CySure

Small business and cyber security: The importance of being cyber ready in an online world

A CySure white paper

Summer 2019

Executive Overview

The finance sector regulator, the UK Finance Conduct Authority (FCA), recorded a ten-fold increase in cyber-crime incidents between 2017 and 2018[i], however, across all sectors more businesses are reporting being impacted by a cyber incident year-on-year. According to a recent report conducted by Hiscox[ii], there has been a sharp increase in the number of cyber-attacks this year, with more than 60% of firms having reported one or more attacks - up from 45% in 2018.

However, often hardest hit is small to medium enterprises (SMEs), that lack the expertise and financial resources to withstand the fallout from a cyber incident. According to the Cyber Security Breaches Survey 2018[iii], 42% of small businesses identified at least one breach or attack in the last 12 months. SMEs have become an enticing target because of their lack of security defences.

Depending on the severity of the attack, SMEs can suffer severe disruption; impacting business operations and preventing staff from carrying out their day to day work.

In a rapidly evolving landscape of cyber threats it is vital that organizations of all sizes and sectors understand the risks and act fast. Being underprepared is no longer an option and organizations that ignore the problem risk their reputation and potentially, for SMEs, the failure of the company. In this white paper, we explain why in an online world no business can afford to ignore the risks associated with cyber security.

Missing out on lucrative supply chain contracts

For supply chains to work effectively they require every organization involved to communicate within a central system to avoid issues such as inaccurate inventory reporting, unexpected shortages and supply chain fraud. With information and security arrangements shared across the open supply chain, the cyber-security of every organization within the chain is potentially only as strong as that of the weakest member.

The Hiscox report revealed that supply chain incidents are now common place and contributing to the rise in cyber-crime. Nearly two-thirds of firms surveyed (65%) have experienced cyber-related issues in their supply chain in the past year. This echoed findings from a recent UK Finance report [iv] that cited connections with third parties as a point of weakness that cyber-criminals are exploiting.

A determined attacker will stress test the security of a supply chain, seeking to identify the weakest link and use any vulnerabilities present to gain access to other members of the chain. Whilst not always the case, it is often SMEs with their limited IT expertise and resources, that have the weakest cyber-security arrangements.

Organizations that are subject to the EU General Data Protection Regulation (GDPR) have a limited time to report a data breach to the Information Commissioner's Office (ICO). Under the GDPR, data controllers are responsible for their own compliance as well as that of any third-party processors. As a result, organizations are closely examining the security practices of any potential third party and seeking agreements to the measures it will take to secure its systems.

Cyber Essentials Plus is a Government-backed, industry-supported scheme developed by the UK Government with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF). By gaining Cyber Essentials Plus certification, organizations are able to demonstrate that their cyber security has been verified by independent experts. This auditable proof is often requested during tender bids as part of the warrants and liabilities process.

With so many prolific data breaches occurring due to flaws in third-party partners, SMEs need to step up and prove their security credentials – or risk missing out on lucrative business opportunities.

65% of UK Small Businesses do not have plans in place to deal with potential supply chain disruption, including cybercrime

Source: *Federation of Small Business*

Data loss, fines and tarnished reputations

The sharp rise in the number of cyber-incidents reported by the UK's financial sector is likely to have been driven in part by the EU's General Data Protection Regulation (GDPR). The regulation introduced an obligation on all organisations to report certain types of security breaches.

The new significantly bolstered powers issued to the Information Commissioners Office (ICO), and its European counterparts, came with greatly enhanced powers to levy fines. The ICO has recently shown that it will not hesitate to punish companies that break laws protecting consumers' data. British Airways and the Marriott hotel chain were among the first firms targeted by the watchdog, which handed them fines totalling almost £300m.

Cyber criminals are motivated by financial gain and data is a lucrative currency. Organizations such as legal and accountancy firms are viewed as rich pickings, as they are a "gateway" to client information. Criminals are attracted by the vast amounts of valuable data they hold. New client intake procedures require firms to check personal identifying information such as passports, bank statements, tax statements and national insurance/social security numbers. For corporate clients, law firms hold commercially sensitive information on mergers and acquisitions, contracts and intellectual property. All this information is profitable currency in the wrong hands.

SMEs in these sectors are perceived as soft targets with few security barriers, limited cyber security tools and little or no in-house expertise. Unfortunately, many organizations are in denial about the risks. A survey by Accenture found that 78%[v] of financial institutions were confident in their cyber-security strategies. Yet 1 out of every 3 firms is successfully attacked, with an average of 85 breach attempts per year.

Regardless of size, if your business handles personal information then data protection laws apply. Failure to comply will not only result in a hefty fine and a tarnished reputation. Should a business be implicated in a data breach it may be forced to cease operating during the investigation process if data procedures are classed as unsafe. The temporary barrier to access market opportunity could prove impossible to recover from.

The ICO has made an example of British Airways and the Marriott and the fines should provide a cautionary tale for all organizations. The ICO has shown that it is a regulator to be respected and it will not hesitate to fine companies that fail to ensure appropriate standards of technical and organizational security.

59% of financial service organizations admitted that it took them months to detect a successful breach

Source: *Accenture, Building Confidence - Solving Banking's Cybersecurity Conundrum*

SMEs – the new target for cyber crime

The benefits of operating in an online world present many opportunities for small businesses however it also opens up a host of cyber risks. Many SMEs hold the belief that they are too small to be attacked and that their sector would not be of interest to a cyber-criminal. Unfortunately, SMEs are as much at risk from cyber threats as large organizations. Criminals recognise that SMEs hold significant amounts of valuable data and are unlikely to be protected by sophisticated network security frameworks backed up by multimillion-pound budgets.

The cost to launch cyber attacks is negligible and small firms are just as likely as large ones to be targeted by criminals by way of ransomware, malware and phishing. Attacks on high profile organizations may make the headlines but they are not the most obvious and easy target. Unfortunately, many small businesses are making the task easier for criminals by underestimating the threat. In a recently published report, almost two-fifths (38%) of IT leaders say that they simply do not have the time needed to fully understand cyber-security threats to the business, which according to a recent report rose to 51%[vi] of financial services firms.

Untargeted attacks, where hackers have no specific vertical, business or person they are attacking, are far more common than a targeted attack simply because they are easier to execute. Instead of trying to determine how to infiltrate a specific system, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet. The most common technique is phishing, where attackers create a generic email with malicious content such as an attachment or link. From there, they will send it out to every email address they have access to requesting sensitive information, such as bank details or encouraging recipients to visit a fake, but very convincing, website.

On average the proportion of small and medium firms that have experienced an attack has increased 59% in the last 12 months.

Source: *Hiscox Cyber Readiness Report 2019*

Two-fifths (38%) of SME respondents say their business is too small to be targeted by cybercriminals

Source: *Webroot, Size does matter report, 2019*

Friday afternoon fraud – an example of a phishing scam

The Solicitors Regulation Authority (SRA) Risk Outlook 2017/2018 [vii] in the UK revealed that from the first quarter of 2016 to the end of the first quarter of 2017, solicitors reported over £12m of client money stolen by cyber criminals. A total of 80% of all cyber crime reports to the SRA in the second quarter of 2018 were related to email modification fraud, where criminals intercept and falsify emails between a client and firm leading to bank details being changed and money being lost. When used to steal conveyancing money it is also known as 'Friday afternoon fraud', as many of these transactions take place on Friday afternoons.

The consequences of a data breach can be calamitous to SMEs which is why cyber-security should be a fundamental component of business operations. The repercussions of a breach extend far beyond the costs that are easiest to calculate, such as incident response, external technical services and communications and fines from the Information Commissioner's Office (ICO). The indirect financial cost can be harder to calculate and remediate such as lost business stemming from the erosion of customer and supplier trust and damage to brand reputation.

Approximately 80% of law firms reported phishing attempts in the last year.

Source: *UK Law Society Cyber Security poll, 2018*

Minimize Risk – 7 simple steps to cyber resilience

No business is too small to be attacked, however with the right approach to cyber-security no business is too small to protect itself. SMEs can pave the way to cyber resilience by following these top tips:

- Invest in effective firewalls, anti-virus and anti-malware solutions and ensure any updates and patches are applied regularly, ensuring that criminals cannot exploit old faults or systems. The National Cyber Security Centre advises updating software as soon as a new patch or update is available. Additionally, user passwords should be changed regularly and unused or end-of-life equipment disposed of securely
- Ensure business critical data, such as customer data and financial information, on all company assets is securely backed up and can be restored at speed
- Have simple, clear policies in place to create a cyber-conscious culture in the workplace and ensure it is communicated to all personnel so they are familiar with it
- Have regular awareness training so that personnel are constantly reminded of potential scams or tactics that can be used to trick them
- Review contracts and policies with suppliers to ensure they have an accredited standard for cyber-security for themselves and their partners to protect the supply chain
- Have an up-to-date incident response plan that is practiced regularly so that employees know what to do when they suspect there is an attempted breach or if an actual incident occurs
- Consider investing in cyber insurance to cover the exposure of data privacy and security. Accountancy firms should research insurance policies carefully to understand the level of coverage offered and their responsibilities to stay within the conditions of the policy.

Cyber resilience = Business resilience

The risk of an attack cannot be minimised, cyber criminals are business like in their approach, to them attacks are a low-risk, high-reward model. This particularly applies to SMEs and sectors such as accountancy and law firms where the criminal gains can be significant. A recent poll conducted by the UK Law Society showed that approximately 80%[viii] of firms have reported phishing attempts in the last year.

According to the 2018 Verizon Data Breach Investigations Report, 30%[ix] of phishing messages are opened by targeted users, and 12% of those users click on the malicious attachment or link. 85% of organizations have suffered from phishing attacks making it a lucrative criminal activity.

Although cyber security is cited as a high priority by numerous organizations, many are still trying to get the basics right. The FCA study found that a third of firms do not perform regular cyber assessments. Although most know where their data is, they describe it as a challenge to maintain that picture and nearly half of firms do not upgrade or retire old IT systems in time. More concerning is that only 56% say they can measure the effectiveness of their information asset controls.

Unless there is awareness of the potential risks then it is almost impossible to create a strategy for minimizing them. Increasingly we are seeing company boards requesting assurance on how a company is preparing for cyber breaches and how it will deal with the aftermath through agreed protocols. Part of a board's fiduciary responsibility is to identify and mitigate those risks that could impact the organization. Good cyber hygiene not only demonstrates good information governance; when performed properly it results in the protection of stakeholder assets and the potential mitigation of legal and compliance risks.

Certification provides a practical framework for an organization to assess its current cyber hygiene levels. In the UK, Cyber Essentials is a government and industry backed scheme to help all organizations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they set out basic technical controls for organizations to use which is annually assessed. In the US the National Institute Standards and Technology (NIST) framework guides organizations through complex, emerging safety procedures and protocols.

48% of SMEs report that they have had to deprioritize activities that would grow their business to address cybersecurity challenges

Source: Webroot, Size does matter report, 2019

Don’t get caught out

Criminals are continually lowering technical barriers to entry, making crimeware-as-a-service available on the dark web. Webstresser, the online cybercrime market, has been used to launch approximately 4 million Distributed Denial of Service (DDoS) attacks around the world. The site offered its DDoS services from around €15 per month, allowing people to perform crippling attacks without the need for specialist knowledge.

The result is that the global current threat level is significant, being unprepared is no longer an option. Organizations need to get proactive in protecting their data and that of their customers – or risk the consequences. Cyber Essentials and NIST can help organizations implement strong, cyber security hygiene practices. Being fully Cyber Essentials compliant is said to mitigate 80%[x] of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking. It aims to provide businesses with a strong base from which to reduce the risk from these prevalent cyber-attacks. Typically 90% of breaches are the result of employees making errors in identifying or reacting to threats. By utilising an online information security management system (ISMS) that incorporates NIST and Cyber Essentials Plus, organizations can undertake certification, guided by a virtual online security officer (VOSO), as part of its wider cyber-security measures.

By creating a positive security culture, organizations of all sizes and sectors can build a truly resilient business. There is no silver bullet to solving cyber crime, it is a question of when, not if a firm will be a victim of a cyber attack. However, steps can be taken to minimise the risks. Security should not be seen as a hindrance but as a significant component of the overall culture of an organization and as a business enabler that can allow innovation by supporting modern working practices. Through people and processes working cohesively, organizations can react and respond to threats quickly, dealing with issues before they become an incident.

[i] https://www.scmagazineuk.com/third-parties-contribute-1000-increase-finance-sector-cyber-crimes/article/1589653
[ii] Hiscox Cyber Readiness Report 2019
[iii] Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
small-companies-cyber-attack-60%-out-of-business/
[iv] Accenture Insight Cyber Security Conundrum
[v] Webroot Size does matter report July 2019
[vi] https://www.sra.org.uk/risk/outlook/risk-outlook-2017-2018.page
[vii] https://www.lawsociety.org.uk/communities/the-city/articles/cybersecurity-biggest-threats-legal-sector/
[viii] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
[ix] https://www.ncsc.gov.uk/section/products-services/cyber-essentials
[x] https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organizations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

VOSO

VOSO is a simple to use web-based solution that incorporates a comprehensive range of features such as remote monitoring and secure configuration of all networked devices, asset mapping, vulnerability scanning and patching, dashboards to display compliance progress against selected standards including General Data Protection Regulation (GDPR) as well as online security training videos for continual staff training. VOSO mitigates the risk of law suits and regulatory fines and ensures employees are trained regularly and kept informed of the latest cyber security updates.

CySure

Contact Us:
United Kingdom
+44 (0)808 189 3226

Visit us online:
www.cysure.net