Cyber Security, The Human Factor

"Changing Cyber Behaviour to Reduce Risk "

Introduction

Cyber attacks can have severe consequences for businesses with worldwide costs mounting over £484 Billion in 2019. The threats from cyber criminals come in many forms and are getting more sophisticated. Many businesses have invested heavily in infrastructure and systems which are excellent at keeping most threats at bay, but cyber criminals are typically a step ahead and will find vulnerability. It's not uncommon for organisations to feel protected due to the investment in systems and overlook the human element, their people. Unfortunately, the largest threat landscape for a cyber criminal is your end users.

According to IBM 95% of cyber breaches where caused by human error.

The great news is that there are solutions that can be put in place to quickly reduce the risk and encourage cyber safe behaviour. This e-book contains information on considerations that should be made on the pursuit of cyber safe behaviour and provides an overview of the following:

- Why the problem is worth addressing
- The role of the human in keeping your business safe
- Why awareness only is not the answer – behaviour must be changed
- How to ensure the training is continuous, defined and varied to appeal to multiple learning types
- Key areas a comprehensive programme should cover

The Problem Worth Addressing

74% of all Cyber Attacks start at the inbox

92% of Malware is delivered via Email

14% of global Phishing is aimed at Office 365 account takeovers

7 out of 10 businesses currently don't invest in any Cyber Education or Awareness

More than **35%** of leaders think their site will suffer a Cyber Breach in the next **12 months**

Over **90%** of Cyber Attacks involve Staff Error

54% of SMB Leaders perceived they are too small for Ransomware, **Cyber Criminals disagree**

Hackers target file corruption via **Malware**

The Role Of The Human

With an ever-increasing threat landscape for businesses to defend themselves against, it's now more than ever critical that businesses don't ignore the human factor. There are many variables involved in a cyber attack, with human error being the most consistent accounting for 90% of breaches. Clicking phishing emails, logging in to malicious O365 accounts, weak passwords, making fraudulent payments are all examples of errors that can increase the threat of a Cyber Attack and all are driven by human error. The reality is regardless of how comprehensive your cyber security systems are, cyber criminals will find entry points and attacks will get through. A final defence layer needs to be created, developed, tested and analysed – this is your human firewall.

89% of Business Leaders see Cyber Security as a top 5 priority

The good news is that the human factor can be addressed, your workforce can be educated on how to act under a cyber attack and most importantly you can create a culture of cyber awareness. The remainder of the e-book is focused around how to successfully implement a programme to start protecting your businesses at the last line of defence, your end users.

Exist To Change Behaviour, Not Just Increase Awareness

The key to creating a cyber aware culture is to involve all employees, it is not the sole job of the Info-Sec team or IT team to protect your business from cyber attacks, it is a shared responsibility across all staff. Cyber criminals don't discriminate. It's important that the shared responsibility is made clear, this must come from the top for existing employees and at the beginning for new. The messaging should not command, as this can create fear, it's about finding the balance of holding everyone accountable and responsible for their part to play, while at the same time encouraging employees to notify IT teams of potential threats and to raise any concerns they have.

Examples of measures a business can implement in addition to simulations and training to increase a security awareness culture:

- Posters containing useful information to reinforce training material
- Regular reminders to set strong passwords (and what these look like).

123456 – was the most popular password worldwide in 2019

- Praising staff that make suggestions to improve cyber defence and report potential threats – perhaps via your typical company staff bulletin or company meeting
- Awareness scores leader boards could be visible, so your people know if they are on the top 10 list of either least or highest risk (based on simulations and quiz scores)

How To Change Behaviour, Not Just Increase Awareness

Unfortunately, changing behaviour isn't as simple as just deploying security awareness training to all employees - which is why most organisations fail to build resilient security cultures. The following suggestions can help not only improve awareness but change behaviour.

1. Identify and prioritise the behaviours that put your organisation at risk from real time emerging threat intelligence – this can be achieved via a well thought out Simulation strategy

2. Continuously assess each behaviour at an employee level – this can be achieved via average grade scoring and simulation history in a reporting dashboard. The sum of all parts builds the organisational picture

3. Make it easy for employees to report phishing inline with incident management processes and ensuring employees understand the importance of "good" cyber behaviour and ultimately care enough to report a phish

4. Inhibit employees' automatic reaction to click on links

5. Run workstreams for each employee to improve behaviour, covering; Email Phishing Capability Intentions/Attitudes, Awareness, Passwords. Social Media Use, etc

By adopting a new, automated way of learning, you can deliver results over and above a typical "Awareness Campaign"

Features of a "new way" of learning

- Automated to reduce burden on internal resources
- Simulations relevant to your employee
- Real Time Analysis of Secure Behaviour
- Tailored learning journey relevant to the role
- Culture of secure behaviour – encourage the reporting of a Phish

"Employee training may prove to be the best ROI on cybersecurity investments for organizations globally over the next 5 years".

Source: Herjavec Group

Catering For Multiple Learning Types

An important factor when considering the success of a cyber awareness programme is to ensure that the solution meets the needs of multiple learning types. Therefore the way in which the training is delivered requires thought and structure to accommodate the user base. Traditional cyber awareness programmes have typically not been as effective as new ways of working. For example, making users sit and listen to a presenter for 2 hours a year will have minimal impact. It may help an organisation "tick a compliance box" but have very little impact on reducing risk in the environment. The main reason being the limited amount of information a person can absorb at a given time.

The most effective strategy in our opinion is continuous, defined and bite sized (think structured learning jounreys), combined with learning while in workflow (think regular simulations).

For awareness training to drive a security conscious culture its important that end users see the training as engaging, active and ongoing and get the ability to test their newfound skills and knowledge via both expected quizzes, but also unexpected simulations - learning in workflow.

Learning that is spread out over time drastically increases knowledge retention.

Source: Effective Learning Techniques, Promising Directions From Cognitive and Educational Psychology

Different Learning Styles To Consider

Learning Style	Description	How A Learning Journey Can Accommodate
Aural (auditory-musical)	You prefer using sound and music	Engaging videos and simulations
Verbal (linguistic)	You prefer using words, both in speech and writing	Infographics and white papers
Physical (kinaesthetic)	You prefer using your body, hands and sense of touch	Achieved via regular, visual webinars
Logical (mathematical)	You prefer using logic, reasoning and systems	Questions and testing
Social (interpersonal)	You prefer to learn in groups or with other people	Simulations, gamification, webinars and quizzes
Solitary (intrapersonal)	You prefer to work alone and use self-study	Infographics and white papers

Key Areas To Cover – In Awareness Programme

When implementing an "awareness programme" it is key to develop a comprehensive plan and learning journey. The level of detail is critical when designing an awareness programme, the goal is not to have your people become experts in Ransomware and Social Engineering (for example), the objective is to ensure people understand the landscape, the threats are able to spot them and ultimately act with company's best interest at heart. This education and knowledge needs to be delivered in a continuous manner as efficiently as possible, at the right level of detail to allow everyone to continue with their day job.

The following section lists the key areas an awareness plan should cover as a minimum:

1. Simulations relevant to the environment
2. Email Best Practise and Phishing Attacks
3. Safe Internet Usage
4. Social Engineering
5. Ransomware
6. Account Compromise
7. CEO Fraud
8. Hyperlinks
9. Working Remotely Best Practise
10. Information sharing
11. Reporting of Phishing Emails

Conclusion

Senior Leaders should not underestimate the damage a severe Cyber Attack can have on a business, not only the potential cost (CEO Fraud and Ransomware), the disruption to recovering the network (Malware and Downloadable Viruses), the real cost can often be the reputational damage. Often reputational damage can be very difficult to quantify but if your customers stop trusting you with their data and personal information there will be a price to pay, creating a Cyber Safe culture can give your business a comprehensive last line of defence. Make the investment now to a Cyber Safe culture and start protecting your business now.

SMB Cyber Attacks up 424%

Source: Hashedout

55% SMB Businesses cite lack of Cyber knowledge as a challenge

Source: BB Bureau

43% of all Cyber Attack target SMB

Source: Verizon

About Boxphish

Boxphish offer automated, intelligent & interactive training in Cyber Security Awareness to teach organisations to identify email-borne threats and change behaviours accordingly. Our defence strategy centres around our four features - Simulator, Reporting, Artificial Intelligence & University - which are designed with industry knowledge in mind for an effective solution against phishing, ransomware, social engineering & CEO Fraud. With online training modules, simulated phishing attacks, videos, quizzes, and helpful resources sent straight to your email, there is an option for every schedule and learning style, all can be delivered as a managed service.

For an initial discussion and demo visit **www.boxphish.com**

BOXPHISH

BOXPHISH.COM