Security First

The technology landscape is always changing. Its inhabitants evolve and predators adapt. In order to survive, organisations and individuals must adopt a security first mentality. For organisations, security cannot be an afterthought. Instead, it must be planned and built into the fabric of your IT infrastructure. You also need clear security policies that are regularly reviewed and updated.

The Weakest Link

Any security system is only as good as its weakest link. In the cyber security world, the weakest link is nearly always people. Around 50% of UK firms have suffered at least one data breach in the last 12 months. The most common form of breach is a staff member unwittingly clicking on a malicious link within a fraudulent email (phishing attack). In 2017, 17 million Britons were victims of cybercrime costing them £4.6 billion*.

Human Error

Public awareness of high profile cyber-crimes seems to have little effect on our workplace behaviour. Research by AXELOS found that most UK organisations significantly underestimate the human element of cyber risk. Last year, 88% of UK data breaches were caused by human error. The most common errors include sending data to the wrong recipient, loss or theft of paperwork, forgetting to redact data, and storing information in unsecured locations such as public Cloud servers**.

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

Tel: 01462 426 500 I Email: info@modern-networks.co.uk I
Web: www.modern-networks.co.uk

balances. User education will play a critical role in raising awareness of cyber security risks and changing behaviours.

Regulation

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. The regulator also fined them £400,000 for negligence, as the cyberattack was completely preventable. The new General Data Protection Regulations (GDPR) require every organisation to report data breaches to the Information Commissioner's Office. Penalties for failing to do so are severe.

Security First

Having a security first mind-set can pay big dividends in your work and private life. According to the 2018 Cost of Data Breach Study, the average cost of a data breach is £2.95 million, with an average cost per lost or stolen record of £113. Although the public perception of cyber criminals is comic book archvillains and high-tech hoodies, the reality is very different. In fact, most cyber crime is perpetrated by low-tech script kiddies and unsophisticated fraudsters. The uncomfortable truth is that many businesses and individuals simply fail to take the most basic IT security precautions. We use short, easily guessable passwords; we use the same password for multiple accounts; we open unsolicited emails and click on links without thinking; we leave paperwork on office printers; we use dubious mobile apps to share personal and work information; we plaster our personal data all over social media; and use free public WiFi services that anyone can intercept.

Awareness Training

A recent Dashlane survey found that nearly half (46%) of employees use personal passwords to protect company data. Staff need much better cyber security training and greater awareness of everything from opening suspicious emails to password management. 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 the main threats to your business. Typical user awareness training should include:

- Acceptable use policies
- Social engineering attacks
- Email management
- Password best practice

Tel: 01462 426 500 I Email: info@modern-networks.co.uk I
Web: www.modern-networks.co.uk

Security First

- Safe browsing
- Data backup
- Patch management
- Data protection regulation
- Incident reporting

The UK's National Cyber Security Centre suggests, "Giving the right user training and awareness interventions at the right times can help prevent security compromises. An organisation's staff can be one of its most effective defences, yet for many businesses a lack of user-centred security design is leaving them vulnerable."

No Simple Answers

The cyber-threat landscape continues to evolve, and no one security vendor can offer a complete solution to the problem. Instead, organisations will have to work with security firms and trusted partners like Modern Networks to combine best-of-breed solutions to meet your own unique set of requirements, challenges and risks. Today, successfully changing employee attitudes and indifference towards cyber security will go a long way to prevent accidental data breaches, phishing and other social engineering attacks in the future.

Sources: theguardian.com and verdict.co.uk

Images courtesy of Hacker by iaBeta, Flickr and Freepik.com

Tel: 01462 426 500 I Email: info@modern-networks.co.uk I
Web: www.modern-networks.co.uk