OliverWyman

CYBERSECURITY IS AN ORGANIZATION WIDE

Julian Granger-Bevan
Paul Mee
James Cummings
Tavor

and innovative, they have also made our personal data increasingly vulnerable to theft and attack.

The risk of cyber-attack has never been higher. The Global Risks Report 2022, published by the World Economic Forum in collaboration with Marsh McLennan ranked “cybersecurity

and Europe.[1] Among business leaders, 88% consider cybersecurity as a direct risk that will impact functions beyond technical IT teams.[2]

CYBER-ATTACKS WILL ONLY GROW IN SCALE

In late September 2022, an Australian telco disclosed that it was the subject of a major

of its c. 10 million customers. Among the sensitive information that was stolen were dates numbers.

While concrete information about how the attack occurred is yet to be revealed, the incident represents only the latest example in a worrying trend of rising cyber-attacks.

3

While attacks of public sector organizations remain high, research shows that bad actors are increasingly targeting private companies with deep pockets and vulnerable legacy systems.[4] It’s no surprise that incidents of ransomware have spiked by 435% in 2020, in tandem with the ongoing and rapid digitalization of modern business functions.[5] Globally, ransomware alone is estimated to cost potentially cost businesses US$30 billion in damages by 2023.[6]

The frequency and scale of these attacks are rapidly increasingly, as hackers move away from “spray-n n “s-12fspk dy3 anm s sis3sh9 (e)-9 (t)s.

to understand how a company's tarnished reputation could have a direct impact on customers.

action initiatives. These lawsuits are common in the US, where related spend topped [11]

happen.

CYBERSECURITY IS AN ORGANIZATION-WIDE ISSUE

As more of our key infrastructure and resources become digitalized, responsibility for cybersecurity within organizations must expand. This is especially the case given that demand for cybersecurity professionals has over time by far outpaced the capacity [12]

No single team should — or can — be the sole line of defence in an organization, especially when 95% of cybersecurity issues can be traced to human error.[13] Further, every employee needs to be trained as internal actors are responsible for 43% of data loss, half of which was intentional, and half accidental.[14] As we noted in a 2018 paper, it's practically impossible for

In light of potential regulatory and legal risks, the playbook can also act as evidence to prove that companies have an adequate response in place for when a cyber event does occur, and aftermath.

Prioritize cyber skills at the board level. As cyber-risks rise in importance, company

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information, please contact the marketing department by phone at one of the following locations:

Americas	EMEA	Asia
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700