# Cybersecurity Awareness

## Implementing Effective Staff Training and Communications

Treasury and Trade Solutions

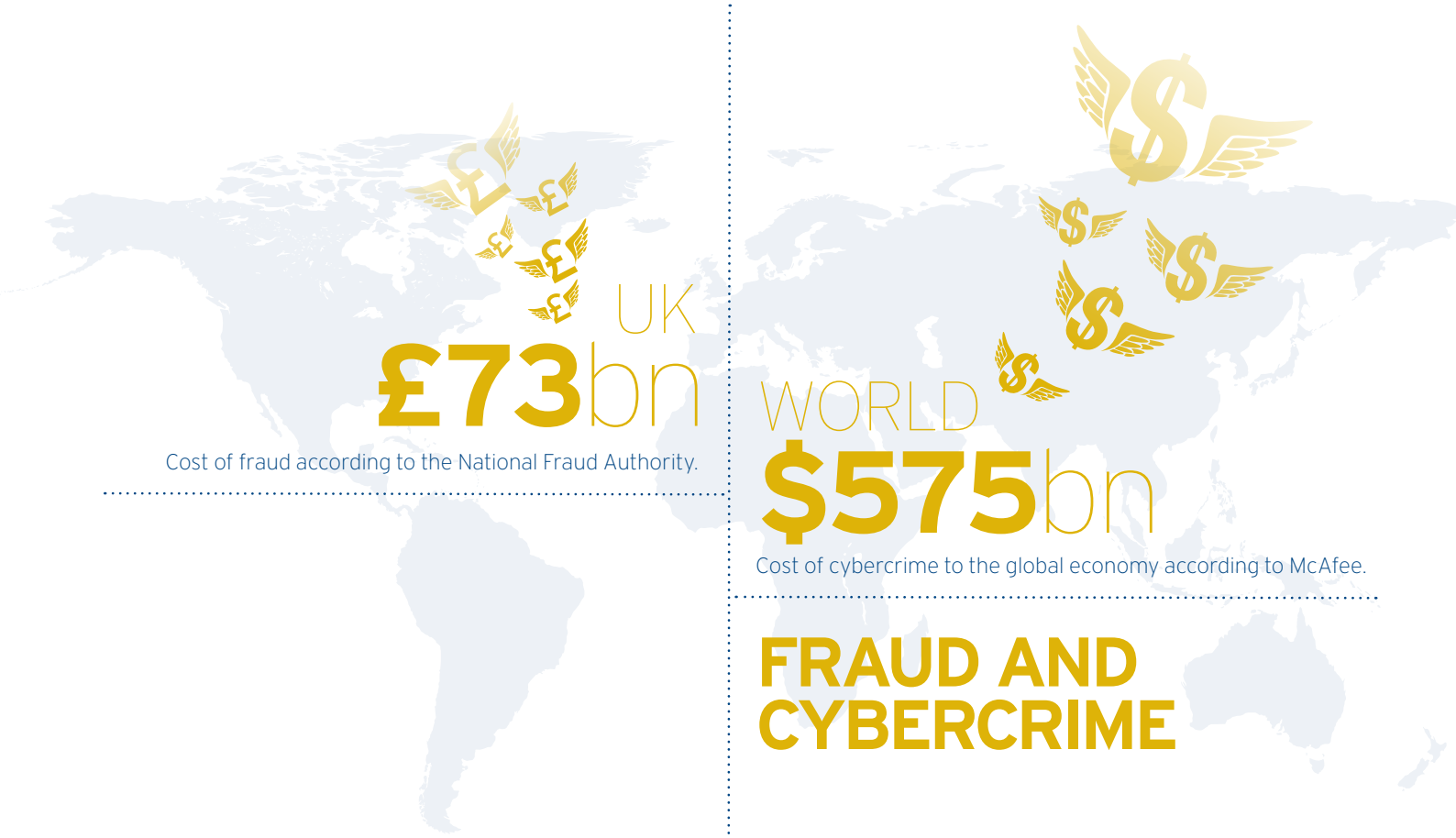
citi

# How Effective is Your Cybersecurity Staff Training and Communications Programme?

Fraud in the UK costs the economy over £73 billion a year, while cybercrime could cost the global economy up to USD575 billion.

By knowing what tactics are being used to drive fraud and cybercrime, businesses can work basic controls into their policies and processes.

What follows is a short guide that you can use straight away to help you start developing a training programme for your organisation to raise awareness of this very widespread and potentially damaging corporate crime.



# Think You Know Cybercrime?

Saying cybercrime is an act of deception by an attacker trying to deprive a target of goods, services or money only tells half the story. An act need not have succeeded or resulted in the attacker's personal gain: it need only have been intended to create a loss or a risk of loss to the target.

We are all familiar with the headline-grabbing dollar-figure cost of cybercrime to the global economy. But when an attack only has to create a risk of loss – that another need not have been deprived of any goods, services or money – the stakes for businesses are all at once higher. In fact, estimates suggest some 800 million people may have had their information stolen (McAfee). That puts organisations across the financial spectrum at risk.

But knowing that the cost and the risks to a business are really the byproduct of a human action – that there are attackers motivated and prepared to seize opportunities to commit fraud (learn why people commit fraud on page 3) – brings the matter to a point: counteraction is the best line of defence.

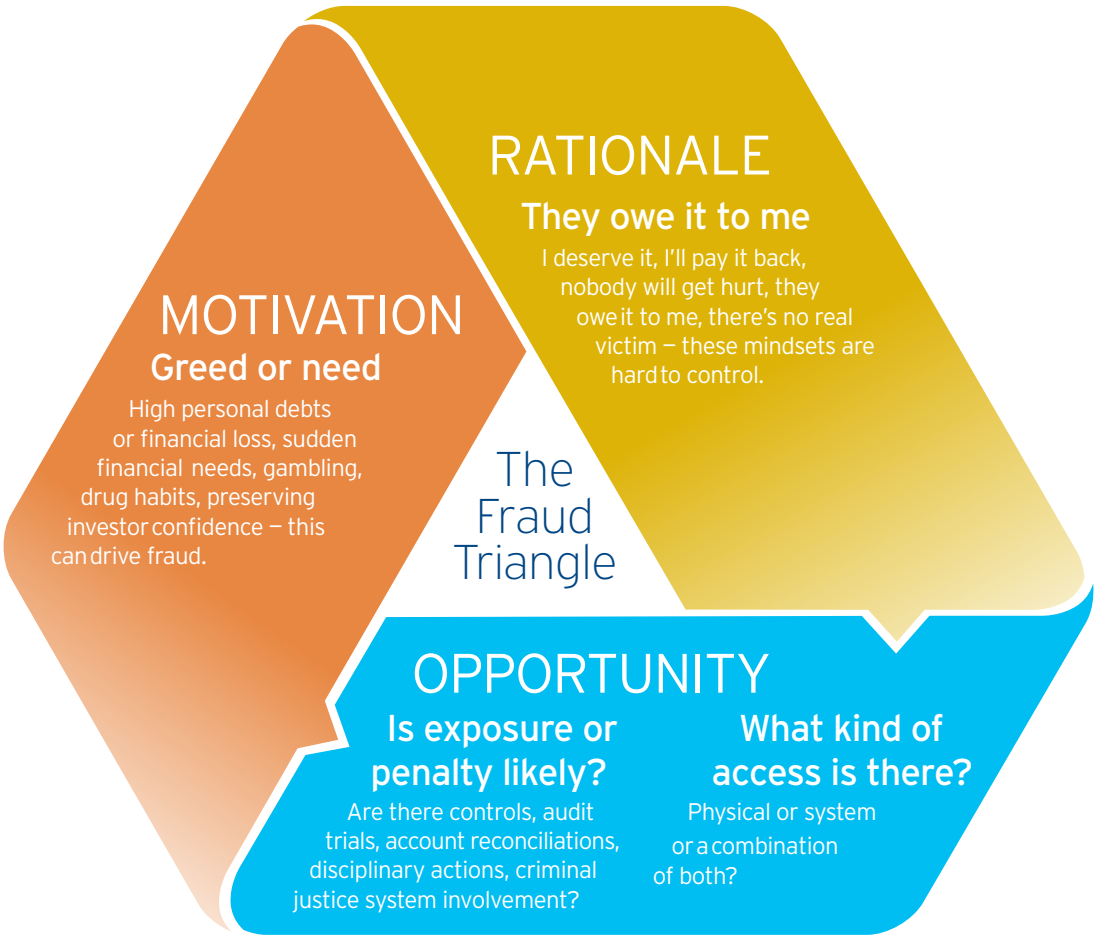
Implementing an informed cybersecurity staff training programme is a good way to go. The pages following present a three-phase approach to make a start: phase one: **pre-deployment**; phase two: **deployment**; and phase three: **post-deployment**.


AROUND 1 IN 8 PEOPLE
or 12% of the world's population
could be a victim...

**HAVE 800 MILLION PEOPLE LOST INFORMATION EITHER TO FRAUD OR TO CYBERCRIME TODAY?**

# Why Do People Commit Fraud?

There are many answers to this question, but strong indicators tell us that they appear to fall under three categories that make up the fraud triangle – motivation, opportunity and rationale.



# PHASE 1 PRE-DEPLOYMENT

The first phase is to prepare your communications and training programme for deployment. The evidence shows that having full senior management buy-in from the outset can guarantee the programme will have traction beyond deployment.

## Get Endorsement

To launch an effective programme, you will need support from management. Getting senior managers or controllers to endorse and sponsor the programme will give it the impetus it needs.

## Agree the Approach

Get senior management to agree on what the business's approach will be to managing fraud and security threats. This will set an authoritative "tone from the top" that others will follow.

## Make the Business Case

Use industry-specific fraud and cybersecurity metrics and intelligence to make the business case to senior management. If you need industry scenarios to support your case for your programme, Citi can help.

## Look at Gaps and Risks

If you haven't looked at your existing policies and procedures or evaluated where potential risks lie, you can't know what controls to put in place. Analysing gaps and assessing risks will help.

In particular, they tell you where to modify existing or create new protocols, reinforcing weak points, e.g. conducting a risk assessment of your supply chain practices could see if counterparties are complying with company policy and if you are mitigating any risks as a result.

Citi can provide case studies that illustrate the types of fraud and cyberattacks that are being experienced. Your existing policies and procedures should be evaluated in light of this information to ensure that you are protected from these common attacks.

## Assign Responsibilities

Senior management should nominate, approve and relay to all staff responsibility for managing fraud and cybersecurity. What these staff members do should be clearly defined and documented, and any staff so appointed should be given suitable training. This ensures that in the case of actual or suspected fraud or a cyberattack staff are aware of their roles and responsibilities and can act quickly.

## Escalate and Respond

Develop an escalation and post-incident response procedure that is a part of the programme. Housed and encrypted on your intranet, it should be accessible to all staff, covering more than just internal and external investigation procedures and contacts.

The incident-response component should also cover bank contacts and escalation touchpoints, lateral and vertical fraud and cyber-incident escalation, primary and secondary legal counsel, and even when and how to engage law enforcement.

## Create a Test Strategy

To monitor the effectiveness of the fraud and cybersecurity training programme, develop and then implement an efficient test strategy or form of self-assessment for it.

# PHASE 2 DEPLOYMENT

The second phase involves creating and rolling out your programme. Again, experience shows there are some points to keep top of mind to ensure it reaches your staff as effectively as possible.

## Create and Roll It Out

As you create your programme, there are some essential programme elements that should be included. Start by identifying your risk-based target audience, and tailor training and comms collateral appropriately for appointed key security administrators.

Then agree your deployment calendar, bearing in mind holidays and business events, agreeing the format and method of distribution for all materials in keeping with the company's size and its geographical span, which may make remote training most effective.

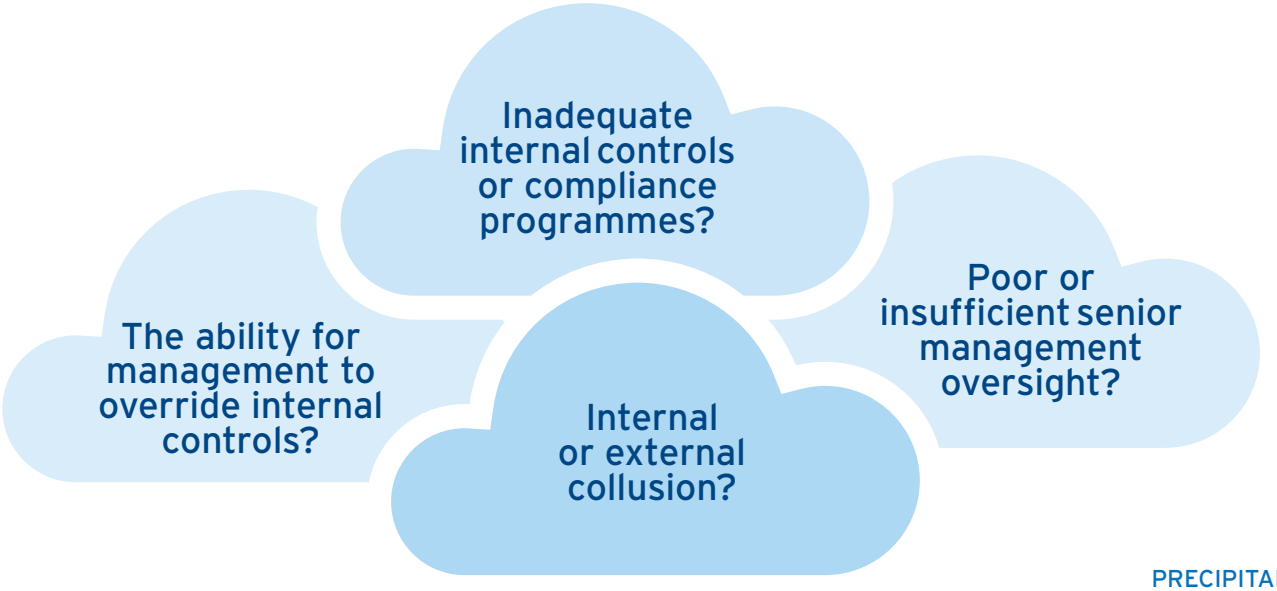
## Keep These Tips in Mind

Develop a calendar and targeted content. Dates for training and comms should be rolling, flexible and planned around holidays or other business activities. And be sure to disseminate content from your "toolkit" that is relevant to staff and their area of business, especially in light of any recent or attempted fraud or cybersecurity incidents.

Avoid duplicate efforts and spamming. Check that you aren't duplicating what other fraud and cybersecurity administrators within your company might be doing. Bear in mind, too, that when you over-communicate you risk turning your important awareness and training material into spam.

Tailor your training and be flexible. Adapt training to your target audience – for example, training on social engineering fraud might be suitable for customer service reps or entitlement review for managers. And don't limit activities to your deployment project plan: if an ad hoc need arises to promote topics in light of current events, do it.

# What Precipitates Fraud?




PRECIPITANTS

PRECIPITATES

# PHASE 3 POST-DEPLOYMENT

The third and final phase involves maintaining programme momentum. Fraud and cybersecurity threats are constantly evolving, adapting to how businesses work and changing to circumvent their defences.

## Plan Continuous Comms

Send out frequent communications and training prompts so you don't lose momentum or impact (but not so often as to run the risk of having your content seen as spam). Developing a comms calendar will allow you to release critical, updated or timely information, especially in response to attack attempts or new intelligence.

## Measure Success

Use key performance indicators (KPIs) and measurement tools to find out if your programme is running smoothly, ensuring the right controls are in place and performing as intended. Some examples of KPIs include:

- Mystery shopping, for example distributing placebo emails or phone calls to help gauge whether staff are responding to potential internal and external threats.
- Fraud or cyber metrics: these help to indicate whether or not increased referrals or escalations of suspicious activity are being dismissed or following protocol.
- Surprise audits: these are most effectively conducted and especially useful when undertaken during periods of staff absence, especially prolonged absence.

## Make It Easy to Access

Ensure your training materials are visible and easy to access: if you are able to add to your company intranet, develop a webpage that hosts all essential fraud and cybersecurity materials and links.

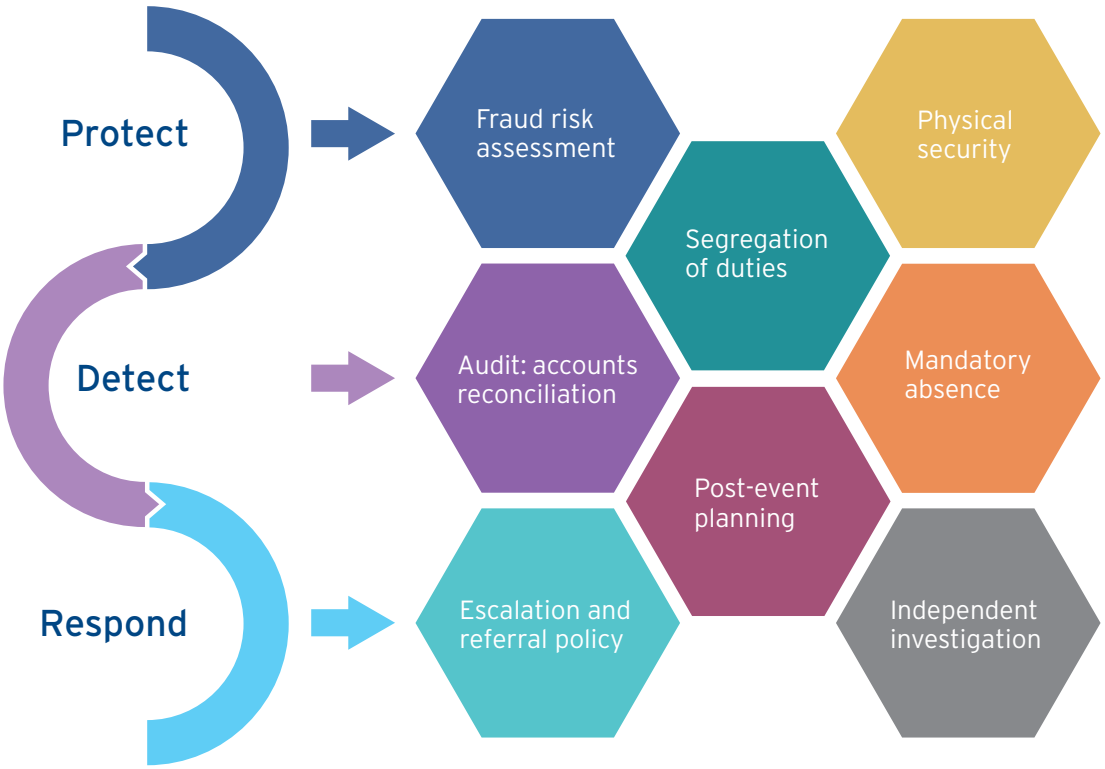
## Accredit Your Staff

Consider developing a fraud and cybersecurity curriculum for staff that includes industry endorsements from external specialists, such as certification from the Association of Certified Fraud Examiners (ACFE).

## Undertake Continual Reviews

The fraud and cybersecurity landscape is continually evolving, keep up to date on the latest trends and threats and review your programme to ensure there is adequate information and training available to staff to manage the latest threats.

### Developing a strategic defence that uses people, processes and technology...



**www.citi.com/treasuryandtradesolutions**



GRA29064 01/18