ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 February 2020

www.computerfraudandsecurity.com

The business benefits of cyber security for SMEs

Guy Lloyd

Guy Lloyd, CySure

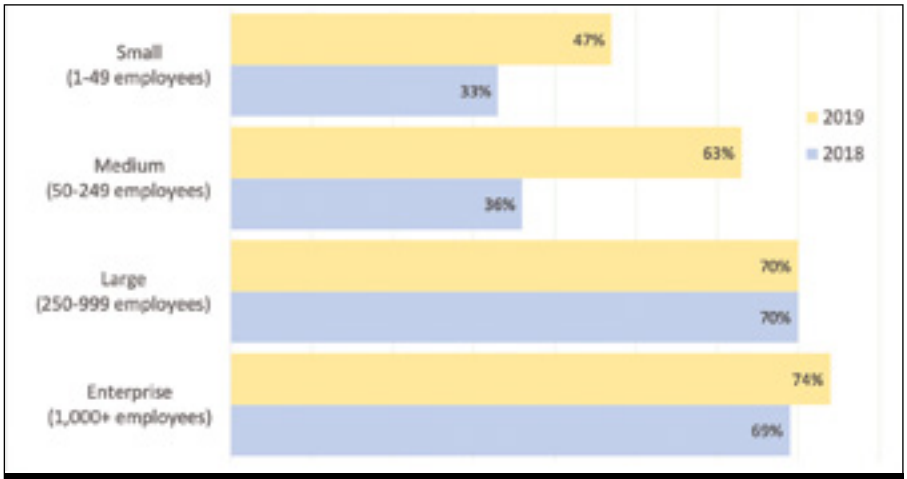
Cyber security is often discussed in terms of data breaches, regulatory fines and business disruption. The advantages are seldom highlighted. For example, effective cyber security makes it possible for companies to innovate and this drives revenue, profit and growth. Defending against cybercrime can deliver genuine benefits for small and medium-size enterprises (SMEs) and result in more valuable organisations.

The digital world presents many opportunities for SMEs, which can extend their reach further by operating online. Cyber security is essential if SMEs are to remain safe but it's not just about safety. As organisations of all sizes move towards driving efficiency through digitising processes, it's important for business leaders to redefine how they think about cyber security.

Not exempt

A 2019 survey from insurers Hiscox reveals that 55% of British businesses faced an attack in 2019, up from 40% in 2018[1]. When it comes to cybercrime, small and medium-size businesses are not exempt from the disruption that impacts large organisations. If anything, their size can make them more vulnerable as they are perceived as a softer target.

That isn't to say that SMEs are unaware of cyber risks, according to the 'Cyber Security Breaches Survey 2019': 78% now see cyber security as a high priority.[2] However, this raised awareness has not translated into action, with the survey reporting that only 15% of small businesses have a formal cyber incident management process.



Proportions of organisations worldwide targeted by cyber attacks over a one-year period. Source: Hiscox.

Many assume the main purposes of cyber security are to reduce risk, prevent data breaches and mitigate threats posed by viruses and hackers. However, to realise the full potential that cyber security can deliver, business leaders need to reposition it as a growth enabler.

Harnessing established technologies such as the web, mobile and cloud can help companies gain a decisive advantage. Effective cyber security provides SMEs with the ability to create, innovate and personalise product offerings that can deliver substantial market opportunity and business growth. So let's look at three benefits of having a robust cyber security and compliance programme.

Retain customers and show commitment

One of the most important factors in company growth is customer retention, as losing customers drags down growth.

Behind every data breach is a consumer, employee, business partner or supplier that has to deal with the fallout – not to mention the reputational risk that it places on the organisation involved. Would you want to do business with a company that is careless with your personal details?

Creating a culture of prioritising data security and data privacy demonstrates a high level of corporate social responsibility. It also makes financial sense. Converting prospects to customers is costly and losing a loyal customer or business partner is even more so. Demonstrating commitment to security and privacy provides assurance that yours is a trusted organisation to do business with.

Lucrative supply chain contracts

Large organisations rely on a network of SMEs. If they operate within the EU they are subject to the EU General Data Protection Regulation (GDPR). Under the GDPR, data controllers (those that collect the data) are responsible for their own compliance as well as that of any third-party processors.

Lax compliance in implementing regulations has in fact created a unique opportunity for those SMEs that make the effort to invest in cyber security. With so many damaging data breaches, large organisations are closely examining the security practices of any potential third party and seeking agreement with partners to ensure that secure systems are in place. It is the responsibility of the data controller to ensure that third parties within its supply chain take appropriate technical and organisational measures equal to their own.

The UK Government-backed framework Cyber Essentials Plus provides SMEs with a way to demonstrate their security credentials. By gaining Cyber Essentials Plus certification, SMEs are able to demonstrate that their cyber security has been verified and audited by independent experts. Auditable proof is often requested during tender bids as part of the warrants and liabilities process. Being Cyber Essentials Plus certified can leapfrog a business ahead of the competition.

"With so many damaging data breaches, large organisations are closely examining the security practices of any potential third party"

Supply chains are only as strong as their weakest link and therefore require standardisation in terms of security across the whole chain. SMEs able to prove their cyber security credentials can differentiate themselves from the crowd and maximise on lucrative business opportunities. Some 65% of UK small businesses have no plans in place to deal with potential supply chain disruption, including cybercrime.[3,4] Ensure your company isn't one of them by staying ahead of the game – don't lose business due to supply chain weaknesses.

Capitalise on risk

The business landscape is constantly evolving, with technology and regulation changing how business is conducted. With change comes risk but it also presents opportunity. SMEs that identify, analyse and evaluate risk are better prepared to weather a storm and select the appropriate cyber security controls.

With effective measures in place, organisations can capitalise on risk and carve out opportunity. Customers are more willing to subscribe to marketing updates if they know how their data will be used and secured. SMEs who fail to invest in data security and governance will miss the chance to seize that marketing opportunity. Instead they face relegation to the sidelines, watching their competitors leap ahead.

Innovation not stagnation

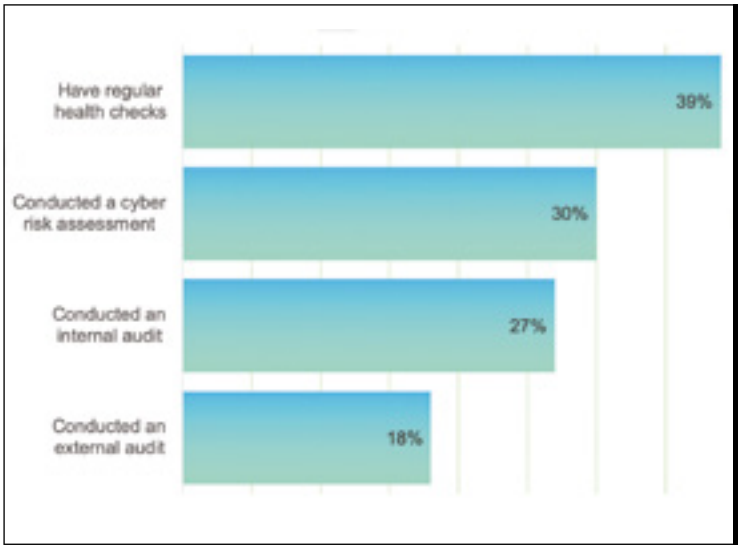
Cyber security is now a growing business priority and can no longer be considered merely as a cost of doing business. The frequency of security threats and breaches means that businesses with credible cyber security defences have a competitive advantage in their respective market. When cyber security is relegated to the back burner, it can become a growth inhibitor.

In a study conducted by Cisco, 71% of executives said concerns over cyber security had impeded innovation at their companies.[5] Among respondents, 39% said they had halted mission-critical initiatives due to cyber security issues. These responses highlight how cyber security weakness impedes the ability of companies to innovate at precisely the time they need to do so to compete.

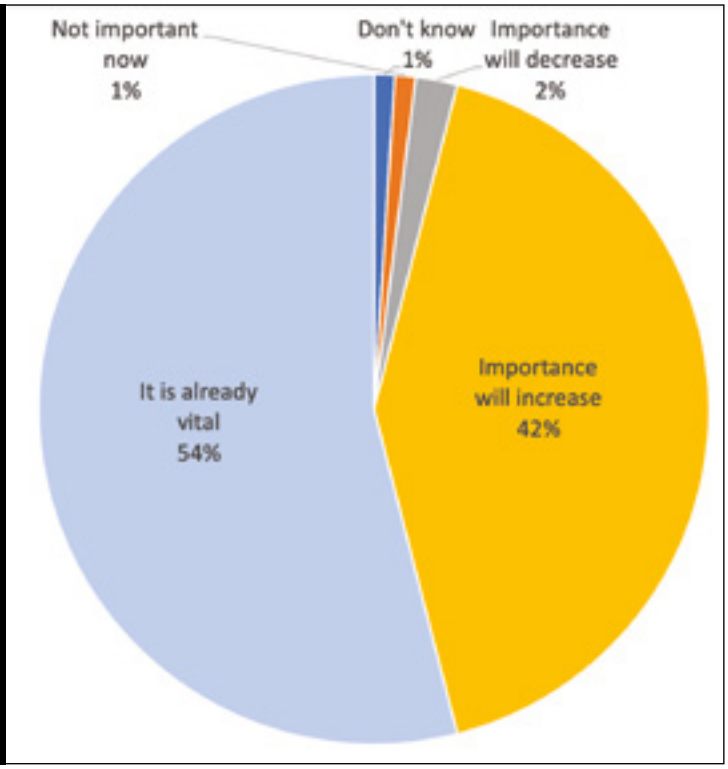
Organisations that turn cyber security excellence into true competitive advantage can innovate faster. This in turn helps them to respond faster to rapidly changing markets, making them more effective and improving financial performance. Cyber security excellence also gives organisations the opportunity to differentiate themselves as a brand that customers can trust.

Agile and resilient

According to the Business Population Estimates conducted by the UK Government, small and medium-size businesses make up 99.9% of all private sector businesses in the UK and employ 16.1 million people, or 60% of the country's private employment.[6] However, almost half (43%) of UK SMEs admit



The UK Government's 'Cyber Security 2019' found that 62% of small businesses had taken action to identify cyber risks in the preceding 12 months. The actions included the four activities listed here. Source: Department for Digital, Culture, Media & Sport.



The importance that organisations believe cyber security audits will have on merger and acquisition activity in the next two years. Source: (ISC)[2].

to having no business continuity, disaster recovery or crisis management plans in place, despite almost the same number of UK businesses (46%) suffering at least one cyber security breach or attack.

Smaller organisations are by nature agile and innovative, harnessing the power of technology and the Internet to reach their customer base: however this also increases the attack surface. The path to becoming cyber resilient can be daunting but it is not insurmountable. Demonstrating responsible business practice means being prepared for anything. Developing a cyber resilience stance based on following a few simple steps will enable SMEs to not just survive but thrive in the new digital world.

Cyber-ready culture

SMEs must be able to function safely in the online world if they are to exploit the potential opportunities. An effective cyber security strategy with the right risk management provides the springboard to innovate, differentiate and ultimately deliver revenue growth. The importance of good cyber security can sometimes be lost in translation when the emphasis is purely on the expense. Rather than cost, the focus should be on the business benefits of a robust security posture and the opportunity for growth.

A recent report revealed that 96% of respondents indicated that cyber security readiness factors into the calculation when assessing the overall monetary value of a potential acquisition target.[7] The Hiscox survey reported that 83% of respondent organisations feel there is industry pressure to display good cyber security. More than three-quarters (76%) believe that having a cyber secure brand is important for competitive advantages.

Whether long-term goals are to sell the company or seek investment to grow, business leaders can't ignore the benefits of cyber readiness. Ultimately, organisations that can make the leap from cyber security as a protective measure, to its being a strategic value driver will prosper. The rewards include being able to command greater public trust, loyalty and market growth opportunities by leveraging a reputation for security readiness. An organisation that is aware of the potential risks and how to mitigate them has its house in order.

Minimise risk: seven 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 tips:

- Invest in effective firewalls, antivirus and anti-malware solutions and ensure that any updates and patches are applied regularly, so that criminals cannot exploit old faults or systems. The National Cyber Security Centre (NCSC) 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 that 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 tacticsthat 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 practised 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. Companies should research insurance policies carefully to understand the level of coverage offered and their responsibilities to stay within the policy conditions.

References

1. 'Hiscox Cyber Readiness Report 2019'. Hiscox. Accessed Jan 2020. www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.pdf.
2. 'Cyber Security Breaches Survey 2019'. Department for Digital, Culture, Media & Sport, UK Government, 3 Apr 2019. Accessed Jan 2020. www.gov.uk/government/ statistics/cyber security-breachessurvey-2019.
3. 'Majority of small businesses unprepared for business interruption'. Federation of Small Business, 19 Jun 2018. Accessed Jan 2020. https://firstvoice.fsb.org.uk firstvoice/majority-of-small-businessesun prepared-for-business-interruption.
4. Rajab, Talal; Patefield, Dan. 'Protecting SMEs from business and supply chain disruption'. TechUK, 22 Jun 2018. Accessed Jan 2020. www.techuk.org/insights/news/item/13380-protecting-smesfrom-business-and-supply-chaindisruption.
5. 'Cyber security as a growth advantage'. Cisco. Accessed Jan 2020. https://discover.cisco.com/en/us/security/whitepaper/cyber security.
6. 'Business population estimates for the UK and regions 2017'. Department for Business, Energy & Industrial Strategy, UK Government, 30 Nov 2017. Accessed Jan 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/ file/663235/bpe_2017_statistical_release.pdf.
7. 'Cyber security assessments inmergers and acquisitions'. (ISC)2. Accessed Jan 2020. www.isc2.org/Research/The-ROI-of-Sound-Cybersecurity-Programs.

About the author

Guy Lloyd is a director at cyber security company CySure (www.cysure.net), which offers a cyber compliance management solution. He is a software engineering graduate who originally worked in software development before moving into commercial roles at IBM in the US, Zurich, Prague and London. Lloyd's passion for cyber security and risk began when he worked at Juniper Networks and since joining CySure in 2019 he has helped build a channel strategy. He chairs the Advisory Board at the Association of Professional Sales.

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and 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.

Contact Us:

United Kingdom
+44 (0)808 189 3226

Visit us online:
www.cysure.net