A CYBER INCIDENT IS INEVITABLE: IS YOUR ORGANISATION FULLY PREPARED?

As the cyber threat landscape continues to evolve, cybersecurity resilience becomes a critical priority for firms

Among much else, the Covid-19 pandemic will be remembered as a global turning point in both digitalisation and cybersecurity. According to the FTI Consulting Resilience Barometer ® Covid Edition, 80 per cent of G20 companies surveyed say they have accelerated the digitalisation of their business since the start of the pandemic. Sadly, the exponentially accelerating rate of change in digitalisation we are seeing has been accompanied by a broadening of the cybersecurity threat. An astonishing 75 per cent of organisations we surveyed said they had been negatively impacted by a cyber attack in the past year[1].

Some of the increase in cyber threat can be attributed to security vulnerabilities in newly and more widely deployed technologies coming on stream. But, as always in cybersecurity, much of the challenge is about the inherent vulnerabilities in us, the human users. This combination of societal confusion, uncertainty, and new ways of working in a distributed environment, enabled by technology, has made us all more psychologically susceptible to manipulative social engineering attacks.

With workforces now under temporary lockdown, or more permanently embracing a new way of working, it is more compelling than ever before that organisations consider afresh their cybersecurity. If cybersecurity wasn't already a strategic priority in the boardroom, the scope and impact of the audacious nation-state linked SolarWinds attack detected late last year should help ensure it is now. Some 45 per cent of the companies we surveyed have seen cybersecurity climb up the board's agenda as a result of Covid-19[2].

Cyber threat actors are not bound by laws, regulation, nor geographical boundaries. And no industry or organisation is safe. Cyber attacks increasingly cause major disruption for organisations' revenue and operations, while reputational damage can prove fatal. One recent report estimated that the global annual potential value at risk from cyber breaches would reach as much as $5 trillion by 2024, up from $3 trillion where it is already today[3]. With the levels of cyber risk we're seeing, it is no exaggeration to say that the most successful organisations in the coming years will be those that prioritise building cybersecurity resilience. Before long, they (and their various stakeholders) will see cybersecurity as a source of competitive advantage, while less well-defended rivals are increasingly seen to be suffering negatively as their vulnerabilities bite deeper.

So, what should organisations like yours and your clients be doing to build cybersecurity resilience at a time like this?

Firstly, focus on getting the basics right. Most organisations have established policies and procedures for their security. But how closely are these policies being followed and updated? Every organisation should be reviewing and updating policies and procedures, ensuring they have a strong security posture, conducting security monitoring, training staff regularly (including on the use of VPNs and two-factor authentication wherever possible), patching software in a timely fashion, and providing clear messaging from leadership about the importance of cybersecurity.

Secondly, organisations should seek to re-identify and protect their 'crown jewels' – the critical assets, data, and systems without which the organisation cannot function. If cybersecurity resources are not focused on the crown jewels, then they are focused in the wrong place.

Thirdly, organisations must tighten their third-party management. Ultimately, businesses are only as secure as their suppliers, and most organisations underestimate their exposure, and the sheer volume of data they share with third parties on a daily basis. When organisations sign onboarding contracts, are they truly aware of the risk exposure? How confident are they in knowing where their data is right now?

In practice, resilience needs to be both practical and attitudinal. There is of course a range of concrete steps that organisations can – and should – take to improve their resilience, spanning people, process, and technology. But the broader objective must be to develop an organisation-wide mindset of cybersecurity: a culture of resilience. Such a mindset acknowledges that cybersecurity breaches are inevitable – a matter of when, not if. Are you confident that your organisation is fully prepared?

FTI CONSULTING™ | CYBERSECURITY

FTI Consulting, Cybersecurity, 200 Aldersgate St, London, EC1A
Web: fticybersecurity.com/thelawyer

[1] FTI Consulting Resilience Barometer ® COVID Edition

[2] FTI Consulting Resilience Barometer ® COVID Edition

[3] https://www.infosecurity-magazine.com/news/breach-costs-trillion/#:~:text=The%20cost%20of%20global%20data,new%20predictions%20from%20Juniper%20Research.