Despite major cyberattacks, businesses have been slow to react

blogs.lse.ac.uk/businessreview/2017/05/12/despite-major-cyberattacks-businesses-have-been-slow-to-react/

5/12/2017

If you think you know cybercrime, think again. The modern-day scammer isn't averse to changing the rules of play and, increasingly, businesses of all shapes and sizes are finding themselves exposed.

In the past year, more than half (57 per cent) of businesses surveyed in The Hiscox Cyber Readiness Report 2017 said they experienced an attack. Two in five (42 per cent) had at least two incidents in the same period, and just over 10 per cent experienced five or more cyber security breaches. The threat is clearly growing and finding new weaknesses to exploit.

In fact, the most commonly perceived challenge that businesses face in cyber security is the evolving nature of threats. Just last year, when hackers directly interfered with the US presidential election, it was clear cybercrime had entered a new era. The threat of digital attacks had reached a disturbing maturity that businesses, government bodies and presidential candidates were unable to confront.

Given the growing complexity of cybercrime, we wanted to shine a light on how vulnerable businesses are.

A digital attitude

Despite widespread publicity around major security breaches, a number of businesses have been relatively slow to react. They also display attitudes towards cyber security that seem worryingly optimistic given the severity of the threat they face.

'Not relevant' – Many businesses seem to believe they're too small, too niche or too traditional to become a target, and don't protect themselves accordingly. The cyber readiness survey found that 26 per cent of firms had no plans to take out cyber insurance and it's UK firms that are the most likely to think it's not relevant for them. It's understandable that smaller businesses might find the plight of Ashley Madison, Yahoo and AT&T a little unrelatable, but despite appearances cybercrime doesn't discriminate – and smaller businesses potentially have just as much to lose from an attack.

Not reactive – Incredibly, even when disaster strikes, a large proportion of businesses don't react quickly enough. Over a third of those surveyed in the UK admitted they'd changed nothing following a security incident in the past 12 months. Complacency is an even bigger issue among smaller businesses, with 29 per cent revealing they hadn't made any changes since their breach. Putting a defined cyber security strategy in place also seems to be on the backburner for some businesses. While 91 per cent of businesses considered "experts" by the cyber readiness report had a strategy in place, just 66 per cent of "novices" could say the same.

Not interested – Even with the 2016 revival of industrial-sized security breaches, businesses in Europe are still shrugging off the threat. Over a third of German firms told us they're not interested in protecting their business with cyber insurance, which is more than twice the figure (15 per cent) of the US.

There also appears to be a lack of top-level executive involvement in prioritising cyber security – something that businesses with an "expert" level of cyber readiness tend to have, according to the report. However, only 62 per cent of businesses considered "novices" said they had made executive level buy-in a top priority.

When the threat of cybercrime is evolving daily, disinterest – and disengagement from – online security can be a damaging attitude to have.

The ripple effect of poor cyber security

As well as a relaxed attitude to implementing security measures, our report also found businesses are less prepared than they should be to deal with the aftermath of an attack.

Much of the problem is that **businesses are unaware of what's happening.** In the past 12 months, while it took less than 24 hours for three in five businesses (62 per cent) to become aware of their biggest attack, 37 per cent of the businesses we surveyed said it took them two days or more to discover the problem.

Another stark finding from the report was that when a business comes under attack, **getting back to "business as usual" takes time**. Just under half (46 per cent) of businesses said it took them two days or more to return to normal. Only 45 per cent of UK firms said they managed to resolve their attack within one day, and 29 per cent of IT teams in the US were still recovering for four or more days after an incident.

The tyranny of a cyber-attack can also persist long after the initial blow, as **costs continue to rise** from damage to parts of the business not immediately affected by the breach. One in ten businesses that experienced a breach in the last 12 months revealed they'd lost customers or experienced increased difficulty in attracting new ones because of their attack. In the US, this figure rose to almost one in six (15 per cent).

Recovering from a breach is costly for any company but **the impact can be huge** for smaller businesses. While it's the big company breaches with their massive clean-up costs that make the headlines, the financial impact of cyber-attacks is disproportionately high for the smallest companies. In the UK, the cost of a breach for these businesses is around 41 per cent of the cost experienced by the largest firms, despite operating on a much smaller scale.

Becoming a more proactive digital community

While there's been a slow start in responding to cyber security, businesses are planning to adapt their digital behaviour. As the report reveals, progress for many firms is happening in three key areas.

New kit: 59 per cent of cyber security budgets are reported to be rising in the next 12 months, with one in five firms (21 per cent) increasing their budgets by a double-digit figure.

New people: In the year ahead, almost half of businesses (47 per cent) say they intend to increase their spending on cyber security staffing by at least 5 per cent.

Better training: Almost three in five (59 per cent) firms claim they are going to increase their spending on cyber security training for staff by 5 per cent or more in the coming year.

For many, improving security measures is an immediate necessity and in the greater campaign for cyber awareness, all businesses have their part to play. So, whether it's unsolicited spam, sabotaged software or the next generation of cyber threats on the horizon, the business community needs to be shrewd enough to clamp down on the risks that threaten the way they do business.

♣♣♣

Notes:

- *The post gives the views of its author, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Computer data hacker, by Blogtrepreneur, under a CC-BY-2.0 licence*
- *Before commenting, please read our* Comment Policy.

Steve Langan is CEO of the Hiscox Insurance Company, which he joined in October 2005 after a global career in blue chip fast-moving consumer group companies. He is responsible for Hiscox's retail product lines across the UK.