RESILIA™

Are your people playing an effective role in your cyber resilience?

AXELOS
GLOBAL BEST PRACTICE

Cyber attacks are now ‘business as usual’ for organizations around the world.

Organizations have typically trusted in technology to protect them from the financial and reputational losses that can result from a cyber attack, the impacts of which can take many months, if not years, to repair.

The increasing success of cyber attackers shows that technology – while important – does not provide a ‘silver bullet’. Organizations need to recognize the importance of the ‘human factor’ in protecting their most precious information assets and systems: that means their own employees represent both their most effective security control and, potentially, their greatest vulnerability to attack.

The methods used by cyber criminals to breach organizational systems and networks prey on human vulnerability. By tempting people to open an email attachment or click on a link, for example. In 90% of attacks the success of the attacker requires the help of an innocent person. The natural human responses we all make – to be helpful or curious – can be the beginning of a corporate disaster.

That is why it’s imperative to know whether your staff – all of them – are capable of recognizing, responding to and recovering from a cyber attack. Cyber awareness learning and training is central to minimizing the risks to information security. That’s what 99% of IT security training decision makers told us in research carried out by Ipsos MORI.

Cyber awareness learning and training is central to minimizing the risks to information security.

This AXELOS guide helps you ask the right questions about your existing information security training and learning strategies – and start your organization’s journey to greater cyber resilience.

How cyber security aware is your organization?

The 6 key questions to ask:

01 How relevant is the cyber security awareness learning you're providing to all staff?

Your training and awareness learning might be telling staff to do things that are not relevant and not part of their working life. The learning needs to be directly related to what they do. Is your training also made relevant to your location in the world and the information security laws in place? You might also need specific, role-based awareness training and learning: for example, if your call centre staff are exposed to fraudulent callers posing as someone else, do you make staff aware of the policies and processes you have in place, designed to verify who the caller is?

02 Does everyone who needs awareness learning receive it?

Your training needs to reach – and be tailored to – everyone whose working activities could pose a risk to your cyber resilience. For example, everyone with access to the network needs training on phishing attacks. This means that the awareness learning is as relevant to the board and senior management team as it is to the most junior member of staff. The challenge that can arise when persuading busy, senior executives to undertake some form of learning is dilution: the director or manager asks for the main points of the course to be summarized in an email instead of actually taking a short, engaging learning module. Consequently, they can become a weak link in your cyber security chain.

03 How do you know people are engaging with your cyber security learning?

Unfortunately for most organizations, vital information about cyber security can get lost among the corporate 'noise' which leaves employees overwhelmed with the volume of company communications. So how can you make your essential learning about cyber security stand out and become adopted by staff?

Get the language right: Language is vital: for example, would your staff understand that the cyber security risk of 'social engineering' refers to the work of a trickster or fraudster?

Make learning accessible: Information security awareness learning needs to be accessible, across technologies, language and at a time that suits your employees. Having a learning management system gives you the opportunity to measure how many times staff view the learning materials. Running information security awareness learning roadshows can be used as an important part of any engagement program helping to build confidence and team commitment.

Fun and engaging: Awareness learning must be fun and engaging. We don't all learn in the same way. Use different formats, such as video, animations and games. Many enjoy and consume information better while playing educational games.

Involve the comms team: Ensure that your internal communications people are on-side from the outset to create greater engagement with the topic. Utilize their skills and knowledge to get your messages to stand out.

04 Is your awareness learning giving people knowledge they can use?

Giving your staff the right information at the right time helps them make the right decisions. A poster that says “think security” is not enough, nor is telling them “don’t do this” or “don’t do that”. Instead, if you want staff to understand the power of a strong password, give them sensible advice about effective use of passwords: explain what a strong password looks like, how to select a password, and share techniques for remembering multiple passwords. If the advice is relevant for home computing cyber security as well as professional, you’ve got a better chance of them remembering and adopting it.

05 Do you have the right ‘tone from the top’?

Does your cyber security awareness learning have the support and financial investment from senior executives? Clear leadership from the top of the organization, as well as funding, is needed to create effective cyber security learning.

Can your senior executives answer the “so-what?” question? In other words, do they have the knowledge to understand what’s important when a member of staff tells them about a suspected or actual cyber attack on the organization, or about a high profile case of cyber breach elsewhere? To make sound, strategic decisions that protect the company, the board needs to know what it’s doing in relation to cyber security.

06 How do you know your cyber awareness learning and training is effective?

To understand whether your cyber security training is working or not, you need to ask questions such as:

- What’s changed in staff behavior?
- Have we had more phishing incidents reported?
- Has the number of security incidents reduced?
- Has the average test results score increased?
- Has the number of times people attempting the test risen?
- How often are people looking at useful, cyber security learning materials?

If you are delivering training and learning materials multiple times during a year, it’s possible to measure what’s changed and map it against improvements in the organization.

> If you want staff to understand the power of a strong password, give them sensible advice.

What should your cyber security awareness training include as a minimum?

The content of your company's cyber security awareness learning and training is critical.

What we call the "human factor" – i.e. the knowledge and capability of your staff to recognize, respond to and recover from a cyber attack – is too important to trust to outdated and irregular learning approaches.

The awareness learning you provide should be directly relevant to the work of your employees and the information security risks they face. Staff need the ability to anticipate and withstand the ever-changing methods used by hackers and other cyber criminals.

There are a number of essential topics you should consider including, that will equip your staff for a cyber attack:

Phishing

Phishing is an email that contains a link or attachment to launch malicious computer code into an organization's network, giving an attacker a route into your computer systems. This is how more than 90% of attacks start, relying on the error of someone in an organization to help attackers gain access; without that, the attack fails.

Typically, a phishing email plays on human behavior, inviting you to "click this and win money" or playing on the emotions by asking you to help someone in need. The email could also claim to be from someone senior in your own company. They can be targeted at an individual (known as spear phishing) and can appear very convincing.

Training needs to make staff aware of the risk, to help them understand what a phishing email looks like, what to do next as a consequence and how to recognize its potential impacts (e.g. the loss of data, the network compromised).

Social engineering

This is the work of a con artist, trickster or fraudster trying to play on people's willingness to be helpful and to manipulate them to share confidential information. Social engineers may email or phone people, pretending to be someone they are not. This could be someone from within the organization, e.g. the Help Desk, or from a trusted organization, e.g. your bank.

The objective is the same – to gain information. This can be a password, a username, personal details, bank details, etc. Social engineers are usually trying to gain access to your corporate network or personal computer/device so that they can install malicious software that will allow them to steal sensitive information. The threat from social engineering – which, along with phishing, is the starting point for 90% of attacks – has to be addressed more effectively through engaging awareness learning.

Passwords

Passwords are needed for everything in the digital world: online shopping, logging into our computers at work and home, plus banking and social media. On average we have about 26 online accounts, all requiring a password. In 2014, a survey in the UK for Cyber Street Wise found that 75% of people were failing to follow simple password best practice, therefore putting sensitive information at risk. If criminals gain access to passwords, it can lead to theft of money from accounts, fraudulent activity or hacking into company networks to obtain commercially sensitive data.

Staff need to learn how to keep passwords safe, to avoid sharing them, writing them down or sending them via email. They also need to learn the principles of using strong passwords which have a minimum number and mixture of characters, avoiding words that can be associated easily with them, what to do if a password falls into the wrong hands, and using passwords (PIN) on mobile devices.

Handling information

When people entrust information to an organization they expect it to be treated confidentially and securely. Failure to do so can open the door to criminals, hacktivists, malicious insiders, even nation states and have far reaching consequences for both individuals and organizations. There is an increasing amount of legislation governing how information must be treated at all stages of its life – creation, storage, retrieval, transmission, and destruction. Your staff must be able to ensure that they handle information securely at all times.

The risks from poor information handling include loss of data, financial loss, regulatory fines and sanctions, loss of customer confidence, market position and reputation. Individual employees may also be subject to disciplinary action or dismissal, identity theft and loss of personal information.

In addition to the topics outlined above, other vital topics that should be covered in any cyber security awareness training are: Bring Your Own Device (BYOD), personal information, removable media, online safety, remote and mobile working and social media.

The essential steps to take today towards greater cyber resilience

Assessing your organization's current level of cyber security – and in particular the effectiveness of the training and learning you provide to make your staff cyber-savvy – can't wait until the next time your systems are breached and your most precious information put at risk.

We hope this introductory guide gives you a starting point to improve how your organization prepares for, responds to and recovers from a cyber attack.

And these are the 8 must-do actions you need to take TODAY:

01 Find out whether your employees, regardless of their role or position, have the right information, at the right time to make the right decisions – that might need a new approach to cyber security awareness training and learning.

02 Ask the question: have you imagined the very worst that could happen following a successful cyber attack on your organization?

03 Find out how resilient your organization is to cyber attack – are you confident that attacks could be stopped at source? Could you respond quickly and recover from an attack?

04 Identify whether your organization's suppliers are taking cyber security seriously – the level of attention they give to it affects you too.

05 Ask the questions: are your critical stakeholders in the business collaborating effectively to ensure your cyber risks are being managed and acted upon consistently?

06 Engage with multiple people in your organization – talk to IT operations, IT security, incident response teams, corporate communications and HR – to plan roles, responsibilities and a clear response to a cyber attack.

07 Assess whether your most precious information and systems are protected and backed up appropriately so that the organization can recover quickly from an attack.

08 Ensure that everyone across your organization knows their individual responsibility for resilience to cyber attacks.

AXELOS’ RESILIA™ CYBER RESILIENCE BEST PRACTICE PORTFOLIO

AXELOS’ RESILIA™ cyber resilience best practice portfolio includes certified training, awareness learning for all staff, leadership engagement and a cyber maturity assessment tool, designed to put people at the heart of an organization’s cyber resilience strategy.

The RESILIA Awareness learning program for all staff helps to fill critical knowledge and skills gaps across all staff, enabling them to make the right decisions at the right time to better protect their organization’s most valuable and sensitive information and systems.

For more information about **RESILIA™**, visit **AXELOS.com/RESILIA**. If you have specific queries, requests or would like to be added to the **AXELOS** mailing list contact **ask@AXELOS.com**