Cybersecurity: a blind spot for SMEs

TRRI news

Published 21-Feb-2025 by Dominic Holden, Lawrence Stephens

In an age where people are ever more reliant on digital communication and storage, cybersecurity has never been more important for businesses.

For many smaller organisations, protecting themselves from the increasingly sophisticated threats posed by bad actors can be overwhelming. In many cases, these businesses are choosing to do very little to protect themselves, hoping that they will not appear on a hacker's radar. The fallout from this inertia is potentially catastrophic for the UK economy.

The Association of British Insurers (ABI), in partnership with Grant Thornton, last month produced a report titled "Cyber Resilience for SMEs: The Insurance Gap Explored," calling for small and medium enterprises (SMEs) to take out insurance products to protect themselves from cyber threats.

The reasoning is clear to see. SMEs typically have a turnover of up to £36 million and no more than 250 employees. They make up 99.9% of all businesses in the UK, contributing £2.6 trillion to the UK economy. Only 10% to 15% of SMEs are estimated to have cyber protection. Cyber threats, including phishing, malware and ransomware attacks, can cause irremediable harm to businesses.

Far-reaching implications

A survey in 2024 by the Department for Science, Innovation and Technology found that 50% of UK businesses suffered some form of cybersecurity breach or attack, costing SMEs between £5,000 to £250,000 to address.

Many SMEs exist on a financial knife edge, and the business interruption, claims, fines and reputational damage that often follow a cyberattack can be the final event pushing these companies into insolvency. This can ruin decades of work and leave customers and suppliers in the lurch. Around 60% of small businesses suffering a successful cyberattack go out of business within six months. Brushing cybersecurity under the carpet, hoping it will not affect business, is an extremely risky strategy.

The ABI's report (although welcome) and others like it will unfortunately drive the threat further. They signal to hackers, fraudsters and cyber criminals that SMEs are less likely to be protected against cyberattacks than their insured, larger peers, making SMEs prime targets for future attacks.

Aside from the obvious threat to SMEs, the implications of such attacks can be far-reaching. The corporate world is an ecosystem, with SMEs providing critical services to larger organisations through the supply chain. A hacker who gains access to or control over an SME's system can dupe a larger company into giving the hackers access to their business. The compromised SME becomes the weak link in a larger, more significant chain.

The damage can cost billions to remedy. For example, consider the recent Crowdstrike attack, which cost the UK economy an estimated £1.7 billion to £2.3 billion. It is little wonder that insolvency becomes such a frequent byproduct.

Cyber insurance and cybersecurity policies

In the face of such threats, insurance can provide SMEs with some peace of mind. Cyber insurance need not be expensive. Premiums for reasonable coverage have started to come down in recent months, and basic policies can be available for less than £100. SME policies with a fuller suite of services may encounter significantly higher cyber insurance costs.

A cyber insurance policy will give the SME a fighting chance to get the help they need to hire and pay for experts who can move quickly to identify the type of attack and respond accordingly. This can prevent days or weeks of interruption and better arm the SME to manage the consequences without burning through their cash and credit reserves.

Aside from cyber insurance policies, there are several relatively straightforward and cost-effective methods for dramatically reducing the likelihood of falling victim to an attack.

Training staff on identifying phishing emails and other common attacks can be particularly effective alongside a strong information technology team that establishes basic monitoring and protective software. Using two-factor authentication and strong passwords are easy safeguards that are often overlooked.

As part of its report, the ABI makes several recommendations to encourage greater uptake of cyber protection products among SMEs, including: driving awareness through campaigns to help address poor understanding of cyber threats, and the use of clearer and consistent language and terminology to boost understanding and increase uptake of cyber insurance.

Governmental support

Given the harm cyberattacks are already causing to the UK economy and the considerable further damage likely to come, mitigating such risk cannot rest solely on cash-strapped SMEs; the government must also take responsibility.

Public support could take the form of tax breaks for SMEs, such as an insurance premium tax waiver/reduction, to incentivise cyber insurance. More controversially, given the seriousness of the threat and its contagion effect, the government should also consider making it mandatory for SMEs to have cyber insurance in place.

As long as SMEs are playing catch-up with cybersecurity, their systems will remain vulnerable to the exploits of hackers and other bad actors. While cyber insurance can offer valuable peace of mind, proactive compliance and cybersecurity policies will always be the most effective way to safeguard businesses.

Failure to implement such policies or acquire effective cyber insurance can have wide-reaching implications for businesses and the broader corporate ecosystem.

(Dominic Holden, Lawrence Stephens)