to 'move laterally' to find assets of value. There is a command-and-control mechanism that directs the hack, and they can sometimes lie in wait for days before exfiltration.

They are often able to exfiltrate a massive amount of data over weeks or even months since they are very good at avoiding detection. By the time the breach is detected, the damage is severe.

Given the changes in the cyber environment, what do you think are the most important investments that should be backed in the field and how is Citi Ventures tackling this?

We look at the interplay of four vectors of change: (1) a changing threat landscape; (2) changes in enterprise IT architecture that creates new vulnerabilities and new attack surface areas like mobile and cloud; (3) new technologies such as Machine Learning that can be leveraged to solve existing and known problems; and (4) how increasing regulatory and compliance needs are impacting security and audit requirements. With this framework in mind, we look for investment opportunities both driven by Citi's needs and priorities, as well as by identifying major pockets of venture investment activity in these areas. The latter is an important signal that helps identify emerging trends.

With increasing threats and new actors, is the cybersecurity market a continually expanding market?

As investors in cybersecurity over several years, we've noticed that the cyber market is cyclical because organizations react to the external threat environment – to some extent, this is an arms race. When the enemy has new ways to attack, enterprises need new defenses. New companies are formed and technologies are developed to solve for those risks, but then growth slows down until the next up-cycle. Because of this dynamic, the volume of good opportunities for vendors and startups tends to ebb and flow.

In Citi Ventures' view, we're coming to one of those maturity plateaus. In addition, we're seeing increasing consolidation among cybersecurity players — several startups that developed those next-gen tools have been acquired by larger companies. So we see a slow-down in the number of attractive opportunities in cyber in the short run until new factors emerge as mentioned earlier.

On top of the increasing number of threats and threat actors, what other trends do you see in the security ecosystem?

One of the trends we are watching is called "Zero Trust Security." Essentially, the traditional perimeter within the enterprise doesn't exist anymore. It used to be that applications were run completely inside the enterprise, and the primary defense was a firewall to secure the perimeter. Hence, you could 'trust' everything inside your firewall. In today's world, the enterprise perimeter is porous — there is data on mobile phones, there is data in the cloud because enterprises are either running SaaS (Software as a Service) applications such as Salesforce, or are running their own application workloads on public cloud infrastructure such as Amazon Web Services — so the data of the enterprise is much more scattered.

The concept of ‘Zero Trust Security’ is that you protect the data wherever it is — inside and outside the four walls of the enterprise — and not simply trust whatever is within the perimeter. When it comes to things like securing the cloud, there are several new technologies coming online and new companies and vendors that are quite interesting.

How can cyber companies be more proactive and look to solve future cyber issues?

Many of the threats of the future are solved by startups. It’s common knowledge that large players are slower to innovate and build products to address emerging needs. That is a pattern we’ve seen over many years in cybersecurity. At Citi Ventures, we identify the startups solving these emerging issues early. We evaluate whether companies we meet are solving problems that pertain to Citi and other large companies, and can scale to operate in complex IT environments. We use that as one filter to figure out whether it’s an interesting investment or not, and partner with our cybersecurity team extensively.

The flip side is that being future-focused is difficult due to how human psychology works—often startups are not rewarded for being too proactive. It’s only when a company gets hit by a cyber incident that there is urgency and budget is allocated. When we meet companies that are seeing rapid adoption, that is a signal that perhaps Citi should be looking at this as well.

Cyber and People

Although few could argue with the notion that Internet connectivity has transformed the lives of individuals around the world, however the results and implications of these transformations, remain the subject of ongoing debate. According to the United Nations' International Telecommunications Union (ITU), by the end of 2019, 51.2 percent of the global population, approximately 3.9 billion people, will be using the Internet. However, the advantage (for some) that accompanies an increasingly digitized world also brings unexpected challenges, many of which require new ways of thinking about risk.[148] Cyber risks grow as the number of internet-connected devices and end uses increases, which increases the surface attack.

Increased Connectivity – Increased Cyber Risk

Technology is rapidly changing the way we operate, as well as the way we shop, communicate, pay for services, work etc. But with this technological evolution comes the increased risk of cyber attacks, targeted not only at organizations as described in the previous chapter but also at individuals. In particular, high risk populations like children, teens, and the elderly are particularly susceptible to cyber risks. In certain cases, a lack of experience, precaution, or sophistication could expose them to additional attacks.

The elderly, children, and teens are particularly susceptible to cyber risk

According to Aviva's 2017 Real Retirement Report, the elderly are increasingly at risk of cyber fraud, with more than a million older people duped by email scammers and eight percent over age 75 who have been targeted, have fallen victim. The estimated annual total dollar amount of the losses suffered by victims of elder financial exploitation is estimated at $2.9 billion.[149]

However Haddington and Chivers (2018)[150] in their study state that young people are actually more vulnerable to cyberattacks than elderly people. They interviewed a selection of the population and divided them into different categories — (A) already protected, (B) digitally unaware, (C1) trusting, (C2) unconnected and somewhat protected, (C3) relatively savvy, (D1) unsuspected and unprotected, (D2) unconcerned and unprotected, and (E) unware. They conclude that higher-at-risk segments are a feature of under 40 age groups —- for example 60% fell into the unaware segment, and 61% were classified as 'digitally vulnerable'. In contrast, 70% of those over the age of 41 were classified as (A) already protected. This study presents a clear contrast to the often-presented view that it is the older generation that is more vulnerable to cybercrime. What is also interesting is that they found undergraduate students in particular are more likely to fall in the category of trusting (C1) and unconcerned and somewhat protected category (C2). The authors of this research suggest the reason for this is that students and young people in general are more likely to be engaged in the digital world through online media, social media etc. but they ultimately lack the capacity to detect risks related to cybercrime. As connectivity increases through the adoption of Internet-enabled devices and other technologies, so does the available attack surface, which potentially increases the risks of cybercrimes to individuals.

[148] Manyika (2016).
[149] *2011 MetLife Study of Elder Financial Abuse.*
[150] Hadlington and Chivers (2018).

Individuals face threats from identity crime, financial loss and blackmail from cyber attacks

So what are the risks that individuals face? The main risks relate to the theft of personal and financial data which criminals could use for a number of things, including but not limited to:

- **Identity Crime:** This usually takes the form of identity theft, the creation of counterfeit documents, or the misuse of documents. Once criminals have stolen an identity, they can use it to typically commit fraud, or even to travel across borders undetected;
- **Financial Loss:** Stealing of debit and credit card data, or in some cases the direct theft of savings, in fact it has been reported that some individuals were not aware that they have been robbed until after their savings have been stolen;
- **Blackmail:** If the attackers accessed potentially damaging or compromising information on any individual, they could use that information in an attempt to blackmail the employee. This is potentially more concerning in the case of senior employees, or those with access to critical systems.

Criminal actors in particular could also leverage the combination of stolen private data and publicly available data to identify and target victims with access to information or resources they are seeking. This type of information is also valuable to groups who use Business Email Compromise schemes where an adversary obtains access to a business email account and imitates the owner's identity in order to defraud the company, its employees and its clients or partners.

Risks to Corporations from People

Individuals are also a risk to corporates as malicious actors can take advantage of human vulnerabilities to infiltrate corporate systems

It is not only individuals that are directly affected from personal data breaches — in some cases businesses are affected as adversaries weaponize stolen data to target individuals at any organization with spear phishing emails or other tailored social engineering attacks.[151] In theory, any institution could be impacted directly in the event of an attack on an employee or contractor, or indirectly if a client or supplier is targeted. Targeted attacks could result in a range of possible outcomes including financial losses. Organizations also leverage social media platforms to engage with clients and customers, market their products and services, and to build or cultivate their brand.

While social media platforms are powerful tools in this space, they also offer adversaries a public platform to undermine a company's brand or reputation. Armed with details on a company's employees, hackers could attempt to impersonate individuals affiliated with that company, or spoof official communications. This could devalue a company's brand and perceived value to customers, clients, and investors. While the availability of social media has undoubtedly opened up new opportunities for organizations to advertise and market, organizations must be hyper-vigilant about protecting their digital assets and brand.

[151] If the success of social engineering attacks is positively correlated with the amount of information available on a particular target, data leaked from the breach could be combined with other publicly available data for bespoke targeting and potentially increase the attackers' probability of success.

Risk of 'Single' Point Entry via Single Sign On (SSO)

Certain organizations, including but not limited to, financial services firms, travel websites, and various mobile applications, allow individuals to log in through identity providers which offer a range of services. This method (SSO) leverages a trusted relationship between major social networks and other applications, and websites to provide easy and convenient access for shared users. Once authenticated by the shared identity provider, a user can visit any number of sites or applications offering the ability to log in through the shared identity provider. However, despite the convenience this configuration offers users, some security researchers maintain the single point of entry poses a 'massive security risk' as it gives attackers a single target which, if permeated, can be used to gain and retain access to a number of other sites. Further, given the complexity of the relationships between providers, it is difficult to map out the downstream effects. Separately, if data belonging to customers from financial institutions is stolen from a third-party application linked to a single-identity provider, firms could, in certain cases, be liable for losses where merchants' security posture was assessed to be robust enough to detect fraudulent or unauthorized activity. A primary (unanswered) question concerns how third parties providing this service are positioned to protect data belonging to institutions and their customers.

Social Networks and Privacy

The posting of vast amount of personal data on social media creates cyber risk

Social media use has enabled unprecedented *"levels of communication, social interaction, and community building across boundaries of time, place, and social context."*[152] Further, it continues to facilitate the democratization of knowledge and provide business and educational opportunities for people in under-served communities and regions.[153] However, because cyberspace is essentially global in nature, concerns regarding individual privacy and the integrity and availability of data raised as a result of peoples' willingness to post vast quantities of personal and professional data online, are subject to the legal and cultural norms observed in each country respectively. Questions and considerations associated with select downside risks that accompany broader adoption of social media are outlined below.

Research, Investigation and Analysis – Potential Implications

Personal data found on personal and professional social networks is valuable to both legitimate and illegitimate actors looking to surveil or locate persons of interest, better understand individuals and groups, draw connections between people and places, and/or assist in pre-emptive or investigative activity related to threats or crimes. To gain additional insights into competitors' activities, corporations can comb social networks to monitor senior executives' social media profiles, and view their locations and interests.

Whereas in the past, for competitive intelligence, a corporation might have needed access to an insider, they instead can now potentially rely on what is publicly posted. Threat actors, such as foreign intelligence services, criminal actors, and terrorist groups have also demonstrated interest in exploiting this information. Although their objectives may differ, criminals and terrorists, are likely interested in much of the same data for the same or similar purposes.

[152] World Economic Forum (2016).
[153] Ibid.

Personal data on social media creates risks to corporates through many avenues including blackmail, social engineering attacks, and surveillance

For example, criminal actors could identify potential targets, such as selecting homes to vandalize or rob based upon knowledge that a particular individual is out of town, as reflected in status updates or geotagged photographs. Criminal actors in particular could leverage the combination of stolen private data and publicly available data to identify and target victims with access to information or resources they are seeking. Separately, terrorist organizations and their offshoots may look to identify individuals for recruitment, based upon their perceived likelihood of receptivity to a particular message.

- **Individuals:** While information belonging to any individual could be stolen and leaked, information on high profile and well-known individuals could cause relatively more damage. Most companies have strict policies related to inappropriate use of corporate email accounts; however the same individuals sometimes have more liberty in personal communications conducted via email or on social networking sites. In certain cases, employees may not have more liberty, but employers may be more likely to turn a blind eye to this behavior, perhaps limited by both resource and legal constraints on monitoring external activity. While employees are generally prohibited from sharing proprietary or confidential data via a personal email account or on a social networking site, personal details, which are not generally forbidden, could, in certain cases, be combined with publicly available information on an individual, and used to make inferences about that individual's activity. In the event a social network or email provider is breached, individuals could be embarrassed if their information is shared or they may potentially suffer consequences professionally, depending upon the nature of the disclosed information. In the past, senior executives of large, multinational companies have stepped down as a result of private email communications posted publicly.[154]

- **Blackmail:** If the attackers accessed potentially damaging or compromising information on any individual, they could use that information in an attempt to blackmail the employee. This is potentially more concerning in the case of senior employees, or those with access to critical systems. Specifically, an adversary could threaten to release compromising information on an individual if he or she does not carry out the adversary's demands, which could include, but are not limited to, data exfiltration, IP theft, theft of other sensitive information, or high value payment fraud.

- **Increased Likelihood of Social Engineering Attacks:** If an adversary breached a social media network, they could weaponize stolen data to target individuals at any organization with spear phishing emails or other tailored social engineering attacks.[155] In theory, any institution could be impacted directly in the event of an attack on an employee or contractor, or indirectly if a client or supplier is targeted. Targeted attacks could result in a range of possible outcomes including financial losses.

- **Brand Integrity and Preservation:** Organizations leverage social media platforms to engage with clients and customers, market their products and services, and to build or cultivate their brand. While social media platforms are powerful tools in this space, they also offer adversaries a public platform to undermine a company's brand or reputation.

[154] Rushe (2015)

[155] If the success of social engineering attacks is positively correlated with the amount of information available on a particular target, data leaked from the breach could be combined with other publicly available data for bespoke targeting and potentially increase the attackers' probability of success.

Armed with details on a company's employees, hackers could attempt to impersonate individuals affiliated with that company, or spoof official communications. This could devalue a company's brand and perceived value to customers, clients, and investors. While the availability of social media has undoubtedly opened up new opportunities for organizations to advertise and market, organizations must be hyper -vigilant about protecting their digital assets and brand.

- **Surveillance:** *"As smartphones have become ubiquitous and technology more accurate, an industry of prying into people's daily habits has spread and grown more intrusive."*[156] According to a recent investigation conducted by The New York Times, at least 75 companies receive *"anonymous, precise location data from apps whose users enable location services to get local news and weather or other information."*[157] Further, many of those businesses claim to track up to 200 million mobile devices in the United States.[158] While this information can be used to help businesses understand people's patterns, behavior, and activity, and businesses claim they are not interested in the specific identity of any particular consumer, raw data could allow an organization to identify a person without his/her/their consent.[159]

Human Behavior Increases Vulnerabilities

Adversaries can exploit the lack of understanding of security risks as well as human behavior to stage an attack

Human behavior amplifies the benefits and drawbacks that accompany the increasing degree with which devices are connected to the Internet. As such, *organizations' ability to protect their assets, infrastructure, and reputation, depends largely upon employee awareness of, and compliance with, best practices in cyber security and hygiene.*

Today's cyber risks grow as the number of Internet-connected devices and corresponding end users increases,[160] leading to an increase in attack surfaces. Further, in cases where organizations may not yet understand the security risks associated with these new connections, adversaries can exploit this lack of understanding, which in many cases, is accompanied by fewer controls or safeguards.

Although many groups possess sophisticated technical abilities, human weaknesses are frequently exploited, as it is often easier to target a human vulnerability than it is to bypass a sophisticated technical control. Recent examples include the ransomware WannaCry and Petya attacks. These campaigns were launched by bad actors deploying social engineering tactics like phishing, where fraudulent emails are sent to individuals to obtain confidential data or information, such as credentials. Some phishing emails can cause malware to download onto a user's computer and begin a ransomware campaign that can limit the user's own privileges.[161] Alarmingly, tactics like this are being used as weapons in broader geopolitical conflicts. For example, nation state governments are reported to have the capabilities to develop malware to target its adversaries in support of broader national objectives.

[156] Valentino-devries, et al. (2018)
[157] Ibid.
[158] Ibid.
[159] Ibid.
[160] Harvard Business Review (2017)
[161] Haber (2017)

The Best Defense is a Good Offense

Educating employees can be an effective defense against a range of attacks

Educating employees, particularly those deemed high risk by virtue of their role or responsibilities can be an effective defense against a range of attacks. Company awareness training programs can be highly effective when designed to improve users' behavior in a way that also allows for a feedback loop in real time.[162] Promotional marketing campaigns aimed at educating a company's workforce and clients, respectively, can raise awareness about security threats and educate them on good behaviors. These employees become a part of a solution and can act as a defense against threats. This is one way in which a behavioral flaw can be converted into a benefit by taking appropriate action.

Additionally, some companies employ behavioral analysis to better understand who is using their network and how they are using it. Behavioral analysis baselines users' activities and when a pattern change is identified, the irregularity can trigger deeper analysis and/or further security action.[163]

Human behavior is a substantial risk which can increase either the benefits or the adverse effects resulting from increased connectivity. However, training, awareness, and communication are powerful tools in any organization's arsenal, and combined with other measures, such as behavioral analysis, organizations can begin to tackle the next generation of cyber threats.

[162] Greengard (2018).
[163] Accenture (2018).

Changing Data Protection Landscape

Most consumers may not fully appreciate how much of the data they generate is being collected and how this ends up being used

From the perspective of the consumer, the fact is that pretty much everything we do as consumers online is tracked in some way, shape, or form. Cookie tracking is clearly the most widely known technique, but there are many other ways users can be tracked and that tracking has become more sophisticated. For many consumers this will be part of an accepted value exchange whereby information is knowingly surrendered in return for a valued good or service. That said, most consumers may not fully appreciate how much of the data they generate is being collected and how this ends up being used. The number of high profile data breaches and instances of data being used in nefarious ways has led to this becoming a social and political area of debate.

With new regulation, we are moving from an environment where organizations no longer have untrammeled access to data

The opportunity from data is clear but in the rush to exploit the data opportunity, not all companies have paid enough attention to both cybersecurity and/or privacy. The consequences of this are becoming apparent in the form of cyber risk, and ultimately both financial and reputational damage. The other consequence is that this has prompted regulators to act, which means we are moving from an environment where organizations have become accustomed to untrammeled access to data, to one where data minimization and transparency presides, consumers are empowered to take more control of personal data, and organizations are forced to think carefully about their use of data. After years of the Internet being 'loosely' regulated, the widespread collection of data has led to the rise of data asymmetry and, consequently, consumer trust is low. Consumers believe that cybersecurity and privacy risks are amongst the biggest risks facing society. Regulators have been compelled to act to protect consumers; in most markets the right to privacy is a fundamental human right.

Over 100 countries now have some form of modern data protection with the EU's GDPR the most comprehensive in scope and ambition

The number of countries with some form of modern data protection has increased from 0 in 1970 to over 100 now. The intention has been to protect consumer's privacy rights. The General Data Protection Regulation became legally binding across EU member states on 25 May 2018, and is an attempt to take a uniform approach to data protection (replacing the Data Protection Directive which brought about different treatments at a national member state level). The GDPR has raised the bar and we see this regulation as a game changer in terms of the scope and ambition. The main changes or requirements that the GDPR brought in are:

- The headline grabbing fine of up to 4% of global annual turnover for non-compliance.
- The regulation expanded the definition of personal data, the territorial scope (any entity offering goods and services within the European Economic Area) and the entities it is applicable to (both data processors and data controllers).
- Tighter conditions for processing personal data especially in relation to consent requirements.
- Privacy by Design and Privacy by Default are central to the regulation in order to minimize risk associated with processing and storing personal data. Increased transparency and information around data processing.
- Increased consumer (data subject) rights such as the Right to Object to processing of personal data, Right to Access your Data, Right to Erasure and Right to Data Portability.

See our GPS report Who Watches the Watchers? – How Regulation Could Alter the Path of Innovation for more details on the GDPR requirements.

As noted earlier, we believe that the threat of cyber will worsen with attacks increasing in both size and complexity. This could make it hard to meet the requirement set by the GDPR to report a data breach to the Data Protection Authority within 72 hours of becoming aware of it. For processors this means they will need to notify controllers within the timeframe, which could have a significant impact on supplier relationships. Research by the Ponemon Institute found that the mean average time to identify a data breach is 201 days, and the mean time to contain the breach is 70 days. The number of days is higher for criminal attacks, and lower for human-error related breaches.

The intent of the GDPR is to increase transparency and consumer control over data and is focused on the principle of data minimization

The intention of the GDPR is to increase transparency and consumer control over data and is focused on the principle of data minimization. A challenge for companies is that this often contradicts industry specific regulation, which tends to require data maximization.

One of the major areas of contention for privacy groups is that of data surveillance by governments. The Snowden revelations about the U.S. National Security Agency (NSA) mass surveillance were a major factor behind GDPR getting through the approval process in Europe as well as the cause of the downfall of the Safe Harbor agreement between the U.S. and EU, since replaced with the Privacy Shield. Consumers expect to be kept safe and access to data is a crucial tool in providing the intelligence services with a means to do so. The GDPR broadly leaves interpretation open to the individual member states in relation to data being processed for the purpose of prevention, investigation, detection, or prosecution of criminal offences and preventing threats to public security. As recently as November 2016 the controversial Investigatory Powers law was passed in the U.K. (enabling certain state surveillance). The Cyber Security Law in China has raised concerns around whether it could lead to increased surveillance as it requires network operators to store Internet logs for at least six months, block the dissemination of illegal content, and provide 'technical support and assistance' to the authorities in national security and criminal investigations.

GDPR applies to all EU citizens, not just to data processed in the EU, therefore rules around international transfers have become more relevant

Data protection regulation typically retains very strong geographical boundaries, which is increasingly difficult given the global approach to the use of data by businesses. Given the GDPR applies to all EU citizens, and not just to data processed in the EU, the rules around international transfers have become more relevant. There are only 12 countries that currently have adequacy status with the EU, which allows for free flow of data between the EU and other countries. The agreement between the U.S. and EU to allow the free flow of data is via the Privacy Shield.

There have been significantly differing approaches to data protection globally. For example, the U.S. has typically taken a more principle- and sector-based specific approach than the EU, which means U.S. regulation has comprised of a patchwork of difference, industry-specific regulations rather than overarching federal legislation. We see the GDPR as the start of a step change in the approach to data protection regulation and we are starting to see signs of this. Governments realize the value of data, as well as the need to protect it, and so we are seeing increasing requirements for data to be physically stored locally (i.e., Russia, India, China). The proposed e-Privacy regulation in Europe, if approved in its current form, could lead to a further tightening of rules for certain industries and uses of data in the EU.

The California Privacy Act, which is GDPR-like, is set to come in from 2020. There are proposals for a Federal Privacy Law in the U.S. and signs of other countries looking to tighten data protection rules across Asia and Latin America. Continuous news flow about data breaches and questionable uses of data continues to increase the risk that personal data becomes an area that has to be more tightly regulated. This could have implications for how companies use data and areas such as artificial intelligence and the speed of data related innovation (see ePrivacy & Data Protection: Privacy Matters: Navigating the New World of Data Protection) but it also another support for the rise of products and services to help manage and tackle cyber risk.

Section 3: Managing the Risks of Cyber – How Do You Protect Against It?

Cyber and the Insurance Market

The cyber insurance has been around since the 1980s, when the first cyber worm — the Morris Worm — appeared, and error and omission (E&O) policies in the tech field provided some coverage for glitches and errors in blue chip organizations and financial firms.[164] The idea of a specialized, standalone insurance for digital losses came to the fore through the 1990s with the threat of Y2K, but it was not until after the turn of the century, with the dot-com crash and the advent of 9/11, that the current industry climate became established.

Over one-third of large companies in the U.S. having specific cyber insurance

Today, cyber insurance is a growing market. As the cyber threat has become more tangible and publicly understood, companies have become more aware of the risks that come with mandated digitization, and insurers have brought more specialized products to market in response. In 2018, over a third of all large companies in the United States had specific cyber insurance, and the coverage density in other countries is increasing.

Developing the Cyber Insurance Market

The first major market for cyber insurance appeared in the United States. In 1996, the U.S. Health Insurance Portability and Accountability Account established the first major protections for personal data and health information, introducing penalties for leaks and bringing the prospect of data breach to international attention. States began to pass laws requiring companies to disclose data breaches and healthcare providers began to seek appropriate cyber insurance. Accordingly, during the initial growth phase of the cyber insurance market in the early 2000s, products provided cover for third-party liabilities stemming solely from data breaches. This did not fully encompass the range of cyber threats which existed but were little understood at the time, and cover for first-party losses, losses stemming from business interruption, cyber extortion, and network asset damage ultimately came to market by the middle of the decade. The staggered introduction of state regulations and wider Federal standards led to a 'patchwork' of frameworks in the U.S., which drove demand but has presented challenges for uniform coverage ever since.[165]

As the number of data breaches increased, so did the demand for cyber insurance

Demand for cyber data breach insurance rose through the 2010s, as the number of publicly reported data breaches in the U.S. rose from 1,800 in 2009 to 6,700 in 2013.[166] Breaches of user data between 2013 and 2015 from Target, Anthem, Ebay and Yahoo remain some of the largest ever recorded. Premiums of cyber data breach insurance grew to over a billion dollars between 50 providers in 2015.[167] Overall, the market for affirmative cyber insurance products reached more than $4 billion among 150 providers in 2017, during an otherwise static period for the industry across other lines.[168] The expansion of the market appealed to more mainstream insurers, industry pillars, and specialist carriers, who began offering bespoke cover for physical damage from cyber to energy and gas suppliers. Around five major insurers write more than half of all cyber insurance policies. 90% of policy volume applies to exposure in the United States alone.

[164] Camillo (2017).
[165] Coburn, et al. (2019).
[166] Ibid.
[167] Ibid.
[168] Statista (2019).

P&C Insurance

The P&C Insurance brokers may play a bigger role in the cyber insurance market going forward. They tend to invest in faster growing markets, such as cyber, in order to boost their own growth rates. Plus, as previously mentioned, there are capacity issues in the cyber market as insurers are not fully comfortable with the risk. As such, alternative sources of capital outside of traditional insurance may hold the key to expanding the cyber market. In 2018, alternative capacity totaled $92 billion, or 21% of total capacity of around $437 billion, while growth in alternative capacity has been much faster at around mid-teens, versus low single digit growth in traditional capacity. The industry is starting to explore whether alternative sources of capital can be applied to capacity constrained lines of business, such as cyber, in order to satisfy market demand for the product. If it happens, the cyber market could expand and become a bigger piece of the overall insurance market.

In May, 2018, the EU rolled out new regulatory framework for data protection and privacy called the General Data Protection Regulation (GDPR). The laws cover almost every aspect of information management, and all businesses that process the data of an EU citizen are required to comply. One requirement is that any firm hit with cybersecurity breach must report the claims, or face fines if they don't. Over time, compliance with the laws will increase the number of cyber claims reported, and the need for cyber insurance for anyone doing business in the EU.

The U.S. is the largest affirmative insurance market, with 30 other countries offering equivalent products

Cyber's damage footprint is not bound by traditional geographic or regulatory boundaries, and so the international insurance market has grown in response to the indiscriminate risk. Although the United States has the largest share of the affirmative cyber market, equivalent products are offered in at least 30 other countries. Since 2010, more than 70 countries around the world have passed data protection laws, reflecting the widespread emphasis on cyber security and the standards expected of data aggregators to both safeguard their information and demonstrate timely transparency when failings in security are discovered.

There are around 20 different types of cyber cover currently available on the global market, as shown in Figure 18, though these offerings differ greatly from country to country.[169] The triggers for cyber cover include data exfiltration, contagious malware, distributed denial-of-service, and financial thefts. Key loss processes may also include the failure of counterparties or suppliers which rely on networked systems and are vulnerable to outages and software failures. These loss processes account for roughly 90% of all economic business damage as a result of cyber attack, technological failure, and other malicious digital interference.[170]

Cyber Insurance Products

Cyber insurance policies are either 'affirmative', meaning that they explicitly cover cyber risk and specific losses associated with it, or 'non-affirmative', meaning the coverage is non-explicit. The following types of insurance may be offered in these categories:

[169] Cambridge Centre for Risk Studies and RMS 2016.
[170] Cambridge Centre for Risk Studies (2019).

Figure 18. The 20 Coverage Types Available in Cyber Insurance Products

	Cyber Loss Coverage – Primary Category	Lloyd's Min Recommended	Party	Description
1	Breach of privacy event – direct costs	Security Breach of Privacy	First	The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
2	Breach of privacy event – liability	Liability	Third	The cost of dealing with and compensating third-party individuals whose information is or may have been compromised by a data breach, including notification, compensation, providing credit-watch service, and other third-party liabilities to affected subjects.
3	Data and software loss	Replacement of Lost Data and Software	First	The cost of reconstituting data or software that have been deleted or corrupted.
4	Network service failure liabilities	Security Breach of Privacy	Third	Third-party liabilities arising from security events occurring within the organization's IT network or passing through it in order to attack a third party.
5	Business Interruption	Business Interruption	First	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures.
6	Contingent Business Interruption	Business Interruption	Third	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
7	Incident response costs	Security Breach of Privacy	First	Direct costs incurred to investigate and close the incident to minimize post-incident losses. Applies to all the other categories/events.
8	Regulatory and defence coverage	Regulatory Fines	First	Covers the legal, technical, or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defense costs, investigations or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so.
9	Liability – Product and Operations	Liability	Third	Third-party liabilities arising in relation to product liability and defective operations.
10	Liability – Technology Errors & Omissions	Tech E&O / Programming ENO	Third	Coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
11	Liability – Professional Services Errors & Omissions	Liability	Third	Coverage for third-party claims relating to failure to provide adequate professional services or products (excluding technical services and products) including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
12	Liability – Directors & Officers	Liability	First	Costs of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents and can result from alleged misconduct, or failure to act in the best interests of the company, its employees, and its shareholders.
13	Multi-media liabilities (defamation and disparagement)	Liability	First	Cost for investigation, defense cost, and civil damages arising from defamation, libel, slander, copyright / trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
14	Financial theft & fraud	Extortion	First	The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities, or other property.
15	Reputational damage	Reputational Damage / Public Relations	First	Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
16	Cyber extortion	Extortion	First	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
17	Intellectual property (IP) theft	Replacement of Lost Data and Software	First	Loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share.
18	Environmental damage	Physical Damage	First	Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
19	Physical asset damage	Physical Damage	First	First-party loss due to the destruction of physical property resulting from cyber attacks.
20	Death and bodily injury	Bodily Injury	Third	Third-party liability for death and bodily injuries resulting from cyber attacks.

Source: Cambridge Centre for Risk Studies and RMS 2016

Cyber Terrorism

Cyber insurance has recently expanded to include losses that may be caused by terrorists or political actors

Cyber insurance has recently expanded to include losses that may be caused by terrorists or political actors that are similarly classed. In December 2016, the U.S. Terrorism Risk Insurance Act (TRIA) confirmed that stand-alone cyber insurance policies classed under Cyber Liability codes would be considered valid "property and casualty insurance" under the stipulations of the act, effective confirming that physical damage and FLEXA triggers caused by digital interference would be honored by the act.[171] In 2018, the U.K.'s terrorism pool, Pool Re, became the first organization of its type to specifically extend cover to include material damage and direct business interruption caused by terrorists using cyber tools or digital means.[172] In cases, certain mitigations taken by companies, such as regular system patching or staff training, may lower premium costs, thus incentivizing an active approach to bottom-up risk management. These decisions have heralded a wider conversation about the future shape of the cyber threat, particularly as it pertains to geopolitics, crime, and acts of war, and how the insurance industry can provide an incentive into innovative research into the risk.

Silent Cyber

Another term for non-affirmative cover, 'silent cyber' refers to the ambiguous coverage for cyber attacks in pre-existing policies and is an issue of unknown exposure for insurers. It is particularly relevant in aviation, aerospace, transport, marine and property lines, where business interruption losses or physical damage resulting from digital interference may be claimed under traditional policies. In 2016, the Bank of England's Prudential Regulation Authority (PRA) brought the issue of silent cyber to wider attention when it expressed concerns that the amount of implicit cover assumed for digital risks was growing year over year. A year later, the PRA issued a Supervisory Statement to the U.K. insurance industry, urging them to limit the growth of silent cyber using robustly worded exclusions, *"specific limits of cover"*, and adjusting premiums *"to reflect the additional risk."*[173]

Developing the Cyber Insurance Market

The current global market for affirmative cyber insurance amounts to around $6 billion in premium versus $120 billion overall expenditure on cyber security

The current global market for affirmative cyber insurance amounts to around $6 billion in premium. This is a respectable pot, but one which is still relatively minor in comparison to other lines of specialized insurance which have been around far longer and may have total premiums closer to $1 trillion. It also stands in significant contrast to the overall expenditure on cyber security, which stands at more than $120 billion globally. Current projections for the industry suggest that the cyber market will only continue to grow, perhaps becoming a standard peril in a number of years, as higher numbers of SMEs purchase cover for their digital assets and as a degree of cyber disruption becomes more commonplace.

The cyber insurance market, however, cannot currently provide adequate protection from the developing threat. The current practice for low limits and explicit exclusions means that the growth of the market will be severely limited if it is to grow cautiously. If companies find that they are unable to purchase insurance to cover more than 10% of the losses they might expect from a major cyber attack, then insurance will only form a minimal part of their risk management strategy going forward. For cyber insurance to become a standard, insurers will have to switch to offering larger limits, a decision that must be backed by their confidence in their assessment of the risk and subsequent capacity allocation.

[171] Willis Towers Watson (2017).
[172] Vincent (2018).
[173] Bank of England (2017).

Cyber 'Catastrophes' and Insurance

To date, most payouts for cyber loss have been unremarkable

Crucially, the cyber insurance industry is yet to suffer a truly 'catastrophic' cyber event, which may trigger major claims in a broad swathe of policy holders resulting from the same attack. To date, most payouts for cyber loss have been unremarkable, or, in cases of large payout, have been from cumulative loss processes. It is likely, however, that such an outcome is inevitable, given the growing digitization of society, the introduction of great numbers of unsecured devices into complex networks, and the development of more malicious actors.

Cyber risk is nascent, and there is no long historical catalog by which to determine the size and shape of the threat in the future

Many long established classes of insurance have the benefit of historical insight, and years of profitability between the major catastrophes — such as earthquakes, terrorist attacks etc. — which trigger significant losses across the industry and drain years of surplus, which may then be built back over time. This pattern of adjustment forms the tail risk for a catastrophe, but given that the true catastrophic potential for cyber is not yet fully understood, some industry expertise feel it is unwise to provide broadly applicable cyber cover in the interim. Cyber risk is nascent, and there is no long historical catalog by which to determine the size and shape of the threat in the future. The rate of cyber 'catastrophes' in an average decade is liable to change given the development of the risk landscape, and events qualifying as catastrophic may occur with greater frequency than the industry is able to support. In this eventuality, it may be that cyber insurance becomes unfeasible as an offering.

Insurers have exhibited caution in entering the cyber insurance market and are using probable maximum loss assessments to explore the potential of large scale losses

Given this possibility, insurers have exhibited caution in entering the cyber insurance market. Almost half of all policies are capped at a $1 million limit; limits over $10 million are rare, occurring in less than 10% of policies written.[174] Losses from cyber attacks, however, can already amount to hundreds of millions of dollars, with most companies left to absorb the majority of losses. The market for cyber insurance, therefore, does not match demand, and likely will not do so until the upper limits for cyber risk can be better estimated.

Insurers are using Probable Maximum Loss (PML) assessments, hypothetical scenarios of massive loss, in order to explore the potential for future large scale losses stemming from cyber attack. These exercises give an idea of the cost of a massive cyber attack, but provide little insight into the question of return periods between events, which can only be estimated from expert consultation and added experience. In this regard, many insurers view themselves as 'buying loss experience' in the emerging cyber insurance market – building a dataset on claims year over year, building a record for historical cyber damage for consultation in the future. The length of the historical record for cyber losses is now roughly twelve years.

[174] Coburn, et al. (2019).

Figure 19. Published PML Scenarios and Hypothetical Stress Test Scenarios Used by the Insurance Industry to Assess Impacts and Risk Appetite Adjustments for Cyber Catastrophe

PML Scenario	Description	Variants	Source
Sybil Logic Bomb	A software bug is introduced into an industry standard database, creating repeating algorithmic failures which are embedded in years of backups	3 variants	Cambridge Centre for Risk Studies (2014)
Business Blackout	A malicious attack on transformers causes a major power failures in the US Northeast	3 variants	Lloyd's/CCRS (2015)
U.K. power distribution failure	An attack on substations creates rolling blackouts in the Southeast UK	3 variants	Lockheed Martin/CCRS (2016)
Leakomania	Data exfiltration affects thousands of companies using a zero-day compromise	3 variants	CCRS/RMS (2016)
Cloud compromise	A technical error causes outages in cloud service providers	3 variants	CCRS/RMS (2016)
Extortion spree	A virulent ransomware attack affects corporate networks with high monetary demands	3 variants	CCRS/RMS (2016)
Financial transaction interference	Attackers carry out multi-million dollar cyber heists by compromising online payment systems	3 variants	CCRS/RMS (2016)
Mass DDoS	E-commerce servers are hit by intense and lengthy denial of service attacks by hacktivists	3 variants	CCRS/RMS (2016)
Cloud service provider breach	Exposure study using cloud service provider failures with variable durations	SQL programmable script	AIR (2016)
Payment processor disruption	Credit card payment data is breached via an outsourced payment provider	SQL programmable script	AIR (2016)
Accidental data breach	Accidental loss of protected personal data from insured businesses	SQL programmable script	AIR (2016)
Domain Name System (DNS) provider outage	Variable outage lengths affect business continuity in insured companies	SQL programmable script	AIR (2016)
Data theft from an aggregator	An outsourced payroll firm suffers a malicious data breach	SQL programmable script	AIR (2016)
Cloud computing service provider	A malware infection creates lengthy outages in a market-leading cloud service provider	Scenario spec for regulatory reporting	Lloyd's (2016)
Offshore energy - MODUDP attack	An attack on control systems for multiple offshore drills causes oil spillage and physical damage	Scenario spec for regulatory reporting	Lloyd's (2016)
Aviation - navigation control attack	Malware causes two full passenger jets to crash at different airports	Scenario spec for regulatory reporting	Lloyd's (2016)
Marine - ballast control system attack	Compromise of digital ballast control systems causes large ships to lose control and founder	Scenario spec for regulatory reporting	Lloyd's (2016)
Cloud service provider hack	Multiple cloud service providers experience lengthy outages from a hypervisor hack	2 variants plus confidence intervals	Lloyd's/Cyence (2017)
Mass vulnerability attack	Malicious actors with access to an zero-day vulnerability in a market-standard operating system exfiltrate masses of data	2 variants plus confidence intervals	Lloyd's/Cyence (2017)
Cyber-induced fires in commercial buildings	A malicious software update allows hackers to start fires by overloaded battery management systems in common laptops	3 variants	CCRS/RMS (2017)
ICS-triggered fires in industrial processing plants	A remote hack of industrial control systems (ICS) causes fires in factories	3 variants	CCRS/RMS (2017)
PCS-triggered explosions on oil rigs	A maliciously motivated insider causes oil rig explosions and leaks after manipulating network operations centers	3 variants	CCRS/RMS (2017)
Cyber-enabled cargo theft from port	Criminals steal cargo from multiple ports by spoofing port management systems	3 variants	CCRS/RMS (2017)
Lloyd's RDS cyber - major data security breach	Multiple attacks on multinational organizations in one industrial sector	Scenario spec for regulatory reporting	Lloyd's (2018)
Cloud outage	Multiple methods of causing lengthy outages of a cloud service provider	3 variants	Lloyd's/AIR (2018)

Source: Coburn, et al (2019)

Growing Confidence in the Understanding of Cyber Tail Risk

Given the growing catalog of experience with cyber claims, insurers are becoming more familiar with and confident in considering cyber as a line of insurance. The proliferation of new PMLs since 2015 shown in Figure 19 alone is indicative of the industry's interest in developing its understanding of the threat and actively pursuing solutions to the question of maximum limits and return periods. Similarly, many insurers and reinsurers have established their own cyber boards of expertise and built internal models to estimate tail risks and the cost of risk capital. Several modelling companies are also now providing consultancy services and licensing models for specific insurance use with a specific cyber perspective. With this growing confidence, comes the expectation that the cyber insurance market will continue to grow, at least for the time being, despite the unique obstacles the risk presents.

The Future of Cyber Insurance?

There is concern the cyber market may become uninsurable — in similar cases, the government historically has stepped in as a backstop

Spokespeople for the insurance industry have aired the opinion that cyber risk may ultimately be uninsurable, as the tail risk is dangerous and too poorly understood for the private market to solve on its own. Historically, in cases where individual risks have become too costly for the industry to shoulder alone, governments have stepped in to provide a backstop. This was the case following 9/11, when size of the physical damage losses to the insurers in the U.S. was so large that governments worldwide put a practice of shared compensation into practice in the event of any future acts of terrorism. It may be that the future of the cyber insurance market is a similar risk pool or backstop provision to those set up to provide protection against terrorism in the early 21st century. This would likely be the case in the event of a major catastrophic event, or an escalation of aggression between nation state cyber teams, verging on an outbreak cyber war. For now, the issue of providing the level of protection for cyber attacks expected for corporates remains a private market predicament.

Fundamentals of an Intelligence-led Approach

'Defense in depth' network security programs need to evolve to active defense strategies as cyber risk escalates

As the speed and sophistication of the adversary continues to escalate, 'defense in depth' network security programs need to evolve to active defense strategies. Furthermore, active defensive strategies must incorporate the results of independent assessments by a second line of defense, such as a risk management entity. Across sectors, the three lines of defense model is critical to maintaining adherence to industry standards. In its simplest form, the three lines includes the first line, who owns and manages the risks to the business as well as the controls necessary to mitigate these risks; the second line who monitors the risk types and controls to ensure they are bringing inherent risk to a residual risk level within tolerance for the organization's appetite; and the third line who acts as an independent assurance function to audit both the first and second line to ensure effectiveness of risk and control management. [175]

Key drivers affecting cyber activity globally: geopolitical flashpoints, domestic issues, demographics, and economic states

The complexity of the cyber threat environment is compounded by a number of drivers, which have influenced the need for organizations to mature beyond a reactive defensive approach to a proactive, intelligence led one. To be intelligence-led is to know yourself and to know your enemy, and to be able to fully define your crown jewels and understand both the motivation and capability of potential adversaries to attack what is core to your operations. Organizations cannot apply a traditional risk management approach to cyber and expect the same level of success as seen in the way credit and liquidity risks have previously been managed. Rather, organizations need to change their approach to match the dynamic threat environment. Just as banks and clients have moved away from brick and mortar branches to online banking, so too have bank robbers moved from away from bank heists to cyber attacks to steal money from victims. As such, many banks have downsized from investing in physical security in order towards increasing the number of Security Operations Centers they have to monitor and secure their networks. Several drivers are factored into the analysis of how cyber attackers may act; however four key drivers affect cyber activity globally:

- **Geopolitical Flashpoints:** Over the last several years, countries around the world are increasingly using cyber tactics as a tool of statecraft, both in times of high conflict and in times of peace. Geopolitical flashpoints are situations in the geopolitical sphere that create an aura of unknown and prompt nation state actors to use cyber tools to further understand how other nations or even private corporations are going to respond to a geopolitical situation. Some general examples include Brexit in Europe, and the ongoing China and South China Sea conflict driving espionage activity on both sides.

- **Domestic Issues:** Within a country, a variety of domestic issues often drive the development and shape the evolution of advanced cyber tools used against both private and public institutions. The use of propaganda, or 'fake news', is one recent example of how sentiment is controlled on domestic issues of interest by governments. However, domestic issues can range from those cited as part of a political agenda to those that certain segments of the population are progressively advocating, such as gender equality, freedom of speech or the right to access the internet. Hacktivists and cyber criminals have been known to embarrass governments and bring into question the reputation of corporations by defacing websites and releasing sensitive government or corporate information obtained through hacking emails, computers, or servers.

[175] Anderson and Eubanks (2015).

- **Demographics:** Changes in demographics and domestic politics in a region have influenced how nation state actors behave. A good issue and example is healthcare. As countries face an aging population — from the U.S. to China and Russia — actors in locations experiencing these pressures are using espionage to target private healthcare organizations, pharmaceutical dispensers, durable medical equipment providers, and healthcare service companies. This is due to the need to produce healthcare products at a lower price for the growing aging population.

- **Economic States:** The overall economic health in a country or region can influence nation state actors to fulfil a need by using cyber espionage. How an industry in a host country is performing has been known to directly influence cyber attack activity. Where a nation is showing the greatest weakness or deficit presents an opportunity for nation state or even criminal actors. These actors may infiltrate nations who have demonstrated strong performance in these fields to steal intellectual property or to syphon off large amounts of cash to procure what is needed, or to fund necessary research.

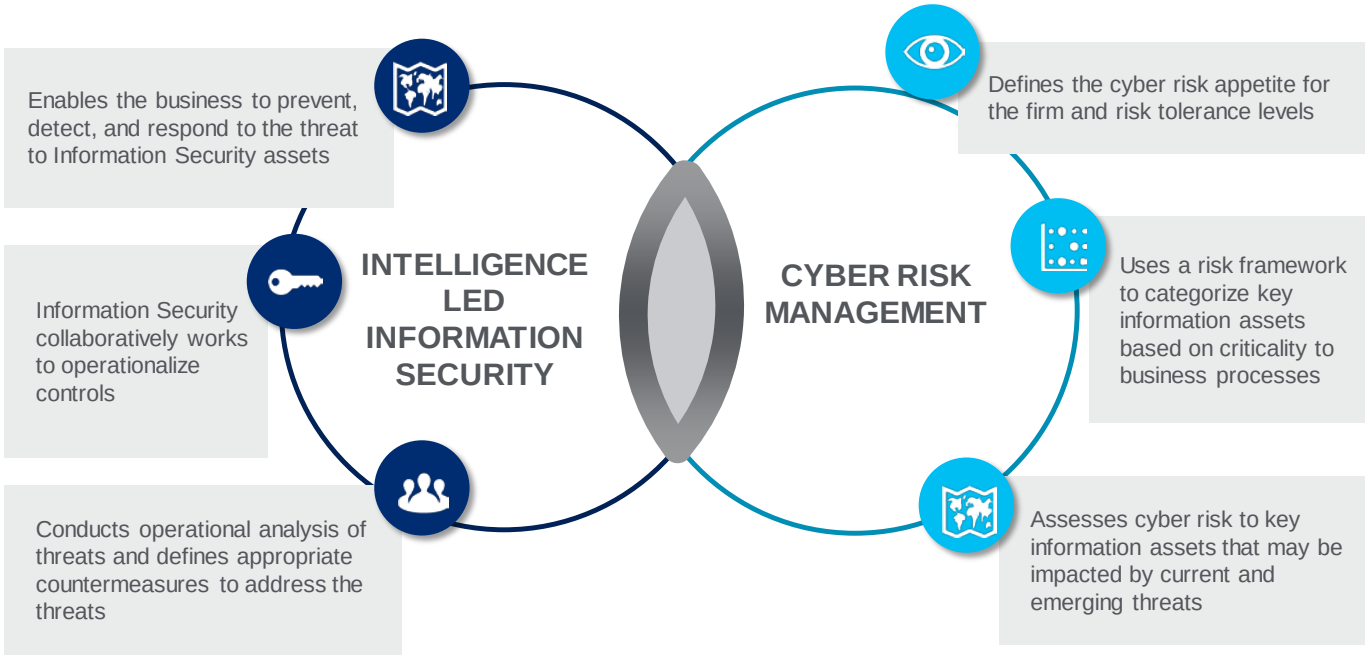
Sketching out a longer-term cyber plan helps corporations plan investment budgets for cyber defensive tools

Understanding key drivers and how they might impact an organization helps proactively build a cyber security program that can quickly scale to meet demands over a one- to two-year period. Forecasting out 24 months also helps corporations plan investment budgets for cyber defensive tools. A strategy can even be laid out over a five-year period; however it's important to recognize the need for annual updates to take into account the rapidly changing threat environment. Building an effective strategy requires a strong partnership between an organization's business lines and risk management teams to customize a cyber security program that instills trust and confidence both within the organization as well as externally to the Board of Directors, advisors, investors, and clients. A strong network defense capability is necessary to map adversarial attack activity to the Cyber Kill Chain® —a concept developed by Lockheed Martin that helps analysts identify where attackers might be located on the network. At the same time, second line risk management infrastructure must be structured to handle cyber risk activity separate and apart from technology risk.

Cyber risk must be pulled apart from technology risk as they have different key drivers

For years cyber has been treated by organizations as a natural subcomponent of technology risk; however today, cyber risk must be pulled apart from technology risk as the drivers and causes for cyber attacks differ from the causes of technology failures. Corporations cannot build an effective risk management program to address both types of risk without first understanding this fundamental difference. A blend of both technology and cyber risk programs under operational risk within an organization is optimal because of the synergies between the programs which naturally enhance an organization's resiliency.

Figure 20. Enhancing Defensive Posture by Assessing Cyber Risk



Source: Citi

Operational risk, cyber risk, and technological risk should be reviewed collaboratively instead of in silos

Collaboration between information security, businesses, and cyber risk silos will support a credible challenge to current cyber risk assessments. This review will produce actionable recommendations along with management oversight to harden the perimeter around an organization's critical assets.

- **Operational Risk:** Operational risk can be defined as the risk of loss resulting from inadequate or failed internal processes, systems, human factors, or from external events. Technology and cyber risk are types of operational risk that could adversely impact the organization.
- **Cyber Risk:** This is commonly known as the risk to a business associated with the threat posed by a cyber attack, cyber breach, or the failure of an organization to protect the most vital business information assets. Threat activity can be conducted by a variety of malicious actors, including insiders, organized criminals, nation state actors, hacktivists or cyber terrorists, each with different motives and the use of a myriad of attack methods.
- **Technological Risk:** Technology risk may refer to business risks associated with the delivery and operation of technology solutions in support of business requirements. Threats to technology may be from the failure of people, processes, systems, or other operational issues; including events relating to the design, development, and execution of technology solutions.

Figure 21. Role of Intelligence – The Intelligence Cycle

Source: Citi

With an active defense plan, defenders should have the opportunity to stop an attack at multiple stages of the cyber attack cycle

The cyber threat environment continues to be daunting considering the increase in speed and the effectiveness of attacks. In addition, cyber attacks have complex anatomies to defend against. Most say it is an impossible job to defend against a cyber actor who only needs to be successful once, whereas the defenders have to be successful 100% of the time; but if defenses are built at each stage of the Kill Chain fully covering the anatomy of an attack as part of an active defense plan, defenders actually have the opportunity to stop attacks at multiple stages of the attack cycle, increasing success of deterrence more times than the attacker suspects.

The foundational elements of an intelligence-led risk management approach include: (1) understanding the threat; (2) integrating threat intelligence & analytics into decision-making; (3) establishing a learning culture; (4) building a foundation for information sharing; (5) executing strong program management; and (6) maximizing collaboration

Integrating a risk management approach with the firm's business strategy to anticipate cyber risk early on is an example of successfully employing an intelligence-led mindset. In this case, cyber security is an enabler, enhancing the business' resiliency by being built into operations' metrics, with a commitment to creating a learning organization as the foundation for decision making and strategy development. An intelligence-led strategy can have a variation of elements; however a few are considered foundational:

- **Understand the Threat:** Gain knowledge of the adversary and their tradecraft; know yourself, identify valuable assets, and recognize challenges early in the cyber threat lifecycle.
- **Integrate Threat Intelligence & Analytics into Decision-Making:** Deliver tactical and strategic intelligence analysis that delivers knowledge and insight into the threats of greatest importance to your organization and potentially your industry.

- **Establish a Learning Culture:** Ensure there are management processes and tools that enable lessons learned and other key learnings to be raised in a collaborative environment and integrated into how you do business.
- **Build a Foundation of Information Sharing:** Increase internal and external information sharing in a trusted environment. One detected event, shared, can serve as defense for a sector.
- **Execute Strong Program Management:** Support an enterprise approach to integrated processes while conducting incident response in a learning environment.
- **Maximize Collaboration:** Promote collaboration and partnership both internal and external; sharing best practices and benchmarking against peers and competitors. Operate your cyber security program in a non-competitive environment.

Employing an intelligence-led strategy means actively keeping up on threat activity. The analysis of this activity should then be integrated into decision making. For example, threat information may be used to drive risk management challenge activity to assess if controls that were implemented 12 months ago to mitigate the tactics and techniques used by threat actors are still adequate in today's threat environment. Being intelligence-led also means embracing a learning culture to critically self-evaluate actions taken, such as in response to a cyber event. Incorporating these learnings makes an organization stronger, but should also be shared out to industry partners. This is because information security is no longer considered a competitive advantage among organizations. Given the size and impact of an event, it is generally accepted that when one organization within and even across sectors is attacked, the security of national interests is potentially at stake. Executing strong program management therefore ensures the consistent application of standards within an organization to govern its cyber security program.

Additionally, there must be an emphasis on collaboration across all three lines of defense, ensuring that departments within an organization work day-to-day in unison by recognizing that being constantly challenged serves to strengthen the organization as a whole. Furthermore, within an industry, when corporations act as partners, they come together to fulfill a common mission to prevent attack activity. By doing so, they are not only defending themselves, but by extension, their clients, investors, and other key stakeholders through the application of sound cyber security practices.

Defining a Cyber Risk Management Strategy

An intelligence-led mindset allows for a strategy with a common purpose across all three lines of defense

With an intelligence-led mindset, an effective cyber risk management strategy can be built. Without a strategy, a common purpose across the three lines of defense is lost. The strategy, at a high level, should incorporate governance, which is centered around implementing a framework with policies and standards. The framework should be flexible to enable an organization to scale its assessment responsibilities depending on the appetite that is set at the top of the house for risk management. Key components of a framework may include establishing the scope of the program, defining the risk appetite categories, setting forth a target operating model that includes management processes for applying oversight, and defining the key assessment tools that will support evaluating how well a business is doing in applying effective controls to reduce inherent risks.

Establishing a Risk Appetite

Establishing a risk appetite is critical for an effective cyber risk management program

In order to carry out effective governance of a cyber risk management program, it is critical to establish a risk appetite. This sets the thresholds against which the organization will measure how well it is performing in managing its cyber risk. Depending on the type of business an organization engages in will dictate what the core technology and cyber risks are, versus the identification of key enterprise level operational risks that have a technology and/or cyber risk component. By way of example, system availability and data security represent core technology and cyber risks. The application of controls to ensure confidentially, integrity and availability (CIA) of systems and data directly influence the reduction of inherent risk to an acceptable residual risk, in line with the organization's appetite. In contrast, data quality, fraudulent activity, transaction processing and legal/regulatory risks are fundamentally managed by other operational risk types, but under which technology and cyber events can result in failures. Taking the time to define core technology and cyber risks helps to prioritize areas of focus for a firm to invest its resources.

Defining an Operating Model

A dynamic approach to cyber risk identification is required

Once the core risk appetite categories are established, an operating model can be defined to capture the management processes that will enable a credible challenge of the way an organization manages its risk within its established appetite. There is no one-size-fits-all model in order to allow for the flexibility needed by risk management teams to build according to their resources and scope of their program. In some organizations a risk management component may be made up of several teams, each assigned to review a particular line of business; however in other organizations, risk management may just be a handful of professionals because the nature of the business has a singular focus. Regardless of the size of the risk management function, when it comes to performing cyber risk identification, a dynamic approach is required. For example, incorporating the viewpoints of risk assessors, emerging technology analysis, and business product manager insights may result in identification of risk in deploying a new product across an organization's enterprise instead of confining it for a specific application. This enables incorporation of necessary controls before product deployment to ensure systemic risk is appropriately managed.

Assessing and Measuring Cyber Risk

Clearly defined processes for assessing and measuring identified risks is also critical

Processes for assessing and measuring identified risks should be clearly defined to ensure there is a repeatable methodology with documented evidence to support findings. At a minimum, an organization needs to develop the capability to challenge how its business lines have assessed the risks to its crown jewel assets and the application of controls to reduce those risks. One way to achieve this is through conducting scenario analyses of possible cyber events that could impact internal operations. As resourcing allows, organizations can also benefit from conducting lessons learned for both internal as well as external events. Internal events could be near miss incidents where a business was almost impacted, such as a corporate treasurer receiving a fraudulent instruction to wire millions but did not do so because they detected an error in the instruction.

Equally important is conducting lessons learned from events that happen to other corporates. For example, an energy provider lost their ability to power part of a city due to their systems being under a ransomware attack wherein a cyber actor encrypts the system and demands a ransom to unlock it. Understanding how the energy company was able to roll onto backup servers to work around the affected system, as well as communicate reasons for the power failure and how incident responses were then conducted, can help other companies be better prepared.

It is then the responsibility of the risk management teams to challenge whether or not these scenarios and lessons-learned assessments are being done and, if appropriate, action has been taken to reduce the potential for similar events to negatively impact their organization.

Managing, Monitoring and Reporting Cyber Risk

Forward-looking indicators are critical for monitoring risk and it is essential results of monitoring are documented

Having set tolerance levels for risk in the firm's appetite as well as identifying and assessing the cyber risks to critical assets or business processes, organizations should then prepare to manage, monitor, and report on those risks. Establishing a strong governance framework that incorporates policies and standards to guide how the organization manages its technology in alignment with its appetite will set a solid foundation. In order to then monitor how well the policies and standards are being adhered to, a system to review outstanding issues is critical. Understanding the risk acceptances a firm has decided to take and the plans for remediating the accepted risks over a defined period of time holds the business lines accountable for resolving risk that could ultimately introduce catastrophic damage.

In monitoring for risk, forward-looking indicators are critical. Indicators are a key tool for understanding if a business is performing within the thresholds defined in a risk appetite statement. Every organization has dozens of metrics to draw from for measuring performance; however when it comes to measuring risk performance, organizations may find the metrics they track are not actually measuring what matters. Although a bold move, it may be necessary to stop measuring current activity and reassess what measures can capture performance that demonstrate a firm is within its risk appetite.

It is essential that results of monitoring are documented in a repeatable report so all key stakeholders understand the areas of vulnerability that must be prioritized and addressed. Reporting is also not a one size fits all format as different audiences need to see different slices of the data in order to understand what actions they can take to close gaps and mitigate risks. For example, a business may be measuring and reporting on the risk of engaging with third parties around the protection of confidential data; however to be compliant with the firm's low tolerance level for data breaches as stated in its risk appetite, indicators of data security may need to be customized for fourth party relationships vendor providers frequently engage.

Sustaining Success

Driving for change and progress is challenging in any ordinary environment. In today's cyber environment, with the constant flow of emerging issues, being successful over time is even more complex. Many organizations view cyber as one of their leading risks — often because the drivers and threats are unpredictable and the impacts are challenging to quantify. The focus on this risk often leads to constant asks from senior leadership, clients, and Boards about cyber-related issues plaguing the industry and other fields.

This level of interest will not wane — it may dissipate as other issues crop up, but confusion and concern will persist. Organizations and their leadership can take this interest and leverage it for good by promoting awareness, investing in sound risk management practices, and positioning their cyber function as a differentiator in marketing products or services; however the most challenging effort will be for organizations to contribute to the common good by creating partnerships through shared resourcing efforts in order to share knowledge on cyber threats and risks threatening an industry.

But perhaps the most critical factor in defining an organization's success in reducing cyber risk will be its ability to implement a strong internal interaction model between its business lines and risk management professionals. While the business lines are responsible for identifying, assessing, monitoring, and managing its cyber risks, risk management must take a step back to challenge each of these areas without impeding cyber security efforts. Some of these efforts will be in parallel to what the business is doing to assess and manage its cyber risk, which results in a 'belt and suspenders' approach — organizations actively reinforcing their defensive posture by ensuring all risks and drivers of threat activity have been considered, risk mitigation actions have been taken, and monitoring via forward looking indicators is activated to ensure residual risk is being driven to an acceptable level in light of the current threat environment.

Spotlight on the Criticality of Talent

Smart people need to be leveraged in a cyber risk strategy and talent needs to be built around cyber technology and risk

People, process, and technology are often the three pillars of any successful organization operating in the global economy. From operating small businesses to multinational and diverse corporations, if smart people are not leveraged following sound processes that use technology appropriately, it can be a challenge to generate successful outcomes in a sustainable manner. In a technology or cyber role, or really in any emerging field, people are often the cornerstone of these three pillars as many organizations lack existing processes or technology; therefore they need talent to build these elements. Within the people pillar, leaders struggle with many variables but understanding skillsets, recruitment, retention, and strategies for bringing a function to sustainable operation are often quite challenging.

Knowing Yourself is Often the Biggest Hurdle

Due to the surge in demand for 'cyber' professionals, there is no shortage of educational programs, certifications, or enrichment opportunities to prepare for a career in cyber security. The sheer volume of talent needs to grow to keep up with the digital revolution — in 2015, Frost & Sullivan assessed that the global economy will have a deficit of 1.5 million cyber professionals by 2020. In order to recruit smartly, management within an organization needs to be better attuned to precisely what skills are needed to address the demands of the industry.

Team leaders for cyber require a strategy and vison to execute against and must be savvy in the processes needed to deliver against that strategy

When an organization is designing a cyber security program, the most critical input is often the assets that must be protected, juxtaposed against the risks and threats targeting them. It's critical that building a team follows a similar approach — leaders require a strategy and vision to execute against and must be savvy in the processes that need to be performed to deliver against that strategy. They have to know their own organization and how to capitalize upon efficiencies and staff the components with employees of diverse backgrounds that can navigate often complex environments to deliver a result.

For example, a security strategy office may handle policy, governance, audit, and possibly some central functions like vendor management. While the strategy office is often a cost center within an organization that does not deliver core security functions to clients, leadership should consider talent with focused specializations that can be leveraged across functions rather than generalists in one area. In this example, a high-potential Security Operations Center (SOC) analyst that has worked extensively on network security could be a good candidate for a mid-level strategy role as they would have prior vendor relationship experience, have actioned corrective action plans from governance leaders, and have implemented programs which executed against information security policies. With guidance and mentorship, an analyst with this experience has the capability to drive development of stronger approaches to cyber security that wouldn't be possible from a generalist. Cultivating this technically-savvy talent and advancing their skillsets is central in building and sustaining successful teams that not only deliver against core functions but also address core needs that are unique to an organization.

Finding the Right People and Keeping Them

Recruiting and retention are often efforts managed by different teams within corporate human resource functions. While these efforts are sometimes prioritized, they are largely treated in a domino-style approach focusing on hiring first then figuring out how to retain.

Diversity among the talent pool is the lynchpin and core dependency to hiring the right people and retaining them

Diversity among the talent pool is the lynchpin and core dependency to hiring the right people and to be able to retain them. Advancing a mix of diversity in skillsets, culture, location, education, and professional background addresses the core shortage of cyber talent. Furthermore, a diverse organization is more agile and often better prepared to weather any changes in mission, leadership, or environment.

Driving a change in cultivating cyber talent will require that both private and public organizations move into the driver's seat to shape how the technology and cyber educational system is building future leaders. While the foundational training is often provided, the current educational process — with a rich focus on information technology converted to cyber security tracks — needs shaping to clearly illustrate the career path needed for modern-day talent.

By advancing clarity around the career path in corporate entities, more diverse candidates will be increasingly likely to identify opportunities and be attracted to the rich work environment. For example, modern-day cyber security formalized educational programs should offer technical foundations with multiple layers to advance understanding of the environment – intelligence, strategic analysis, policy, governance, incident response, leadership, data science, mobile, innovation. The common pitfall in this approach is disjointed layers – each element should be presented through the lens of cyber, not solely information technology.

Along with diversity and more formal educational programs, corporate managers need to better engage with their communities to constantly be looking for synergies across skillsets that can be leveraged and transferred to their programs and be involved in steering groups and advisory committees driving educational change. Peers and employees will recognize this engagement and when they observe leveraging of synergies in skillsets, other managers will be encouraged to follow suit.

Section 4: Technology Solutions

Current IT Solutions

Securing the Platform – Change is the Menace to Stability

With much of what we highlight here being a technology problem, it is logical to expect a technology solution. But as we have shown in the pages before, technology is not the only solution — people, process, governance, management attention, and other means are also part of the solution

Much of what drives new security challenges are changes in the underlying technology architecture. As noted in the early science-based novel Brave New World *"change is the menace to stability"*. It has generally been recognized that a mature IT architecture is easy to secure while new, still evolving architectures introduce new security challenges. As new architectures are born, evolve, and ultimately go mainstream, innovation is usually the primary basis for differentiation amongst early entrants to the market. What usually falls to secondary or tertiary priority is security and this has occurred time and time again.

History Shows Platform Players Haven't Solved Problems Adequately

Security in PCs didn't become a focus until 10-20 years after they entered the mainstream

As the speed of technology innovation accelerated with the proliferation of PCs and broad-based networks, security quickly became an afterthought in the development of these platforms. The rapid advances in functionality of the PC and the cultural priority of putting computing power in the hands of the user meant that new features and 'openness' were put on the front-burner. As soon there was a means to transmit malicious files, there were computer viruses that spread from machine to machine through a means that brought significant productivity (sharing of information with floppy disk). While the PC began to enter the mainstream in the mid-1990s, it was not until the release of Windows 10 about 20 years later (2015) that Microsoft bundled effective security defenses for the PC into the operating system. Some would point to Microsoft's "Trustworthy Computing" in 2002 that halted product development for some time to focus on security as a positive step along the way. It is hard to determine what impact this development had, however, the Microsoft PC operating system remained the primary source of vulnerability for many years to come in the years that followed. We believe this shows, even with focus from a platform player, the extraordinarily difficulty in balancing security as a priority while keeping pace with the competitive demands around functionality that pervades the technology sector.

It was a similar case on the network side where security was 'added on'

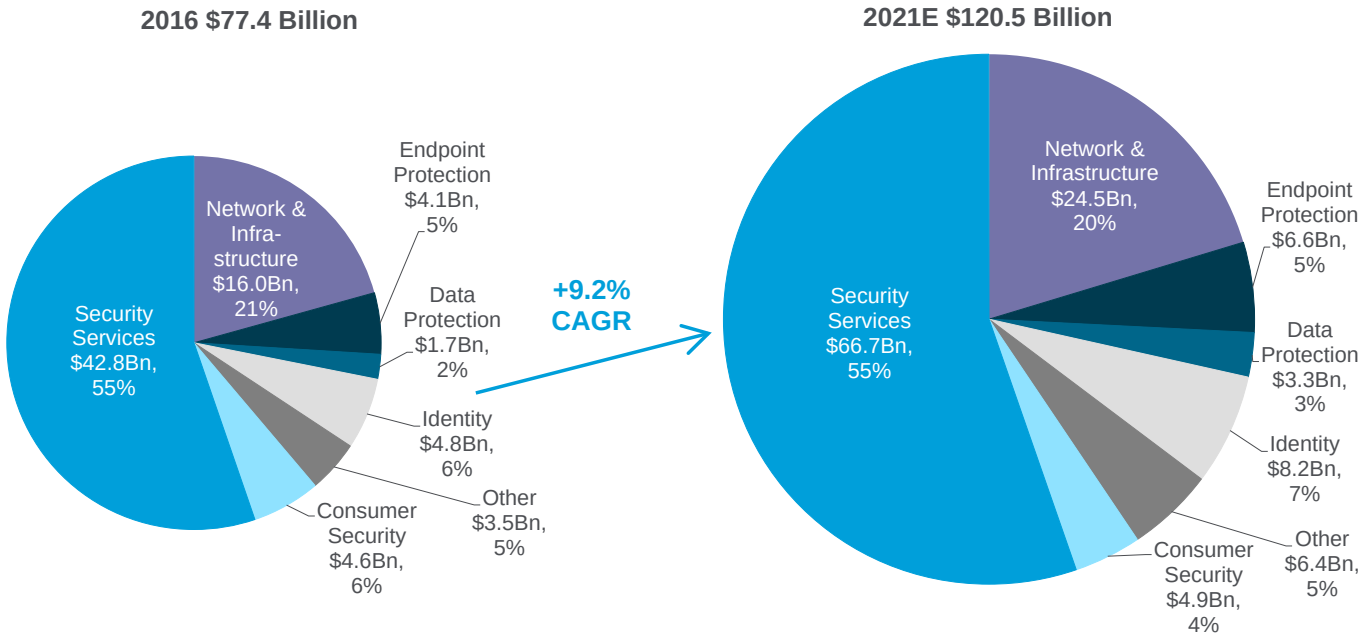
Similarly, on the network side, Cisco out-executed its early competitors in the Ethernet switching and Internet routing markets to become the dominant market player, a position it still holds today, according to Synergy Research Group. Unfortunately, security was never designed into the fabric of the network. Instead, after Cisco established its dominant position in networking in the late 1990s, it began acquiring security assets. This technology was not integrated into the network and instead had to be 'added on' in a somewhat 'clunky' fashion.

Without a focus on security by PC and network providers, a large add-on security market grew

In both the example of the PC and the network industries, large markets grew up around providing security as an add-on to these important technology components to counter vulnerabilities exploited in early attacks. In the case of the PC, this was signature-based anti-virus technology. In the case of the network, while Cisco embedded a simple packet filter and access control lists into routers, the more sophisticated 'stateful inspection' technology in the modern firewall was invented elsewhere.

We see this repeated over and over. Microsoft's dominant position within the email market (Exchange/Office365) has happened without it solving the security issues that leave email as the most common 'vector' for cyber-attack. The dominant digital document format 'pdf', with Adobe 'shepparding' the standard, has never dealt with some of the security issues that attackers use to gain control of a system that hosts pdf documents. In more recent times, the Android operating system has become notorious for having security vulnerabilities that attackers directly exploit or are exploited by applications that users download.

Figure 22. Security Addressable Market



Source: Citi Research, Gartner, IDC

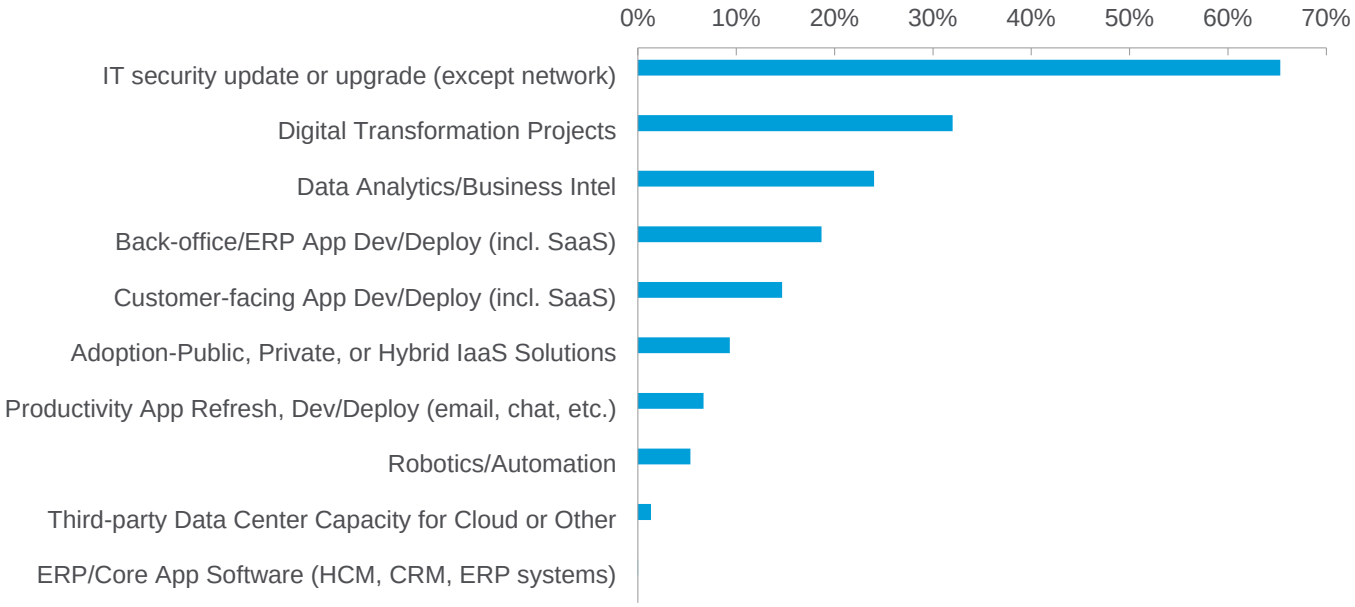
Necessity is the Mother of Invention for the $80B IT Security market

The IT solutions and services market has now reached almost $80 billion

One might say that, as a result of the platforms not solving the problem, one of the more vibrant technology markets has been created. This market, centered around IT security solutions and services, has grown to be an $80 billion market (2018E), with growth rates (~9% year-over-year in 2018) that are consistently above the growth rates of the overall IT solution market (3%-5% year-over-year) and the even faster-growing software market (7%-8% year-over-year). This market is also host to one of the largest number of individual vendors, most of which are small and driving the tip of the spear of innovation in the market.

Growth in this IT security market continues to be ahead of related broader IT segments like software, services and networking. The market has attracted disproportionate venture capital investment and had seen a significant number of strategic acquisitions, with enterprise IT incumbents as the buyers.

Figure 23. Top 10 Areas of Increased Investment Priority Over the Next 12 Months ('lower' netted against 'higher' priorities)

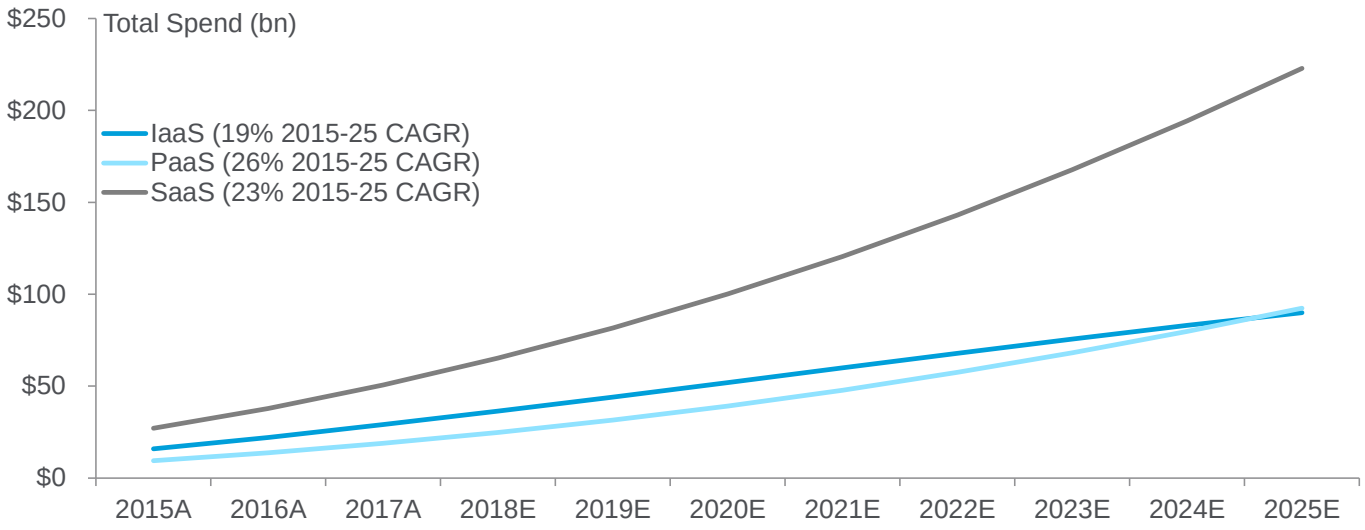


Source: Citi CIO Survey March 2019

Public Cloud Growth Will Be Next Force that Impacts IT Security Market

We've seen rapid growth in 'hyper-scale' public cloud offerings, notably from the likes of Amazon (AWS), Microsoft (Azure), and Google (Google Cloud Platform). The platforms are commonly thought of as offering 'infrastructure as a service' (IaaS, raw technology elements like compute and storage 'on-demand') and 'platform as a service' (PaaS, elements used by a developer delivered 'on demand'). We also see broad proliferation of 'software as a service' (SaaS, application software that is delivered as a finished product, 'on-demand').

Figure 24. Citi Cloud Spending by Category (Excluding 'Born in the Cloud' Workloads)



Source: Citi Research

Growth of next-generation technology like public cloud and SaaS suggest there will be a significant 'add-on' security market for both

The sheer size of the public cloud market and the adoption by enterprise customers that are using these public clouds to run their business, suggests there will be a significant 'add-on' security market. This likely comes as a result of the use of public cloud to operate in sensitive customer or competitive data — revenue-generating systems running in public cloud (e-commerce, online marketing, etc.), and the potential reputation damage of a cyber-attack are now inner-twined with an additional business partner (the cloud provider). While the public market is in the likely earlier phases of adoption, commitments from enterprise customers are accelerating and this is when we would expect security demand inflects.

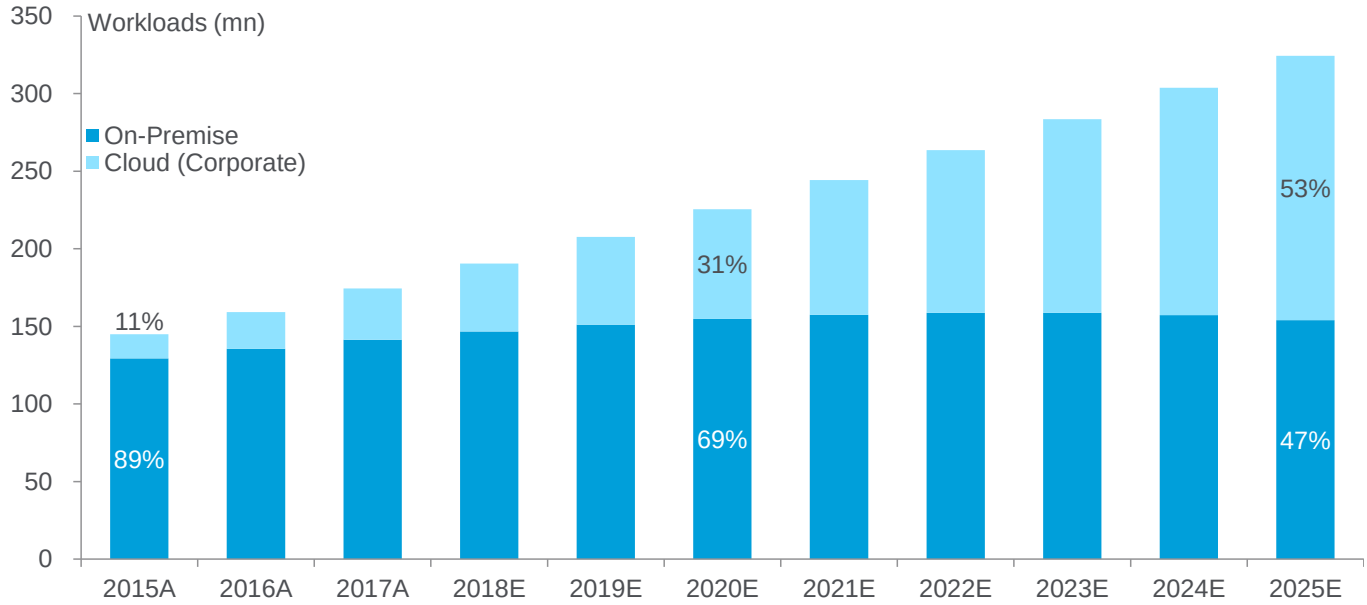
Securing the Public Cloud Many Times Requires a New Approach

Public cloud services differ from on-premises (on-prem) architecture in that much or all the technology components are resident in the data center of the IaaS, PaaS or SaaS providers. In this way, many times the end-customer (corporate / enterprise) cannot chose the security technologies that are used within the public cloud environment. This is not unique to security and no different in infrastructure areas such as storage, compute, and networking componentry. This dynamic, at a minimum, changes how the cloud must be secured as compared to on-prem.

Initial cloud adopters are comprised of less mission-critical workloads which generally carry fewer security requirements

In the early era of cloud adoption, we are seeing a number of changes in security. We are likely in the early days, as we estimate just ~20% of enterprise / corporate workloads are in public cloud. Beyond this percentage, we believe it is the less mission-critical workloads, which generally carry fewer security requirements that have initially appeared in public cloud.

Figure 25. Workload Growth Driven by Cloud (Excludes 'Born in the Cloud' Workloads)



Source: Citi Research

Virtual firewalls can be deployed as a virtual machine on any cloud

What is the new approach? First, along with the 'virtualization of everything', we are seeing the virtualization of security; primarily network security functions. With the firewall one of the largest categories of technology in securing traditional enterprise networks, we are seeing significant growth in 'virtual firewalls', which can be deployed as a virtual machine on any cloud.

In a world where networks have become very 'flat' (all objects connected at the same level in the 'hierarchy') and even abstract (connections between IT components are a logical API, not a physical network), there is a need to segment the virtual network more finely than a firewall can provide. This has led to firewalls at the 'workload' level and 'firewalls' that apply policy using native public cloud capabilities. Suffice to say, the firewall market is changing quickly and this will require investment from the all major players in the market.

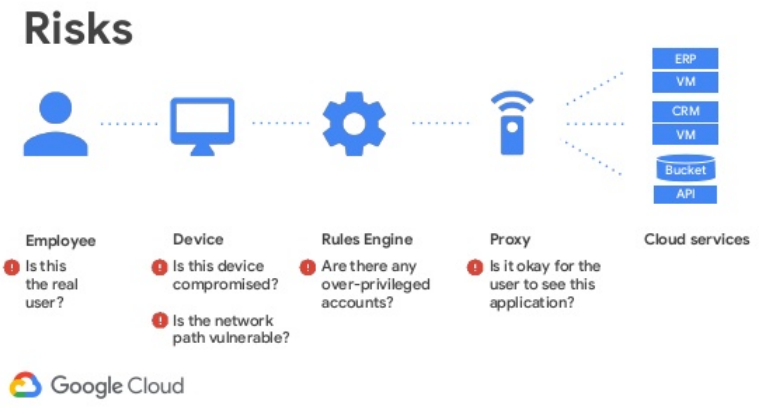
An increasing focus on web protocol has led to a growing cloud access security broker (CASB) market

Next, we are seeing deeper inspection of web traffic, especially given the fact that most SaaS-based applications ride over the web protocols (HTTP and HTTPS). Beyond this focus on web protocol, there is a change in the orientation of traffic inspection from looking at network ports and protocols (which are less obvious in cloud) to understanding the application, what its behavior is and how that compares to stated security policy. The most new technology here is in the 'cloud access security broker' (CASB) market. Ironically, with HTTP becoming the 'new network' (with all modern applications essentially riding over this protocol), the CASB and traditional web proxy functionality (at least the security component there) are converging with the firewall. CASB is increasingly extending outside the reach of the firewall and relying on native connection into a cloud service. Instead of monitoring traffic in and out of a network (HTTP or otherwise), the cloud application program interface (API) is the key control point. As we discuss later, this is a critical, yet still-evolving and therefore challenging integration surface to leverage in securing the cloud.

With increasing public cloud uptake, identity has increased in importance

Lastly, identity is coming to the fore as having renewed importance in the public cloud. With users sometimes inside the corporate and many times outside, it is challenging to connect users with the right applications using a trusted network. Instead, it is important to establish who a user is (including when their environment is changing – PC, mobile, remote) and what applications (and application sub-components) they can connect to. This security model is more relied upon inside organizations that have built their IT architectures in the last 10-15 years. The most famous such model here is Google's 'BeyondCorp' security framework in which even 'internal' Google networks as semi-trusted, but never assumed to be fully secure.

Figure 26. Google's BeyondCorp Security Framework



Source: Google

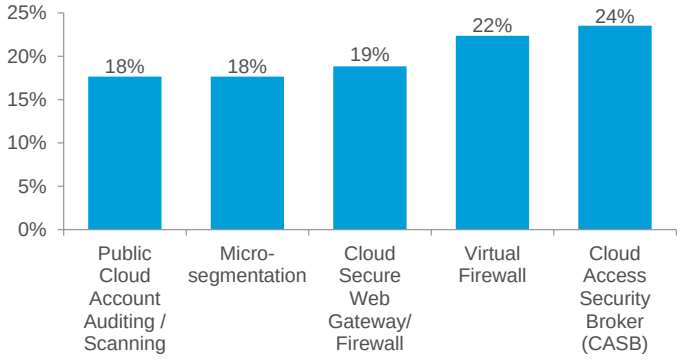
Critical to this architecture is identity management technology. Cloud native technology here is nascent and prior generations of technology in this area, is very platform specific, with solutions focused on mainframe, client server and web architectures. There is a significant challenge around both dealing with new complexities of the cloud and also a solution that is holistic enough to tie together the legacy that still represents the majority of systems that most large organizations rely on to conduct their business. We expect to see a significant battle over identity management from the hyper-scale cloud providers, as well as independent providers, that are able to provide 'cross-cloud' identity.

Survey Results Paint Picture of Early Evolution of Cloud Security

Virtual firewall and cloud access security broker (CASB) are likely to lead in terms of new security technology maturity and adoption

Cloud security is comprised of a growing collection of technologies aimed at securing cloud applications / SaaS and cloud infrastructure / IaaS ('security for the cloud). This product market is still nascent and we see customers struggling to find for a complete strategy based on existing tools. We see solutions such as Virtual Firewall and Cloud Access Security Broker (CASB) leading maturity and adoption. Separately, customers are also adopting traditional security controls that are delivered from the cloud ('security in the cloud) such as hosted web proxy service.

Figure 27. Which Do You Plan to Buy Over the Next Year? (% Selections)



Source: Citi Research

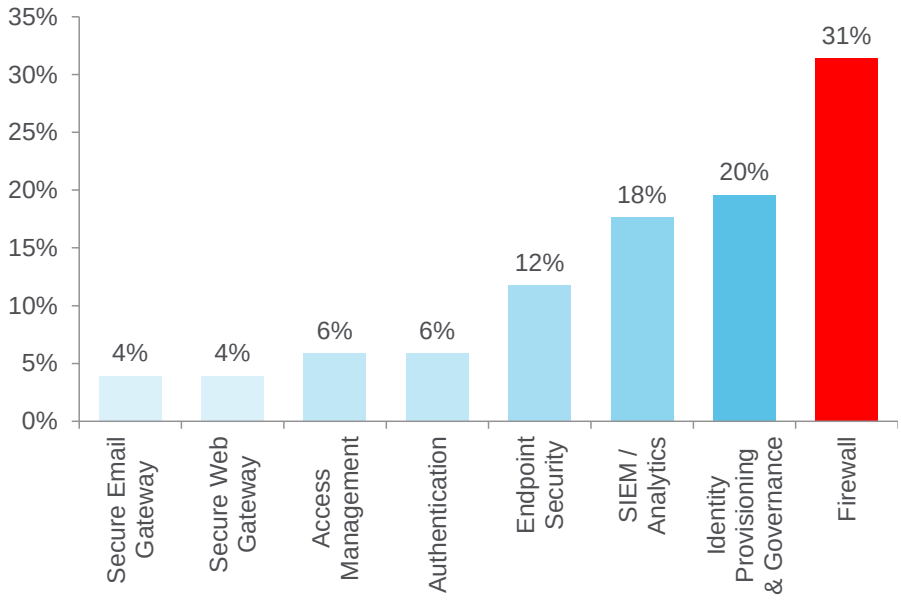
Figure 28. How Would You Rank the Maturity of Solutions Aimed at Securing the Cloud (% of Respondents)

	Very immature: and fragmented; no good solution out there yet	Immature: but showing signs of significant improvement	Satisfactory: but room to improve	Mature: I have all tools necessary to comfortably secure the cloud
Virtual Firewall	18%	29%	45%	8%
Micro-segmentation	18%	31%	41%	10%
CASB	16%	31%	41%	12%
Container-based Firewall	20%	35%	35%	10%
Public Cloud Auditing/ Scanning	14%	39%	41%	6%
Total	17%	33%	41%	9%

Source: Citi Research

While cloud adoption is enabling emerging technologies such as CASB, virtual firewall, and microsegmentation, it is also viewed to have a negative impact on traditional, on-premise security infrastructure spend. Network security and specifically firewall spend is viewed as most vulnerable here. The main idea behind this is as core infrastructure migrates to public cloud and SaaS adoption grows, compounded by a mobile workforce, the need for a traditional perimeter (and firewalls protecting it) is lessened and datacenter footprints contract.

Figure 29. As You Transition to Cloud Infrastructure, Which Area of Security Would See the Most Negative Impact (Total Dollar Mount of Spend, % of Respondents)

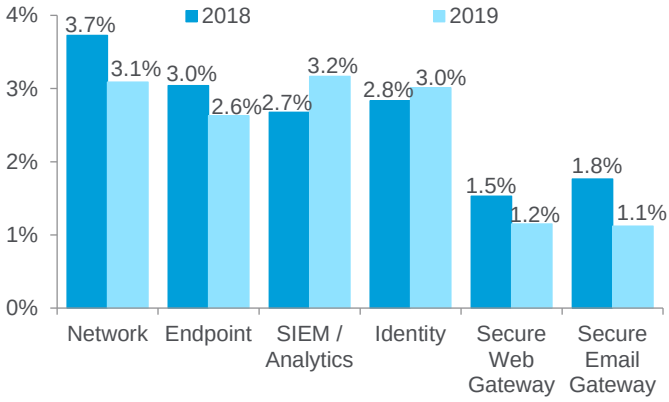


Source: Citi Research

Our surveys find that firewall continues to anchor core enterprise security strategy, despite new available technology

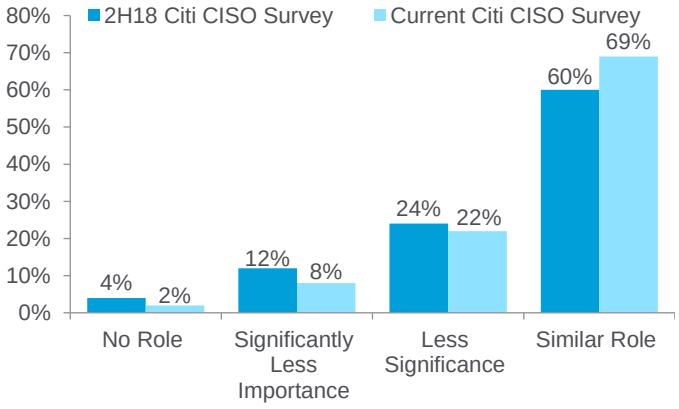
Despite this long-term view, firewall continues to anchor core enterprise security strategy and we have found incremental cloud security areas (such as virtual firewall) to be largely additive in the near-term. Our survey supports this with customers expecting firewall spend growth in-line with other major priorities (SIEM / IAM), higher mix of customers now expecting a similar role three years from now, and a lower mix of cloud services replacing appliances vs. prior survey.

Figure 30. Average Segment Growth Rates



Source: Citi Research

Figure 31. In 3 Years from Now, Firewall Technology Will Have... (% of Respondents)

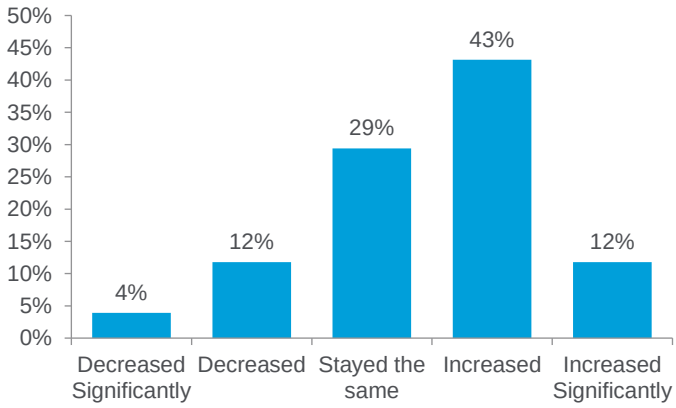


Source: Citi Research

The ever increasing number of vendors and solutions in the market is fueling debate around product best-of-breed and platform approach in security. The value of higher efficacy point solutions is typically weighed across benefits of platform integration, shared telemetry, and ease of deployment. Ultimately, we do not see this debate getting settled given the rapid product innovation cycles required to address an evolving threat landscape.

This dynamic is driving an influx of new technologies (and VC funding / startups outlined above) which understandably take time to integrate into platforms. Therefore, despite an organizations' desire to consolidate products, we see vendor counts increasing. Over time however, as product maturity develops, we have seen point solutions effectively get consolidated into broader platforms. Certain markets are naturally more susceptible to consolidation based on the level of difficulty of integrating and deploying the technology. Network security is one category where platform consolidation has been largely successful with network Sandbox and Intrusion Prevention Systems (IPS) as recent examples. Endpoint security is also a segment that has historically consolidated rapidly (antivirus, device control, host integrity, etc.) onto a single agent. We see customers now prioritizing consolidation of a new wave of 'Next-Gen Enpoint (NGEP)' technologies.

Figure 32. Has the Number of Security Vendors You Are Buying From Increased, Decreased, or Stayed the Same vs. a Year Ago? (% Respondents)



Source: Citi Research

Figure 33. Please Describe Your Efforts to Consolidate Vendors, or Willingness to Expand the Number of Vendors from Which You Purchase Products and Services (% Respondents)

	Aggressively consolidating vendors	Would like to consolidate vendors but not actively doing	Number of vendors stable	Would consider adding new vendors with innovative product	Actively adding new vendors
Network Security	33%	20%	37%	6%	4%
Endpoint Security	35%	24%	24%	8%	10%
Security Analytics SIEM	29%	16%	35%	10%	10%
Identity & Access Management	29%	14%	35%	8%	14%
Secure Web Gateway	22%	16%	49%	12%	2%
Secure Email Gateway	22%	16%	49%	12%	2%
Total	28%	17%	38%	9%	7%

Source: Citi Research

We see large tech incumbents as the most likely suitors to consolidate security vendors in the market

Similar to other areas within software, we see large tech incumbents as most likely suitors to consolidate security vendors in the market. We also expect cloud hyperscale vendors to be aggressive as both a way to 'secure the platform' but also take on the security market more directly. The strategic focus of these vendors is geared towards the high priority, non-appliance areas mentioned above such as Identity, SIEM / Analytics, and cloud security.

Will the Public Cloud 'Platforms' Be Significant Players in Security?

With the IT architecture changing and with IaaS, PaaS and SaaS players as the drivers of this change, it is reasonable to think the likes of Amazon, Microsoft, Salesforce.com and others will have a hand in solving problems such as security, in this new environment. We see both IT security market incumbents, as well as investors, debating this trend with a number of forces both pushing towards and pulling against these platform providers playing a significant role.

In terms of what is driving in favor of a prominent role, we see many of the same forces as the past, as well as some new factors, that are unique to public cloud. In our view, these forces combined are likely to result in the cloud platform players, especially those in the IaaS and PaaS markets, playing a more significant role than we have seen in the past.

Drivers Suggesting Cloud Players Will Play Prominent Security Role

It is somewhat over-commented, at this point, that public cloud is having a significant impact across the IT landscape. However, we believe many of attributed reasons that are pointed to really do have a lot of validity and are highly relevant when it comes to the role impact public cloud players could have on the security market.

All execution of code, storage of data, and inbound / outbound network traffic goes through the data centers of public cloud providers and they have first-hand visibility on interactions

Most profoundly, all execution of code, storage of data, and inbound / outbound network traffic goes through the data centers of public cloud providers and they have first-hand visibility as to these interactions. Even if their visibility is at an aggregated or anonymized level, the fact they see all of what is happening across all their customers, puts them in a unique position. This potential even extends into SaaS applications that are built on top of a hyper-scale public cloud, such as CRM recently 'going live' on AWS in Canada and other SaaS providers standardizing on AWS and to a lesser degree Azure and Google Cloud Platform (GCP). In the past, platform players have not had real-time visibility, instead, at best seeing logs and other remnants of interactions in support situations. With all interactions at least starting or ending in a public cloud facility, the provider can collect information in real time, analyze it and act on it, all within its own four walls. It is more of a question of whether the cloud providers here can execute on providing this service and whether customers want them empowered to do this. We note that, recently, Microsoft (Sentinel) and Google (Backstory) released products in the 'cloud SIEM' market, which brings together both the events they see from all code executing on their platform, as well as the 'big data' capabilities inherent in cloud.

Thus far, the public cloud approach has been mostly to partner with pure play security companies and with their customers in a sort of 'shared security model' (the AWS moniker for their security approach). This partnership approach has, at its center, the necessity for the public cloud providers to open up their services, to give customers and security partners the ability to gain visibility into the behavior of services, and also the ability to make a configuration or other change to the public cloud environment through rich APIs.

Many times the business is the buyer of public cloud services vs. traditional IT relationships with on-prem suppliers therefore more holistic security solutions may be required

In addition to this architectural difference, we note that many times the business is the buyer of public cloud services, vs. traditional IT relationships with on-prem suppliers. As a result, the public cloud providers may be asked to sell more holistic solutions, as we see from the most strategic on-prem suppliers bundling products together in solutions. The driver of this is that suppliers that provide discrete solutions in individual markets (an application, storage, certain developer platforms) are not in a position to tie all these products together with a security offering. The broader, pubic cloud product line lends itself better to be secured by offerings that are not 'point product' in nature. This still will require the public cloud providers to deliver effective solutions in security, something that has been more challenging for the diversified IT suppliers to do. However, we believe the public cloud providers have an even more permissive license from customers to play this role.

U.S. Infrastructure

Public data center companies such as Interxion, Equinix, and Digital Realty, provide space, power, and cooling for their enterprise customers IT equipment. This enables customers to store data, quickly connect to other companies or individuals to exchange data, and connect to cloud resources such as Amazon and Salesforce. Essentially, the data center can be thought of as the nexus where data is stored, exchanged, and transmitted.

Data center companies take a number of different approaches to securing customer data. Most data centers are protected with physical security, including: non-descript buildings, fencing around the facility, security checkpoints, guards (sometimes armed), security cameras and monitoring rooms, barriers around customer equipment, and strict access privileges.

Additionally, data center rooms are continuously monitored for any sudden changes in temperature, condensation, smoke, or changes in power that could compromise customer equipment and data.

From a software perspective, most data center firms leave the non-physical security of the data up to their customers. Enterprises will often utilize security software in addition to the physical security provided by data center firms. In this sense, data center operators like Interxion, Equinix, and Digital Realty are truly 'neutral' and do not interfere with the software that their enterprise customers utilize within their IT equipment.

In May of 2018, the 'General Data Protection Regulation' (GDPR) took effect. This law provides a framework for how companies across Europe will handle private data on EU citizens. The regulation also applies to data on EU citizens that is processed outside the EU. At its heart, the additional regulatory framework provided by the GDPR around processing, storing, and sharing customer data may entice enterprises to further decentralize how they store data, by moving away from a centralized hub into a more region-by-region format. As data becomes more decentralized, this could help European data center and colocation demand on a country by country basis. We believe this will benefit data center firms with a retail-centric presence and European exposure. The scaling of cloud infrastructure and services by firms across Europe should also provide an additional tailwind to data center providers as enterprises look for platforms where they can connect to cloud resources inside data center facilities.

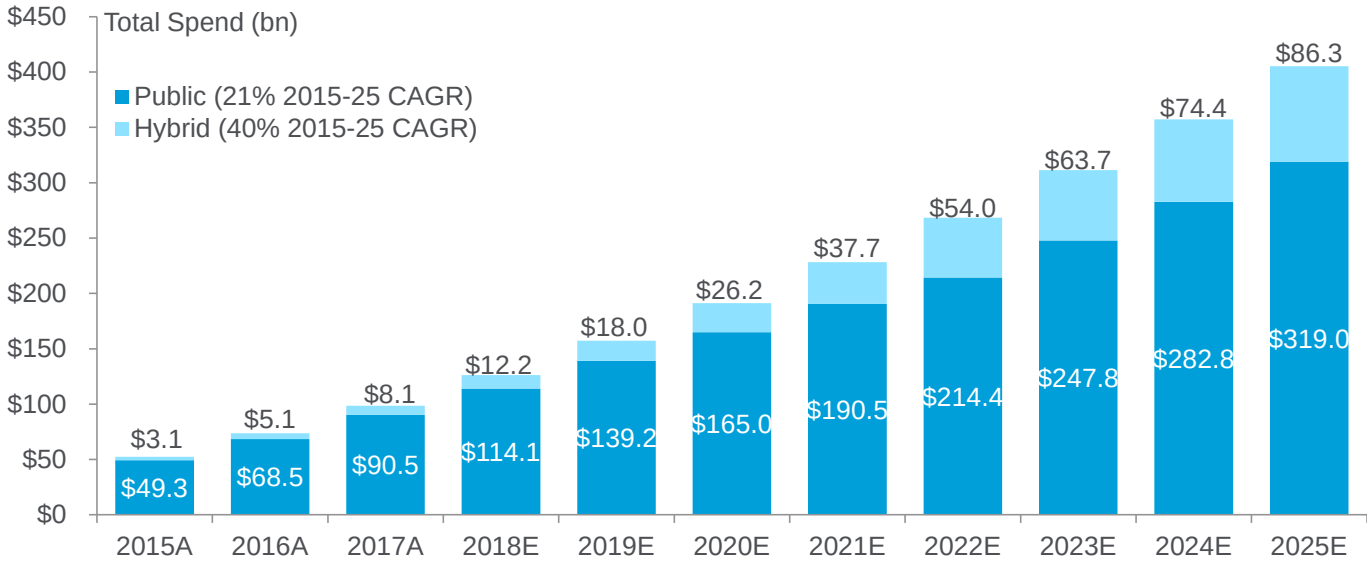
Hybrid and Multi-cloud Architectures Challenge Public Cloud Providers in Security

While there are architectural reasons we site above that make sense for security functions to be embedded into public cloud services, the realities of public cloud adoption is likely to be much more complicated. This will also have implications on how public cloud is secured and ultimately implications for how the IT security solutions market will play out over the next decade.

In adopting public cloud, the larger enterprise customers will employ a path that includes adoption of 'hybrid cloud'

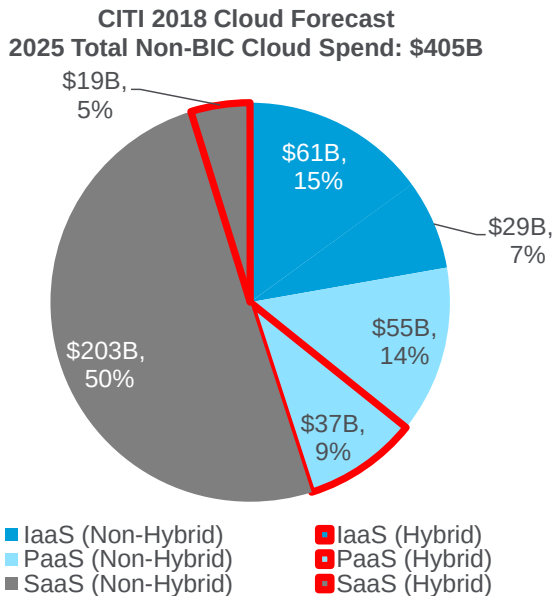
We believe that in adopting public cloud, the larger enterprise customers will employ a path that includes adoption of 'hybrid cloud', in which their 'on-prem' footprint evolves and services that are run in public cloud connect with these on-prem capabilities. These hybrid offerings take many forms, although the most common we see extend on-prem capabilities into public cloud. The advantage here is that it is easier to adopt and gain benefit from public cloud capabilities. While some point out that 'hybrid' is still saddled with some of the inefficiencies of on-prem (vs. native public), many times the cost of re-writing or re-factoring a workload is not warranted.

Figure 34. Hybrid and Public Cloud Worldwide Market Outlook (Excludes "Born in the Cloud")



Source: Citi Research

Figure 35. Hybrid Cloud Share of Non-"Born in the Cloud" Total Warehouse Cloud Spend



Source: Citi Research

These hybrid cloud offerings are likely to carry with them, security capabilities that are similar to what organizations are used to running on-prem. If the move to the cloud is slow and the path is 'hybrid', we expect the security solutions market to change less than if the market moves faster towards native cloud.

Key Areas to Focus for Future Trends in Cyber Security Solutions

We expect this market to remain a 'short-cycle' sector, meaning that product cycles are measured in duration of 3-5 years vs. decades

As we have summarized, with the nature and source of the security threat changing constantly, the security solutions market is also constantly evolving. We expect this market to remain a 'short-cycle' sector, meaning that product cycles are measured in a duration of 3-5 years. This compares to other technology markets where refresh timelines are a decade or more. This has been a constant force and one that we expect to continue into the future. For this reason, to both understand how to mitigate new challenges, as well as be an investor in the market, it is necessary to understand the evolving threat landscape.

Combined with this, there is the once in a decade (or more) shift in technology architecture underway, that is the early (i.e., 20% of workloads are in cloud). Beyond the constant shift in the threat landscape, this force has the most potential to drive change in the market.

Emerging Technology Solutions

Biggest drivers for adoption of these emerging tech solutions are large volumes of data, an increase in computer processing power, and the need to adapt and counter ever-evolving cyber threats

An emerging technology is a technology with a level of novelty, having certain coherence over time, and that could cause profound positive impact on business or society. Some notable emerging technologies include artificial intelligence (AI) / machine learning (ML), blockchain, behavioral biometrics, biometric authentication technologies, data analytics, and emerging cloud services. Emerging technologies provide an enhanced ability to predict and analyze threats, identify and prevent threats to a large surface area such as a customer base, and detect and stop cyber-attacks all at a speed and scale that would not have been possible without the use of these newer technologies. The biggest drivers for adoption of these emerging tech solutions are large volumes of data, an increase in computer processing power, and the need to adapt and counter ever-evolving cyber threats.

With the extreme growth in volumes of data and increased capacity to store large amounts of data, the next logical step is to analyze the data to further an organization's goals, including cyber defense capabilities. For example, analysts in a Security Operations Center (SOC) typically view a large number of alerts, logs, and other kinds of security data. Tools have been available for some time to help SOC teams manage this data, but with the increased sophistication in attacks, the need to automatically analyze the data with predictive decisioning is critical.

Predictive decisioning is something that is now possible given the advancement in computer processing power. It is a critical need given the skills gap in the current cyber security workforce. One study by Cybersecurity Ventures estimates there will be 3.5 million unfilled cyber security jobs by 2021. The use of AI/ML and other emerging tech helps to automate analytics and decision-making capabilities thereby augmenting the existing workforce with advanced tools to potentially mitigate the shortage of future cyber security professionals.

As business models are evolving, so too is the threat landscape, creating a need for new tools and technologies to support business objectives while reducing the risk of exploitation

As business models are evolving, so too is the threat landscape, creating a need for new tools and technologies to support business objectives while reducing the risk of exploitation. Expanding business models, such as digital banking, inadvertently create a larger cyber attack surface by increasing the number of endpoints for possible infiltration. With existing cyber threats, like malware, growing at an unprecedented rate, there is a need to use AI/ML capabilities to keep pace in improving our cyber security posture. According to Av-test gmbh, since 2010, there has been an increase of around 800 million in the number of malware types. The application of AI can enable traditional antivirus products to learn how malware morphs to avoid detection so that the antivirus detection algorithms can be appropriately updated at the same speed. This and other drivers incentivize organizations to adopt emerging technologies as time to market pressures are demanding efficient security features for needed business products.

Emerging Technology Tools for Cyber Defense

Machine Learning (ML)

ML enables analysis of large amounts of data, and the ability to recognize and label unknown patterns

A machine learning system can automatically learn when exposed to new data and draw inferences without humans having to reprogram the system. It is a technology transforming how key decisions in areas such as trading, autonomous vehicles, and medical research are being made or will be made in the future. ML enables analysis of large amounts of data, and the ability to recognize and label unknown patterns. Microsoft uses ML in its Windows Defender program as it, "*allows Microsoft 365 to scale next-gen protection capabilities and enhance cloud-based, real-time blocking of new and unknown threats.*"

Deep learning techniques within the ML domain mines the vast quantity of data to identify threat activity and anomalous activities which could provide real-time indicators of compromise or malicious activity.

Artificial Intelligence/Natural Language Processing (NLP)

NLP techniques could power large-scale vulnerability detection systems to efficiently identify vulnerabilities, which could be potentially very hard to detect using existing tools

Natural Language Processing reads and understands the context of a given text. The ability to read and understand text provides the capability to detect and analyze threats which, when combined with other tools, leads to the execution of an appropriate response strategy. Cisco has built an 'NLPRank' system, which is based on NLP techniques. When combined with OpenDNS data, it provides the ability to detect malicious domains, such as a website that appears to be an official banking institutions' landing page, but is actually a duplicate of the landing page designed to capture the username and password when typed in by a customer, in real time. NLP techniques could power large-scale vulnerability detection systems to efficiently identify vulnerabilities, which could be potentially very hard to detect using existing tools.

Biometric Technologies

Biometric and behavioral biometrics show promise in authentication as well as fraud detection

Identification, authentication, and authorization of resources are a critical component of cyber defense. Biometrics use unique physical characteristics of human beings like iris patterns, fingerprints, voice, face, etc. for identification and authentication. The ability to personalize authentication and use human features that currently are difficult to fraudulently replicate, provides an enhanced authentication capability.

Behavioral biometrics is a technology that identifies people by how they do what they do, instead of what they are (e.g. fingerprint), what they know (e.g. password), or what they have (e.g. token). Behavioral biometrics captures behavioral (e.g. mouse movements), cognitive, and physiological parameters to create a unique user profile within online and mobile applications. This technology is being used to detect fraud, and malware in real-time.

Blockchain/ Distributed Ledger Technology (DLT)

Blockchain technology is currently being explored for potential use in preventing fraud and data theft

Distributed ledger technology (DLT), primarily blockchain, provides a distributed network and potentially a solution to one of the fundamental challenges of technology solutions – trust. Blockchain technology is currently being explored for potential use in preventing fraud and data theft. Blockchain could be used to prevent Distributed denial-of-service (DDoS) attacks, which is when a website crashes due to the number of requests to access the site being received all at one time. Other uses of blockchain to enable cyber security are under exploration. For example, blockchain provides a fully decentralized option for the Domain Name System (DNS). DNS is used to translate the name of a website into an Internet Protocol (IP) address, which is needed to find the computer services the customer is requesting. Currently DNS is managed by a centralized authority. By using blockchain technology, there wouldn't be a need for a centralized authority as the technology would manage the mapping of domain names to IP addresses. Without a centralized authority to attack, it would be hard for a malicious actor to seize domain ownership and the risk of root servers as a central point of failure will be largely mitigated.

Emerging technologies have significant potential for enhancing cyber defense capabilities. These technologies in all probability will not replace humans completely, but will augment human capability for enhanced output.

Governance of Emerging Technology Solutions for Effective Cyber Defense

Successful application of emerging technology capabilities for cyber defense requires a robust, adaptable governance and risk mitigation strategy

The successful application of emerging technology capabilities for cyber defense requires a robust, adaptable governance and risk mitigation strategy. The strategy should include — roles and responsibilities, an accounting of emerging technology products, testing and security, enhanced monitoring and anomaly detection, a knowledge sharing platform, and continuous risk identification and mitigation plans.

The application of emerging technologies as well as technical research in general has been relatively strong. For example, in the last 10 years, the number of AI/ML research papers in ArXiv.org has increased by more than 7,000%. However, an area that needs more focus is governance and risk management of these emerging technologies. A more integrated approach across various organizations would help build a knowledge sharing platform, including the building of best practices for the use of emerging technologies in cyber defense and other potential areas. Within an organization, the overall cyber security defense strategy needs to have consensus across the first line network defenders, second line risk management group, and third line auditors. An integrated approach among these lines of defense enhances the probability of managing potential risks at the front-end of implementation and use of emerging technologies.

Governance Framework

A governance framework is required to manage the entire lifecycle of emerging tech adoption and the management of potential risks

As businesses adopt products that use emerging tech, or use emerging tech to develop in-house products, a governance framework is required to manage the entire lifecycle of adoption and manage potential risks. The framework should enable responsible innovation at an organization by providing higher transparency and reporting, improved adoption speed and an adaptable risk management framework.

With increased adoption by vendors of emerging tech to provide cyber security solutions, organizations need to adequately understand and monitor best practices adopted by third parties. A questionnaire with a list of specific questions adapted to the emerging technology and product could be a good starting point for improved understanding and transparency of the entire process of technology adoption.

The scope of implementation of a specific emerging tech used for cyber defense should lead to subsequent governance steps. For example, if ML is being widely adopted across various businesses, including vendor products, a top of the house Center of Excellence (CoE) for the technology will help build guardrails, best practices, and a knowledge sharing platform across the businesses. On the other hand, the limited application of an emerging tech could have a smaller working group with participants from the first and second lines of defense to front end the implementation of the technology with risk identification and guidance for the management of that risk.

Emerging Technology Risk and Controls

Emerging technologies also increase the probability of emerging risks. With increasing maturity of these technologies and their wide adoption, the malicious actors also exploit these technologies for their own benefit. IBM researchers presented at the Blackhat 2018 conference, DeepLocker, a new breed of highly targeted and evasive attack tools powered by AI. The researchers developed this tool to better understand how several existing AI models can be combined with current malware strains to create a stealthy and targeted malware.

Although IBM developed DeepLocker to understand how malicious actors can exploit AI, it shows the dangers of what attackers can achieve, especially those who are state sponsored with unlimited resources to conduct attacks.

Risk of Emerging Technology Use

A cyber defense strategy should cover identification and mitigation of threats with the use of emerging technologies

A cyber defense strategy should cover identification and mitigation of threats with the use of emerging technologies. As with any technology, emerging technologies has potential technological and cyber risks. With increasing adoption of emerging technologies, the attack surface and the probability of a potential negative impact increases.

Currently researchers are trying to establish potential negative uses of AI/ML emerging technologies, along with vulnerabilities in these technologies themselves. For example, researchers conducted attacks against live ML models provided by Cloud Service Providers and they were able to extract AI/ML models using model extraction techniques. Some adversarial attacks could negatively affect data privacy of the training data used in AI/ML models.

A risk mitigation strategy should ensure effective design of controls to reduce inherent risks based on the threat environment.

References

Anderson, Douglas J. & Eubanks, G. (2015). The Institute of Internal Auditors® Committee of Sponsoring Organizations of the Treadway Commissions (COSO) Governance and Internal Control Leveraging COSO Across the Three Lines of Defense. https//na.theiia.org/standards-guidance/Public%20Documents/2015-Leveraging-COSO-3LOP.pdf.

Anstee, D. et al (2016). Worldwide Infrastructure Security Report. *Arbor Networks Special Report*. 11. NETSCOUT http://www.icir.org/vern/cs261n/papers/Arbor-WISR2016.pdf.

APT Group. (2019). Emerging Threat: Dragonfly / Energetic Bear. Accessed February 19. http://www.symantec.com /connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group.

Armor. (2018). The Black Market Report: A Look Inside the Dark Web. https://cdn.armor.com/app/uploads/2018/03/ 27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf.

Asur, S., & Huberman, Bernardo A. (2010). Predicting the Future with Social Media. Social Computing Lab, HP Labs. Palo Alto, CA. https://arxiv.org/pdf/1003.5699.pdf

Baker, S. (2017). Cybersecurity Becoming Big ESG Concern. Pension & Investments. Accessed January 22. https://www.pionline .com/article/20171002/PRINT/171009985/cybersecurity-becoming-big-esg-concern.

Bank of England. (2017). Cyber Insurance Underwriting Risk. http://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss.

BBC. (2015). Web Attack Knocks BBC Websites Offline. https://www.bbc.co.uk/news/technology-35204915.

Bekker, G. (2017). Thales Data Threat Report: Trends in Encryption and Data Security. Thales. http://enterprise-encryption.vormetric.com/rs/480-LWA 970/images/Thales_2017_Data_Threat_Report-Global_Edition.pdf. Accessed 24 February 2017.

Benner, K., et al. (2018). Saudis Image Makers: A Troll Army and a Twitter Insider. The New York Times. October 20, 2018. Accessed March 5. https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html.

Blau, A. (2017) Better Cybersecurity Starts with Fixing Your Employees Bad Habits. Harvard Business Review.

Bojanc, R. & Jerman-Blazic, B. (2008). An Economic Modeling Approach to Information Security Risk Management. *International Journal of Information Management*, vol. 28(5), pp. 413–422.

Bronk, C., & Tikk-Ringas, E. (2013). Hack or Attack? Shamoon and the Evolution of Cyber Conflict. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2270860.

Bryant, C. (2017). How to Justify Your IT Security Budget. RiskLens. https://www.risklens.com/blog/how-to-justify-your-it-security-budget. Accessed January 22.

Budd, C. (2018). Don't Panic About Software Supply Chain Attacks. Research Center, Palo Alto Networks. July 21. https://researchcenter.paloaltonetworks.com/2018/06/unit42-dont-panic-software-supply-chain-attacks/.

Business Sweden. (2018). Understanding the Cloud: It's Childs Play. Data Centers by Sweden. Accessed October 12. https://www.business-sweden.se/en/Invest/industries/Data-Centers-By-Sweden/news-and-downloads/investment-news/understanding-the-cloud-its-childs-play/.

Cabinet Office. (2018), Strategic Framework and Policy Statement - on Improving the Resilience on Critical Infrastructure to Disruption from Natural Hazards. https://asset. publishing.service.gov.uk/government/uploads/system /uploads/attachment_data/file/62504/strategic-framework.pdf.

Calzada, H., et al. (2016). Risk Beneath the Surface of a Cyber Attack. Deloitte. https://www2. deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

Cambridge Centre for Risk Studies, & RMS. (2016). Managing Cyber Insurance Accumulation Risk. Cambridge Judge Business School. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/managing-cyber-insurance-accumulation-risk/.

Cambridge Centre for Risk Studies. (2015). Lloyds Business Blackout Scenario. Emerging Risk Report - 2015. Lloyds of London. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/lloyds-business-blackout-scenario/.

Cambridge Centre for Risk Studies. (2016). Cyber Exposure Data Schema. Cyber Accumulation Risk Management. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/cyber-exposure-data-schema/.

Cambridge Centre for Risk Studies. (2016). Integrated Infrastructure: Cyber Resiliency in Society. *Cambridge Risk Framework for Critical Infrastructure Threat Scenario*. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/integrated-infrastructure-cyber-resiliency-in-society/.

Cambridge Centre for Risk Studies. (2019). Cyber Risk Outlook 2019

Cambridge Centre for Risk Studies. (2019). CyRiM Scenario: Bashe Attack. Cambridge Judge Business School. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/space-and-technology/cyrim-scenario-bashe-attack/.

Camillo, M. (2017). Cyber Risk and the Changing Role of Insurance. *Journal of Cyber Policy 2* (1): pp 53–63.

Cisco. (2018) .Annual Cybersecurity Report. Cisco. https://www.cisco.com/c/en_uk/products/security/security-reports.html.

Citi GPS. (2018). ePrivacy and Data Protection: Privacy Matters, Navigating the New World of Data Protection. Citi. May 2018. https://www.citivelocity.com/citigps/eprivacy-data-protection-2/

Clapper, James R. (2016). Worldwide Threat Assessment of the U.S. Intelligence Community. Director of National Intelligence. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ ATA_SFR_FINAL.pdf [https://perma.cc/2YY5-4PTN].

CNN. (2019). Staged Cyber Attack Reveals Vulnerability in Power Grid - CNN.Com. Accessed January 8. http://edition.cnn.com/2007/US/09/26/power.at.risk/.

Coburn, A., Gordon W., & Leverett, E. (2019). Solving Cyber Risk. Wiley.

Cohen, B., et al. (2017). Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy. Antitrust 32, no. 1. Accessed July 26 https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.authcheckdam.pdf.

Collaboration with Willis Towers Watson. (2016). Impact of Digital Media on Individuals, Organizations and Society. Accessed February 08, 2019. http://reports.weforum.org/human-implications-of-digital-media-2016/section-3-impact-of-digital-media-on-individuals-organizations-and-society/.

Commission Nationale de l'Informatique et des Libertés. (2018). Data Protection around the World. CNIL. https://www.cnil.fr/en/data-protection-around-the-world. France.

U.S. Committee on Homeland Security (2005). SCADA Systems and the Terrorist Threat: Protecting the Nations Critical Control Systems. U.S. House of Representatives.

UK Consumer Protection. (2002). Statutory Instruments 618. The Medical Devices Regulations 2002. Accessed January 17. http://www.legislation.gov.uk/uksi/2002/618/pdfs/uksi_20020618_en.pdf.

Corero Network Security, Inc. (2018). Half Year 2018 DDoS Trends Report. http://info.corero.com/rs/258-JCF-941/images/H1-2018-Corero-Trends-Report-Final.pdf.

Grigsby, A. (2018). The United Nations Doubles its Workload on Cyber Norms, and Not Everyone is Pleased. Council of Foreign Affairs. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Carbon Black. (2018). Carbon Black Threat Report: Cryptocurrency Gold Rush on the Dark Web. https://www.carbonblack.com/2018/06/07/carbon-black-threat-report-cryptocurrency-gold-rush-dark-web/.

Cnet. (2019) .Huawei pleads not guilty to trade secret theft charges. https://www. cnet.com/news/huawei-pleads-not-guilty-to-trade-secret-theft-charges/

Cyber Security for Manufacturing. (2018) EEF, AIG and RUSI. https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers.

Cybersecurity Ventures. (2016) Cybercrime Damages $6 Trillion by 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Deloitte (2016) Telecommunications - Cyber Executive Briefing. Accessed November 07. https://www2.deloitte.com/global/en/pages/risk/articles/Telecommunications.html.

DeNisco-Rayome, A. (2018) .51% of Companies Publicly Exposed Cloud Storage Services in the Past Year. TechRepublic. Accessed May 15. https://www.techrepublic.com/article/51-of-companies-publicly-exposed-cloud-storage-services-in-the-past-year/.

DLA Piper. (2018). Global Data Protection Laws in the World. Accessed August 22. https://www.dlapiperdataprotection.com/.

Dr. R Jayamaha (2005). Basel II and Operational Risk. Keynote Address by Dr. R Jayamaha, Deputy Governor of the Central Bank of Sri Lanka, at the 10th SEACEN-FSI Regional Seminar for Bank Supervisors and Regulators. December 12, 2005. Accessed February 15. https://www.bis.org/review/r051222g.pdf.

Dragos. (2018). TRISIS Malware: Analysis of Safety System Targeted Malware. https://dragos.com/wp-content/uploads/TRISIS-01.pdf.

Dugan, K. (2017). Equifax Says it Hasn't Lost Any Big Clients Since Data Breach. New York Post, 10 November 2017. https://nypost.com/2017/11/10/equifax-says-it-hasnt-lost-any-big-clients-since-data-breach/

Emsley, J. (2018). Blockchain and Cryptocurrency: Japans Economic Elixir?. CryptoSlate. https://cryptoslate.com/blockchain-cryptocurrency-japans-economic-elixir/.

Engadget. (2019). How Huawei Planned International Robot Espionage via Email. https://www.engadget.com/2019/01/30/huawei-t-mobile-emails-espionage-tappy-robot-steal-2012/.

Engineering & Technology Magazine. (2017). The Elderly Most at Risk from Cyber-crime, Report Warns. https://eandt.theiet.org/content/articles/2017/01/the-elderly-most-at-risk-from-cyber-crime-report-warns/

Ernst & Young (2018). EY - Board Agenda 2018 Top Priorities for European Boards. Home. Accessed February 03. https://www.ey.com/us/en/issues/governance-and-reporting/ey-board-agenda-2018-top-priorities-for-european-boards.

European Union. (2019). GDPR in Numbers. https://ec.europa.eu/ commission/sites/beta-political/files/190125_gdpr_infographics_v4 .pdf.

Europol. (2018). Internet Organised Crime Threat Assessment (IOCTA) 2018. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

Facebook Newsroom. (2018). An Update on the Security Issue. Accessed March 05, 2019. https://newsroom.fb.com/news/2018/10/update-on-security-issue/.

Facebook. (2018). Security Update. News release, September 28, 2018. Facebook. Accessed October 19. https://newsroom.fb.com/news/2018/09/security-update/.

FERC. (2019). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Accessed January 9. https://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf.

Foltyn, T. (2018). Biggest DDoS Attack in History Takes GitHub Offline. https://www.welivesecurity.com/ 2018/03/02/github-knocked-briefly-offline-biggest-ddos-attack/.

Fruhlinger, J. (2018). The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet. CSO Online. https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

Fruhlinger, J. (2018). Top Cybersecurity Facts, Figures and Statistics for 2018. https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

Galling, L. (2017) Total WannaCry Losses Pegged at $4 Billion. Reinsurance News. https://www.reinsurancene.ws/ total-wannacry-losses-pegged-4-billion/.

Gandhi, P., Khanna, S., & Ramaswamy, S. (2016). Which Industries Are the Most Digital (and Why)?. *Harvard Business Review*, April 1. https://hbr.org/2016/04/a-chart-that-shows-which-industries-are-the-most-digital-and-why.

Gartner (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed 124 billion in 2019. Accessed January 22. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

Gartner. (2017). Leading the IoT: Gartner Insights on How to Lead in a Connected World. Gartner, Inc.

Gelinne, J., Fancher, J. D., & Mossburg, E. (2016). The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property. Report. Deloitte. Accessed December 17. https://www2.deloitte.com/ insights/us/en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html.

Gemalto Blog. (2018). 2017: The Year of Ransomware. https://blog.gemalto.com/security/2018/01/18/2017-year-ransomware/.

Ghasemisharif, M. et al. (2018). O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web. Report. University of Illinois-Chicago. In the Proceedings of the 27th USENIX Security Symposium.

Gibbs, S. (2017). WannaCry: Hackers Withdraw £108,000 of Bitcoin Ransom. The Guardian, Technology Section. https://www.theguardian.com/technology/2017/ aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

Giles, M. (2019). Triton is the world's most murderous malware, and it's spreading. https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

Goldman, J. (2019). WannaCry Ransomware Hits U.S. Critical Infrastructure. Accessed January 31. https://www.esecurityplanet.com/threats/wannacry-ransomware-hits-u.s.-critical-infrastructure.html.

Gorenc, B., & Fritz S. (2017). Hacker Machine Interface: The State of SCADA HMI Vulnerabilities. Trend Micro Zero Day Initiative Team.

Goshen, Z., & Parchomovsky, G. (2006) .The Essential Role of Securities Regulation. *Duke Law Journal*, Vol. 55, No. 4.

Greenberg, A. (2017). Crash Override: The Malware That Took Down a Power Grid. Wired, https://www.wired.com /story/crash-override-malware/.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed 5 March 2019.

Greengard, S. (2003). The Real Cost of Cybersecurity. Business Finance. http://businessfinancemag.com/technology /real-cost-cybersecurity.

Greengard, S. (2018). Behaviors Can Say a Lot, Even in Cybersecurity. Securityroundtable.org.

Grobman, S. (2018). When Nation-states Hack the Private Sector for Intellectual Property. The Hill. Accessed December 17. https://thehill.com/opinion/technology /380948-when-nation-states-hack-the-private-sector-for-intellectual-property.

Haber, M. (2017). WannaCry Ransomware Attack Explained – Makes Me Wanna Cry. BeyondTrust.com. https://www.beyondtrust.com/blog/entry/wannacry-ransomware-attack-explained-makes-me-wanna-cry

Hadley, M. (2014). Target Sees Drops in Customer Visits After Breach. USA Today. https://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/

Hadlington, L. & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors, Policing, pp 1-14

Healey, J.,et al. (2018). The Future of Financial Stability and Cyber Risk. Report. Cybersecurity Project, Brookings Institution. New York, NY.

Hedrich, W. et al. (2017). Cyber Risk in Asia-Pacific: The Case for Greater Transparency. Marsh & McLennan. http://www.mmc.com/content/dam/mmc-web/Files/APRC/aprc-cyber-risk-in-asia-pacific.pdf.

Helms, K. (2018). Big-Name Insurers Stepping Up Their Crypto Game. Bitcoin News. https://news.bitcoin.com /insurers-crypto/.

Henriksen (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 22 January 2019, Vol 5, issue 1

Higgins, K. (2018). Unpatched Vulnerabilities the Source of Most Data Breaches. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465.

Homeland Security Committee (2018). Understanding Cybersecurity Threats to Americas Aviation Sector, 116th Cong. (2018) (testimony of Christopher Porter). https://homeland.house.gov/hearing/understanding-cybersecurity-threats-to-americas-aviation-sector/?wpisrc=nl_cybersecurity202&wpmm=1

House of Commons. (2018). Cyber-Attack on the NHS. https://publications. parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

Hughes, O. (2017). Full Scale of WannaCry Ransomware Attack on NHS Revealed in FAO Report. Digital Health. https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/.

IBM Security Services. (2018). The 2018 Cost of a Data Breach Study by the Ponemon Institute. https://www.01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.

IBM X-Force Threat Intelligence Index. 2018. November 23. https://www.ibm.com /security/data-breach/threat-intelligence.

ICS-CERT. (2018). Overview of Cyber Vulnerabilities. Accessed April 6. https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#under.

IEEE Access (2018). Cyber-Threats and Countermeasures in the Healthcare Sector. IEEE Access. March 31, 2018. Accessed July 24, 2018. http://ieeeaccess.ieee.org/special-sections-closed/cyber-threats-countermeasures-healthcare-sector/.

Insurance Day. (2018). Pool Re Extends Retro Programme to Include Cyber Terrorism Cover. March 1. https://insuranceday.maritimeintelligence. informa.com/ID1121541/Pool-Re-extends-retro-programme-to-include-cyber-terrorism-cover.

ITU. (2017). Global Cybersecurity Index (GCI). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Jay, J. (2018). Britain to spend £250 Million on "offensive cyber-force" to combat Russian threat. https://www.teiss.co.uk/cyber-warfare/britain-offensive-cyber-force/.

Kaspersky Lab (2015). Collateral Damage: 26% of DDoS Attacks Lead to Data Loss. Kaspersky. https://www.kaspersky.com/about/press-releases/2015_collateral-damage-26-of-ddos-attacks-lead-to-data-loss.

Kaspersky Lab. (2018). IT Threat Evolution Q2 2018. Statistics. Securelist. Kaspersky Labs Cyberthreat Research and Reports. https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/.

Kelleher, K. (2018). Facebook Loses Around $13 Billion in Value After Data Breach Affects 50 Million of Its Users. Fortune. http://fortune.com/2018/09/28/facebook-stock-falls-after-security-breach/.

Kirk, J. (2018). Banco de Chile Loses $10 Million in SWIFT-Related Attack. Bank Info Security. https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

Knott, D. & Van Kuiken, S. (2013). The Big-data Revolution in US Health Care: Accelerating Value and Innovation. McKinsey & Company. Accessed January 21. https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.

Kohout, J. (2018). How DDoS Attacks Can Sink Your Business. TeskaLabs. Accessed October 30. https://www.teskalabs.com/blog/how-ddos-can-sink-your-business.

Larcheveque, E. (2018). 2018: A Record-Breaking Year for Crypto Exchange Hacks. CoinDesk. December 29. https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks.

Larson, D. (2018). Global Survey Reveals Supply Chain as a Rising and Critical New Threat Vector. Crowd Strike. https://www.crowdstrike.com/blog/global-survey-reveals-supply-chain-as-a-rising-and-critical-new-threat-vector/.

Le Bris, A. & El Asri, W. (2016). State Of Cybersecurity & Cyber Threats In Healthcare Organizations. Report. School of Business, Essec. Cergy, France. http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf

Lee, R., Assante, M. & Conway, T. (2014). German Steel Mill Cyber Attack. ICS Defense Use Case. Industrial Control Systems. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Lee, S., et al. (2018). Quantifying Improbability: An Analysis of the Lloyds of London Business Blackout Cyber Attack Scenario, 54. https://www.jhuapl.edu/Content/documents/QuantifyingImprobability.pdf.

LexisNexis. 2018. LexisNexis Risk Solutions 2018 True Cost of Fraud Study -- Retail Edition Pdf.

Lloyds & AIR. (2018). Cloud Down: Impacts on the US Economy.

Mackie, K. (2018). Microsoft's Cloud Outage Postmortem: What Went Wrong in Texas. Redmond Channel Partner. https://rcpmag.com/articles/2018/09/11/microsoft-cloud-outage-postmortem.aspx.

Manion, A., et al. (2015). VRDX-SIG: Global Vulnerability Identification. 27th Annual FIRST Conference, June 14. https://www.first.org/resources/papers/conf2015/first_2015_-_manion-_uchiyama-_terada_-_vrdx-sig_20150619.pdf.

Manyika, J. (2016). Interview with Penny Pritzker, Former U.S. Secretary of Commerce. Report. McKinsey Global Institute, McKinsey. Accessed January 8, 2019. https://www.mckinsey.com/industries/high-tech/our-insights/fostering-an-open-secure-digital-economy.

Marsh McLennan (2014). Cyber Security And The Boardroom. Report. Marsh Risk Management Research, Marsh. 2014.

Marsh McLennan (2014). Cyber: The Stakes Have Changed for the C-Suite. Report. Marsh & McLennan Companies. Marsh, Special Report with FireEye.

Massacci, F. (2016). Economic Impacts of Rules- Versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers. IEEE Security & Privacy, vol. 14, no. 3, 2016, pp. 52-60, doi:10.1109/MSP.2016.48.

McAfee. (2018). McAfee Labs Threats Report June 2018.

McMillan, R. & Seetharaman, D. (2018). Facebook Finds Hack Was Done by Spammers, Not Foreign State. The Wall Street Journal. Accessed March 05. https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869.

Milhorn, H. Thomas. (2007). Cybercrime: How to Avoid Becoming a Victim. Universal Publishers.

Moore, D. & Rid, R. (2016). Cryptopolitik and the Darknet. *Global Politics and Strategy*, vol. 58, Issue 1.

National Grid ESO. (2019). Black Start | National Grid ESO. Accessed January 8, 2019 https://www.nationalgrideso .com/balancing-services /system-security-services/black-start.

National Transportation Safety Board. (2009). National Transportation Safety Board Safety Recommendation. https://www.ntsb. gov/safety/safety-recs/recletters/H09_15_16.pdf.

NCCIC. (2019). Incident Response Pie Charts (YIR 2016 Addendum). ICS-CERT. Accessed January 11. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf.

Netcraft. (2018). Web Server Survey. Netcraft. https://news.netcraft.com/archives/category/web-server-survey/.

Newman, Lily H. (2018). How Facebook Hackers Compromised 30 Million Accounts. Wired. October 12, 2018. Accessed March 05. https://www.wired.com/story/how-facebook-hackers-compromised-30-million-accounts/.

NIST (2014). *Disaster Resilience Framework Report*, Hoboken, NJ. https://www.nist.gov/sites/default/files/documents/el/building_materials/resilience/Chapter-8-Communications_v0-1A.pdf

O2 Outage Highlights Importance of Software Certificate Audits. 2019. Accessed February 19. https://www.computerweekly.com/news/252454067/O2-outage-highlights-importance-of-software-certificate-audits.

O'Boyle, M. (2018). Mexico Central Bank Says Hackers Siphoned $15 Million from Five. Reuters. https://www.reuters.com/article/us-mexico-cyber/mexico-central-bank-says-hackers-siphoned-15-million-from-five-companies-idUSKCN1IH38Q.

OECD. (2018). Unleashing the Potential of the Cyber Insurance Market . http://www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm.

Office of Financial Research. (2017). Cybersecurity and Financial Stability: Risks and Resilience. Report no. 17-01. 2017. 1-12.

Osborne, H. (2016). HSBC Suffers Online Banking Cyber-Attack. The Guardian, Business Section. https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack.

Oxford Analytica. (2018). Cybersecurity & Geopolitics. http://www.oxan.com/ media/2150/oxford-analytica-cybersecurity-and-geopolitics.pdf

Paul K., & Diemontt, T. (2018). The Impact of SWIFT Security Requirements. KPMG. September 28. https://home.kpmg.com/nl/nl/home/insights/2018/09/the-impact-of-swift-security-requirements-on-the-banking-community.html.

Pinto, A. C., et al. (2005). Challenges to Sustainable Risk Management. EScholarship. http://escholarship.org/uc/item/1rq3640c#page-7. Accessed 25 February 2017.

Ponemon, L. (2018). Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT. Security Intelligence. July 11. https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/.

Ponemon. (2016). Cost of Data Center Outages. Data Center Perfomance Benchmark Series.

Privacy International (2018). State of Privacy. https://privacyinternational.org/type-resource/ state-privacy.

Prokop, A. (2019). Justice Department charges Russian national with conspiring to interfere with 2018 midterms. https://www.vox.com/policy-and-politics/2018/10/19/18001362/trump-russia-troll-justice-department

Ray, J., et al. (2018). Cyber Threatscape Report 2018. *Midyear Cybersecurity Risk Review*. Accenture. https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report-2018.

Reinsurance (2018). PCS: NotPetya Insured Losses Now $3bn+. Re-Insurance. https://www.re-insurance.com/news/pcs-notpetya-insured-losses-now-3bn/1627.article.

Reo, J. (2017). Theft and DDoS Attacks Go Hand in Hand. Corero. https://www.corero.com/blog/846-theft-and-ddos-attacks-go-hand-in-hand.html.

Reuters. (2018). Aluminum maker Hydro battles to contain ransomware attack. https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUSKCN1R00NJ

Rightscale. (2018). Rightscale 2018 State of the Cloud Report. https://assets.rightscale.com/uploads/pdfs/RightScale-2018-State-of-the-Cloud-Report.pdf.

Roberts, D. (2018). 10 Ways Digital Could Transform Healthcare. Accessed January 21. https://www.ey.com/en_gl/digital/10-ways-digital-could-transform-healthcare.

RSA. (2016). Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise 2016. https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf. Accessed 22 January 2019.

Rushe, D. (2018). Amy Pascal Steps down from Sony Pictures in Wake of Damaging Email Hack. The Guardian. Accessed October 20. https://www.theguardian.com/film/2015/feb/05/amy-pascal-leaving-sony-pictures-email-leak.

Saini, K. (2018). Aadhaar security breach. various sources.

Schechner, S. (2018). Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach. Wall Street Journal, September 30, sec. Tech. https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906.

Schneier, B. (2010). The Story Behind the Stuxnet Virus. Forbes, October 7, 2010. https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#232b2d8951e8

Scroxton, A. (2018). TechTarget. https://www.techtarget.com/contributor/Alex-Scroxton

Seals, T. (2017). #WannaCry Hits Medical Devices in U.S. Infosecurity Magazine. https://www.infosecurity-magazine.com:443/news/wannacry-hits-medical-devices-in-us/.

SecurityZap. (2015). Vulnerabilities in Industrial Control Systems - SCADA. Security Zap. https://securityzap.com/vulnerabilities-in-industrial-control-systems/.

Slay, J., & Miller, M. (2007). Lessons Learned from the Maroochy Water Breach. In Critical Infrastructure Protection, edited by Eric Goetz and Sujeet Shenoi, 253:73–82. Boston, MA: Springer U.S.

Spilotro, T. (2018). Japan Sees Rising Crypto Theft, $540 Million Stolen in First Six Months of 2018. NewsBTC. https://www.newsbtc.com/2018/09/20/japan-sees-rising-crypto-theft-540-million-stolen-in-first-six-months-of-2018/.

Statista. (2019). Cyber insurance-Statistics and Facts. https://www.statista.com /topics/2445/cyber-insurance/

SWIFT. (2018). Customer Security Programme (CSP). SWIFT. Accessed October 30. https://www.swift.com/myswift/customer-security-programme-csp/security-controls.

Symantec. (2019). Internet Security Threat Report (ISTR) 2018. 2019. Accessed February 4. https://www.symantec.com/security-center/threat-report.

Synergy Research Group. (2018). Cloud Revenues Continue to Grow by 50% as Top Four Providers Tighten Grip on Market.https://www.srgresearch.com/articles/cloud-revenues-continue-grow-50-top-four-providers-tighten-grip-market.

Tavernise, S. (2016). As Fake News Spreads Lies, More Readers Shrug at the Truth, N.Y. Times, https://www.nytimes.com/2016/12/06/us/fake-news-partisan-republican-democrat.html.

Telegraph. (2019). Power Station Break-in Sparks Security Review. Accessed February 19. https://www.telegraph.co.uk/news/uknews/3705073/Power-station-break-in-sparks-security-review.html.

The Council of Economic Advisers. (2018). The Cost of Malicious Activity to the U.S. Economy. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

The Economist. (2010). Twitters Transmitters. Accessed January 10, 2019. https://www.economist.com/special-report/2010/01/28/a-world-of-connections.

The Economist. (2017). The World's Most Valuable Resource Is No Longer Oil, but Data. Accessed October 20, 2018. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

The Economist. (2017). Data Is Giving Rise to a New Economy. Accessed October 21, 2019. https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

The Guardian. (2017). Climate Home, and part of the Guardian Environment Network. Tsunami of Data Could Consume One Fifth of Global Electricity by 2025. The Guardian.

The White House. (2013) .Presidential Policy Directive – Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The Wire. (2019). What Security Breach? The Unchanging Tone of UIDAIs Denials. Accessed February 1, 2018. https://thewire.in/tech/uidai-aadhaar-data-breach-right-to-privacy.

Thomas, D. R., Alastair, Beresford, R. & Rice, A. (2015). Security Metrics for the Android Ecosystem. In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM 15, 87–98. Denver, Colorado, USA: ACM Press.

Thomson, C. (2018). Accenture, What's the Cost of Cybercrime to Your Company and How Should You Respond?. https://www.accenture.com/us-en/blogs/blogs-cost-cyber-crime

ThreatMetrix. (2018). Q1 2018 Cybercrime Report. Global Insights from the ThreatMetrix.

Treadgold, A., & Reynolds, J. (2016). The Emergence of New Business Models. Boston Consulting Group. Navigating the New Retail Landscape.

Tynan, D. (2018). Huge Facebook Breach Leaves Thousands of Other Apps Vulnerable. The Guardian, Technology Section. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens.

U.S. Department of Defense. (2018) Summary of Cyber Strategy. https://media.defense.gov/2018/Sep/18/ 002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

U.S. Department of Homeland Security (2017). Cyber & Infrastructure (CISA). https://www.dhs.gov/CISA.

U.S. Department of Homeland Security (2017). Communications Sector. Accessed November 07, 2018. https://www.dhs.gov/communications-sector.

U.S. Department of Homeland Security. (2015). Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper (February 2015/1st Edition). https://www.dhs.gov/publication/isc-ppd-21-implementation-white-paper.

U.S. Government Accountability Office. (2007). Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. https://www.gao.gov/new.items/d071036.pdf.

U.S. SEC, Office of the Investor Advocate. (2018). 2011 MetLife Study of Elder Financial Abuse as quoted in Stephen Deane, Elder Financial Exploitation: Why it is a concern, what regulators are doing about it, and looking ahead. https://www.sec.gov/files/elder-financial-exploitation.pdf

UK Department of Health and Social Care. (2018). Securing cyber resilience in health and care. Progress Update. https://assets.publishing.service.gov.uk/ government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf

UK Government. (2018). New Fines for Essential Service Operators with Poor Cyber Security. https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

UK Government. (2019). Cyber Security Breaches Survey 2018. https:// assets.publishing. service.gov.uk /government /uploads/system/uploads/attachment_data/file/ 702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

UK Parliament. (2019). Cyber Security of the UKs Critical National Infrastructure - Joint Committee on the National Security Strategy - House of Commons. Accessed January 10. https://publications.parliament.uk/pa/jt201719 /jtselect/jtnatsec/ 1708/ 170802.htm.

Universität Basel (2017). From Healthcare to Warfare: How to Regulate Brain Technology. December 17, 2017. Accessed January 21. https://www.unibas.ch/en/News-Events/News/Uni-Research/From-Healthcare-to-Warfare.html.

Valentino-Devries, J., et al. (2018). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. The New York Times. Accessed January 11, 2019. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?action=click&auth=login-email.

Vincent, S. (2018). Pool Re extends retro programme to include cyber terrorism cover. https://insuranceday.maritimeintelligence.informa.com/ID1121541/Pool-Re-extends-retro-programme-to-include-cyber-terrorism-cover

Wang, B. (2017). Characterizing and Modeling Patching Practices of Industrial Control Systems. Proceedings of the ACM on Measurement and Analysis of Computing Systems 1 (1): 1–23.

Willis Towers Watson. (2019). Careful How You Code: Cyberterrorism Coverage under TRIA and Stand-Alone Cyber Policies. Accessed February 19, 2018. https://www.willistowerswatson.com/en-GB/insights/2017/07/decode-cyber-brief-careful-how-you-code.

Wilshusen, G. (2012). Cyber Security: Challenges in Securing the Electricity Grid. U.S. Government Accountability Office. https://www.gao.gov/assets/600/592508.pdf.

Wired. (2019). Feds: Hacker Disabled Offshore Oil Platforms Leak-Detection System. Accessed February 19. https://www.wired.com/2009/03/feds-hacker-dis/.

Woollaston, V. (2018). How to access the dark web: What is Tor and how do I access the dark websites?. Alphr. Accessed February 2018.

Wooton, Benjamin. (2018). Using DevSecOps to Meet Regulatory Challenges in Investment Banking. Contino. https://www.contino.io/insights/using-devsecops-to-meet-regulatory-challenges-in-investment-banking. Accessed 22 January.

World Economic Forum (2016). Impact of Digital Media on Individuals, Organizations and Society. Collaboration with Willis Towers Watson. Accessed February 08. http://reports.weforum.org/human-implications-of-digital-media-2016/section-3-impact-of-digital-media-on-individuals-organizations-and-society/. Part of the broader series: *Digital Media in Society-Implications in a Hyperconnected Era*

Yanofsky, D. (2019). Every US Airline Glitch in 2015, 2016, and 2017. Quartz. Accessed January 7. https://qz.com/535967/tech-glitches-keep-plaguing-us-airlines-this-dashboard-keeps-track-of-them-all/.

Zetter, K. (2015). A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. Wired. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

Citi Global Perspectives & Solutions (Citi GPS) is designed to help our clients navigate the global economy's most demanding challenges, identify future themes and trends, and help our clients profit in a fast-changing and interconnected world. Citi GPS accesses the best elements of our global conversation and harvests the thought leadership of a wide range of senior professionals across the firm.

All Citi GPS reports are available on our website www.citi.com/citigps

Bank X
The New New Banks
March 2019

2019 Corporate Finance Priorities
January 2019

Investment Themes in 2019
January 2019

Car of the Future 4.0
The Race for the Future of Networked Mobility
January 2019

China's Belt and Road Initiative
A Progress Report
December 2018

Feeding the Future
How Innovation and Shifting Consumer Preferences Can Help Feed a Growing Planet
November 2018

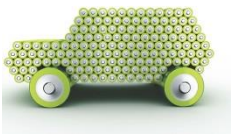
Migration and the Economy
Economic Realities, Social Impact, & Political Choices
September 2018

Rethinking Single-Use Plastics
Responding to a Sea Change in Consumer Behavior
August 2018

Disruptive Innovations VI
Ten More Things to Stop and Think About
August 2018

Putting the Band Back Together
Remastering the World of Music
August 2018

UN Sustainable Development Goals
A Systematic Framework for Aligning Investment
June 2018



Electric Vehicles
Ready(ing) For Adoption
June 2018

ePrivacy and Data Protection
Privacy Matters: Navigating the New World of Data Protection
May 2018

Sustainable Cities
Beacons of Light Against the Shadow of Unplanned Urbanization
April 2018

Disruptors at the Gate
Strategic M&A for Managing Disruptive Innovation
April 2018

The Bank of the Future
The ABC's of Digital Disruption in Finance
March 2018

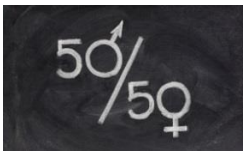
The Public Wealth of Cities
How to Turn Around Cities Fortunes by Unlocking Public Assets
March 2018

Securing India's Growth Over the Next Decade
Twin Pillars of Investment & Productivity
February 2018

Investment Themes in 2018
How Much Longer Can the Cycle Run?
January 2018

2018 Corporate Finance Priorities
January 2018

China Entering a New Political Economy Cycle
The World According to Xi Jinping Thought
December 2017



Women in the Economy II
How Implementing a Women's Economic Empowerment Agenda Can Shape the Global Economy
November 2017

Disruptive Innovations V
Ten More Things to Stop and Think About
November 2017

Inequality and Prosperity in the Industrialized World
Addressing a Growing Challenge
September 2017

Technology at Work v3.0
Automating e-Commerce from Click to Pick to Door
August 2017

Education: Back to Basics
Is Education Fit for the Future
July 2017

Solutions for The Global Water Crisis
The End of 'Free and Cheap' Water
April 2017

ePrivacy & Data Protection
Who Watches the Watchers? – How Regulation Could Alter the Path of Innovation
March 2017

Digital Disruption - Revisited
What FinTech VC Investments Tells Us About a Changing Industry
January 2017

2017 Corporate Finance Priorities
January 2017

2017 Investment Themes
A Wind of Change
January 2017

Car of the Future v3.0
Mobility 2030
November 2016

Infrastructure for Growth
The dawn of a new multi-trillion dollar asset class
October 2016

Virtual & Augmented Reality
Are you sure it isn't real?
October 2016

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

NOW / NEXT

Key Insights regarding the future of Cyber Security

INFRASTRUCTURE

A number of deliberate, targeted cyber attacks on areas of critical national infrastructure have occurred in part of the Europe and the Middle East/ As key utilities in the supply of power, water, healthcare, and transport become increasingly integrated with digital systems, the system as a whole becomes more reliant on the securitization of all parts.

REGULATION

Despite all governments facing threats from cyber, each country is addressing the threat in their own way. / Some collaboration between national governments has occurred and the UN General Assembly has adopted two separate resolutions on the action of nation states in cyberspace but there is no international legislation.

TECHNOLOGY

Corporations currently house their tech architecture on-premise and are able to use firewalls to protect their networks. / As enterprises/corporations move their workloads to the public cloud and their tech components are resident in the data center of IaaS, PaaS, or SaaS providers, virtual firewall and cloud access security brokers (CASB) will become dominant.