


CYBERSECURITY IS AN ORGANIZATION WIDE RESPONSIBILITY


Julian Granger-Bevan
Paul Mee
James Cummings
Alon Cliff Tavor

Although digital technologies have made society, government, and business more efficient 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 failure” as a top five risk for governments and businesses across Asia-Pacific, East Asia, 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 security breach that had compromised the personal information of a significant proportion of its c. 10 million customers. Among the sensitive information that was stolen were dates of birth, email addresses, and passport 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. Recent freedom of information requests made to the Office of the Australian Information Commissioner suggest it is not even the first of its size as there have been at least 11 other breaches of a similar scale within the first half of 2022.³

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 increasing, as hackers move away from “spray-and-pray” tactics towards targeted hits.⁷ The 2022 Global Risks Report also notes the “heightened risk of cyber espionage attacks” that could levy significant costs on both public and private sector organizations.⁸

1 Global Risk report 2022, 17th Edition: [Digital Dependencies and Cyber Vulnerabilities](#). World Economic Forum.

2 [30+ data breach statistics and facts](#). Comparitech.

3 [Optus breach was huge, but companies lose our data all the time](#). Financial Review.

4 [Exploring the Costs, Risks and Causes of a Government Data Breach](#). Security Intelligence.

5 See footnote 1.

6 [Acronis Cyber Protection Operation Centers Report 2022](#). Acronis.

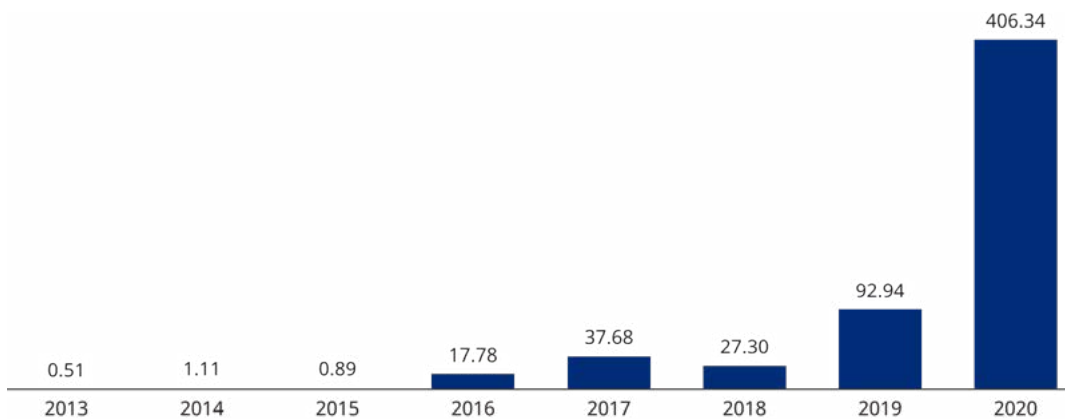
7 [Ransomware Statistics in 2022: From Random Barrages to Targeted Hits](#). DataProt.

8 Global Risk report 2022, 17th Edition: [Page 49](#). World Economic Forum.

The technologies involved are also growing in sophistication. While phishing emails remain a key source of attack, hackers are beginning to implement cutting-edge tech such as deepfakes and voice modulators.⁹ Organizations’ vulnerabilities will continue to change as more business increasingly shift to cloud-based tools and teams embrace longer term remote working, leading to more touchpoints for hackers to exploit.

Exhibit 1: Total cryptocurrency value received by ransomware addresses

Cryptocurrency value in millions, US\$



Note: Currencies included: BCH, BTC, ETH, USDT.
 Source: The Global Risks Report 2022

A FINANCIAL AND LEGAL QUAGMIRE

The recent attacks on Australian telcos have also proven instructive in terms of the scale of the reputational and financial consequences potentially facing businesses.

The most obvious financial costs are directly associated with the ransoms demanded by hackers. In 2021, the average ransom rose to US\$2.2 million, more than double the amounts registered in 2020.¹⁰ Add to that the costs of post-breach compensations and remediation work, which could be extensive depending on the damage. The telco, for instance, could potentially be held responsible for the replacement of thousands of passports which, at an estimated US\$121 apiece, could become very expensive.

That’s in addition to fines that regulators could levy. The legal implications could be especially wide-ranging if a company operates in multiple jurisdictions with different regulatory standards. Firms could find themselves locked into years-long legal quagmires that could prove costly and reputationally damaging.

⁹ [Cyber threats: Living with disruption](#). Control Risks.

¹⁰ [2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner](#). Unit 42.

While the monetary impacts of reputational damage are difficult to quantify, it's easy to understand how a company's tarnished reputation could have a direct impact on attracting and retaining customers.

Companies that fall prey to cyber-attacks could also find themselves vulnerable to class action initiatives. These lawsuits are common in the US, where related spend topped out at US\$2.9 billion in 2020, though they tend to be rarer in other jurisdictions.¹¹ However, it is reasonable to assume that interest in class actions will grow as more of these breaches 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 available within the market.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 companies to entirely erase the possibility of security breaches, especially when faced with a motivated hacker.

While technical IT teams have a crucial role in the development and design of robust and secure corporate networks, responsibility for cybersecurity must expand to include senior executives across the entire organization, particularly when it comes to responding to breaches and addressing them.

That means embedding security protocols into every function — from procurement to finance to sales — to ensure there is a company-wide “playbook” for responding to breaches.

¹¹ [U.S Class Action Spending Reaches New High of \\$2.9B: Companies Report Spike in Volume and Complexity of Matters, Survey Says](#). Carlton Fields Class Action Survey

¹² [Cybersecurity is too big a job for governments or business to handle alone](#). World Economic Forum.

¹³ See footnote 1.

¹⁴ [Grand Theft Data: Data exfiltration study: Actors, tactics, and detection](#). McAfee.

CRAFTING A CYBERSECURITY PLAYBOOK

A playbook can set out how the entire company should respond to a cyber event from the moment a breach is discovered while also emphasizing a sense of effective governance amidst a crisis. Established protocols also ensure an organized response which can have implications for how the company, its shareholders and customers are perceived.

Who should be called into so-called “war rooms” to mitigate further damages? Who decides whether to pay a ransom to a hacker? How should the organization communicate with their stakeholders — customers, regulators and shareholders — in order to ensure stability and trust? What sort of documentation is needed as evidence of an organization’s adequate response?

CASE STUDY

Mind of a Hacker

A large corporation serving consumers noted an increase in attempted and realised fraud. They undertook a typical security review and cyber assessment which helped direct investments to improve security compliance in a number of areas. Soon after, in a collaborative effort, the Chief Compliance Officer and CISO determined to undertake a more creative in-depth approach to a cyber risks assessment.

The method involved two primary strategies. One was to engage a tight team of ethical hackers who had strong technical expertise and experience across many and varied social engineering ruses. They relayed what types of data, across multiple scenarios, would be attractive to a bad actor depending on their motivations. This revealed a notable difference between what the enterprise considered valuable and what hackers would pursue.

The second strategy involved a number of working sessions with small groups long-tenured employees. The individual groups were asked a simple question, *“Based on your experience and a little cunning, what are the ways you could get interesting or sensitive documents, data, or information across the enterprise?”*.

The results were often astounding revealing for example, access rights that had accumulated and become broader over time, informal unlocked databases (e.g., complaints cases), unfettered access to executive calendars, annual report drafts in widely accessible folders, team or divisional contact/address spreadsheets, shared or common printer queue access codes, etc. As a result of the findings an overhaul of policies, procedures, controls, and surveillance was implemented. While fraudulent activity has not been fully eliminated, the frequency and financial significant became significantly diminished.

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 the resulting governance can effectively mitigate risks that occur in the aftermath.

Prioritize cyber skills at the board level. As cyber-risks rise in importance, company boards need to understand the risks and the consequences. Corporate boards need more tech experience and skills to be able to challenge and question executives on these issues.

Raise cybersecurity standards. Growing regulation around data privacy has already set a minimum-security standard, especially when it comes to consumer data. For instance, the European Union's General Data Protection Rules (GDPR) require companies to report a breach within 72 hours. Incorporating these standards into a playbook not only helps build credibility but also ensures companies remain agile in the face of new and potential laws.

Embed security standards across all functions. As responsibility for cybersecurity expands beyond IT teams, companies will need to marshal the cooperation of leaders in every function to ensure an organised response to breaches. This also ensures that an active, cyber defence culture is embedded throughout the organization.

Invest properly in cyber insurance. Insurance policies play a role in risk mitigation by placing a price tag on a business's cyber risk. By evaluating the potential profits of any venture against the impacts of the reputational and financial risks of a cyber event, firms can establish stronger governance guardrails at their most vulnerable touch points.

Innovations in better security technologies. Advances in tokenization, digital identity products, and quantum cryptography are emerging every day, and could add another layer of security over firms' data.

As recent cyber breaches have demonstrated, companies are under more pressure than ever before to mount a robust response to cyber events. These attacks will not abate — in fact, there is little doubt that more frequent and severe data breaches are on the horizon, and the stakes have never been higher. Companies need proactively mitigate their cyber risks and leverage a whole-organization approach in order to minimize their impact.

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
+1 212 541 8100

EMEA
+44 20 7333 8333

Asia Pacific
+65 6510 9700

Copyright ©2022 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.