CYBER SECURITY BASICS

Richard Kennedy *explains the simple steps you should be following to keep your organisation secure*

UK SMEs have been found to be negligent in their approach to IT management, placing cyber security at risk according to a recent report by Xperience Group. The study found that 70 percent of those surveyed felt that there was room for improvement when it came to their data management practices. Meanwhile, 40 percent shared that they do not have a cyber security strategy in place, despite the fact that 84 percent said that they currently have an employee who is dedicated to managing cyber security and IT in the workplace.

As cyber attacks on businesses increase, firms ranging from large corporations to SMEs have been targeted, resulting in sensitive business data being exploited. 51 percent said that at present they believe their business is at risk of a cyber threat, with 92 percent experiencing some form of security or data breach in the past 12 months.

Just 67 percent said that they felt somewhat prepared for any cyber attack that occurred, with 87 percent confident that the current protocols they have in place would be enough to deal with an attack.

Security audits were found to be something that isn't being carried out regularly by SMEs as just over half (53 percent) said that they have carried out a security audit in the past three months – in fact, 11 percent could not remember the last time that they had audited their security processes.

As businesses begin to prepare for the upcoming GDPR regulations in Europe, which come into effect in May 2018, the above statistics paint a worrying view of how organisations are currently managing their data and IT security. As GDPR requires businesses to have stricter data management protocols in place, you would perhaps expect businesses to have already taken the necessary steps to place cyber security in the highest regard. GDPR is the biggest review of Europe's data protection regulations in two decades and, therefore, is set to be one of the largest data policy overhauls that many will see.

No two cyber attacks happen in the same way, so it is vital to remain vigilant

GET INTO SHAPE

Similar to how you would always lock your home or vehicle, business owners and IT and security managers need to have the same view when it comes to their businesses data and IT security.

Done is never enough. Rather than viewing cyber security as a task to be ticked off of a to-do list, it is something which should be continually audited and reviewed – a task that the study found businesses were not doing regularly enough. And with GDPR requiring a solid data protection approach, it's time for businesses to get their practices in shape.

Technology is continually evolving, and the same is true for the threats that businesses face. No two cyber security threats may happen in the same way, and this means that organisations should always be wary of when an attack will occur, and how.

All employees should be educated on the importance of cyber security and how their negligent actions could impact not only themselves but the business as a whole. Communicate how a robust security strategy will protect their work and data, but also the businesses and customers too.

A security breach could result in lost clients – in fact, according to Government estimates, businesses lose out on between £75 and £311,000. A figure made up of compensation, lost sales and disruption. Therefore, a cyber attack not only threatens to impact an employee and their work, but the business's bottom line too.

Employees are your first line of defence when it comes to security, and so should be educated on the practices that they should be following on the computers, networks, and systems that they come into contact with.

Share the different types of attack that could occur and that employees could face such as phishing emails, using an unsecured device or network, or sharing passwords. To improve employee engagement, real-world examples should be provided to increase relatability – and when attacks occur and are discussed in the media, these too should be discussed as it's likely to pique interest on the repercussions it could have if it were to happen to the business.

Discuss with employees the issues that they face and look at how you can create a security strategy that addresses these problems. By directly conversing with them on what they feel should be done it is more likely to engage them better when it comes to implementing the process.

Awareness of security policies within a business should also be raised through regular training sessions and security updates briefings – diarising these in advance will ensure that they are properly followed through.

GDPR requires organisations that have "regular and systematic monitoring" of individuals on a large scale or process a high number of sensitive data will have to employ a Data Protection Officer (DPO) to oversee their data management.

The role requires that senior staff members are kept informed of data issues in the business, that compliance with GDPR is adhered to and that they are key point of contact for employees and customers. Educating employees on data processing and compliance, regular security audits should also be conducted as part of the role.

IN 2016, ONE IN 131 EMAILS CONTAINED SOME FORM OF MALWARE – THE HIGHEST IN FIVE YEARS

Placing GDPR as a topic that now sits in the boardroom, GDPR is making data mismanagement a subject that is managed from the top down and infiltrated through to all areas of an organisation.

Although many organisations are likely to have someone in the position already, the regulations ensure that all businesses are following the same guidance when it comes to data management – ensuring that security risks are reduced.

While hiring a DPO is not mandatory for all businesses, it can be good practice to have someone dedicated to managing data and security in-house as it will ensure that it gets the required attention and that standards are upheld.

BE PREPARED

Greater importance should be placed on this role, as despite many hiring someone for this position, organisations have still said that they feel that they are unprepared for a cyber attack.

According to the National Cyber Security Alliance, after a cyber attack, 60 percent of small and medium-sized businesses will go out of business after six months. While large-scale security breaches are the ones that make the headlines, it is smaller companies that often suffer more when a cyber attack is carried out. Why? Smaller companies often do not have the infrastructure in place to deal with the fall out, or may not be in a financially secure position, meaning that losing clients places them in the red.

Rather than just being a reputational risk, a cyber attack can have serious financial implications, and businesses should be proactive in their approach to preventing an attack, rather than being reactionary. An attack could happen at any time and businesses need to ensure that they are fully prepared for any eventuality where their IT security and data could be compromised.

System and data back-ups should be carried out regularly to ensure that important documents and data sets are safe and stored somewhere that isn't your computer hard drive. Ensuring that your data is backed-up will mean that if you are hacked, you can still access documents elsewhere and can prevent them from getting into unwanted hands, or computers.

DATA PROTECTION

Completing multiple back-ups is recommended as it gives you numerous sources from which you can regain access to your data if required – of course, these will also need to have strict security processes in place.

As well as back-ups, encrypting your data will mean that if it does get into the hands of a cyber hacker, it is unusable unless the correct authorisation is input. Tools such as BitLocker are free to use and can be used with Window 7 and upwards.

All computers and devices with internet access – including those organisations with a BYOD policy – should ensure that anti-virus software is enabled. With many manufacturers providing free trials, these should be enabled, and security settings on devices reviewed to ensure they are working to their potential.

Cloud-based spam filtering, should also be implemented as this can reduce attempts to gain access to unauthorised data and documents that enter the system via email inboxes. In 2016, one in 131 emails contained some form of malware – the highest rate in five years, therefore quarantining inbox threats can help to protect the rest of the business.

These basic security practices should be followed to ensure that cyber attackers do not have the opportunity to infiltrate where weaknesses occur. Simple steps such as not opening emails from unknown senders, using complex – and different – passwords and activating security functions can greatly help to improve overall due diligence and protect the business.

> 40% OF COMPANIES SAID THAT THEY DO NOT HAVE A CYBER SECURITY STRATEGY IN PLACE

As mentioned above, done is never enough, and it is this mind-set that should be used when evaluating cyber security. There is always more to be done to ensure that security standards are upheld and of the highest quality. Therefore, be proactive in your approach to avoid becoming a business that lands itself on the hacked list ●

Richard Kennedy is Director of Cloud and IT Infrastructure at Xperience Group. Recognised as one of Northern Ireland's '40 under 40' and funding his own cloud computing business from the age of 16, he is an expert in cloud deployment and security solutions.

Cyber attacks can have financial implications and can damage a company's reputation