TRANSPUTEC

When will it HAPPEN TO **YOU**?

How **SMEs** can manage and mitigate the risk of data breaches

Executive Summary

While cybersecurity breaches at major international firms tend to grab the headlines, small and medium sized enterprises (SMEs) are in fact much more likely to fall prey to cybercrime. This whitepaper will provide you with the essentials for understanding the threats facing your business and detail the steps you can take today to minimise your chances of having business-critical information stolen.

Introduction: behind the headlines

When they strike, major cybersecurity incidents tend to dominate the headlines. Whether it is for the financial toll on businesses, the disruption they cause, or the embarrassment they engender for individuals whose details are leaked online, these breaches have a huge impact on the public imagination.

Take May 2017's WannaCry attack, which infected thousands of computers in hundreds of organisations around the world. Users of infected machines were presented with a ransom note explaining that their data had been encrypted and that to regain access, they would have to pay a fee of between USD$300 and $1200. The attack was unprecedented in scale and in the UK its largest victim was the NHS. The impacts were real: numerous outpatient appointments and operations were cancelled following the attack[1].

However, while the occasional breaches at major organisations are widely reported in the press, there is a far more pervasive threat of attacks against smaller British businesses. According to the UK government's 2017 Cyber Security Breaches Survey[2], 46% of all UK firms identified at least one cyber security breach or attack in the last 12 months, and in most cases, these breaches were reported to have adversely affected the organisation. Given that 99% of UK businesses are classified as SMEs[3], most victims will likely be businesses with under 1,000 employees. These findings are borne out across the globe, where SMEs are most often the victims of email phishing, 'CEO scams' and spam[4].

Perhaps most worryingly for SMEs is that the costs of a cyberattack can be much more devastating than for larger companies. According to the UK government survey mentioned above, the average cost of breaches for medium-sized firms is £3,070, relative to size, the cost of breaches to small businesses is normally much more damaging - so much so, that in the US[5], up to half of all small businesses are estimated to close within six months of a major breach.

It is therefore shocking that respondents to the UK government's survey seem to still have a fairly relaxed attitude to cybersecurity. For instance, only 20% of businesses report having actually sent staff on cybersecurity training days in the past year - and the majority of these are specialist IT staff.

46%	74%	33%
Proportion of UK firms who identified at least one breach	Proportion of UK firms that say cyber security is a high priority	Proportion of UK businesses with a cyber security policy

In 2012, Robert S. Mueller III, Director of the FBI at the time, famously stated: "I am convinced that there are only two types of companies: those that have been hacked and those that will be"[6]. Given the ever-increasing number of hacks against businesses of all size in the UK, the threat is no longer something SMEs can ignore.

This whitepaper will outline what the most common threats affecting your organisation are, and then provide a set of simple steps that you can implement to immediately reduce your risk of becoming a victim of cybercrime.

[1] 2017. Financial Times. *No evidence of second wave of cybet attacks on NHS, says Hunt*. Available online: https://www.ft.com/content/a1d0f5a0-38bc-11e7-ac89-b01cc67cfeec

[2] 2017. UK Government. *Cyber Security Breaches Survey*. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[3] 2016. House of Commons Library Briefing Paper No. 06152. Available online: researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf

[4] 2017. Symantex. *Internet Security threat Report*. Available online: https://www.symantec.com/security-center/threat-report

[5] 2015. US Securities and Exchange Commission. *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businessess*. Available online: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_edn16

[6] 2012. Robert S. Mueller, III. *Speeches*. Available online: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

What if it happened to you?

Running a small to medium sized business is time-intensive. Resources are very often stretched, and it's easy to understand how mistakes occur and breaches happen. Without adequate resources or an understanding of the risks posed by cybercriminals, internal leaks or even unintended disclosures, the chances of having your data compromised are not negligible. What might a typical breach look like at an SME?

- A finance officer at a small business receives an email in his inbox containing a link
- The email appears to be from the company who provide your online accounting software
- The email is well written, and simply asks the employee to log in to his online account to view an urgent message about changes to the service
- However, this is a phishing scam. The employee believes he is logging into the accountancy software, when in fact he is handing over his details to a criminal
- Nothing happens when he tries logging in to the system, and so he forgets about the email
- In the meantime, the hacker has access to a treasure trove of information about the company: their customers and accounts, potentially their banking details and a lot of private, business-critical information
- From here, the hacker has a number of options: they can block the SME out of the accounting software until a ransom is paid, or they may do nothing, biding their time to find other loopholes into the target's systems

The example outlined above is far from unusual - most of us have received fake emails to our personal email accounts from would-be banks, telecoms companies and e-commerce providers asking for similar log in details. Cybercriminals use the same methods when targeting businesses - and the effects can be far worse. Not only may the victims lose business and have their reputations damaged, there is also a high chance that they will also receive fines for failing to keep customer data safe.

The Five Biggest Cyberattacks of 2016

1. **Tesco Bank**: £2.5 million was stolen from over 9,000 customer accounts
2. **Three Mobile**: hundreds of thousands of customers' data was stolen
3. **National Lottery**: Camelot had thousands of customers' personal details exposed
4. **Yahoo**: in the biggest data breach in history, over 1bn accounts were breached
5. **Twitter, GitHub, Netflix**: all were affected during the Dyn DDoS attack which disrupted their services

How do breaches happen at SMEs?

Historically, SMEs were not the major focus of cybercriminals. The perceived prizes of hacking a large firm, such as a national bank or government department, meant hackers spent less energy on smaller firms. This has changed over time however, as hackers now see many SMEs as a ‘soft touch’. Many small and medium sized businesses have fewer resources to expend on cybersecurity training, and there is very often a sense that ‘it won’t happen to us’. These factors play into the hands of cybercriminals whose traditional targets have become more effective at protecting themselves.

Before you can even begin protecting your business and your customers’ data, it is essential to understand why breaches happen in the first place. These risks are not exclusive to SMEs, yet when resources are limited, training is more likely to slip and breaches to happen.

1. Technical weaknesses

When a company fails to update its IT systems, the business is immediately exposed to potential threats. The much-publicised 2017 WannaCry attacks occurred because of just this problem: most of the victims had failed to install a patch from Microsoft that was released earlier in the year. As a result, hackers could exploit this loophole in their systems and demand ransoms.

2. Insider threats

Often misunderstood, insider threats typically arise from a frustrated employee or contractor who wants to damage the company for a perceived slight, financial gain from selling information or as some kind of political statement. Insider threats tend to meticulously gather information and download it onto their own devices before leaking it online or to competitors. They may use their colleagues as innocent accomplices, asking them if they can borrow their password for some fictional requirement.

3. Untrained employees

Perhaps the biggest cybersecurity risk for any business comes in the form of untrained employees. A large proportion of targeted criminal attacks simply would never be successful without the unwitting aid of company staff. Whether it’s downloading content from untrustworthy websites or clicking on links in phishing emails, poorly trained employees can do more harm than even the most sophisticated hacker. It’s also worth adding that unintentional sharing of content via email, or publishing sensitive material on external facing websites still happens when employees do not understand how to use technology correctly.

The most common threats to SMEs

- **Ransomware:** this is a kind of malicious software which usually comes from a phishing email. It can encrypt the whole company's network, and then demand a sum of money to return access to the victim
- **CEO fraud**: an increasingly common and sophisticated kind of attack. A criminal hacks the email account of a senior employee at a firm or creates a similar-looking 'spoof' email account, and then sends an email to a junior member of staff ordering them to make a payment to a fictional supplier
- **Hack attack**: often arising through an unpatched vulnerability in a company's systems, or by simply guessing weak passwords, a hacker is able to enter a victim's environment and steal information
- **Denial of service attack**: this happens when a company's website or servers are overwhelmed by the sheer quantity of data being pushed at it. Criminals may extort money from potential victims, knowing that the attack will cause damage to the victim's profitability, as 'punishment' for some perceived wrongdoing by the victim or from unscrupulous competitors aiming to damage the victim's profitability

Five steps you can implement today to reduce your risk

As this whitepaper has demonstrated, the threat facing SMEs from cybercrime, hacking and human error are higher than ever. And, while many larger organisations have begun upgrading and improving their processes to protect themselves, most small and medium firms are still lagging. At Transputec, we have helped countless small and medium sized businesses cut their risk from a cyberattack. And while no organisation will ever be entirely free of the risk of being breached, implementing the following five steps can dramatically cut your chances of a costly attack.

1. Basic training

As this whitepaper has shown, the vast majority of cyber security breaches occur because of human error. Relatively few SMEs ever send staff on cybersecurity training, and when they do, it is almost always members of their existing IT teams - yet in most cases the initial victims of phishing and CEO-scams will almost always be non-IT staff. Cybersecurity training - carried out annually at the very least - should be part and parcel of your employees' training schedules.

Besides updating their awareness of how phishing emails work, or how to verify a CEO-scam, your training should also aim to help employees spot unusual behaviour amongst their colleagues. Is someone asking for passwords of other people's accounts? Are they mentioning their disapproval of the company or airing grievances, or even making veiled threats? Being conscious of this kind of behaviour should help eliminate many potential breaches, and training is the ideal place to start.

Transputec's accredited trainers can provide your teams with expert guidance on cybersecurity best practices, and also provide the latest instruction on keeping your data secure and in compliance with the incoming GDPR regulations.

2. Developing a business continuity and response plan

Even with all the best practices in place, you still face the risk of being victim of a hack attack or denial of service. Nonetheless, you can immediately reduce the damage such attacks can cause by developing a business continuity and response plan. This should include, but is not limited to:

- Identifying the threats you are faced with
- An impact analysis
- The encryption of your most sensitive data
- Backups of your environments, websites, or even your entire servers in a secure environment

A business continuity plan will mean you can continue work, at least to a degree, when an attack happens, and will limit the damage.

Transputec's expert consultants can help you develop a business continuity and response plan which fits your business needs and help you use innovative products like Crises Control as an integrated part of any communications plan.

3. Update all your software

As this whitepaper has reiterated, a major source of data breaches comes through unpatched software. Your IT department or service providers must constantly ensure that all software your employees are using is up to date. This is easier said than done of course - especially in a world of 'shadow IT' where employees store data in unsecure third party apps, on USB sticks or their personal computers. What's more, if you use heavily customised applications, applying patches directly from Microsoft or IBM is trickier than it seems. Given these risks, it may be worth questioning if it is time to upgrade to a more easily managed IT environment.

Transputec help SMEs across the UK keep their systems up to date through our monitoring and support services, giving them peace of mind that the risk of a breach is limited.

ThreatSpike Labs

4. Monitor constantly

Many breaches arise simply because IT departments don't have the time to constantly monitor behaviour across their environments. As company platforms grow, the task of checking that there is no privilege misuse, data leakage or viruses in the network becomes increasingly difficult. To overcome this challenge, it is highly valuable to automate the process of monitoring your network.

ThreatSpike Wire is one tool which can help here: once deployed, it collects, records and continuously analyses network traffic so as to detect harmful activity. By using machine learning, it is able to learn about your network and discover any unusual behaviour, alerting you to potential security incidents. Tools like ThreatSpike can be made even more powerful in conjunction with a team of external security experts to watch out for false positives and alert you to the real threats facing your systems.

Transputec has deployed ThreatSpike Wire on the networks of countless UK SMEs. Our experienced consultants help clients get the most out of the tools and minimise the risk posed by external attackers.

5. Test your defences

Many security breaches occur because businesses mistakenly believe that their networks are secure, leading to complacency. They have done all the usual tests, and so feel confident that they are not at risk. However, cyberattacks normally hit businesses where they least expect, and so constantly testing your defences is essential for ensuring you are safe and secure.

If you don't have access to an army of 'ethical hackers' to test your firewalls, one solution is to use a tool like Cybot. Cybot is a next generation penetration testing tool designed to scan, map and reveal vulnerabilities in your business's defences, and then inform you about how to resolve them. It achieves this through 'attack path scenarios' which visually represent how your network could be breached. By imitating human hacking behaviour and carrying out penetration testing, **Cybot** finds vulnerabilities in real time, and reveals all the potential paths and hops a hacker could use to access your core data. Most importantly, Cybot tells you in easy to understand business language what you can do to resolve your vulnerabilities.

Transputec are the experts at deploying Cybot, helping UK SMEs get the most out of the software, discovering weaknesses in their environment and helping them decide how to resolve problems Cybot highlights.

How much could a data breach cost you?

$4 Million

The average cost of a data breach[7]

29%

How much the cost of breaches has risen since 2013

$158

Average cost of a lost or stolen record

The average cost

of a stolen record varies massively by industry:
Healthcare: $355
Education: $246
Public sector: $80

$16

Savings made on each lost record when encrypted

[7] 2016. IBM & Ponemon Institute LLC. *2016 Cost of Data Breach Study*. Available online: https://www.ibm.com/security/infographics/data-breach

Manage and mitigate the threat to SMEs

This whitepaper has shown that SMEs are increasingly becoming the targets of cyber criminals. These firms are targeted because of a perception among hackers that they often use out of date software, fail to train their staff on best practice or let their defences slip. Unfortunately, this perception is often true. The damage that security breaches can have on SMEs is enormous and, in some cases, can lead to the failure of the business.

The first step to mitigating your risk of becoming a victim of a cyber-attack is to understand the threats that your business is exposed to - both in a general sense, but also with regards to your specific industry. From here, you can begin to implement a plan to review your existing security practices and minimise those risks.

Working with a trusted partner

Many SMEs are well aware of the threat posed by cyber criminals, yet struggle with finding the resources, the time or the expertise to deal with these risks internally. Transputec have helped countless SMEs worldwide monitor, manage and mitigate the risk posed by cyber criminals. We are able to advise on best practice for your specific scenario, implement the most advanced security, monitoring and testing software, and train your employees on the latest dangers.

To learn more about our services visit:
http://www.transputec.com/solutions/cyber-security-as-a-service

ABOUT TRANSPUTEC

Transputec is an established Information Technology Services and Solutions company with more than 30 years of IT innovation and excellent customer service.

Transputec was founded by two computer science students from Imperial College in their dorms. Developing applications for the banking industry and then migrating to a full IT services organisation.

We believe in flexibility, quality, agility. We see this simply as the ability for us to grow our services as quickly and with the speed our clients expect, whether they are enterprises or small/medium sized organisations.

Transputec is a Certified N-able NOC and Service Desk partner.

For more information, please visit:

💻 www.transputec.com

📱 +44 (0) 20 8584 1400 (Enquiries)
+44 (0) 20 8584 1440 (Support Desk)

✉ enquiries@transputec.com
support@transputec.com

PCR AWARDS 2017 WINNER

LLOYD'S REGISTER • LRQA
ISO 9001

Celebrating 30 Successful Years

LLOYD'S REGISTER • LRQA
ISO/IEC 27001

Transputec Ltd, Transputec House, 19 Heather Park Drive, Wembley, London HA0 1SS