OPTIMISING DATA SECURITY

Andrea Babbs *reveals the steps businesses need to take to reinforce their security to protect customers, employees and the business itself*

With the number of cyber attacks and attempted data thefts increasing year on year, IT security should be one of the top priorities for all types of businesses – particularly during the current global pandemic. IT security leaders have witnessed a 30,000 percent increase in COVID-19-themed attacks already, including emails pretending to sell PPE or senders passing themselves off as representatives of the World Health Organisation. With scenarios like this progressively on the rise, businesses must go beyond the basic antivirus software running in the background, it's time for proactive education and engagement from every area of the organisation to ensure a foolproof defence.

It's all the more important considering the changes to work stations, equipment and hours. Workforces are no longer centralised and more independent decisions are required from employees working remotely and away from their teams. The rush to get workers up and running in the switch to home working has meant for many their cyber security may be compromised, such as the risks that come from employees using their own devices and networks. It's clear from the figures that cyber criminals have been eager to take advantage of this change, as many attackers have used the pandemic as a way to leverage existing tactics, techniques and procedures to exploit new opportunities. Without the right layers of protection, businesses will find themselves faced with hefty fines, loss of continuity and a lowered brand reputation.

It's widely documented that phishing scams are one of the most common ways for cyber-criminals to attack businesses

Employees are making critical security decisions on their own with the recent changes to work patterns and styles, and there is no longer scope for easy peer review and questions. Where workers could before reach out to colleagues to ask simple questions, such as: "Does this email look strange to you?", there's now a pressure to deal with things independently. Without the correct education, however, this can lead to data breaches and loss of confidential company information.

SWIFT ACTION

It's widely documented that phishing scams are one of the most common ways for cyber-criminals to attack businesses and data. With employees eager to show managers they are working effectively remotely, it may mean crucial errors aren't picked up on. Email is the number-one threat vector in organisations and the cause of nearly all data breaches, as confirmed by the Identity Theft Resource Center. Moreover, the ICO found that misaddressed emails are the largest source of data loss for organisations – with over 269-billion emails sent around the world each day.

It's imperative that employees are taking the utmost care with all aspects of their work. With today's workforce now working from potentially several locations across a number of devices it's even more important that education is used to reduce the chance of a breach. Furthermore, employees are increasingly trusted with company-sensitive information, assets and intellectual property. Many are permitted to make financial transactions – often without requiring any further approval. Given the data protection requirements now in place – not only GDPR but also industry specific regulation as well as accountability to internal compliance teams – organisations require robust processes to mitigate the risk of data loss.

Fifty three percent of data breaches are classified as insider, clearly the workforce has a critical role to play in an organisation's cyber defence strategy. As such, some businesses operate a penalty system in an attempt to keep data secure, including the threat of dismissal. However, this strategy isn't supportive of a positive culture that helps improve employee growth. Consistent training, for example, and a way to better manage email, with a system that flags potential mistakes before they're sent is the way forward.

There is a solution that can add a layer of employee security awareness, for example simple safety checks that give email users the chance to confirm the identities of email addressee(s), and if present, attachments, it can also help employees avoid common mistakes like missing off the attachment altogether. These types of solutions, for example VIPRE's SafeSend, can provide that layer of data protection while also improving efficiency.

It can also be utilised to check for keywords within the email and this list can be personalised to the business to include not only specific phrases, but also common terms such as confidential, private or strings of data like credit card numbers or National Insurance/Social Security numbers. Any emails – including attachments – containing these key words – or for instance unreleased product names – will be flagged, requiring an additional confirmation before they are sent, providing users a chance to double check whether the data should be shared with the recipient(s).

These solutions can also be deployed on a department-by-department – even user-by-user – basis. For instance, a business may not want HR to be able to mistakenly send sensitive personal information to anyone internally and therefore require a confirmation for all emails. Similarly with financial data – even marketing data at certain times – such as in the run up to a highly sensitive new product launch.

> IT SECURITY LEADERS HAVE WITNESSED A 30,000 PERCENT INCREASE IN COVID-19-THEMED ATTACKS

These layers of security are an essential tool in the fight against data breaches, and importantly also phishing emails – for example an email that purports to come from inside the company, but actually has a cleverly disguised, similar domain name. It enables individuals to feel confident that emails have been sent to the right people and with the right attachments. If a busy employee responds to an email from V1PRE, for example, as opposed to VIPRE, thinking it genuinely comes from inside the business, the technology will automatically flag that email when it identifies that it is not an allowed domain, enabling the user to cancel send and avoid falling for the phishing attack.

With these solutions implemented business-wide, it enables organisations to feel protected and safe knowing that email security as well web and endpoint protection is in place. Attacks are becoming more and more sophisticated, but by evolving and focusing on empowering employees through education and support, the number-one threat to businesses – human error – can be removed. Workers can confidently take on responsibility for data security through memorable, bitesize chunks of training, spread through the year, making every employee honorary members of the IT security team.

Why is it necessary? Without this protection the costs can be detrimental to businesses. Should confidential corporate information fall into the wrong hands the consequences could be devastating, including reputational damage, intellectual property loss or compliance breaches, which businesses must be aware of when deciding how much to invest in their IT security infrastructure. Crucial company information such as proprietary ingredients or the blueprints of an unpatented new product leaking into the public domain could easily be intercepted by the competition, resulting in a lost competitive advantage as well as the loss in revenue.

Human error is inevitable, and a simple missed or added character to an email address – where autocorrect takes over, for example or from pressing send too soon – results in sensitive information reaching the wrong inbox. It could be an unknown individual, competitor or even cyber criminal.

EMAIL IS THE NUMBER-ONE THREAT IN ORGANISATIONS AND THE CAUSE OF NEARLY ALL DATA BREACHES

Data breaches are now reaching considerable sums in fines too. In 2018 the Independent Inquiry into Child Sexual Abuse (IICSA) was fined £200,000 by the Information Commissioner's Office (ICO) for failing to protect the identity of possible victims of child abuse after a human error accidentally exposed victim identities to third parties, when they included their email addresses in the 'To' rather than 'BCC' field. This demonstrates just how seriously the ICO takes these types of data breaches, and the pain of embarrassment from sending an email to the wrong contact pales in comparison with the business pain from financial penalties and reputational damage.

Moreover, the misuse of CC and BCC functions could expose your entire contact database, potentially giving your competitors an opportunity to lure your customers or employees away, or worse – exposing customer emails to potential hackers. Another example is BitMEX, one of the world's largest cryptocurrency trading platforms, which accidentally leaked thousands of private customer email addresses when it sent out a mass mailshot without using the BCC function. While the company maintains that customer privacy remains a top priority, its customers were left wondering how they could trust BitMEX with huge personal assets in the aftermath of this data protection failure.

Workspaces are reopening now, but the majority of businesses have changed dramatically and there will no longer be a return to a centralised office space. The new normal of hybrid workforces must have these correct layers of security to protect all types of employees, for example with the combination of reminders, prompts and continuous training to go alongside technology solutions.

The onus must be on all members of the organisation to remove the weak links and employees can be a vital tool in the fight against cyber-crime, with access to regular training backed up by technological solutions, which support and catch the inevitable human errors. Workers can make informed decisions about the nature and legitimacy of their emails before acting, without adding time or delay to their work, while reinforcing compliance credentials. By encouraging this positive culture around cyber security and implementing layered email security, organisations can evolve and remain protected against attacks now and into the future ●

Andrea Babbs has worked in the IT Industry for over 20 years. She is currently Country Manager and Head of Sales for VIPRE Security Limited, where she manages the UK and Irish business.

The rush to get people working remotely during lockdown has meant, for many, cyber security has been compromised