modern networks

TEL: +44 01462 426 500

Cyber Security Series - 5

Cybersecurity: The Human Factor

Any security system is only as good as its weakest link. In the cyber security world, the weakest link is nearly always the human element. Around 40% of UK firms have suffered at least one data breach in the last 12 months. The most common form of breach was a staff member unwittingly clicking on a malicious link within a fraudulent email (a phishing attack). Like the shockwave from an explosion, the outcome from a cyber-attack can be far-reaching and extremely damaging. In recent years, firms such as payday lender Wonga, Tesco Bank and mobile phone operator Three have had thousands of customer records stolen, lost millions of pounds, seen share prices plummet, and found their brand reputations in tatters.

Human Error

Public awareness of high profile cyber-crimes seems to have little effect on our workplace behaviour, but does inhibit personal online activities, such as banking and shopping. Research by AXELOS found that most UK organisations significantly underestimate the human element of cyber risk. In fact, half of the UK's worst data breaches during 2015 were caused by human error. International standard for information security ISO 27001 and some insurance policies require firms implement cyber security training. However, most companies only provide training to senior managers and the IT department. Typically, end user awareness training is a far more casual, ad hoc affair for everyone else.

phishing.safebro
Phishing attack ahead
Attackers on phishing.safebrowsingtest.com might try to trick you to steal your
information (for example, passwords, messages, or credit cards).

Security Strategy

A cyber security strategy can only be effective where you have clear policies and procedures that everyone understands and follows. Otherwise, your own staff will constantly undermine your IT security regardless of what countermeasures you put in place. First, you need to assess the potential risks to your IT infrastructure, and decide what to prioritise. Next, ensure senior management advocate IT security as a business imperative. Finally, implement a clear information management regime with the appropriate checks and balances. User education will play a critical role in raising awareness of cyber security risks and changing behaviours.

Raising Awareness

Changing how people think and behave isn't easy. You might need some expert help. According to research from AXELOS, "The one-dimensional and outdated cyber security awareness training provided by most UK organisations is not fit for purpose and is limiting employees' ability to understand what good cyber behaviours look like." Before you do anything, you will need to establish a base level of cyber security awareness. Next, rather than bombard staff with masses of information, focus on your top three threats. In the UK, this might be raising awareness of fraudulent email phishing attacks, password protection and use of unsecured file sharing applications, for example.

Audiences Segmentation

When building your end-user awareness programme it is important to consider your different audience groups, and how best to communicate with them. Educational research suggests that interactive rather than passive learning tools and techniques produce the best results in terms of engagement and retention. Remember, there are different types of learners. Some people respond better to visual stimulus while others prefer auditory, text or a kinaesthetic approach (learning by doing).

Games

The more interactive, group-based, relevant and fun you can make your awareness programme the better. Developed by PwC, Game of Threats™ is a cyber security simulation designed to test critical thinking and decision-making. The game rewards good decisions and penalises teams for making poor choices in critical situations. Ultimately, players come away with a better understanding of what steps they must take to improve cyber security across their organisation.

Free Training Tools

Awareness of UK government-backed cyber security initiatives and standards remains low. In a recent survey only 8% of respondents said they were aware of the Cyber Essentials scheme. Currently, only 20% of UK employees receive any cyber security or awareness training, and that

figure is skewed in favour of larger enterprises. However, there are a number of free cyber security courses available such as Future Learn, Responsible for Information e-learning and ESET Cybersecurity Awareness training to get you started. A quick Google search will reveal a dizzying choice of paid tools, techniques and online courses to help you implement a user awareness programme.

Assessment

Having created your cyber security policies and introduced awareness training, you will want to measure the effectiveness of your scheme. As phishing attacks are so prevalent, you might send a fake fraudulent email to all employees as a test. You can then measure the number of people who click on a potentially malicious link and the number of people who report the email as suspicious. You could then repeat this exercise randomly as part of a phishing assessment of end user awareness.

Penalties of Inaction

Incredibly, most cyber attacks and data breaches go unreported. Many firms simply lack an awareness of who to report to, why to report breaches, and what reporting achieves. Nevertheless, failing to take the most basic cyber security precautions, not reporting accidental data loss and malicious activities can prove costly. The 2015 hack of telecoms provider TalkTalk cost the company an estimated £60m and 100,000 lost customers. They also received a £400,000

fine as the regulator found the cyber attack was completely preventable. New General Data Protection Regulations or GDPR will require every organisation to report data breaches to the Information Commissioner's Office from May 2018. Penalties for failing to comply with GDPR will be severe.

Contact Us Now

If you would like to know more about cyber security and data protection then contact us now for more information.

About Us

Modern Networks provides IT and telecoms managed services to over 1600 commercial properties and hundreds of enterprise clients. Our services including computing, enterprise anti-virus, business collaboration software, networking, infrastructure cabling, data backup, storage, VoIP telephony, WiFi, broadband and mobility solutions. Fully managed, continually monitored and expertly supported IT and telecoms services.

Sources: AXELOS, National Cyber Security Centre: 10 Steps: User Education and Awareness, National Archive, UK Government: Cyber Security Breaches Survey 2017, main report.

Images courtesy of Pexels.com, Christiaan Colen, Phishing Warning, Flickr.com, Freepik.com