The world has changed… time to take stock and simplify your cyber security

Author: Jim Fox

Capita

Jim Fox CISM I MBCS I MSyI

Cyber Security Consultant

james.fox2@capita.com

Jim is a Capita cyber security consultant providing advice on cyber governance, risk and compliance. A former police officer, he has 20+ years' experience in critical incident management; contingency & exercise planning and delivery; and cyber response/recovery planning. He is a Certified Information Security Manager (CISM), Certified Red Team Thinker and holds professional membership of the British Computer Society (MBCS); ISACA; the Security Institute (MSyI); Institute of Strategic Risk Management (M.ISRM); and an Affiliate of the Chartered Institute of Information Security (CiiSEC).

It may only be 2022, but in this decade the world is already proving to be a very different place to the decade before. The coronavirus pandemic has changed ways of working for good, and now the rising cost of living and the war in Ukraine is impacting people's lives, supply chains and the wider geopolitical landscape. The shocking and tragic consequences of these world events are well-known, but they also represent critical challenges for businesses when it comes to cyber security.

The Department for Digital, Culture, Media & Sport (DCMS) recently published its **Cyber Security Breaches Survey 2022** in which it found that within the last 12 months 39% of UK businesses had identified they had been victim of a cyber-attack, this was broadly consistent with the previous year however the danger is that companies that do not have sufficiently mature monitoring and detection technology in place are less likely to be able to detect an attack, meaning the actual figure in the UK could be far higher.

Of the 39% of UK businesses that did identify an attack, the most common threat was phishing attempts (83%) followed by more sophisticated attacks such as a denial of service, malware, or ransomware (21%). With high profile attacks and the continued rise in ransomware and data breaches, cyber security is rightly being recognised in boardrooms. However, with the risks that exist today, more needs to be done.

Don't let your pandemic response become your permanent response

At the beginning of the coronavirus pandemic businesses quickly pivoted to enable their employees to work from home. This agile way of working ensured that they could continue to operate and serve their customers while protecting their staff. But the sudden change to working from home meant that many businesses opted for quick 'sticking plaster' approaches to cyber security. Now that the 'new normal' is our permanent normal, it's time for businesses to take stock and simplify their cyber security practices.

We have seen that many businesses have a range of cyber-security solutions from multiple suppliers. This increased attack surface (and indeed vectors for compromise) can cause them to be vulnerable to attack due to how the different solutions are (or are not) connected. Simply bolting on more solutions does not naturally lead to greater protection. If your business is in this position, it's important to audit your current state and reassess your risks when it comes to information technology (IT), operational technology (OT) people, and processes.

Permanent hybrid operations present different risks to having all staff in the office. When employees are at home, they may be more vulnerable to phishing attacks, they don't have the safety net of being able to check with those around them. And those who handle data may act differently at home than when in the office (for example a disgruntled employee may be able to take screenshots of data more freely than they would in the office) That's why cyber security policies that were written before the pandemic will now be out of date and it is important to look again at your cyber risks and ensure that you have a culture of continual review.

Cyber incident response plans must go hand-in-hand with business continuity plans and consider scenarios such as what needs to happen if the business is subject to a ransomware attack and suddenly everyone working from home is unable to log in. Also ask yourself what activities you can undertake to keep cashflow moving through the business. Much can be learned from how businesses responded during the pandemic, but the focus should now be on different scenarios that are considered with just as much seriousness and dedication.

Prioritise upskilling and reskilling to fill the growing skills gap

Protecting businesses from cyber threats and vulnerabilities needs skilled people, but finding these people is already proving to be difficult across all industries. The government's **Cyber security skills in the UK labour market 2021 report** showed that 50% of UK business have a basic cyber security skills gap and do not have enough staff who can confidently store or transfer personal data, set up configured firewalls, and detect and remove malware. A third of businesses say they have more advanced skills gaps in areas such as penetration testing, forensic analysis and security architecture.

The report also makes it clear that standard recruitment will not fill these gaps, as often cyber security is a role that people grow into, rather than having every desirable skill at the outset. That's why it's important that business look again at their recruitment strategy and place more value on upskilling and reskilling from within. There will be countless people within larger businesses who spend their leisure time gaming and coding but do not see that these interests could lead to a career in cyber security. That's why businesses need to free cyber security from just being the realm of IT professionals and look more widely across their organisation for people with skills and interests that could be developed.

All of this needs to be supported by cyber-savvy boards that understand that cyber security should be approached in the same way as health and safety within an organisation. It should be always present and weaved into regular training to ensure it is adopted as standard and considered in all decision making.

At Capita, we have extensive experience of auditing and advising our clients on all aspects of cyber security. Of course, we don't know how the current events at home and abroad are going to pan out, but what we can do is help our clients to ensure they are as prepared and resilient as they can be.

Capita