Compliments of:

MetaCompliance®

Cyber Security Awareness

for dummies®
A Wiley Brand

Change staff security culture

Create a more security conscious workforce

Follow this playbook for cyber security campaigns

Robert O'Brien

Geraldine Strawbridge

MetaCompliance Special Edition

About MetaCompliance

MetaCompliance has over 14 years' domain expertise in staff security training and awareness. Working with clients across all industries, the company helps organisations protect their data, educate staff and manage reputational and regulatory risks. In that time, the regulatory challenge for organisations has increased along with the threat landscape associated with their digital assets.

The company is a thought leader in the 'human aspect' of cyber security and compliance. The MetaCompliance team work daily with public and private sector clients to implement best practice staff security awareness campaigns that really engage people and change behaviour.

Its graphically engaging SaaS platform provides customers with an integrated, multilingual suite of capabilities that includes Simulated Phishing, Cyber Security and Compliance eLearning, Policy Management, Privacy Management and Incident Management. Organisations gain greater regulatory protection through a 'one stop shop' for managing privacy, compliance and cyber projects that make it easier for staff to undertake their compliance obligations.

MetaCompliance's innovative MyCompliance cloud architecture is built upon the Microsoft Azure platform, providing a global enterprise solution. MetaCompliance is based in London, UK; Dublin, Ireland; and Atlanta, GA, with a growing customer base in both the public and private sector.

Cyber Security Awareness

for dummies®
A Wiley Brand

Cyber Security Awareness

MetaCompliance Special Edition

by Robert O'Brien, Cyber Security and Compliance Expert
Geraldine Strawbridge, Cyber Security Editor

for dummies®
A Wiley Brand

Cyber Security Awareness For Dummies®, MetaCompliance Special Edition

Published by: **John Wiley & Sons, Ltd.**, The Atrium, Southern Gate

Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-59826-8 (pbk); ISBN 978-1-119-59827-5 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

Over the past decade, the cyber security landscape has changed dramatically. According to Cybersecurity Ventures, by 2021, the global cost of cybercrime is expected to reach $6 trillion, making it more profitable than the entire global illegal drugs trade. Organisations of every size and in every industry have become potential targets for cybercriminals. New threats are emerging all the time and organisations can no longer just rely on their technological defences to keep them safe.

Cybercriminals target the weakest point in an organisation's defences and, all too often, that's your employees. A huge 90 percent of all data breaches can be attributed to human error, which is why organisations must commit to a cyber security awareness program that enables all staff to recognise and embrace the important role they play in safeguarding sensitive company data.

About This Book

Cyber Security Awareness For Dummies, MetaCompliance Special Edition, consists of six chapters that explore the modern cyber security landscape (Chapter 1), the need for cyber security awareness (Chapter 2), the adoption of cyber security campaigns to promote change (Chapter 3), the integration of policy management into security awareness programs (Chapter 4), the ways to develop a best practice cyber awareness strategy (Chapter 5) and security awareness best practices (Chapter 6).

Each chapter stands on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though we don't recommend upside down or backwards).

Foolish Assumptions

When we wrote this book, we assumed that you're a cyber security or IT professional such as a chief information officer (CIO), chief technology officer (CTO), chief information security officer

(CISO), chief privacy officer (CPO), data protection officer, IT director, head of IT, human resources (HR) manager, training manager, change manager or even a senior executive.

If any of these assumptions describe you, then this book is for you. If none of these assumptions describe you, keep reading anyway. When you're finished, you'll have a heightened awareness of cyber security.

Icons Used in This Book

We occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your grey matter or your noggin.

TIP

We hope you appreciate these useful nuggets of information.

WARNING

These alerts point out practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much we can cover in these short pages, so if you find yourself at the end of this book, thinking, 'Gosh, this was an amazing book, where can I learn more?' check out `www.metacompliance.com`.

IN THIS CHAPTER

- Surveying the evolving threat landscape
- Recognising what makes a cybercriminal tick
- Making security awareness integral to digital transformation
- Clarifying security frameworks and data protection
- Looking at regulatory compliance mandates

Chapter 1
Understanding the Modern Cyber Security Landscape

In this chapter, you discover how sophisticated cyber threats, as well as greater levels of governance, data protection regulations, and the need for security by design have increased the need for cyber security awareness in the modern organisation.

Looking at Cyber Threats That Target People

Cybercrime has rapidly developed into one of the greatest threats affecting organisations across the world. Attack vectors are changing, as cybercriminals utilise a range of different tactics to gain access to valuable corporate data.

If organisations are to minimise the risk of a security breach, they need to understand the different types of cyber threats that could be used to target them:

- **Phishing:** *Phishing* is a type of social engineering attack that attempts to trick victims into disclosing sensitive information or installing malware. Using email, social media, phone calls and text messages, cybercriminals masquerade as a trusted entity to manipulate their victim into performing a specific action. This could be clicking on a malicious link, downloading an attachment, visiting a spoofed website or wilfully disclosing sensitive information. The information can then be used to access personal accounts or commit identity theft.
- **Malware:** *Malware* is a type of malicious software designed to damage or gain access to a computer system without the user's knowledge. Examples of malware include viruses, worms, Trojan horses, spyware, adware and ransomware. Malware is typically installed on a computer when a user clicks on a link, downloads a malicious attachment or opens a rogue software program. Once installed, malware can steal, delete or encrypt sensitive data. It can also block core computing functions, rendering a system inoperable.
- **Insider threat:** An *insider threat* is a security incident that originates within an organisation as opposed to one from an external source. It may be a current or former employee, a contractor, a third-party vendor or any other business associate that has access to the organisation's data and computer systems. Insider attacks can be particularly dangerous because, unlike external actors attempting to infiltrate a network, insiders typically have legitimate access to an organisation's computer systems.
- **Supply chain attacks:** A supply chain attack, also known as a *third-party attack*, attempts to damage an organisation by exploiting vulnerabilities in its supply chain network. *Supply chain attacks* have the potential to infiltrate an entire network through a single compromise. They can be harder to detect than traditional malware attacks.

WARNING

Human nature is a key vulnerability, and cybercriminals know how to exploit it.

Understanding Attacker Profiles and Motivations

Popular culture has depicted hackers in a variety of ways, often as a hooded figure in a basement, or a disgruntled teen intent on putting the world to rights. One of the more notable Hollywood examples is fictional hacker Lisbeth Salander, the main character in *The Girl with The Dragon Tattoo* (Millennium Trilogy) by Stieg Larsson. When the character is first introduced, she applies her hacker skills on behalf of a private security firm. But as the plot thickens, her hacking skills are motivated by revenge, which ultimately allows her to pull off an audacious financial fraud against one of the main villains in the story. This story illustrates the fact that people involved with cybercrime are driven by many different motivations.

Understanding their motivations is important for your organisation in knowing how to deal with hackers. These are some of the reasons hackers do what they do:

- **Financial:** Money is the biggest motivating factor for all criminal activity and cybercrime is no different. It's theft in the digital age, and it's a lot easier to pull off than holding a bank up with a gun. Despite the high-profile hacks of big brand names, there is an increasing focus on small and medium-sized businesses that have weaker security practices. The reality is that it's far more lucrative for a hacker to target multiple smaller organisations rather than a Fortune 100 company that has invested millions in bolstering its technological defences.
- **Espionage:** Hackers frequently use cyber espionage to steal classified information, intellectual property or trade secrets. Whether it's a nation state attack or corporate spying, espionage now poses a significant threat to all organisations.

  Breach after breach highlights just how active hackers have become in pursuing the two key areas of information that motivate them — political and manufacturing.

  Critical infrastructure like transport, water, telecommunications and utilities also experience the persistent attention of state-backed entities. The weaponisation of malware by foreign government entities will tax all but the largest and

REMEMBER

best-resourced organisations, and the startling fact is that the primary facilitator of these attack vectors is people. Social engineering and the exploitation of inadequate security practices are the first areas a cybercriminal will attempt to exploit. For this reason, it's imperative that organisations mobilise their own workforce to help defend against these threats. Implementing a fit for purpose staff awareness program is fundamental in defending your organisation.

- **Fun:** Many hackers are motivated by the thrill and the excitement of infiltrating a company's computer system. For example, at this year's Pwn2Own ethical hacking competition, organisers provided a Tesla Model 3 for participants to hack into. Within a day, two hackers exposed a security bug that allowed them to hack into the car's internal web browser. Rather than face prosecution, the duo walked away with their own Tesla Model 3, $375,000 in prize money and, most importantly of all, recognition from their peers, which is highly sought after in the hacker community.
- **Hactivism:** *Hacktivism* is the act of hacking a computer system or network for politically or socially motivated purposes. There always have been and always will be people engaging in activism for a specific cause that runs contrary to the governing body. What's new is the all-pervasive technology.

  Technology has been weaponised and is increasingly being used to promote ideological aims. One of the reasons for this growth is that launching a cyber-attack is much cheaper compared to direct military action.
- **Resource theft:** Siphoning off computing resources from the general public to mine bitcoin has become a profitable business. Mining bitcoin is all about electricity and processing power, and hackers are exploiting every opportunity they can to steal these resources. Even multinational organisations like Starbucks have fallen victim. For example, a store in Buenos Aires recently discovered that its instore wi-fi had been hacked and that fraudsters were using it to mine bitcoin on unsuspecting customers' devices.
- **Other:** This category includes insider threats, unintended data leaks, misconfigurations, user mistakes and a raft of other threats unrelated to third party hacking efforts. The most likely methods for a compromise are unpatched software and social engineering. These threats represent the biggest risk for most organisations.

Security Frameworks and Data Protection

The most important questions to ask your organisation are: ***What is the best way to implement a security management system for my organisation, and what are the parts involved?***

One answer is the ISO27001 standard, which lays out a best practice approach to information security management.

ISO27001 – The global cyber security standard

Privacy and data protection are important initiatives for modern organisations. The readiness and maintenance activities for privacy are a significant undertaking for any organisation, so it's important that employees are given appropriate time and training to understand the day-to-day obligations of privacy in their jobs.

ISO27001 is a true global security standard, and it's also the only one that is subject to external audit. It enables organisations to have a uniform approach to demonstrate that they're operating to best practice information security processes. Many of the benefits of ISO27001 relate to the fact that the certificate demonstrates the organisation's preparedness in the event of something going wrong. An ISO27001 certificate has become an increasingly valuable business asset as customers look to their supply chain for reassurance on cyber risk.

Reaping the benefits of ISO27001

The effort and management involvement necessary to obtain ISO27001 accreditation ensures that the organisation increases its cyber security maturity. In addition, other benefits include:

- Increased business resilience and protection against security failures
- Improved customer confidence
- Increased reliability and security of core systems and information assets
- Increased focus on risk and its impact on the business

A fit-for-purpose staff awareness regime is required to obtain ISO27001. Specifically, clause 7.2, 7.3 and 7.4 of ISO IEC 27001 focus on awareness and understanding of the information security management system (ISMS) that is being certified. General cyber security training won't necessarily fulfil the requirements of compliance within ISO27001, especially as every organisation's ISMS is unique to the set of risks and systems underpinning their operations.

It's critical that staff members are made aware of the workings of the security processes within their organisations, which usually involves tailored training on the organisation's ISMS. A best practice awareness campaign will cover key cyber threats from phishing to physical security and will also support participation and understanding of the ISO27001 initiative. Specific training relating to the organisation's ISMS is also required, which can be something as simple as an organisation-wide webinar to provide insight into its workings.

TIP

Ensuring that your ISMS is the starting point for your cyber awareness campaign will avoid user fatigue by focusing on the specific cyber threats that are relevant to your organisation and your people. As your threat landscape evolves, so will the response contained within your ISMS. The key is to take your staff on this journey and ensure they're notified of any changes.

Another highly respected framework that's widely used by organisations across the world to standardise processes, reduce risk and improve cyber security operations, is the NIST Cyber Security Framework (see sidebar).

NIST CYBER SECURITY FRAMEWORK

The US National Institute of Standards and Technology (NIST) created the Cyber Security Framework (CSF) to provide organisations with guidance on how to prevent, detect and respond to cyber incidents. The internationally recognised framework outlines a set of best practices, standards and recommendations that help an organisation improve its cyber security posture.

The NIST CFS was initially designed for improving critical infrastructure services but has since been adopted across a variety of industries and has helped organisations become more proactive about risk management.

The framework is divided into these three parts:

- **The Framework Core** provides a set of activities to achieve specific cyber security outcomes. The framework core is based on five functions:
  - **Identify:** Develop the organisational understanding to manage cyber security risk to systems, assets, data, and capabilities.
  - **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
  - **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
  - **Respond:** Develop and implement the appropriate activities to take action in response to a detected cyber security event.
  - **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

These functions are further subdivided into 22 categories and 98 subcategories.

- **The Framework Implementation Tiers** provide context on how organisations view risk and what processes can be put in place to mitigate this risk.
- **The Framework Profile** describes the desired outcomes, based on the framework categories and subcategories.

The Importance of Staff Awareness in Digital Transformation Projects

Digital transformation projects are exciting initiatives within modern organisations. They represent an opportunity for the enterprise to exploit new technologies and adopt products that reduce costs and result in an increase in revenue.

Digital transformation projects are typically ambitious strategies to change the way a company does business using digital technology.

These projects are major change management initiatives, and require significant investment in staff communications. These communications seek to elicit staff support and excitement. Often these initiatives fail to focus on the risk of not exerting due care and diligence on IT security and compliance. However, that's exactly what is required to strike a balance between transformation at all costs and ensuring proper control and safeguards. Head to Chapter 3 to delve more deeply into how best to communicate with staff.

IN THIS CHAPTER

- Grasping the risk profile
- Recognising the challenges of creating a more vigilant workforce
- Being aware of risk and keeping cyber security relevant

Chapter 2
Establishing the Need for Cyber Security Awareness

Very few how-to guides or playbooks provide the necessary guidance on how to plan, develop and implement a staff cyber security awareness program. One of the reasons for this is that the information security industry has been obsessed with traditional technology such as firewalls and anti-malware solutions. These technological defences have provided a false sense of security that the perimeter is being defended.

Despite this heavy investment in perimeter security, there was, and still is, a level of 'plausible deniability' that one single employee's actions can totally circumvent these controls.

With the increasing regularity of data breaches at blue-chip organisations, there is worldwide recognition that the consequences of these incidents are too grave to ignore. Hence, the issue has made its way to the agenda of most modern organisations' boards. Furthermore, regulators are increasingly using sanctions and fines to drive compliance with new data protection regulations. These and other macro influences have meant that a root-and-branch change is required in how employees operate and how they minimise risk.

Having an executive board recognise the importance of cyber security risk as a legitimate business liability is a major step in an organisation becoming more mature. The key restriction of any cyber security awareness project is the extent to which the leadership in the organisation recognises cyber risk and gives it the same significance and resources as financial risk. Chapter 5 discusses more about having executive support for your campaign.

This chapter explains in greater detail what you can to do ensure your organisation is aware of cyber security.

Understanding the Risk Profile

What would happen if your organisation got hacked? What is the likelihood and what would the impact be? To understand the answers to these questions, you need to understand the unique risk profile your organisation faces. The extent to which cyber threats relate to your organisation determines the level of vulnerability that your organisation experiences. Understanding these vulnerabilities and putting in place remediation plans represents a best practice approach to reducing your organisation's exposure to cyber security risk. This is especially pertinent when pertaining to your staff and supply chains because they're common routes of attack by malicious third parties.

The following sections provide hands-on information to help your organisation reduce its risk.

Implementing a risk awareness campaign

Addressing staff behaviours relating to cyber security and data protection risks is important. An awareness campaign seeks to remediate the risks that arise from the human aspect of cyber security.

However, security awareness campaigns that focus solely on delivering staff cyber security training as quickly as possible have limited success. Real behavioural change needs continuous training combined with a major effort on behalf of the organisation. It also needs time, because people are naturally resistant to change.

Identifying your staff's understanding of risk

Your organisation has a few ways to quickly determine your people's understanding of security risks. They include the following:

- **Send all staff a simulated phish and see how many employees fall for it.** Pay particular attention to those users who were prepared to input credentials or real information based on a prompt from a phishing email. This click-through rate will provide you with a starting point.
- **Do a quick analysis of incidents over the previous 12-month period.** Are there similar incidents that resemble a trend or recurrence? Prioritise your awareness program around these risks.

This information is also crucial in explaining to staff why cyber training is so important. For example: 'In the last year, 20 laptops were lost at this company. Please increase your understanding of best practice device management by taking the attached eLearning.'

Focusing training only on who needs it

Cyber security awareness with context and segmentation has enhanced effectiveness. For example, training all staff on laptop and device control is ineffective if only a small number of staff possess a laptop. Only those employees with a device need that type of education. Having the entire employee population undergo generic security training is counterproductive. Where possible, your organisation should target awareness training to an individual's specific role and risk.

Cyber security awareness campaigns have more impact if they relate to understandable risks and when people can identify the real-world consequences that result from negligent cyber security practices.

TIP

Organise information security risks around people and technology assets. The latter relates to an organisation's critical business systems and the data that resides on these systems. From an awareness standpoint, ensuring that the right messages get to the right people at the right time is important. Also, recognise that different users and different data have greater importance in terms of risk.

For example, the Finance Department has a greater risk of a cyber attack than a member of the cafeteria staff. The concept of weighting is important in constructing an awareness campaign because it helps you to focus on your high-risk employees rather than generically targeting everyone.

Recognising who needs more training

Spending time crafting specific communications or providing relevant training to these staff groups is extremely effective, especially if you use language that they're familiar with.

Identifying your vulnerable staff groups takes time. However, the three most important groups that require additional risk training are as follows:

- **The Finance Department:** This department is usually the most at-risk department to be targeted in an organisation because it controls the money.
- **Technical privileged users:** These users are targeted because they can be used to escalate a cyber breach due to their privileged access to secure systems.
- **Senior executives within the company:** The senior executives are targeted because they have authority that can be used to escalate a cyber breach.

Don't forget your entire supply chain and partner network. That's also a large part of your risk profile. Chapter 3 discusses in greater detail how you can identify critical third parties, the risk they pose in a modern agile organisation, and ways to include them in your cyber security activities.

In addition, the length of time that people have been in the organisation relates to the ease with which their behaviour can be changed. New users can accept policies and learn new working methods because they have a more flexible mindset. However, longer-serving staff members can prove more problematic with learning new methods.

Furthermore, identifying the number of commonly used regional languages in your organisation is also important in mapping your risk profile. Not only will multiple languages make a staff awareness program more difficult, but they increase the number of threat vectors that your organisation has to deal with.

For example, an organisation that operates in Brazil has to worry about phishing emails in Portuguese as well as English. Identifying your key cultural and linguistic audiences is important in making the security awareness program relevant to staff.

Prioritising security risk

In many organisations, security hasn't been prioritised to staff in the same way as financial risk. Security was not thought of as a necessary aspect of business as usual, and as a result, users have developed bad habits over several years. Hence, implementing a security awareness campaign is more difficult. The campaign needs to educate users on security, but it also needs to overcome bad habits that have accumulated over time. Only by being consistent and repeating your campaign messaging can your organisation win your employees over.

Legacy systems that are difficult to change are often used as a reason why behavioural change isn't necessary. You may have heard the old saying: 'Our system does it this way, so it's pointless trying to change.' Overcoming this way of thinking isn't easy.

Security challenges surrounding legacy systems can lead to a feeling of hopelessness in how security threats are viewed. For example, where an access control system is managed on a retired Windows operating system, you can understand that replacing all the electronic locks in an organisation for a system that otherwise works perfectly may not be the best investment.

However, these types of legacy systems have to be remediated as soon as possible. Staff need to know that the organisation has identified these challenges and is actively tackling them. Although these activities are background activities and outside the scope of a staff security program, progress on these issues is essential to the integrity of a staff awareness campaign.

Making Cyber Security Real for People in Your Organisation

Cyber security awareness programs are unlikely to inspire enthusiasm among staff and management.

REMEMBER

When thinking about putting together a program to improve staff awareness of information security, bear in mind that most people spend very little, if any, time thinking about this issue. Cyber security is a tough subject to make interesting. However, it's the responsibility of the organisation to make its security communications palatable and even enjoyable, if possible, for their employees.

Obtaining user participation in your cyber awareness programs is one of the key measures of success. For example, if you send out a risk assessment or a piece of eLearning and only 50 per cent of your staff participate by completing the content, you have a big problem. A significant portion of the audience is disengaged. More importantly, your organisation can't demonstrate compliance. The likelihood is also that the 'problem children' of your cyber security program are present in the 50 per cent of staff who didn't respond to the communication and complete the content.

Your organisation has three responses:

- Management can ignore the people who have failed to participate and hope for the best. This approach may be popular but, ultimately, it's doomed. Regulators will expect evidence of your efforts to bring these users into the awareness program.
- Management can begin the tedious process of chasing users to complete their cyber awareness obligations. Doing so is a labour-intensive exercise that only serves to annoy management and further consign information security to the organisational equivalent of the Siberian front.
- Technology solutions can cajole, annoy, chivvy, move along and ultimately make users complete the security assignment.

Ultimately, the cyber awareness campaign has to engage the user, involving the use of good media, graphics and eLearning. So, get the best-quality eLearning you can afford, cover off the key languages within your organisation, and allow users to self-manage the language with which they're most comfortable consuming the content.

Managing Risk and Ensuring Relevance

Nearly every organisation faces some form of digital transformation project. As greater efficiencies and revenue opportunities are explored, new business models are becoming available due to changes in markets and adaption of technologies such as cloud, data management and mobile. These projects are high profile in every organisation and typically have the attention and support of the Board of Directors and the executive team.

Data protection legislation such as General Data Protection Regulation (GDPR) has placed privacy by design and security by design at the heart of new digital initiatives. In some regions, organisations are required to undertake an impact assessment to assess the data protection impact of a new system or new process or business model. Data protection and information security professionals are very important in making sure that digital transformation teams are cognisant of this requirement, as well as making sure the new system or approach has suitable controls and staff communications in place.

REMEMBER

Including communications relating to a digital transformation project as part of your annual cyber security awareness project will increase its relevance to the business and assist with efforts to increase the profile of security among the leadership team. In addition, by getting ahead of these new digital projects, employees can see information security as an enabler rather than the blocking role that inevitably follows the late arrival of security controls to this type of initiative.

When senior management are considering the validity of a digital transformation project, they're already assessing various business risks along with potential upside benefits. The challenge is to approach the project from a risk perspective and attempt to ensure security and data protection risks are ranked alongside financial and other business exposure. Digital transformation projects allow opportunities for cyber security awareness to piggyback a much larger corporate initiative.

IN THIS CHAPTER

- Using effective communication
- Countering apathy
- Relying on people in your organisation to help spread the message
- Considering third-party relationships

Chapter 3
Changing Organisational Culture with Cyber Security Awareness Campaigns

Your organisation may be tempted to get busy with its security awareness program and send out eLearning and simulated phishing attacks to users. However, these approaches are doomed to failure if they don't take into account the key objective – changing people's behaviours in relation to cyber risk. Once you start to consider the concept of changing behaviour, you're in the area of change management. As every organisation knows, change management programs are notoriously difficult. The best security awareness programs approach the task in the same way as other organisational change projects. They bring together a multidisciplinary group to leverage the knowledge of the organisation, including project management facilitators, internal marketing, HR and IT security.

Change isn't a given; it takes time and significant amounts of willpower and effort. Management will inevitably feel a degree of despair, wondering if the awareness project is even necessary and if it will ever end.

This annoyance normally happens when the awareness campaign coincides/collides with other corporate communication initiatives. It's common for the user base to push back under these circumstances. At the planning stage, the organisation can counter this friction by reducing the amount and frequency of awareness communications for a limited period of time. The key is not to stop the program. If you do, you'll never get it started again.

This chapter helps you keep the awareness campaign successful with advice about how to use effective communication, how to keep going when you encounter apathy, how to rely on people in your organisation to help spread the message and how to utilise your third-party contractors.

Communicating Like You Mean It

Your organisation's awareness campaign needs to be tailored specifically for your organisation. To ensure your campaign communicates the message you want, do the following:

- **Make sure it's branded with your logo to give it recognition and weight in the minds of your users.** Because your staff are consuming so much audio-visual content in their private lives, you want to ensure your education has the look of important and relevant content. That being said, any education on cyber awareness is better than none at all.
- **Make your messaging fit the threats your people are dealing with on a day-to-day basis.** Avoid training for show, just to be able to say you have an awareness program.

  If people understand the risks and the personal and corporate consequences, the vast majority of your staff will react positively and change their behaviours. Spend the time to get your messaging right. If that's not a skill set you or your team have, then ask your marketing team for help. Alternatively, obtain outside assistance.

REMEMBER

TIP

Your user population can only cope with so much communication on this subject. Start gently and build up your campaign over 12 months. Think about it, how many eLearning courses would you want to take in a month, even if they were short? If your audience hasn't received this type of training before, issue one

piece of eLearning per month in the first six months so that staff don't become fatigued.

REMEMBER

Furthermore, before you increase the amount of training, ask yourself, how many cyber security policies, simulated phishing attacks and risk assessments can your users cope with in the first six months? It all adds up. To ensure the awareness campaign doesn't come to a premature end, discuss with the leadership team how hard they want to push the user base in consuming this content. From experience, a good general rule is that less is more. You need to bring your audience with you on the journey.

Many security campaigns neglect to educate users on why security is important to them and why the information security management system (ISMS) is in place to alleviate the risks of cyber threats. Make sure you communicate this overall initiative to users to allow them to see that cyber security is a critical part of business as usual in today's digital world.

Maintaining Momentum in the Face of Apathy

Getting executive backing to educate your user audience with a security awareness project is usually straightforward. Senior management are only too aware of the threats to the organisation in terms of fines and reputational damage. However, it's quite common for the campaign to be launched only to fall foul of corporate inertia six months later with poor results. Awareness projects commonly fail to establish and manage a predictable cycle of communication.

Most staff and senior management need to be informed right at the beginning that the security campaign is part of a long-term strategy to improve organisational cyber defences. It's critical that people don't expect a one-off initiative. As a result, you need to establish repeatable communications so that users know the importance of the campaign through regular notifications of key messages, training and assessments. In addition, build a feedback loop into your communications so that management receives timely opinions from staff. Management can use this feedback to improve the overall awareness initiative over time and inform the cadence of your ongoing awareness campaigns.

Trying to keep staff awareness at the top of everyone's mind during the year is difficult for management due to the frequency of active cyber threats throughout the year. Cyber security involves so much firefighting that making time to determine messaging for the awareness program is all but impossible.

THE POWER OF A BREACH AS A CATALYST FOR CHANGE

Nothing positive can be said about being on the receiving end of a targeted cyber attack that results in a data breach. The experience doesn't look good on your CV or resume if you're a security professional. That said, experience in dealing with a major cyber incident is a major coming-of-age event for any executive involved in information security management.

The difference between an organisation that has had a data breach (or near miss) is that the experienced organisation has a workable incident response plan ready to go, whereas the uninitiated organisation often takes a wait and see approach. If seasoned management are employed, then suitable incident planning has likely taken place.

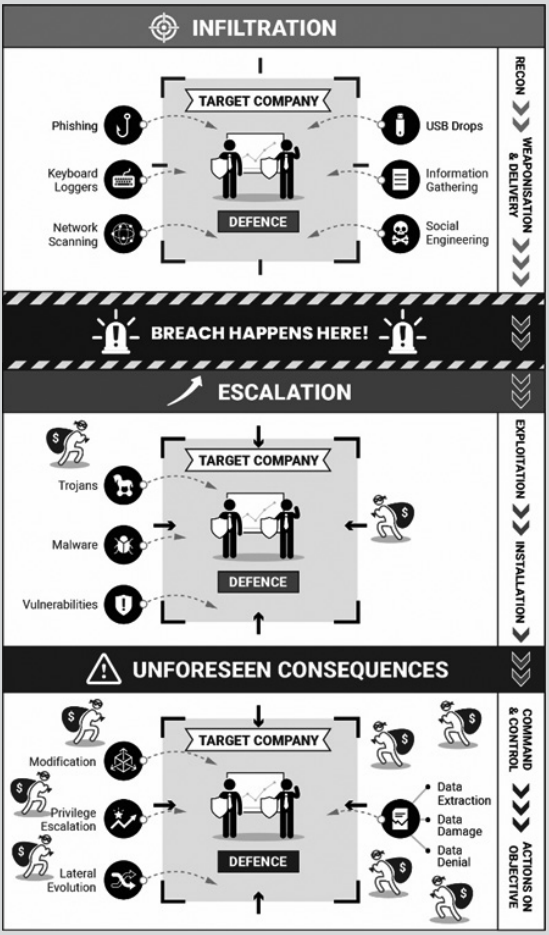
Here's the one good thing that can arise from a data breach or near miss: executive management can no longer indulge themselves in wishful thinking or claim plausible deniability. They have to get involved.

Although everyone is aware of the threats and shares a belief that the chances of their organisation being the victim of a cyber attack are high, investment in cyber security awareness is still unpopular and senior management is tempted to provide a minimum solution. The security industry must bear a level of responsibility in promoting the latest perimeter technology as the panacea for all security problems, always forgetting that the easiest way around defences is via the person behind the firewall.

As a group, data protection, compliance and information security professionals should tread lightly on trying to scare management into action with threats of fines. Rather, highlight the business benefits of standing apart from the less compliant or less secure organisations. The resultant competitive market value needs to be promoted

internally as the reason for investment especially in the area of staff culture change.

Management have a unique opportunity shortly after a breach or near miss, and before the scare has been rationalised, to bind the executive team to the information security mission and obtain the required support. This investment is usually in people and solutions, but the time commitment from this group is what ultimately proves to be most valuable. The figure below shows a typical data breach timeline.



TIP

Spend a week at the beginning of the year setting out the necessary awareness assets (policies, assessments, eLearning, simulated phishing attacks, blogs, competitions, events based on national cyber days) required for the 12 months ahead. Determine the frequency of communication based on best judgement. Then, get buy-in for your plan from senior management and execute on it. Don't have a piecemeal approach such as planning for just the next three months. If you do, you'll inevitably be blown off course as the year progresses. Rather, set out your 12-month campaign and regularly review progress.

Enlisting Cyber Security Champions

Ensuring that people in the organisation don't see the IT department as solely responsible for creating awareness of information security and data protection is extremely important. Rather, you want the organisation to accept that the organisation's digital security is *everyone's* responsibility.

A cyber security awareness campaign needs as many friends as it can get. Your organisation already has people who are active. They report on incidents, simulated phishing attacks and provide feedback. They understand the damage that cyber risk poses to the organisation. Embrace these users. To make sure that everyone understands their responsibility, you want to rely on these users in your organisation. These *champions* can communicate, are personable and are great with people. They're valuable assets for your campaign. Get your colleagues in other departments to help identify possible staff members.

TIP

In other words, management should create an ambassador program that enlists the support of these champions, those that are the most ambitious and interested people in your organisation. Your ambassador program needs organisation-wide support and endorsement from the executive level. You can use this executive support to formally launch your ambassador program and provide the corporate recognition that people love to receive.

You might already have people who already are on the front line of your information security and privacy operations. These people may have been identified as information asset owners from an ISO27001 perspective, or owners of a data processing activity. They may already have obtained relevant data protection or information security training.

Try and celebrate any successes. Build your campaign on positivity. Celebrate the successful recertification of ISO27001 as well as any other accomplishment in this area.


TIP

If possible, your cyber security champions program should have a separate channel of communication on an internal messaging tool, such as Microsoft Teams or Slack to ensure a regular flow of feedback on the health of your cyber awareness project. At the very least use this channel of communication to update the champions on any data breach incidents along with any near misses.

Getting a cyber security champion program off the ground is a satisfying part of a successful awareness campaign. It beds in real support for your change initiative throughout the organisation. It also acts as an early warning system when the campaign is beginning to falter or has missed its mark.

These champions can show through their actions and advocacy that cyber security awareness programs require the entire organisation to make these best practices part of the business-as-usual approach.

Extending Cyber Security Awareness Initiatives to Third-Party Relationships

Managing vendor and third-party risks has often been difficult for most organisations over the last 20 years. As organisations have morphed and evolved, they have outsourced specialisms and non-core activities to trusted partners. In some modern organisations, up to 50 per cent of the staff may not be full-time employees. The use of subcontracting arrangements results in a scalable and agile organisation. However, it has knock-on effects to the deployment of a security awareness campaign. These sections discuss which subcontractors to include in your security awareness plan, and what technology challenges they may face.

Knowing who to include

The level of integration that subcontractors have within your organisation determines the extent to which they should participate in your awareness program. Those third-party relationships who have contact with your information assets, data processing activities and network should at least form part of your awareness

campaign planning process. If appropriate, your organisation should identify particularly difficult or high-risk third-party relationships and then determine the necessary communication for each segment. At the very least, everyone that accesses your internal systems should sign up to your acceptable use policy; you'd then work up the additional requirements in terms of policies and training from there.

For example, professional advisors and technical professionals from trusted third parties might have access to confidential data and require access to key systems, particularly financial, HR and corporate data stores. Ensure that training on the necessary obligations relating to access to your digital assets is given to these types of third-party personnel.

As with permanent employees, management should segment third-party contractors on the basis of the risk they pose to the organisation. The greater the risk, the more controls are required. Make sure you agree on these controls, be they training or policy attestation, with the subcontractor at the time of contract. These preconditions should form part of your standard terms and conditions and should be a critical part of supplier relationships that have access to your IT systems.

Considering potential technology challenges

Sometimes your organisation may have to overcome real technological challenges in bringing third parties into your awareness initiative. For example, remote third parties may not be able to access an on-premise learning management systems (LMS) in order to complete necessary eLearning. The same can be true when it comes to adhering to key policies that govern the relationship between the organisation, the vendor and the individual actually performing the service. In the past, organisations have often glossed over involving third parties in these types of security initiatives. However, vendor management and the cyber risk associated with third-party interactions has become a source of concern for IT management and a focus for international privacy laws.

Gradually introducing cyber security awareness to third parties

A phased approach to adopting third parties into your cyber awareness campaigns is the most sensible method for maturing your

relationship with your vendors. Find a way to manage your key policies first and have a reliable way of obtaining attestation; ideally an electronic policy management solution that can automate this process. Paper is a really bad idea, especially when trying to get signed documents back to a central folder. Determine the key risks that a subcontractor could represent and then provide appropriate training, ideally through a cloud-based LMS that the subcontractor could access either remotely or through your systems before they come on site.

WARNING

You can also find all the bad behaviours that your people exhibit in the vendor community. For example, a subcontractor is as likely to facilitate tailgating as one of your own staff. Yet your internal awareness campaign covers physical security via policy and training. Ensure that the subcontractor is also trained on these topics.

In extending the coverage of your awareness campaign you want to assess the level of awareness training and employee policy management that a vendor adopts within his own environment. This assessment forms part of your vendor due diligence that is an integral part of youvr organisation's vendor onboarding process. Many organisations send the vendor a risk assessment prior to contract. Within this assessment, evaluate the vendor's cyber awareness readiness as part of the questions your organisation asks on general information security such as a firewall and antivirus defences. A vendor that can't provide evidence on a policy or training regime for information security will have difficulty in successfully satisfying the requirements of your awareness campaign.

IN THIS CHAPTER

- Grasping how important policies are within a security awareness campaign
- Helping identify risk
- Training veteran staff and new employees on policies
- Considering the benefits of a centralised technology architecture

Chapter 4
Integrating Policy Management into Your Security Awareness Program

A policy is: *a set of ideas or a plan of what to do in particular situations that a group of people, a business, an organisation, a government or a political party have officially agreed to.*

Policies are a plan of what to do in particular situations. Your security awareness campaign needs clear policies. Management has specified what staff should do in particular situations. Policies need to be communicated to staff because if you don't tell people what to do in certain situations, how can they be relied upon to act in the correct manner?

This chapter focuses on the importance of the role of policies to strengthen your organisation's security awareness campaign.

Understanding the Role of Policies within a Campaign

Policies in an organisation are like the body of law that allows a government to manage its society. They're the backbone of the organisation's response to cyber security threats (social media policies, password policies, network policies and so forth) and for regulatory protection (acceptable use policy, privacy policies, code of conduct policies and so on). They're a key element in a best practice communication process with staff. Training activities and policies are most effective when aligned. If treated separately, they build up, increase employee communications and ultimately result in user fatigue.

REMEMBER

View policies as the laws of your organisation. No government would permit their laws being made up on the fly, nor have a lack of strict executive oversight for approving laws, policies and communications. Yet policy management for the information security and data protection function is often ignored by senior management in many organisations.

When constructing an awareness program, make sure you look at all the key elements that need to be communicated to staff such as policies, eLearning, risk assessments and simulated phishing attacks. The challenge is finding the correct balance of these elements to achieve the objectives of the awareness strategy.

REMEMBER

As with all awareness initiatives, people are key. Obtain staff buy-in to policies so that people accept how they should act in particular situations. Getting this buy-in creates personal accountability with your individual staff members and goes a long way to driving behavioural change.

Policies are the documented organisational standard that people are required to adhere to. It's critical that staff have easy access to a central policy portal that becomes the single source of truth for the organisation. This portal should be tamper-proof to provide the organisation with 'evidential weight' if policies are challenged in a court of law.

In addition, the policies should be subject to strict revision control so that modifications and changes to policies over time are captured, and available to be scrutinised in an audit trail. Policies

are always changing to meet the organisation's needs. As a result, the policy change management process within the organisation should be reviewed to make sure the policy approach is fit for purpose. What is key is that policies are communicated to employees in a manner that supports cyber and regulatory compliance. The best way to achieve this communication is to create a policy communication plan, as shown in Figure 4-1.

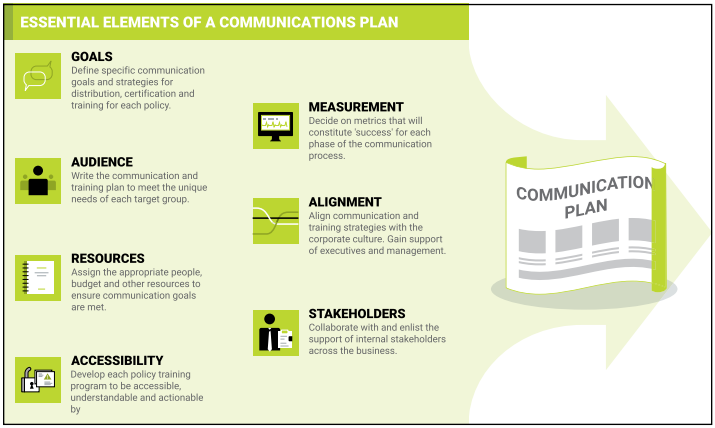


FIGURE 4-1: The essential elements of a communication plan (Source: OCEG and GRC 20/20).

Policy Management: Training Your Staff to Identify Risk

An organisation develops policies to mitigate identified risks in the areas of compliance or information security. Policies are created when risks are of sufficient importance that they require a formal written policy. In addition, a policy will detail the necessary controls to manage the risk. However, the policy is only one step in the awareness process. Staff also need to be trained on the contents of the policy.

The training associated with the policy can take a more abbreviated view of the policy content. Let the policy document carry the burden of covering the multitude of contingencies surrounding the risk remediation. The training should cover the main points that employees are expected to know and not be a verbatim retelling of the policy document.

REMEMBER

Policies play a big role in changing organisational culture. Without doubt, when a staff member is called upon to attest to a policy, either electronically or by signing a piece of paper, they are confirming that they are aware of the significance of their actions. Policies help increase the significance of cyber security in the workplace. Policies help align personal accountability with organisational risks, procedures and regulations.

These sections provide more detail about training current staff as well as new employees.

Training staff on policies

While there is direction for people within the policy staff quite often require training on how to implement it. The risk that the policy is aiming to address, and the level of risk that has been assessed directly relates to the amount of instruction the user will require. Higher risks will have policies that need higher levels of training to ensure the respective control is understood and applied. In addition, you may need to adopt a hybrid approach of policy, eLearning and classroom training for higher risks to ensure maximum adoption and understanding. (Chapter 5 discusses a hybrid approach in greater detail.)

A clear correlation exists between the amount of time and energy spent on policy, training, and awareness and its actual impact on the organisation. Compliance activities that are high profile with executive backing tend to get greater employee mindshare, and result in greater policy adoption, completion of training and related testing.

Refer to Figure 4-2 for important questions to ask when training your staff new policies.

Identifying why policies are important to new staff awareness

Many organisations adopt an approach to new employees that requires them to sign policies and watch eLearning for up to three hours a day for the first week of their employment. This isn't an effective use of the new employee's time. This type of learning is akin to drinking from a power hose.

FIGURE 4-2: Questions to ask (Source: OCEG and GRC 20/20).

Every organisation struggles to deal with new employees in the first few weeks of employment while they come up the learning curve. Organisations need to craft a fit-for-purpose induction schedule. Imagine if you had to do two or three hours of training every day. It would become overwhelming. The problem with new employees is that they have so much to learn. When training them on cyber security, take into account a human being's ability to pay attention and gain understanding.

REMEMBER

Schedule important policies for new employees along with the relevant eLearning in a considered way. Set limitations on how much eLearning the new employee should be expected to complete in the first month. A maximum of three hours per week in the first month is optimum. This amount of time will allow the new employee to complete the key policies and pieces of eLearning that reflects the need to learn the organisational approach, but not to get fatigued. After the first month, cut back the number of policies and eLearning to allow the employee to become productive in their new role.

Recognising the Importance of a Centralised Technology Architecture for Your Policies

Policy management and eLearning in a modern organisation has become too complicated to be managed effectively by people in a manual way. A centralised policy management system can

support the challenge of meeting the ever-changing demands of the organisation, regulatory requirements and the business environment.

Managing the policy's lifecycle on spreadsheets and filesharing systems is difficult. It shows a lack of overall maturity of compliance within an organisation. It also displays an ad-hoc approach to security and compliance management.

The following sections discuss how a centralised policy management system can help your organisation, and who in your organisation can utilise the system.

Identifying the benefits of a centralised system

Here are a couple of the main benefits to using a centralised system:

- **It guarantees 100 per cent participation.** Making sure everyone receives, understands and attests to the policy is a critical benefit to a centralised policy management system.
- **It allows training and policies to be accessible in one place.** The ability to link relevant training to your policies is important for all employees.
- **It reduces the burden on management.** Policy automation can avoid the need for significant management oversight by means of policy enforcement automation. The technology, and not management, notifies and reminds users to complete the policy and training obligations.
- **All policies and training are located in one place.** The key value of a technology solution is in having a single source of truth relating to your compliance activities, specifically in relation to policy, training and the interaction with your employees.

Figure 4-3 further shows how centralised technology can benefit your organisation.

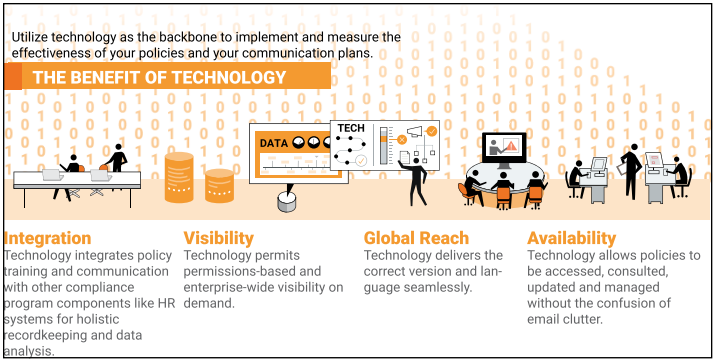


FIGURE 4-3: The benefit of technology (Source: OCEG and GRC 20/20).

Understanding who uses this system

Three main groups use this type of contained policy management system. They are:

- **Administrators who set up the system and send out the policies and training:** They have their own admin interface to create, target, publish and manage organisational policies.
- **The users who consume the training and policy:** They can meet their obligations to sign policies, take training, self-manage their interaction with their content, and access it should they need their knowledge refreshed.
- **The management or oversight view of the system:** Here management can review the system to ensure that employees are completing the necessary compliance communication campaigns. Auditors and regulators can access the system to ensure that the organisation has followed its duty of care and oversight.

IN THIS CHAPTER

- Ensuring executive support
- Putting together a campaign plan
- Creating a baseline for your strategy
- Knowing what success looks like
- Considering a hybrid approach

Chapter 5
Developing a Best Practice Cyber Awareness Strategy

In order for your cyber awareness campaign to be successful, your organisation needs a clear plan of action. This chapter gives you advice on putting that plan together, while making sure you have your organisation's executives behind you. After your plan is in place, you need to be able to measure whether it is working. If required, your organisation should consider a hybrid approach.

Ensuring Executive Support

A successful awareness program often comes down to whether your organisation's leadership supports it. Without executive support, securing adequate funding and resources is difficult and, without them, a security awareness project is limited in what it can achieve.

Cyber awareness programs aim to change staff behaviours and that involves an element of human psychology. If you have support from the leadership team, you can dismantle roadblocks and decisions can be made quickly. Knowing from the outset what the tone is from the top is important. For example, what is the tone in relation to poor cyber security behaviour? Is it light touch or is it zero tolerance? How many simulated phishing exercises would an employee have to fail before disciplinary action is initiated? Failure to set the tone means that every manager and business head can potentially interpret the awareness campaign's implementation.

Changing staff behaviours involves an element of human psychology. For example, people like direction from their leaders. So kicking off an awareness campaign with a message from the top is very effective. This could be in the form of an email or a simple piece to camera.


TIP

When you're preparing your awareness campaign, make sure you have your leadership team's full backing. A good idea is to have a few hours of specific training for the leadership function. This should be tailored training that is face to face and backed up with executive level eLearning.

Getting a Campaign Plan Together

Adopting a planning process based on risk mitigation represents the best way to develop a fit-for-purpose cyber awareness campaign. When creating your plan, make sure it's right for the timescale (usually 12 months) and includes the key risks that the organisation faces at that particular time. Be ready to re-evaluate your risks, as they change and evolve over time.


WARNING

Organisations often rely on an information security professional to organise the planning of an awareness communications plan. It is important to support this function with corporate communications expertise. That said, information security and data privacy

professionals are key to the success of a cyber security awareness campaign. Their knowledge can lead and inform the program. Risk is at the heart of every awareness campaign, and they can identify and prioritise the different types of risk that need to be remediated.

REMEMBER

However, someone in the organisation's project management or corporate communications may need to be a part of this team to ensure the message is being shared effectively and efficiently. The team needs several skill sets to craft a successful awareness campaign.

You may be tempted to send out a few simulated phishing emails and believe that the requirement for cyber security awareness has been met. No doubt this method does highlight the risk of social engineering to staff. However, the awareness program needs to take into account the totality of the threats to the organisation. An awareness program should also record remediation exercises and document follow-up activities. These records are essential for demonstrating compliance and governance.

Creating a playbook (see Figure 5-1) or campaign of activities for the year ahead is key to generate a successful cyber awareness project. The exercise forces the identification of key risks. The organisation has to determine people's ability to digest compliance and security messaging. Management must decide on what types and how many pieces of communication can go out per week, per month and ultimately per year. The challenge is balancing risk against user fatigue. The team implementing this campaign needs to avoid being overambitious in the execution of the security program.

REMEMBER

It takes a long time to change people's behaviour and improve the resilience of the workforce to cyber security threats.

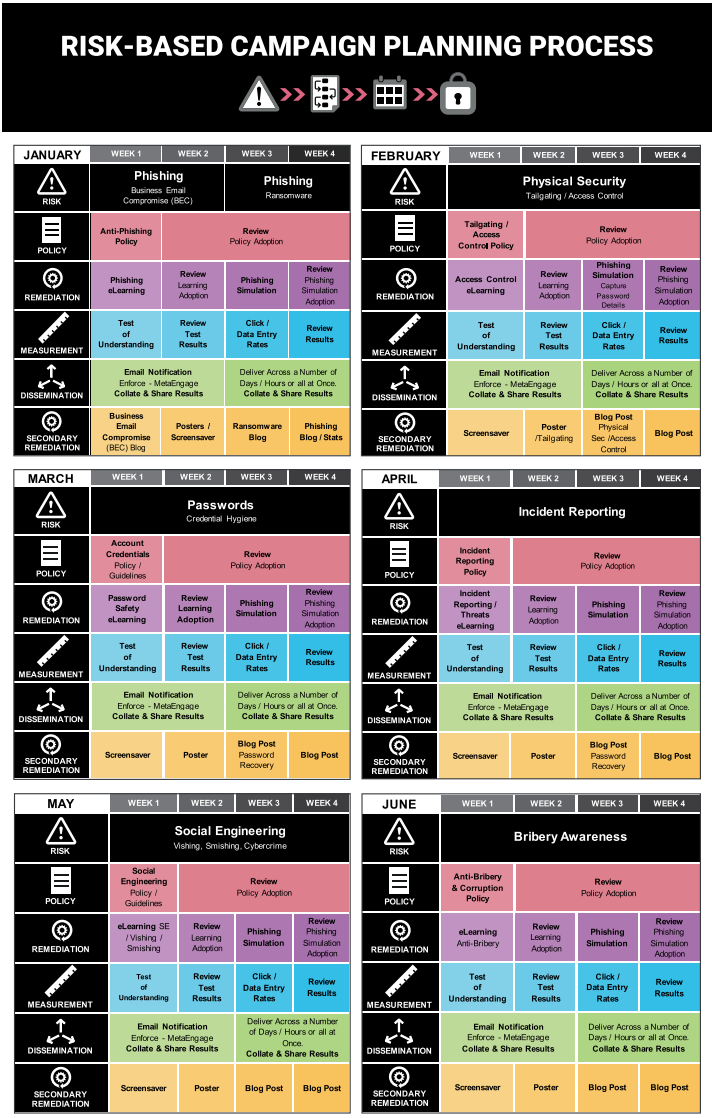


FIGURE 5-1: A 12-month security awareness planner.

Establishing a Baseline

Key performance indicators (KPIs) show whether a project is successful or not. You should manage your information security awareness in the same way. Highlight the KPIs you've identified

to determine a baseline. You can then use this data to measure what progress has been made.

Your awareness programs need to be based on the current risks that your organisation is facing. As a starting point, the recent incidents that have been recorded provide an excellent guide to the issues the program is addressing and what risks need to be remediated.


TIP

The best way to find out how knowledgeable your users are about these risks is to ask them through an online questionnaire/survey. Base the questions in the survey on the risks that the company is facing. Keep the survey short and concise as possible.

These survey findings will then influence any subsequent training program. For example, if the survey highlights deficiencies in staff knowledge of physical security, then you'll need training or policy communication to rectify this knowledge gap. We recommend your organisation tackles a key risk every month. That means that the survey checks what your staff know about a minimum of 12 questions/risks.


REMEMBER

Another quick way to establish a baseline is to implement a simulated phishing attack on employees. Doing so helps determine how susceptible the company is to fraudulent phishing emails and provides a real-time view of the percentage of staff that would have fallen foul had the attack been real. Even more worrying would be those users that had submitted their credentials when prompted.

Policies form an integral part of staff security awareness. At the outset, conduct an exercise to identify the critical policies that staff are required to adhere to. Remember, a policy should only exist if it relates to a risk. Hence, each of your key risks should have an organisational policy. Make sure you determine when your policies were last reviewed and if they are still fit for purpose.


WARNING

Be careful to avoid a mass organisational policy review as it tends to slow awareness campaigns to a crawl. Best practice is to resolve the relevant policy at least a month before the risk features in your awareness schedule.

Defining and Measuring Success

After a baseline has been agreed and documented, tracking your KPIs on a monthly basis is important in order to measure how successful the awareness plan is. Areas to review include the following:

- Percentage of users adhering to key policies
- Percentage of users clicking on a simulated phishing attack
- Number of vendor risk assessments
- Number of data processing activities
- Number of completed staff surveys
- Number of security incidents
- Number of phish reported by staff

The last three metrics are important because they relate to staff awareness of key security challenges to the organisation. ***Note:*** The number of security incidents reported may increase as staff become sensitised to the various risks.

These metrics form the basis of reporting to the Information Governance Steering Committee and will help inform it on risk remediation and the progress of the awareness campaign.

Taking a Hybrid Approach to Awareness

Good marketing campaigns use lots of different methods to attract customers' attention to their product or service. They use a combination of digital channels, email, and social media, along with traditional methods such as in-store promotions and giveaways. So, like marketing campaigns, your security awareness program should use a hybrid approach to attract and retain the attention of your userbase. After you've secured that attention, the next step is to effect some change in behaviour.

The following sections explain how you can use storytelling and other ways you can effectively communicate your message.

Include storytelling in your program

There is no 'one size fits all' when it comes to marketing or security awareness. In the world of organisational communication, various internal parties are fighting for employees' attention. A good awareness program recognises this. It means you must adopt multiple channels of communication to attract your audience's attention, which includes physical, digital and storytelling.

REMEMBER

Human beings have an oral tradition. So tap into that tradition and tell a story, or have a theme that people can relate to in order to get your message across. For example, a good theme for your employees is that they take on the role of government agents trying to defeat the bad guy's efforts. Think James Bond or Wonder Woman!

Being innovative with your communications

Physical methods of communicating with staff involves various inventive approaches. Here are some ways you can communicate with your organisation about the campaign:

- **Posters:** The cheapest and most effective way is a poster campaign that reinforces your key messages and themes. You can utilise all types of posters, including digital signs at reception to small posters in lifts. Make sure and align your posters to the risk you're promoting and change posters every four to six weeks, so people don't become numb to the messaging.
- **Digital methods:** Digital methods are the most common approach to communicating and resolving the risk associated with a lack of staff education. Some organisations have standalone simulated phishing, policy management or cyber security eLearning systems that allow key messaging to be delivered to employees.

AUTOMATING YOUR CAMPAIGN

Automate your entire 12-month security awareness campaign and manage the appropriate delivery of key elements to the right audience at the right time. These elements should include a combination of tailored eLearning, critical policies, relevant blogs, simulated phishing emails, risk assessments and surveys.

Having an automated approach to security awareness allows for the audit information to be recorded to support regulatory defence that could be required in the event of a breach or an audit.

IN THIS CHAPTER

- Setting the tone from the top
- Engaging your audience
- Preparing for a data breach
- Reviewing your awareness initiatives

Chapter 6
Ten Cyber Security Awareness Best Practices

Here are ten best practice tips to help you create the most effective cyber security awareness campaign for your organisation.

Start with CEO Leadership

Cyber security is finally getting the attention it deserves in the boardroom. As the number of high-profile data breaches continues to rise, there's been a greater emphasis on managing cyber risk to reduce the chance of attack.

Cyber security is everyone's responsibility, but resilient organisations require strong CEO leadership. An engaged CEO will implement the correct security measures needed to protect the organisation's digital assets, employees, customers and brand

reputation. If the CEO is taking cyber security seriously, this will permeate throughout the organisation and help create a culture of enhanced cyber security awareness.

Refer to Chapter 5 to help you get your leadership's support.

Know Your Organisational Tolerances

In creating an effective security awareness program, your organisation needs to evaluate the threat landscape and identify your top risks. Doing so gives you a better understanding of the real-world threats that could compromise your organisation's security.

Your risk tolerance needs to be defined at the outset, so you can implement the correct security measures based on the actual threats faced. This avoids resources being directed at threats unlikely to occur or that will have little or no impact on your business.

You need to conduct regular risk assessments to ensure your approach to cyber security is in line with regulatory frameworks, information security standards and laws such as the General Data Protection Regulation (GDPR).

Taking time to properly identify the risks can help shape the messaging, delivery and effective targeting of your cyber security awareness program.

Defend Your Information Assets

To develop a comprehensive cyber security strategy and effectively identify risks, you need to complete a thorough audit of your organisation's information assets.

An information asset is a piece of information that is valuable to your organisation. This can include Personally Identifiable Information (PII), financial information, intellectual property, or any other information that is significant to your company.

You need to determine what the most valuable information assets are, where they're located, and who has access to them. Every asset

should be classified (for example, public, private or confidential) and protected based on its value. Doing so is crucial when identifying risks and prioritising the areas that need to be defended.

After you identify these areas, you can focus on how each information asset could potentially be compromised. Whether it's a system breach, malware or even an insider threat, you can take informed steps to improve these processes and reduce the chance of a cybercriminal gaining access to critical systems.

Focus on High-Risk Groups

The key to an effective security awareness program is ensuring the right training is targeted at the right people. All users are susceptible to cyber threats; however, certain employees have a higher threat profile than others. For example, your HR and Finance departments will be frequently targeted because of their privileged access to sensitive data.

Your CEO, CFO and senior executives are also popular targets due to their high-level access to valuable corporate information. They will often be on the receiving end of sophisticated Business Email Compromise (BEC) scams. In this type of phishing attack, cybercriminals impersonate a high-level executive in order to convince an employee, customer or vendor to transfer money to a fraudulent account or to disclose sensitive information. If a senior executive were to fall for the scam, the results could be devastating, undermining the entire security of your organisation.

Refer to Chapter 2 for more information about which groups are most susceptible and how you can cater training for them.

Make It Engaging with Effective Storytelling

Storytelling is one of the most powerful ways to breathe life into your cyber security awareness campaign. Face it, cyber security can be a dry topic, but it's vital you find ways to engage your staff if you want to positively impact behaviour within your organisation. The message is just too important to get lost in formal, corporate communications.

Stories are fundamental to the way people learn; they help create an emotional response that makes it easier to remember what's being taught. You can bring cyber security messaging to life, making it more relatable to people in their everyday lives. By making the story relevant to the end-user, you greatly increase the chance of that person retaining the information, therefore improving the overall security posture of your organisation. Chapter 5 explains in greater detail how you can include storytelling in your campaign.

Get Your Policy Management Up To Date

Policies are crucial in establishing boundaries of behaviour for individuals, processes, relationships and transactions within your organisation. They provide a framework of governance, identify risk and help define compliance, which is important in today's increasingly complex regulatory landscape.

An effective policy management system is one that has a consistent method of creating policies, adds structure to company procedures and makes it easier to track attestation and staff responses. As a result, this system can help you streamline internal processes, demonstrate compliance with legislative requirements, and effectively target the areas that present the highest risk to data security.

Start Preparing for a Data Breach Now

If you haven't started preparing for a data breach, now's the time to start. Billions of confidential records have been exposed and, according to IBM, the global average cost of a data breach has risen to a staggering $3.92 million.

It's no longer a matter of 'if' your organisation is going to be attacked, but 'when'. You need to start preparing for the inevitable and put a plan in place that ensures appropriate action when security is breached.

Establishing an effective response plan helps educate and inform staff, improve organisational structures, enhance customer and stakeholder confidence, and reduce any potential financial or reputational damage following a breach.

TIP

You need to regularly test your data breach response plan to identify any areas of weakness and to ensure that everyone on your team understands their responsibilities, both in preparing for and responding to a breach.

Enlist Cyber Security Champions

Cyber security is not just about technology. Your people play a key role in defending your organisation and identifying threats that could pose a threat to your security.

Appointing cyber security champions is a great way to empower staff and equip them with the skills needed to prevent a cyber attack. According to the National Cyber Security Centre, half of all businesses experiencing a cyber attack found that the most disruptive threats were reported directly by staff, rather than picked up automatically by software.

Cyber security champions don't need to be technical experts; tapping into them is about adding the human touch to your security strategy and enlisting the help of staff who are committed to raising awareness and implementing good cyber security practices.

Chapter 3 provides specific tips on how to identify and utilise your organisation's champions.

Consider Your Supply Chain

For many organisations, the weakest link in their cyber security defences is their supply chain. Rather than targeting a company directly, cybercriminals will attempt to compromise an organisation's critical networks and systems by exploiting gaps in its supply chain processes and systems.

Supply chains are a vital part of business operations, but often these networks are large and diverse and span a range of different countries. These suppliers typically don't have the same robust cyber security defences in place, which means they have lots of weak points for cybercriminals to exploit.

Some of the biggest data breaches in recent history have resulted from supply chain attacks. A prime example is the 2014 Target breach that compromised the personal data of more than 70 million customers. By launching a phishing attack on one of the company's service suppliers, attackers were able to gain access to Target's point-of-sale (POS) payment card readers.

Every supplier that connects to your business is a potential risk, so it's vital you carry out detailed third-party risk assessments to address any issues that could pose a threat to your security. Doing so can help determine what security measures need putting in place to keep your data secure.

Chapter 3 examines ways you can extend your campaign to third-party suppliers.

Implement Proper Oversight and Regular Reviews

The threat landscape is continually evolving so your cyber security awareness program needs to evolve with it. It's important to conduct regular reviews of staff readiness to identify areas of weakness and establish whether current policies and training need updating.

To support compliance with regulators, it is best practice to document the results of all reviews and make sure to act upon any recommendations for risk remediation. Without these regular audits, your cyber security awareness program might not reflect the threat landscape and could leave your organisation vulnerable to attack.

CYBER SECURITY AWARENESS THAT YOUR STAFF WILL LOVE

www.metacompliance.com

Create a culture of enhanced security awareness

Security threats are evolving and becoming more sophisticated. Traditional technological defences are not enough to secure an organisation from its largest security gap – the human element. Human nature is a key vulnerability and cybercriminals know how to exploit it. Help is at hand in *Cyber Security Awareness For Dummies*, your guide to the strategies, challenges and best ways to change user behaviour within an organisation to recognise and deal with cyber security threats and protect valuable information and assets.

Inside...

- Discover how to implement cyber security awareness successfully
- Comply with stringent regulatory requirements
- Engage staff with relevant and role-specific training
- Integrate policy management into security awareness programs
- Ensure executive support for security awareness campaigns

MetaCompliance®

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-59826-8
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.