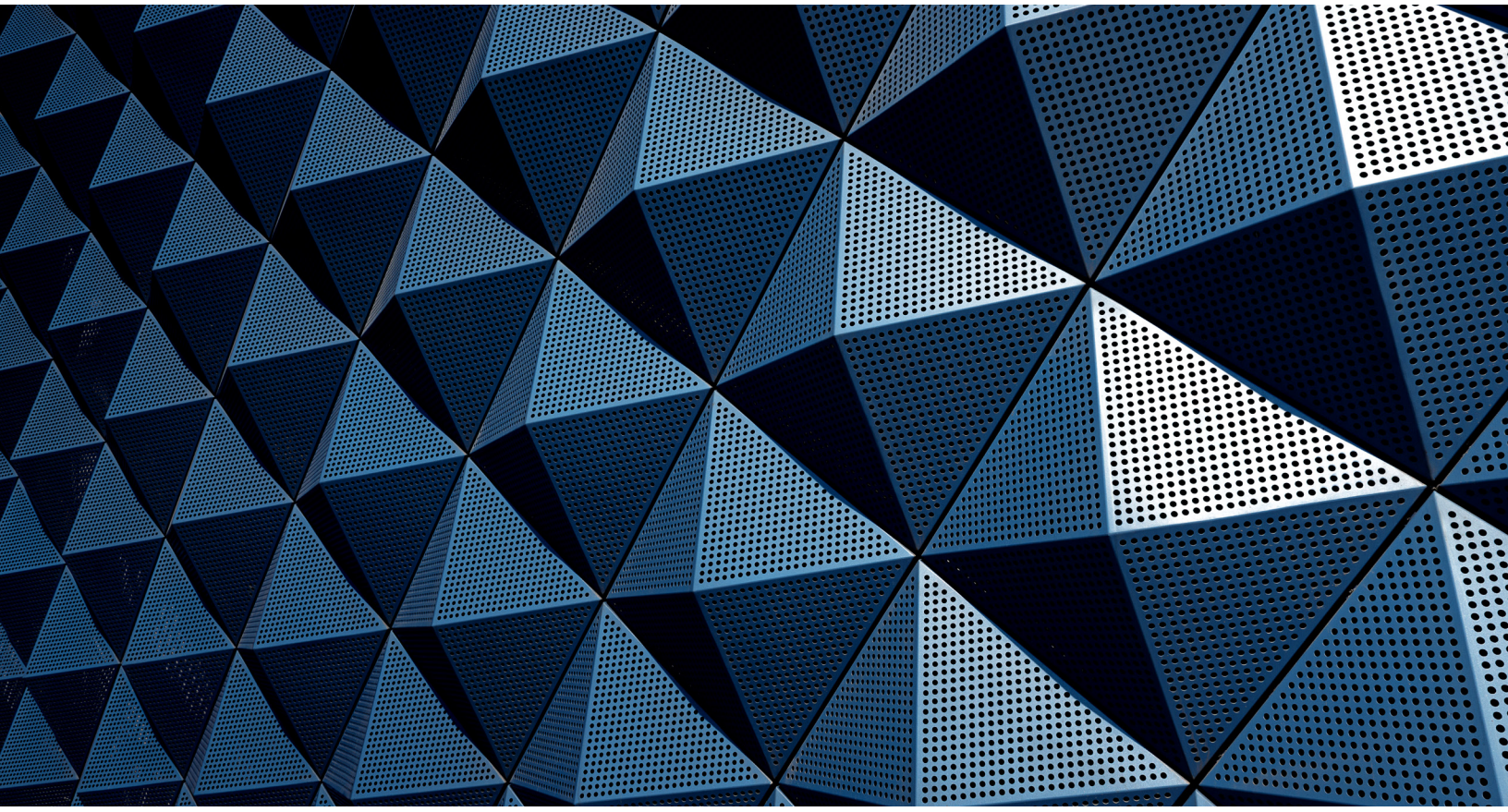
McKinsey & Company

McKinsey Direct

Cracking the code on enhanced digital and cyber risk maturity

A recent digital and cyber self-assessment of organizations in Australia and New Zealand revealed a mix of strengths and areas for improvement needed to address ever-evolving digital-related risks.

by Akash Lal, Charlie Lewis, and Olivia Loadwick



November 2023

The global digital economy has experienced an extraordinary surge in growth in recent years as organizations have embraced modernization and propelled digital transformation of their business models. Although this rapid acceleration in digitalization has created unparalleled opportunities for growth, it has also exposed heightened risks of data misuse and breaches. In fact, organizations globally are experiencing a flood of cybersecurity incidents, including ransomware attacks.

The Australian and New Zealand market has experienced a staggering 23 percent increase in cyberattacks in the past two years, involving both institutional and individual data.[1]

In June 2023, McKinsey assessed the digital and cyber maturity of 18 Australian and New Zealand–based companies across the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors. The assessment studied organizational approaches to the management of a range of digital-related risks to develop insights into where interventions might be best focused, gathering insights across a number of domains:

— cybersecurity capability maturity

— cyberthreat landscape

— cyber spend and full-time-employee structure

— cyber operating model

— data governance, data privacy, and digital trust

— technology resilience

The assessment involved a comparison with a benchmark of global peers based in Europe, North America, and the United Kingdom.

A mixed bag of success and challenges

The results of our digital and cyber self-assessment revealed eight key insights—a mix of strengths that set organizations apart from global counterparts—but it also shed light on areas that need improvement.

1. Overall maturity above global peer average but below top quartile

On average, organizations demonstrate a higher level of digital and cyber maturity compared with global peers, though they are not yet on par with the leading top-quartile performers.[2] The primary factors contributing to this gap are lower maturity in data protection and privacy, identity and access management, and risk management practices related to architecture and engineering. Financial-services institutions (FSIs) self-assessed as more mature compared with organizations from other industries (Exhibit 1).

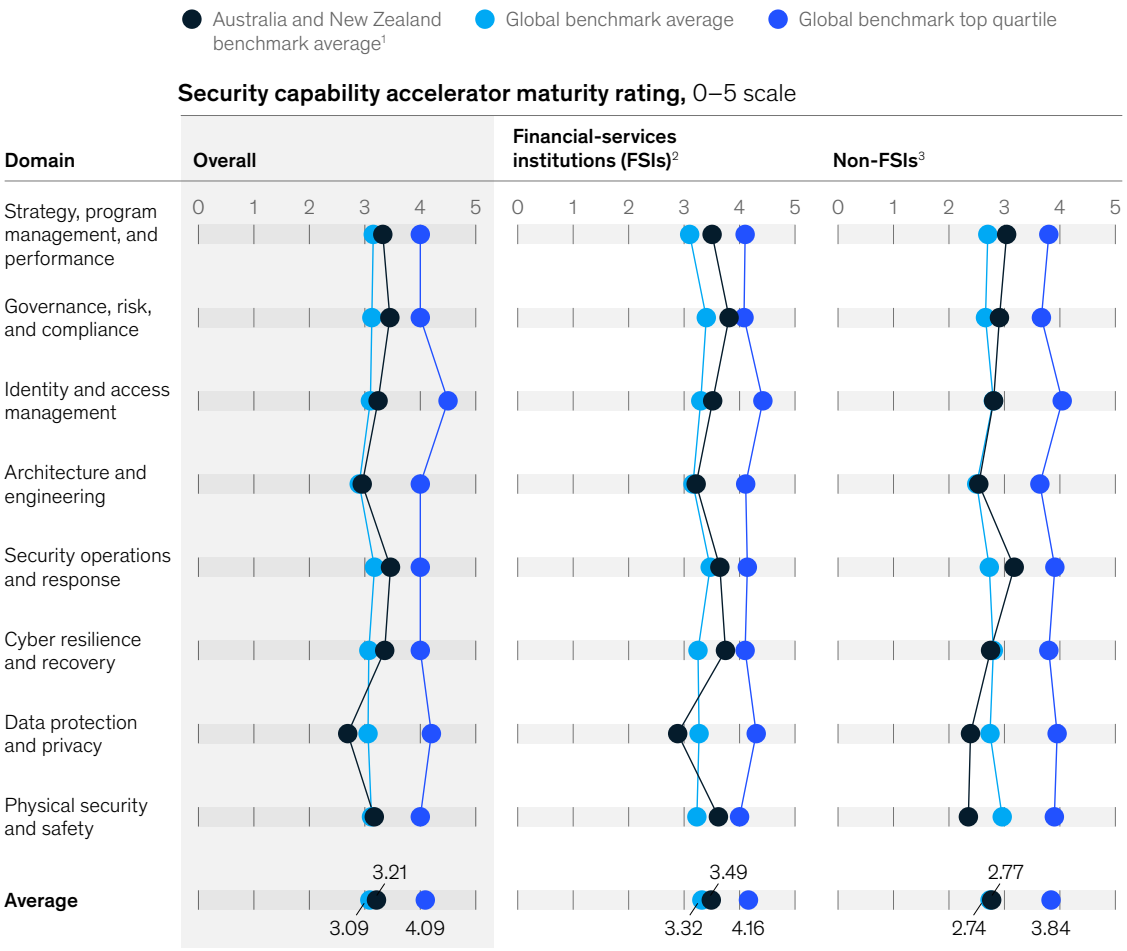
2. Strong risk management foundations in place

On average, organizations self-assess their risk management environment as more mature than global peers. They have relative strengths in the foundational elements of security risk management, security assurance, and policies and standards. These are reinforced by strengths in training, education, and awareness of digital-related risk management. They also responded as having good practices for governance and reporting cyber risk. Organizations have an opportunity to expand reporting of critical measures to a broader suite of stakeholders within the business (for instance, extending beyond the board, CEO, and security teams to business and IT teams), enabling stakeholders to make better-informed decisions and further strengthen their cybersecurity posture.

[1] Mehr Bedi, "Australia's Latitude Group, IPH hit by cyber attacks amid wave of hacks," Reuters, March 16, 2023.
[2] The global peer set includes 25 organizations from the aerospace, banking, consumer retail, education, insurance, and retail sectors in Europe, North America, and the United Kingdom.

Exhibit 1

Financial-services institutions rated themselves slightly higher than other organizations in digital and cyber maturity.



[1]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
[2]The global FSI benchmark average consists of banking and insurance companies in Europe, North America, and the United Kingdom (n = 15).
[3]The global non-FSI benchmark includes aerospace, retail, education, and consumer packaged goods companies in Europe, North America, and the United Kingdom (n = 10).
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

3. Cyber spend as a proportion of IT budgets below global peers

While the proportion of IT budgets dedicated to cybersecurity has grown in recent years, it remains below global peer benchmarks. About 30 percent of companies noted the lack of cybersecurity funding as the biggest risk to achieving cybersecurity program objectives (Exhibit 2).

4. Access to cybersecurity talent unable to keep pace with demand

IT budget allocation to cybersecurity has risen from 4 percent to 9 percent over the past three years. Projections indicate that this proportion is expected to continue growing among Australian and New Zealand–based organizations, reaching 11 percent over the next three years (Exhibit 3).

Meanwhile, 33 percent of surveyed Australian and New Zealand–based companies said the lack of cybersecurity talent is the biggest risk to achieving their cyber program objectives. This talent gap may be one reason for companies' heavy reliance on outsourcing. On average, organizations in the region outsource 43 percent of their cybersecurity activity, while global peers outsource just more than 30 percent (Exhibit 4). Companies in Australia and New Zealand rely on outsourcing particularly for physical security and safety as well as security operations and response (Exhibit 5).

Exhibit 2

Nearly two-thirds of Australian and New Zealand–based companies rank a lack of a funding and cybersecurity talent as the biggest risks for cybersecurity.

Biggest risk to achieving cybersecurity program objectives, % of respondents

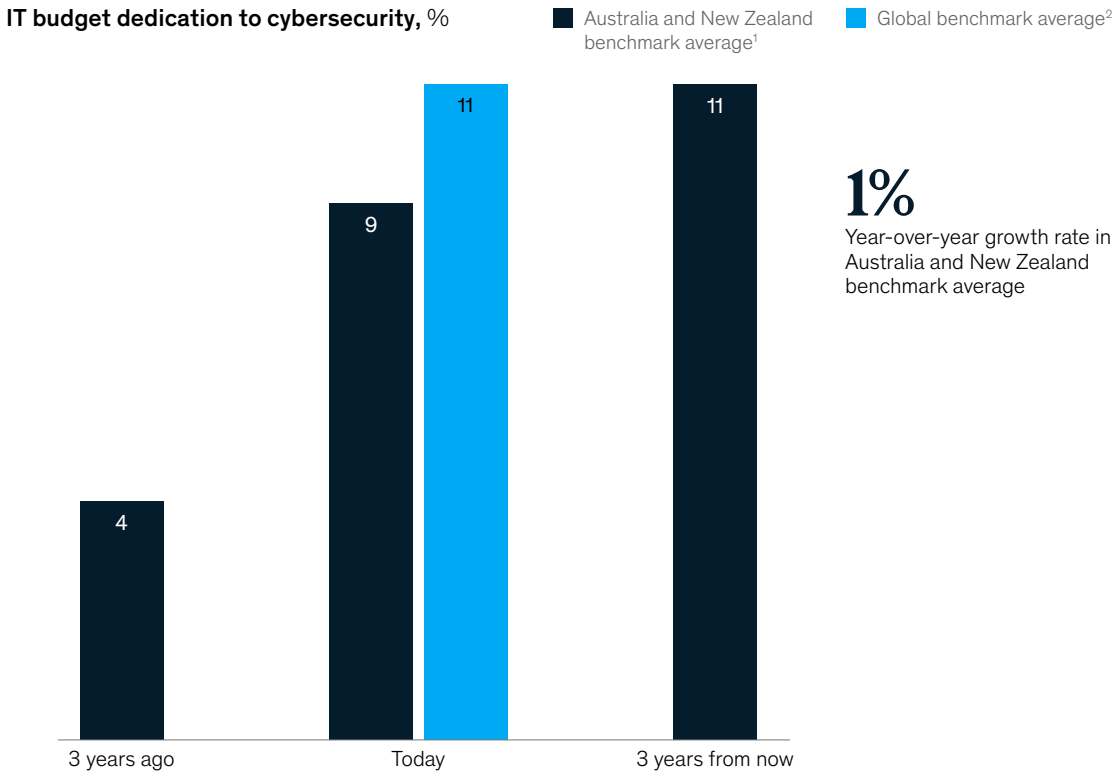
Note: Figures do not sum to 100%, because of rounding.
[1]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

33 percent of surveyed Australian and New Zealand–based companies said the lack of cybersecurity talent is the biggest risk to achieving their cyber program objectives.

Exhibit 3

Companies in Australia and New Zealand expect to match today's global IT budget dedication to cybersecurity in three years.



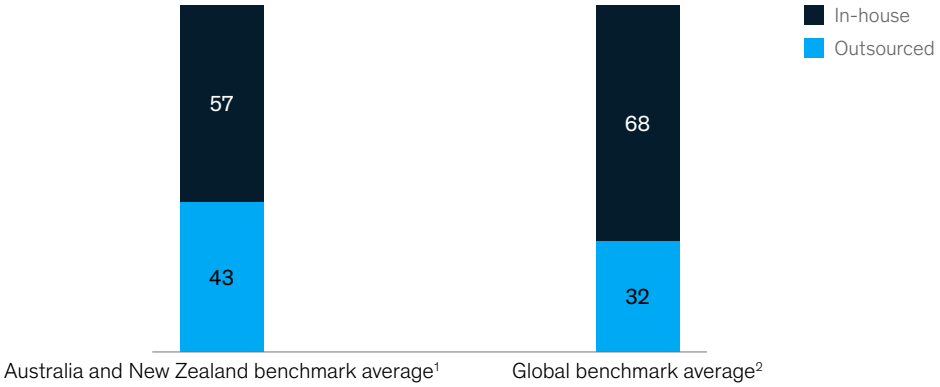
Question: What percentage of your company's annual IT budget is dedicated to cybersecurity?
[1]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
[2]Includes aerospace, banking, insurance, retail, education, and consumer packaged goods companies in Europe, North America, and the United Kingdom (n = 25).
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

Exhibit 4

Australian and New Zealand–based companies outsource cybersecurity work at a higher rate than the global benchmark.

Average breakdown of outsourced and in-house cybersecurity full-time equivalents (FTEs), %



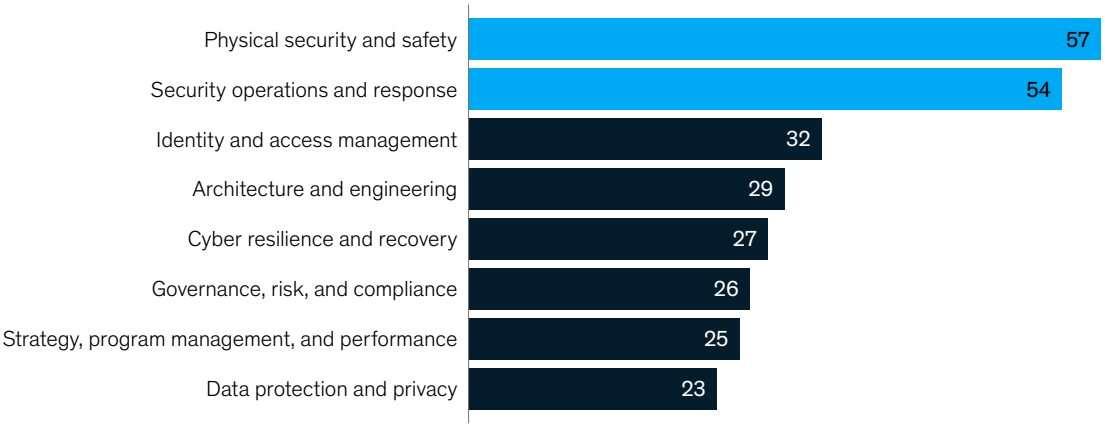
Question: What is the average percentage breakdown between outsourced and in-house cybersecurity FTEs?
[1]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
[2]Includes aerospace, banking, insurance, retail, education, and consumer packaged-goods companies in North America, Europe, and the United Kingdom (n = 25).
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

Exhibit 5

Australian and New Zealand–based companies outsource more than half of their work in two areas.

Workload outsourced to managed services for cyber domains, %
(Australia and New Zealand benchmark average[1])



Question: Do you leverage managed services (eg, a dedicated vendor team) for any of the cyber domains? If so, please indicate the percentage of the outsourced workload.
[1]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

5. Cloud security a challenge

The maturity of cloud security practices aligns broadly with global peer averages but falls significantly behind the top quartile. This is of particular concern because, according to the assessment, organizations already host more than 50 percent of their workloads in the cloud and intend to migrate more in the next three years. However, many organizations have yet to establish cloud security practices in line with leading peers. Best practices in cloud security include the following:

- deploying security-as-code practices across the organization with a defined operating model to ensure clear articulation of roles and responsibilities for crucial governing decisions (such as permissions for policy authoring)
- deploying automated security-as-code practices, including provisioning and monitoring to ensure cloud security controls are enforced in every instance
- shifting security that remains throughout the security development life cycle and embedding security personnel (such as talent with security knowledge) to ensure that highly automated security products are produced

6. Improvement required in data security and privacy risk management

In terms of technology and cyber risks, organizations are most concerned about the misuse of data, disrupted access to data, and the loss of critical and sensitive information. It's likely these concerns are linked to the surge in data breach events in this market in recent years. There is a considerable maturity gap between these organizations and the global benchmark average across all data protection and privacy subdomains. The gap between Australian and New Zealand–based companies and top-quartile global-peer benchmarks is even more significant. Best-in-class organizations are taking an end-to-end approach to understand the range of data the business uses (and the relative risk and value associated with that data) to enhance governance practices in relation to data and improve access management policies, practices, and security tooling.

In terms of technology and cyber risks, organizations are most concerned about the misuse of data, disrupted access to data, and the loss of critical and sensitive information.

7. Increasing insurance premiums and inconsistent coverage

Amid the evolving threat landscape, almost all organizations surveyed (about 95 percent) have purchased cyber insurance. Most have comprehensive coverage, spanning data breaches, business interruption, and digital-asset replacement. However, only about half have coverage for reputational damage and extortion payments. Organizations said premiums had increased about 20 percent on average over the past 12 months.

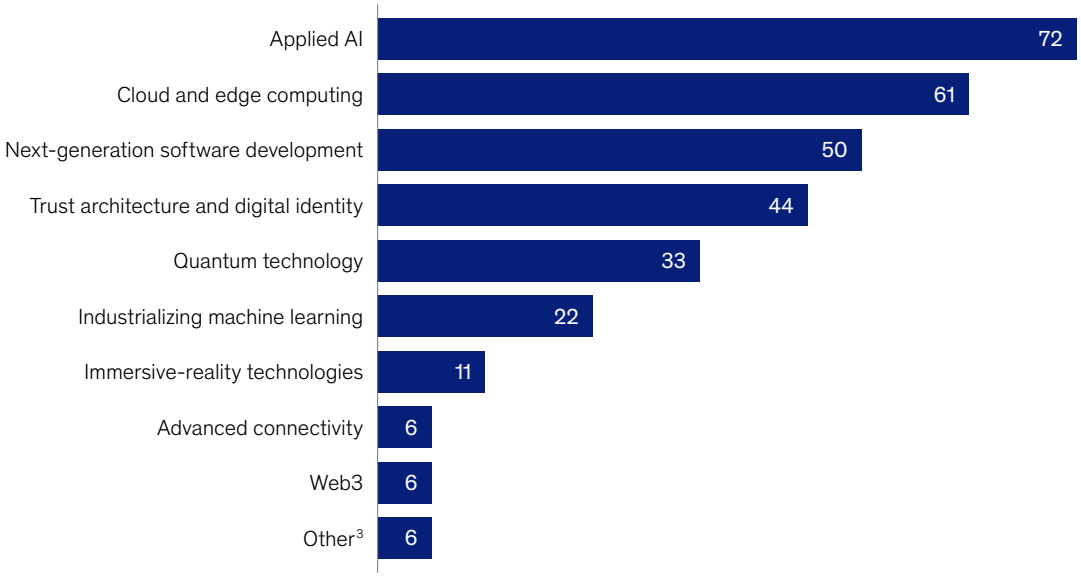
8. Significant implications of AI for cybersecurity

The effects of applied AI on cybersecurity are a concern—namely that AI tools might leak sensitive data. There is also an increasing likelihood that cyberthreat actors will use AI to improve their hacking methods, such as by conducting phishing attacks that are more sophisticated (Exhibit 6).

Exhibit 6

Australian and New Zealand–based companies are most concerned about applied AI as a threat to cybersecurity.

Concern about emerging technology trends' threat to cybersecurity, % of respondents[1] (Australia and New Zealand benchmark average[2])



Question: What emerging technology trends keep you awake at night due to the potential implication on cybersecurity?
[1]Question allowed respondents to give multiple answers.
[2]Includes companies in the airline, banking, consumer retail, insurance, not-for-profit, and wealth sectors surveyed in the McKinsey Digital and Cyber Maturity Assessment (n = 18).
[3]Includes AI, quantum computing, and an industry-wide external attack on financial institutions.
Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

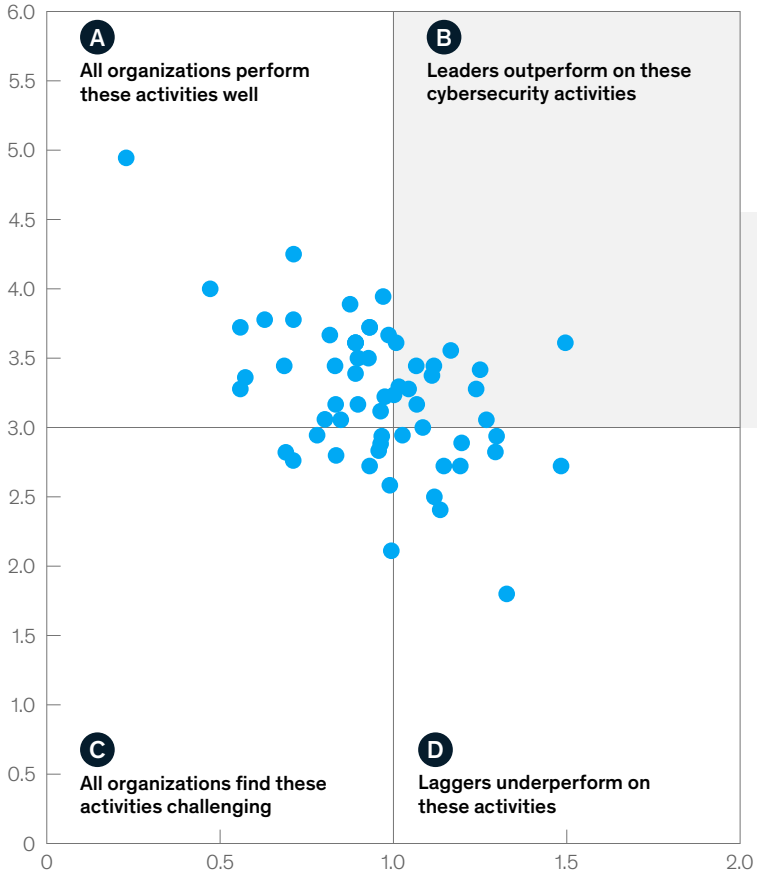
Cybersecurity maturity differentiates organizations and leaders

The assessment revealed a core set of dimensions and capabilities that separate the "great" organizations and leaders from the "good" in the management of digital-related risks. While high-performing organizations demonstrate strengths in table stakes capabilities such as endpoint security, metrics and reporting, communications, cyber insurance, and security risk management, laggers underperformed in edge and Internet of Things security, business relationship management, threat hunting and active defense, data loss protection, and cryptography and key management. The maturity matrix also reveals activities in which leaders outperform, as well as some of the most challenging activities facing organizations (Exhibit 7).

Exhibit 7

A maturity matrix shows the activities with which companies struggle the most and perform the best.

Standard deviation of cybersecurity maturity by activity cluster



A
Table stakes capabilities
1. Endpoint security
2. Metrics and reporting
3. Communications management
4. Cyber insurance
5. Security risk management

B
Activities leaders outperform on
1. Supply chain security
2. Third-party security risk management
3. Access management
4. Threat modeling
5. Forensics and investigations

C
Most challenging activities
1. Cloud security
2. Privacy operations
3. Insider threat program
4. Encryption and tokenization
5. Data life cycle management

D
Activities laggers underperform on
1. Edge and Internet of Things security
2. Business relationship management
3. Threat hunting and active defense
4. Data loss protection
5. Cryptography and key management

Source: McKinsey Digital and Cyber Maturity Assessment

McKinsey & Company

Five immediate actions for organizations to take

Organizations can take immediate action on a core set of domains to improve standards for the management of digital-related risks:

1. *Improve data protection capabilities.* Understand your critical business services, what data supports those processes, and the value of the data and security implications. Ensure data management and monitoring tools are in place (such as data loss protection tools). Design metrics and dashboards to report regularly on data breaches and internal data mishandling.

2. *Review and improve cyber incident detection and response capabilities.* Continuously assess and refresh the incident response and recovery program based on business risks and emerging threats. Orchestrate regular tabletop exercises on emerging threats. Conduct live, online resilience exercises to test response and recovery capacities. Review the cyber insurance policies on the latest premium structure. Ascertain whether sufficient coverage against relevant events is in place.

3. *Review and enhance cloud architecture and security capabilities.* Understand what data has been transitioned to the cloud, and evaluate the risk. Implement a holistic cloud security strategy, emphasizing access management, threat monitoring, and incident response. Conduct regular configuration and application vulnerability testing and audit reviews to ensure the cloud environment is secure.

4. *Allocate the cybersecurity budget based on risk.* Allocate the budget in line with global best practices by evaluating spend against risk areas and risk appetite. Comprehensively capture the most "cost-risk optimal" defenses to provide the same level of overall protection to critical assets in a cost-efficient and effective manner.

5. *Build a skilled talent pool and optimize resources through automation.* Review the cyber and risk teams' roles and responsibilities, determine the complexity of the solutions and environment, and identify skills gaps. Develop a talent attraction and retention strategy. Understand opportunities for upskilling and reskilling existing team members. Provide continuous learning opportunities to help employees adapt to new tools and technologies. Identify operational processes for automation transformation. Consider refreshing the outsourcing strategy.

Accelerating digitalization has delivered excellent outcomes for individuals, companies, and government institutions alike. However, as threats become more sophisticated and frequent, organizations must take proactive steps to safeguard their sensitive data, valuable assets, and reputation. Investing in enhanced digital and cyber maturity not only protects an organization from financial losses and legal liabilities resulting from data breaches but also fosters trust among customers, partners, and other stakeholders.

Akash Lal is a senior partner in McKinsey's Mumbai office, **Charlie Lewis** is a partner in the Stamford office, and **Olivia Loadwick** is a partner in the Sydney office.

The authors wish to thank Jim Boehm, Rich Isenberg, Bartlomiej Kazimierski, Benjamin Klein, Anselm Ohme, Kevin Telford, and Johnson Yu for their contributions to this article.

Designed by McKinsey Global Publishing