The EU's data protection regulation will be a wake up call for companies' cyber security

As businesses, we're more vulnerable than ever. Whether you're a private or public sector organisation, there is now an even chance that in any 12-month period, you'll experience at least one cyber incident. Which means for those who haven't had a potential threat on their radar to date, what you're experiencing is merely the luck of an extremely narrow draw. And no business should balance its future on those odds. What's more, two thirds (66 per cent) of businesspeople now see cyber threats and fraud as equal foes in the battleground of top business risks. And as more personal data is moved online, the margin of exposure to both is increased.

Some businesses are still asleep to the threat

We know from our recent report that in terms of their priorities, preparing for a cyber crisis currently falls just outside the top ten security initiatives for 43 per cent of organisations. As startling as that sounds, the reasons for this lack of urgency could be fairly simple.

Larger firms are still the main target for hackers, and perhaps this is the reassurance smaller businesses continue to depend on to rationalise putting off their commitment to a comprehensive cyber security plan. However, when over 20 per cent of smaller businesses (one to 19 employees) now report at least one cyber incident a year – and those are the attacks they know about – it's becoming an increasingly precarious fall-back position.

Or, if it's the lack of tangible consequences arising from a 'lucky escape' from cyber-attacks which cause some businesses to drag their heels, then the arrival of new data security regulations may force their hand. When the EU's General Data Protection Regulation (GDPR) kicks-in in May, no business can be left (or lag) behind. Where data security is concerned, what was best practice is now the new bare minimum, and every business must review and update its processes to ensure personal data is protected, particularly in the event of a cyber breach.

The regulations bring with them hefty fines for non-compliers – up to €20 million (£17.6 million, with the Euro pound exchange rate as of February 2018 according to xe.com) or 4 per cent of global turnover – which may serve to convince the remaining cyber security latecomers of just some of the risks they face and the need to act now.

While a more advanced mindset is emerging

Among those businesses actively engaged with reforming their cyber security, there's a new mindset emerging. One that's not just concerned with fortifying internal defences but is also outward looking, and focuses on scouting for potential threats.

Date originally posted: 2018-04-23

Permalink: http://blogs.lse.ac.uk/businessreview/2018/04/23/the-eus-data-protection-regulation-will-be-a-wake-up-call-for-companies-cyber-security/

Blog homepage: http://blogs.lse.ac.uk/businessreview/

This mindset leads to a number of key activities: defining a clear strategy for a security breach, engaging in staff training and awareness, and testing environments to see if staff are switched on to threats. It also encompasses the use of a 'scan and search' approach. Businesses achieve this by using applications that monitor web traffic for potential threats to ensure that they are not just ready for an attack, but on the look-out for one. It's this approach to suspicious activity on a network that can prevent a cybercrime occurring at all.

When asked what changes they'd made as a result of an attack in the last 12 months, employing these prevention and detection technologies were at the top of the list of changes. As the foremost activity following an attack, 13 per cent of respondents had implemented this proactive technology, and 9 per cent had increased their spend on threat intelligence capabilities.

But there's a false sense of security among would-be experts

There's no doubt that channelling money into cyber security technology has its merits. In fact, the use of security-based technology is where most people in our survey ranked highest in terms of readiness – and this could be the reason why over half of businesses feel 'very confident' they're prepared for an attack. But despite this preparation and obvious confidence, nearly three quarters (73 per cent) of people surveyed were still deemed to be cyber novices. And given the increasing scope of cyber threats to detect network weaknesses, an over-confidence in, and over-*reliance* on, technology is a worrying prospect.

In this environment, bulking up one line of defence, while ignoring broader security obligations, leaves a firm potentially more exposed than lower-spending, but more lateral-thinking, businesses. In fact, while cyber experts *do* typically spend a significantly higher proportion of their IT budget on cyber defence than the novices, what really sets them apart is how they distribute that budget. Cyber experts, by definition, are more likely than novices to invest in employee training, to allocate security executives and dedicated support teams to their ongoing cyber strategy, and to test their defences for vulnerabilities.

It's this fully formed and proactive approach that will prove essential in combatting cyberattacks, rather than any specific amount of money being spent. Because, as many high profile businesses have come to realise, a cyber strategy is only as effective as its weakest point.

♣♣♣

Notes:

- *This blog post draws on the Hiscox Cyber Readiness Report 2018.*
- *The post gives the views of its authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Hacking, by iAmMrRob, under a CC0 licence*
- *When you leave a comment, you're agreeing to our Comment Policy.*

Gareth Wharton leads the Cyber virtual Business Unit (vBU) of Hiscox, covering areas such as product development, value add services offerings, pricing and branding & marketing. Gareth is a regular speaker on Cyber risks. Previous to this role he was Hiscox chief technology officer, leading the IT strategy and architecture teams, where he was responsible for driving a cloud-first approach, and re-architecting one of the core underwriting platforms to Azure as well as providing DevOps leadership across the wider IT team. Prior to this, Gareth ran the company's infrastructure services division. Before joining Hiscox, Gareth worked in a number of financial services companies, including nine years at Aon in various IT roles.

Date originally posted: 2018-04-23

Permalink: http://blogs.lse.ac.uk/businessreview/2018/04/23/the-eus-data-protection-regulation-will-be-a-wake-up-call-for-companies-cyber-security/

Blog homepage: http://blogs.lse.ac.uk/businessreview/