Mind the Gap: a lack of cyber security skills is leaving SMEs exposed

Submitted by: PR Artistry Limited
Monday, 12 December 2022

Nick Denning, CEO Policy Monitor, looks at the risks and business impacts of shocking statistics showing a lack of basic security skills within UK SMEs.

Almost half of UK businesses have a basic cyber security gap that is leaving them exposed. This stark reality was revealed in a report from the Department for Digital, Culture, Media and Sport (DCMS)(i). It found that the people responsible for cyber security in 48% of UK businesses lack the confidence to carry out basic tasks and are not receiving support from external cyber security providers. So, if your inhouse person isn't confident in doing basic security tasks and you're not seeking support, just who is checking that your business systems are secure, and your data hasn't been compromised?

Size does matter

Many SMEs are unprepared for the cybersecurity threats lurking online, believing they are too small to be a target. The reality is that almost half of UK businesses suffered a cyber security breach or attack in 2019/2020 (ii). Most cyber criminals are looking for a quick payday. If an attack has worked well, they will keep repeating it. That is why phishing scams, where attackers send fraudulent messages to trick a person into revealing sensitive data, remain the most common type of attack that organisations face, with 90% of all data breaches involving phishing(iii).

SMEs need to understand that cybercrime is an organised and profitable business, albeit an illegal and morally bankrupt one. Cyber criminals want a swift financial return on their activities and purposely go after soft targets. SMEs are seen as easy victims because they are less likely to have sufficient security in place to protect their systems and data. Hackers are after the information that SMEs store on their customers and suppliers, such as credit card numbers, bank account details etc. They will either use this themselves or sell it on the dark web to the highest bidder.

Credit card, identity and cyber fraud is costing the UK up to £190bn a year (iv). According to UK think tank the Royal United Services Institute (RUSI), fraud has reached epidemic levels and should be seen as a national security issue. While the profits keep rolling in, cybercriminals will continue their attacks and the sooner SMEs understand this, the sooner they can get serious about security and start protecting themselves more effectively.

The most common cyber security skills gaps identified in the report are in:

- Configuring firewalls
- Performing patching
- Storing or transferring personal data
- Detecting and removing malware.

Help is at hand - build secure foundations with Cyber Essentials

Cyber security tasks are laid out in the government-endorsed Cyber Essentials (CE) scheme which was designed to help protect UK organisations from the most common cyber threats. These fundamental tasks are the foundation to good security.

The scheme sets out basic technical controls for organisations to use. It also lays the foundation to developing policies and procedures to mitigate against threats that can impact business operations. The benefit to being CE compliant is that it mitigates 80% of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking.

Where to start?
Taking the first steps in tackling cyber security can be daunting but the ramifications of not doing so can be devastating to your business. Cyber-attacks and data breaches are often financially crippling for SMEs to resolve. In addition to remediation costs there is also the loss of customers, suppliers and business reputation, plus fines for breaching GDPR data protection rules.

A good place to start is by using an online policy management system that is designed for cyber security which will take you step by step through all the important security workflows. It will guide you through the activities to take, highlight the business areas to focus on and embed GDPR and Cyber Essentials principles so you can achieve certification.

No company can afford to be naïve about cybercrime and the importance of protecting data, the fall out is too great. A cyber security policy manager solution can remove the complexity and guide your company to become Cyber Essentials-certified in a cost-effective way. Being certified with a creditable scheme will bolster cyber defences, put in place policies to ensure you are taking the correct steps to protect your confidential data, and go a long way in protecting your business against common attacks. Use the help available to stop your company becoming a victim of cybercrime and adding to the depressing cyber security statistics.
Nick Denning – CEO, Policy Monitor

About Policy Monitor

Policy Monitor is a cyber security company founded by experts with extensive experience in operational and risk management. The company is based in London (UK). Policy Monitor’s flagship solution Cyber Security Policy Manager (CSPM) is a policy management system that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

For more information, please visit: https://policymonitor.co.uk/
Press contact: Mary Phillips
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk

(i) Cyber-security-skills-in-the-uk-labour-market-2020
(https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020)
(ii) Cyber-security-breaches-survey-2020
gov.uk

(https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020)
(iii)enterprise.verizon.com (https://enterprise.verizon.com/resources/reports/data-breach-digest/)
(iv) rusi.org
(https://rusi.org/publication/occasional-papers/silent-threat-impact-fraud-uk-national-security)