HELP YOURSELF

Don't make your business a sweet shop for cyber criminals

At first it felt like any other day at a US technology company providing back office functions to leading banking groups. But then an email arrived from an unknown source. The company's servers had been breached and reams of sensitive customer information had been stolen.

If the company didn't agree to pay US$20,000 within 72 hours, the email sender claimed they would put the details on the internet.

Sophisticated cyber attacks like this on businesses worldwide are on the increase, according to internet security expert Symantec. It detected a 91% increase in targeted attack campaigns on businesses in 2013, with a 62% increase in the number of breaches. These breaches in turn led to more than 552 million identities being exposed.

As a result of the scale of the problem, in its annual Security Threat Report, Symantec christened 2013 'the year of the mega breach'. It's a situation that's shown little sign of improving in 2014, with online auction site eBay targeted by hackers in May, leading to millions of passwords and other data being exposed.

Worryingly for businesses in the UK and Ireland, the region appears to be one of the most popular targets for cyber criminals, with security firm FireEye reporting a 300% increase in attacks in 2013 compared to 2012.

When you take into account that the scale and cost of security breaches to individual businesses doubled last year, according to data from the Department for Business, Innovation & Skills (BIS), it's clear that this is a threat that companies can no longer afford to ignore.

MID-SIZED COMPANIES OFTEN DON'T HAVE AS MUCH DATA SECURITY IN PLACE AND DON'T HAVE THE IN-HOUSE EXPERTISE TO CONFIGURE OR RUN A TIGHT SECURITY SYSTEM

So what should businesses be doing to shore their defences against cyber criminals and what steps do they need to follow if and when a breach occurs? Although Symantec's research shows that the most commonly targeted sectors are mining, governments and manufacturing businesses, Andy Townsend, Director of Computer Forensics at Newport Africa, says that, "Everyone is fair game. The cyber criminal will go where he/she thinks there is money."

It's a view shared by Colin Tankard, Managing Director at data security specialists Digital Pathways. Although Tankard says his own research shows that financial organisations are targeted the most by criminals, any organisation that holds data on individuals could be subject to an attack. "Mid-sized companies often don't have as much data security in place and don't have the in-house expertise to configure or run a tight security system," he explains.

Although putting protection in place may sound a daunting and potentially costly task, help is available. The UK Government has launched a Cyber Essentials Scheme to assist companies in assessing risks within their organisation and protect themselves against online attacks. When the scheme is fully

>

launched, companies will be able to undergo an independent assessment of their procedures and if successful attain the Cyber Essentials certification badge.

In the meantime, companies that want to make their systems more robust can do so just by implementing a few simple housekeeping rules, according to Townsend. He says the installation of anti-virus software that is regularly updated is vital. Cyber threats are evolving all of the time and as a result, internet security software packages are constantly being patched to ensure they can fight off the latest bugs.

Companies should also back up information regularly and bring in an external expert to carry out vulnerability testing on their systems so that any potential weaknesses can be identified and rectified.

COMPANIES SHOULD CONSIDER DEPLOYING TWO-FACTOR AUTHENTICATION TO IMPROVE PASSWORD MANAGEMENT AS MANY SECURITY BREACHES ARE DOWN TO USERS CHOOSING PASSWORDS THAT ARE TOO SIMPLE

One surprising weakness that Tankard frequently comes across is security tools that are not configured properly. “We find so many badly installed systems, or systems where random ports have been opened with no thought of the impact,” says Tankard. “This often comes from companies using third-party support companies that do not specialise in data security.” He adds that companies should consider deploying two-factor authentication to improve password management as many security breaches are down to users choosing passwords that are too simple, and they should also educate employees on good data security.

This education needs to encompass a wide range of different areas, from teaching people how to make sure company-issued devices like laptops and smartphones are secure – according to Symantec’s Norton Report, 38% of mobile users experienced mobile cyber crime in 2013, with 24% of mobile users storing work and personal information in the same accounts and 21% sharing logins and passwords with family – through to telling them how to avoid falling victim to one of the 156 million phishing emails that are sent every day.

GONE PHISHING

Of these, each day, eight million are opened, 800,000 links are clicked and 80,000 people have their information stolen. If an employee falls for such a scam it’s vital that the employer acts swiftly to minimise the damage caused.

Depending on the level of the attack, it might even be necessary to disconnect a company’s systems from the internet and lock everything down, according to Tankard. “It can be of use to investigate the attack and try to find the level of exploitation, what is being targeted and, ideally, identify the culprits. In this way it makes cleaning the situation much easier,” he explains.

When it’s been confirmed that a breach has occurred, companies need to ensure that they comply with the data protection rules. In March this year, the European Parliament voted in favour of the draft EU Data Protection Regulation, which will provide a unified set of rules to all EU members in 2017.

HONOUR IN THE BREACH

Under these terms breaches would need to be reported to the relevant national supervisory authority in the country where the business is headquartered without delay, and where possible, within 72 hours, otherwise companies could be subject to fines of as much as €100m, or 5% of global annual turnover – whichever is the higher amount.

The cost of breaches has already risen in the last three years. BIS’s Information Security Breaches Survey 2014 showed that for small organisations, the worst breaches cost between £65,000 and £115,000 and for large organisations, between £600,000 and £1.15m.

Companies can limit the extent of the damage imposed on their business by putting in place suitable cover, says Tankard. “Given that the cost of

SIMPLE TIPS TO STAY SAFE

- Install anti-viral software, ensure it is regularly updated
- Back up all information regularly offline
- Don’t choose passwords that are too simple: ‘qwerty’ (the top left six keys), ‘changeme’, the user’s name and the old chestnut: ‘password’ are the most regular offenders
- Don’t share the password with friends, family and colleagues and don’t write it on a PostIt note stuck to the computer
- Don’t give out personal details in emails and check your privacy settings for personal social media accounts are at their highest
- Phishing emails can be very sophisticated and appear to come from someone you know. Always hover the cursor over the email address to check it matches the one you are expecting before you open the email
- Check the web address of the site you are visiting is spelt correctly. Cyber criminals mimic well-known brand home pages to capture your account details but will often have a letter different in the web address

›

rectifying a breach is going up, insurance would be wise," he advises. "If we consider the recent attack on Target in the US, the estimated cost to the business is around US$3bn – enough to bring down the biggest organisations."

Travelers offers a product to segments of the IT and software industries as well as electronic manufacturing and assembly operations. It covers a number of exposures, including first-party hacker damage cover – or 'network security' – and also third-party cybermedia liability cover, which protects against problems such as the unintentional transmission of a computer virus.

According to Mark Lawrence, Development Underwriter for Travelers, there's been a growing interest in this type of cover, driven by the volume of high-profile incidents. "All technology firms have potential cyber exposures, but they vary by company," explains Lawrence. "For example a data centre would have a greater potential exposure around privacy (if they were holding customer information) than an electronics manufacturer."

Travelers also provides cyber extortion cover within its Kidnap and Ransom product. "So if a cyber attack occurs and you are extorted for money it will pay for a professional security services organisation to come in and help you deal with that situation," explains Melanie Simpson-Mills, Development Underwriter at Travelers. "It will also cover the cost of extra staffing or expenses – everything entailed with getting the problem solved." The value of this type of protection is highlighted by the example of the technology provider at the start of this story. Thanks to its insurance, the company was able to call in a security organisation that worked closely with the FBI. They tracked down the extortionist who was arrested when he went to collect the ransom.

CYBER CRIMINALS DON'T CARE IF YOU MAKE CAKES OR CARPETS. THEY DON'T CARE WHAT BUSINESS YOU'RE IN. IF YOU HAVE GOT A COMPUTER SYSTEM, THAT'S ALL THEY CARE ABOUT.

Statistics from the likes of Symantec underline that cybercrime is a real threat that's growing. As Simpson-Mills points out, "These cyber criminals don't care if you make cakes or carpets. They don't care what business you're in. If you have got a computer system, that's all they care about. Everyone is vulnerable." ■

THIS ARTICLE FIRST APPEARED WITHIN TRAVELERS CODE RED, SUMMER 2014 ISSUE.

Click here for more information on our Technology products

INDUSTRY*Edge*®

Travelers Insurance Company Limited
61-63 London Road, Redhill, Surrey RH1 1NA
Europa House, Harcourt Centre, Harcourt Street, Dublin 2, Ireland
Travelers Insurance Company Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.
Registered office: Exchequer Court, 33 St. Mary Axe, London EC3A 8AG. Registered in England 1034343. Registered as a branch in Ireland 903382.