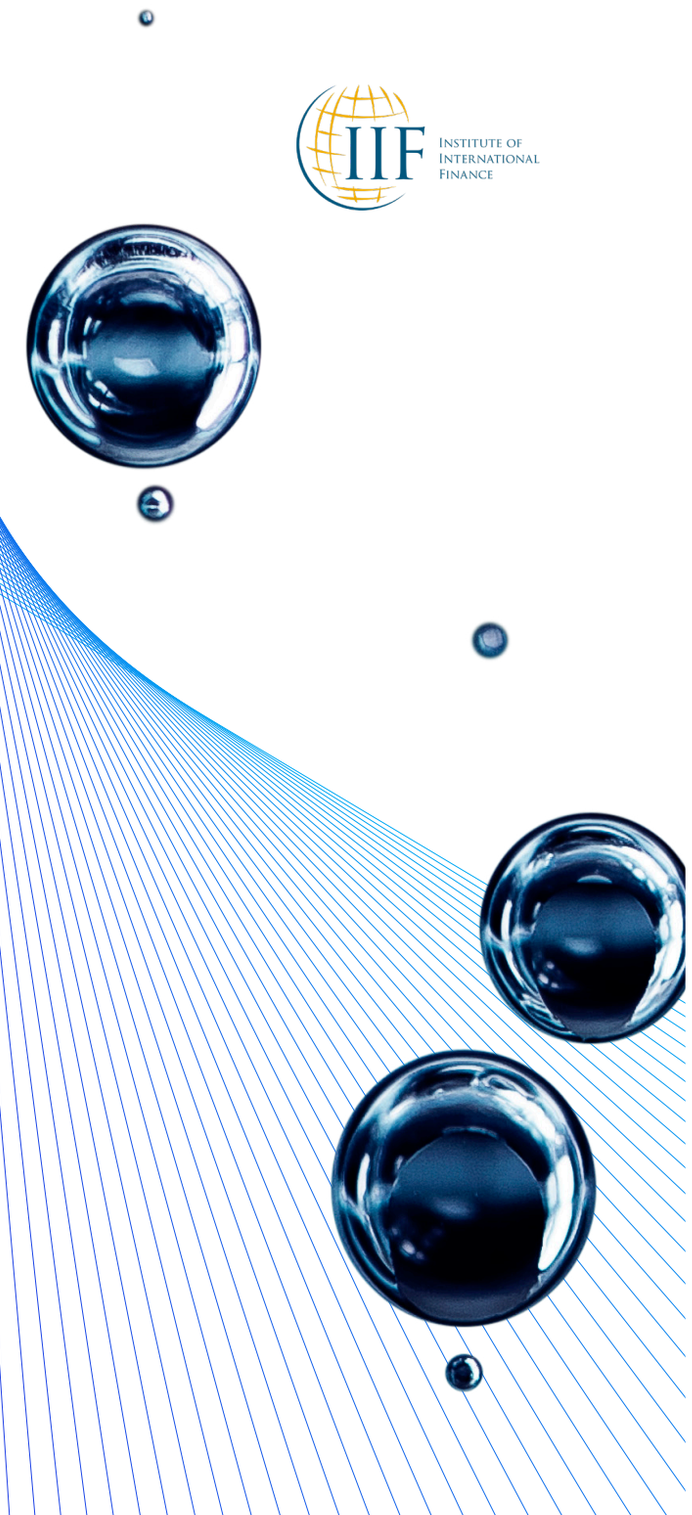
McKinsey & Company

IIF Institute of International Finance

# IIF/McKinsey Cyber Resilience Survey

Cybersecurity posture of the financial services industry



March 2020

**Source:** IIF/McKinsey Cyber Resilience Survey 2019

# Table of contents

# Introduction

### Background on the survey

Cyber risk has become one of the top risk concerns among financial services firms. In response, the Institute of International Finance (IIF) and McKinsey & Company have collaborated on research to provide these firms an understanding of the ways they can enable and strengthen cyber resilience, building on the current and planned practices of peer institutions.

### Structure of the survey

Our research is survey-based. To help streamline member responses, we mapped our survey in part to the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The survey consisted of 107 questions across 4 key areas: firm- and sector-level cyber resilience, costs and FTEs, and next-generation questions.

### Purpose of the final report

This report highlights the themes we saw and observations we made across the 4 key areas, as well as insights we gained from discussions with more than 50 firms during regional and global IIF CRO cybersecurity forums.

# Our research used two mechanisms to obtain information

**Survey**

- Structured in 4 sections with 107 questions
- Mapped in part to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and Financial Services Sector Cybersecurity Profile (FSSCP)
- Responses collected by McKinsey & Company
- Responses sanitized and aggregated for reporting; none attributed to any specific respondent or institution except in individualized playback documents

---

**Group discussions**

- Conducted as part of IIF forums in 2019 and 2020
- Observations and findings are included as part of final report

# A total of 27 companies participated in the survey

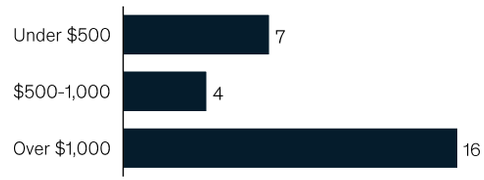
## Breakdown by geography, size, businesses

### Respondents' principal market


### Geographical footprint

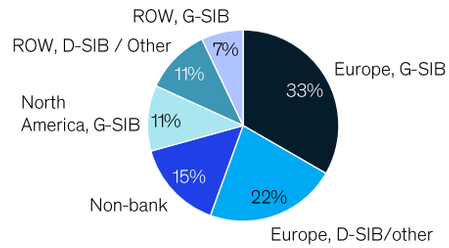

### Size by assets

$ billion, number of participants




### Supervisory class and geography

Percentage of respondents




### Percent of respondents with a presence in these businesses

| | | | | |
|---|---|---|---|---|
| **81%** Asset management | **78%** Payments & clearing | **78%** Retail banking | **78%** Corporate banking | **74%** Investment banking |
| **70%** Capital markets | **63%** Private equity | **44%** Insurance | **7%** Data provider | **19%** Other |

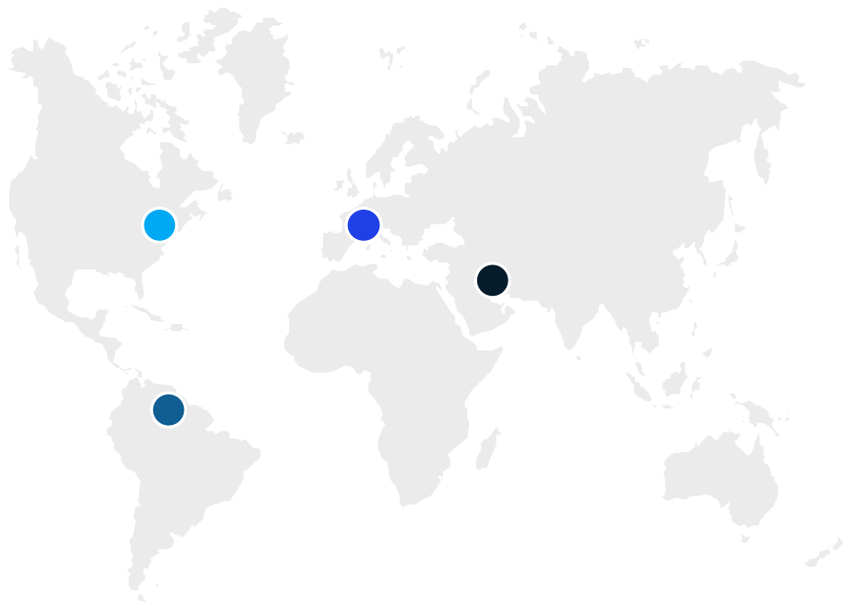
# The 4 survey sections revealed a diversity of challenges

| Section | Topic | Summary of findings |
|---|---|---|
| **A Firm-level cyber resilience** | Capabilities of each firm in developing and strengthening firm-level resilience across 7 Financial Services Sector Cybersecurity Profile (FSSCP) functions | — Firms with over $1 trillion in assets have better cyber resilience<br>— Largest vulnerability could be supply chain/dependency mgmt.<br>— Out-of-date infrastructures are at risk for hacking<br>— 37% said it takes more than 3 months to remediate a vulnerability<br>— Companies are willing to share information with peers |
| **B Sector-level cyber resilience** | Information on collaboration between financial sector firms and the public sector to enhance sector-wide cyber resilience | — Many are willing to work together to raise resilience for all (e.g., 40% would do joint 3rd party / vendor due diligence)<br>— Many would also participate in public platforms or initiatives |
| **C Costs and FTEs** | Participants' cyber risk dedicated spend and FTE numbers, including their roles and responsibilities | — 58% self-reported underspending<br>— The protect function gets the most resources, some others are lacking |
| **D Next generation questions** | Future topics and integration of next-generation technology, agile methodologies, and cyber insurance coverage | — Cyber insurance levels are insufficient<br>— Key challenges include cloud adoption, digital innovation, talent gap<br>— Cloud adoption is both a challenge and an opportunity<br>— Automation and artificial intelligence will see continued adoption |

Note: Resilience scores are calculated for every function of the FSSCP based on self reported responses, so may not accurately reflect overall organizational cyber resilience

# We also gained insights during discussions at 4 IIF CRO roundtables involving over 50 companies

## CRO roundtable sessions in 4 continents



## Insights

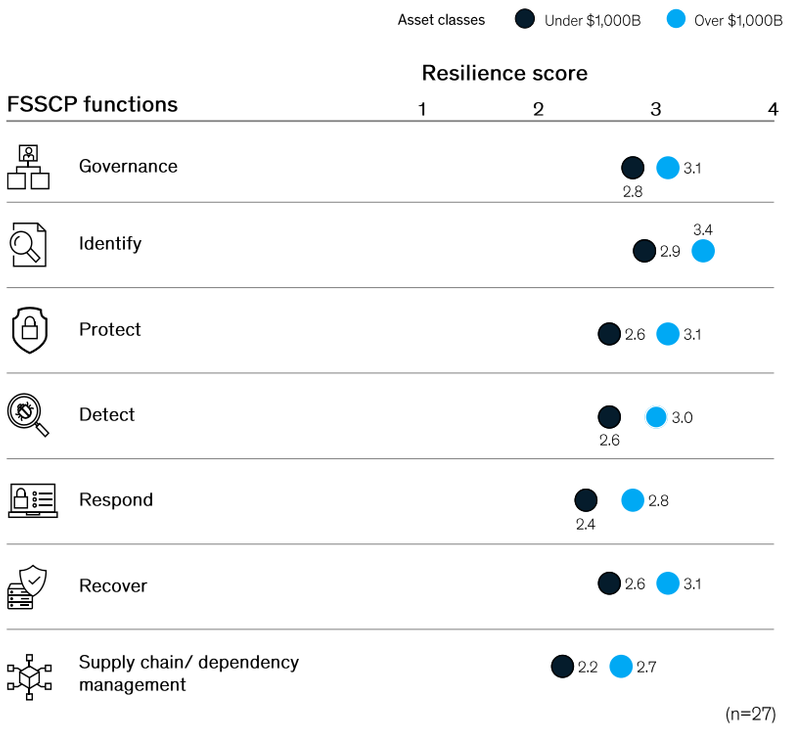
Supply chain cybersecurity risk is overwhelmingly a key concern across firms.

Latin America firms discussed de-risking digital transformations and leveraging cloud adoption as opportunities to increase their cyber resilience.

European firms highlighted concerns about cloud security, and discussed opportunities to increase resilience through a regional cloud user coalition.

Firms in the Middle East and Asia were concerned about nation-state cyber attacks and operational technology (OT) security. They were also looking to increase investments to address cybersecurity resource and talent gaps.

# The largest firms have higher cyber resilience scores across functions




Note: Resilience scores are calculated for every function of the FSSCP based on self reported responses, so may not accurately reflect overall organizational cyber resilience

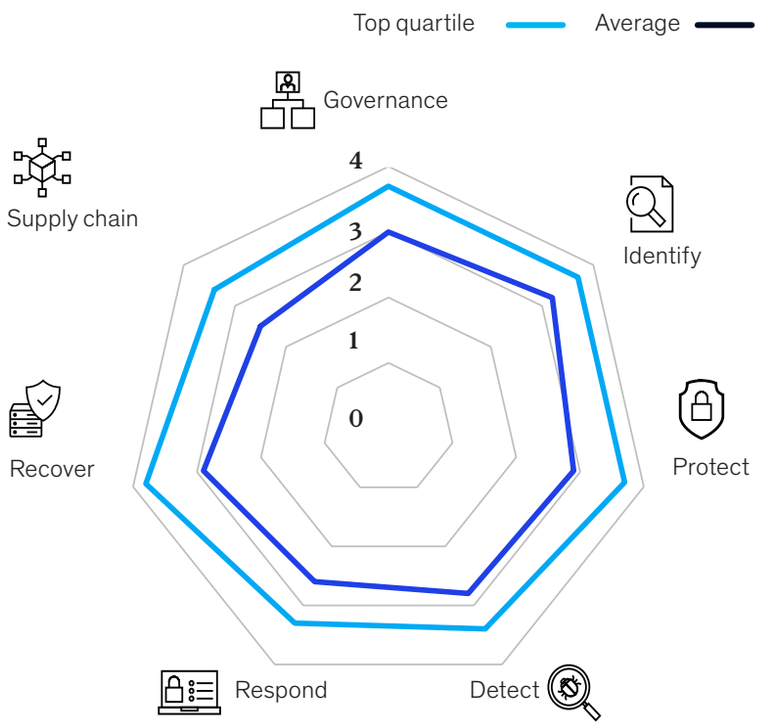
Companies with more than $1 trillion in assets had an average resilience score of 3.0

The companies with asset class under that size had an average score of 2.6

Cybersecurity resiliency requirements get complex as companies grow beyond a certain scale, so it is important to embed resiliency as part of the growth strategy

# Supply chain and dependency management could be the weakest link

## Resilience score averages and top quartile view, by function




Note: Resilience scores are calculated for every function of the FSSCP based on self reported responses, so may not accurately reflect overall organizational cyber resilience

Security around supply chain and vendors, and incident response were reported as the least-mature capabilities

For example, 33% of companies responded that they don't have proper vendor remote access management, with multi-factor authentication

This suggests a need to strengthen access control and other cybersecurity areas for vendors

# Out-of-date infrastructure presents an easy target for hackers

**Percentage of production infrastructure fully up-to-date with patches, or one patch behind**

% of respondents (n=27)

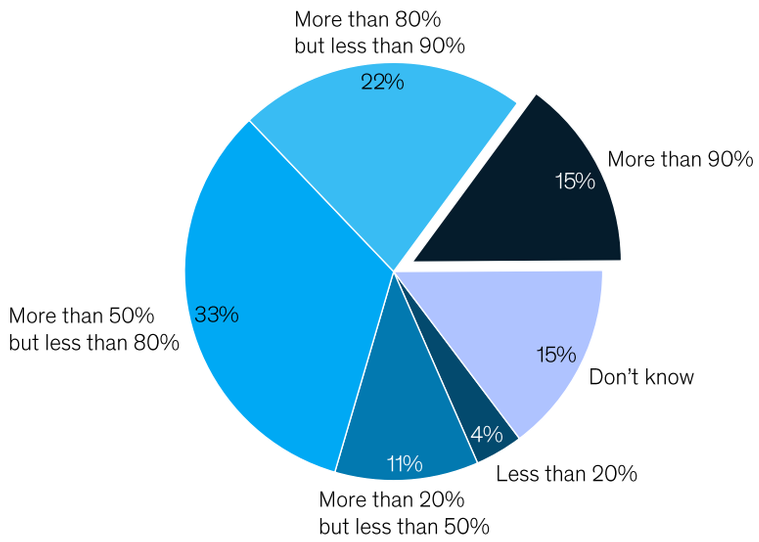



Chart shows only 15% of firms reported that more than 90% of their infrastructure is up-to-date or one patch behind.

Among additional findings, only 48% of companies reported they are actively scanning more than 90% of their IT environment at least monthly to identify vulnerabilities.

Out-of-date infrastructure provides a window for hackers to gain environment control, exploiting known vulnerabilities, stealing data, and other malicious activities.

# Long lead-times to remediate vulnerabilities also increase risk

**Average time to remediate vulnerabilities once they have been detected**

% of respondents (n=27)

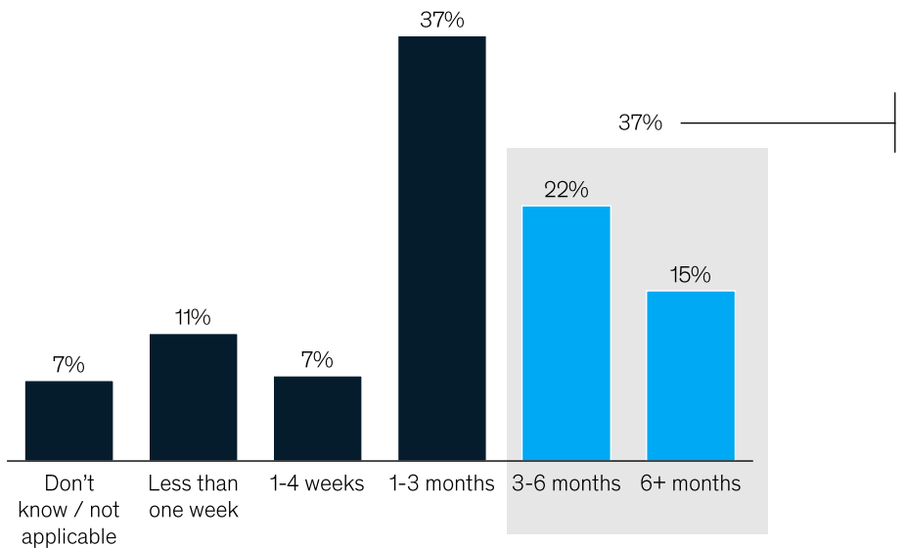



Chart shows 37% of companies said it takes more than 3 months to remediate a vulnerability.

Among additional findings, 30% of companies said they do not provide technology and risk leaders with reporting and decision support on the vulnerability landscape.

And, 52% of companies said they do not assess, document, and aggregate non-remediated vulnerabilities as part of enterprise risk management. This gives hackers time to exploit gaps in the environment.

Lack of visibility across the vulnerability landscape impedes firms from accurately reporting on risks.

# Across sectors, companies are willing to exchange information with peers

**Types of information that firms want to share and receive from peers to strengthen sector-wide resiliency**

Larger words indicate more responses (n=20)


To create these results, we synthesized free text responses and clustered them into topics

Chart shows that many companies are willing to share threat intelligence and indicators of compromise, along with information on incidents and their root causes

Among additional findings, 85% of companies said they frequently participate in sector-wide cyber exercises, and find them helpful

But 64% say that confidentiality and privacy and other regulations are barriers to information sharing

Regulatory guidelines can reduce barriers to information sharing

# Many said they would work together to raise sector-level resilience

**Potential ideas that firms are willing to execute, to raise sector-level resilience**

Larger words indicate more responses (n=20)


To create these results, we synthesized free text responses and clustered them into topics

About 40% of companies were willing to commit to joint 3rd party / vendor due diligence. Most of these were in Europe and Asia.

Many suggested this would help reduce costs and improve efficiency, given that they have a common pool of 3rd party vendors

Some would also commit to joint platforms and initiatives

# More than half the firms acknowledged underspending on cybersecurity

## Spending on cybersecurity

% of respondents (n=24)

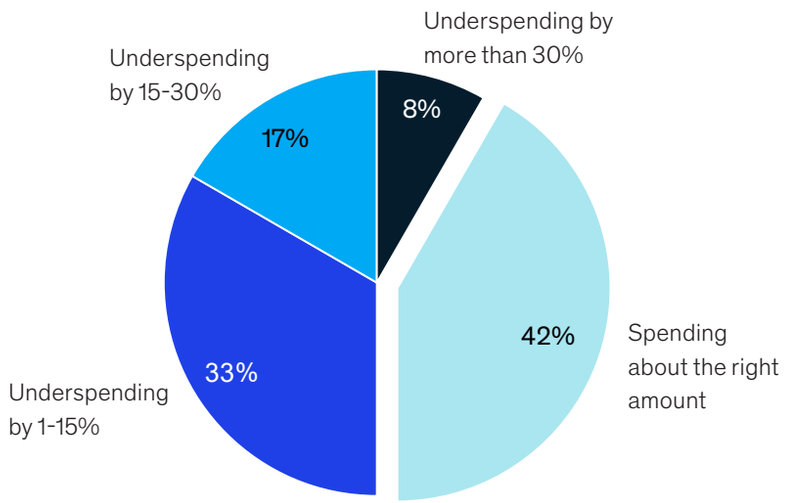



Chart shows that 58% of firms acknowledged underspending, while just 42% said they are spending about the right amount

No one reported overspending.

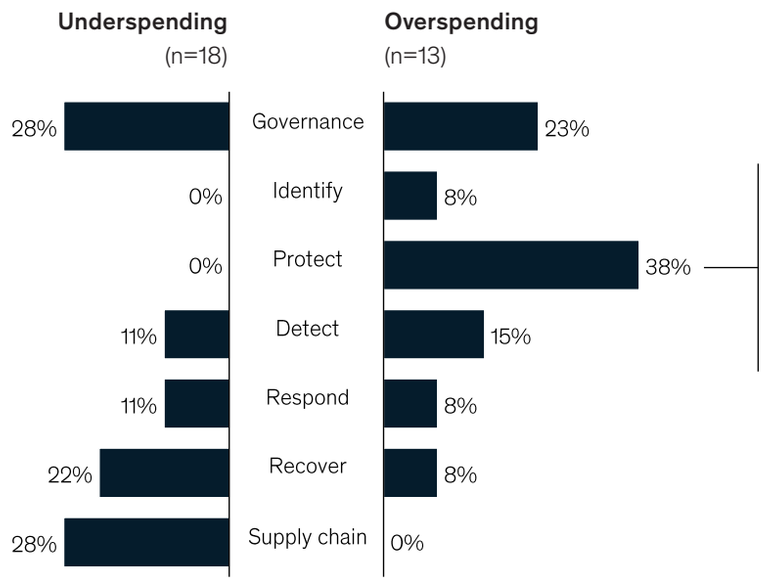
Among additional findings, 50% said they expect to increase the size of their cybersecurity team significantly in the near future

Given the increased threat landscape, it will be increasingly important to optimize resources to maximize cyber resilience

# The protect function is getting the most spending; other functions need more

## Cybersecurity spending by function

% of respondents



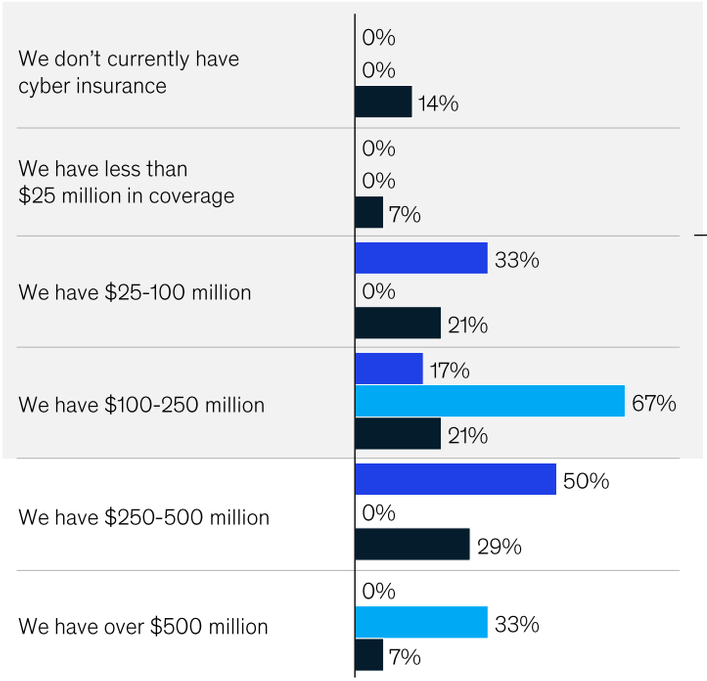

38% of companies said they are overspending on the protect function; this could stem from a past focus on shoring up the network and infrastructure

However, companies may not be paying enough attention to other functions; recovery and supply chain are particular concerns

# Cyber insurance is in the early stages, and there is little correlation between coverage and firm size

## Size of cyber insurance coverage

% of respondents (n=23)



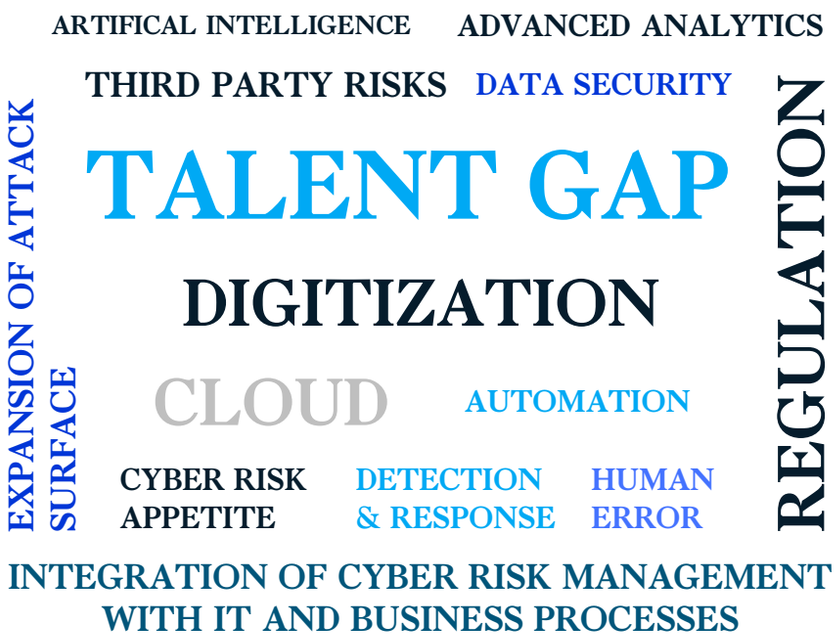

63% of the companies with more than $1 trillion in assets reported less than $250 million in coverage.

Moreover, companies may not be optimizing the impact of cyber insurance. About 65% of companies said they do not expect changes in cyber insurance size or scope in the future

# Key challenges reported by firms are regulations, cloud adoption, digitization and the talent gap

**Word cloud showing key challenges for cyber risk management in the next 3-5 years**

larger words indicate more responses (n=18)




The biggest challenge – the talent gap -- will likely continue given that 50% of the companies said they expect their team size to grow in the near future due to changes in responsibilities and necessary capabilities.

Therefore, companies need to think about talent optimization, leveraging automation, and/or cross-skill development.

# Respondents consider cloud adoption a challenge and an opportunity

**17%**

consider cloud as a key challenge for cyber risk management (n=18)

**17%**

consider cloud as an opportunity for cyber risk management (n=18)

Securing data in the cloud is top-of-mind, as increased cloud adoption creates new cyber risk frontiers

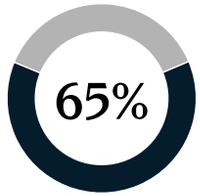
However, equal numbers of firms see it as a challenge in the next 3-5 years and as an opportunity to help them increase their cyber risk management

Cloud adoption is an opportunity if it has security embedded as part of the process, enabling firms to increase their resilience

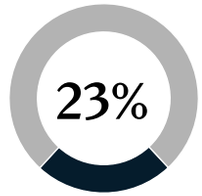
# Automation is seeing extensive adoption soon to be followed by elements of cognitive computing

## New cyber risk technologies, now and in the future

% of respondents (n=26)




Currently use automation technology, with most considering extensive use in the next 1-2 years




Currently deploying or actively using one or more cognitive technologies in cyber risk activities

Automation is seeing significant and growing usage, with nearly two thirds of companies using it now for some cybersecurity activities, and many considering extensive use soon.

Cognitive technologies such as machine learning have not yet seen the same level of adoption, but most firms see them as part of the next generation of cybersecurity improvements.

These technologies take slightly longer to adopt, but firms are considering them in several use cases.

# Companies can draw on six sets of immediate actions to enhance their cybersecurity posture

## 1 Do the basics, patch your vulnerabilities!

- ☐ Assess your current vulnerability scan coverage and patch management practices
- ☐ Build metrics and a dashboard to report regularly on the identified vulnerabilities and patch releases to CISO and BISO
- ☐ Require leadership oversight and accountability for delayed patch releases and accepted vulnerabilities

## 2 Review your cloud architecture and security capabilities

- ☐ Understand what data you are putting in the cloud now and minimize the presence of sensitive information there
- ☐ Implement a holistic cloud security strategy, emphasizing access management, threat monitoring and incident response
- ☐ Conduct regular penetration and vulnerability testing; audit reviews to ensure your cloud environment is secure

## 3 Reduce your supply chain risk

- ☐ Define a supply chain cybersecurity policy, and classify vendors based on the risk exposure they create
- ☐ Enforce enterprise-wide controls and a risk-based approach on your vendor intake process
- ☐ Develop monitoring and a response plan for supply chain cyber disruptions

## 4 Practice your incident response and recovery capabilities

- ☐ Continuously assess and refresh your incident response and recovery program based on your business risks and emerging threats
- ☐ Host regular table-top exercises on emerging threats, and conduct comprehensive resilience exercises to test response and recovery capacities

## 5 Set aside a specific cybersecurity budget and prioritize it

- ☐ Evaluate cyber spending against key risks and its impact on them - is it proportional?
- ☐ Assess ROI for cyber investments based on risk reduction
- ☐ Assess your cyber insurance spend and whether it addresses the cyber risk exposure faced by your business

## 6 Build a skilled talent pool & optimize resources through automation

- ☐ Review your cyber and risk teams' RACI and the complexity of your solutions and environment to identify skillset gaps
- ☐ Provide continuous learning opportunities to help employees adapt to new tools and technologies
- ☐ Identify operational processes for automation transformation to reduce human overhead

# Contact

If you would have any questions about the survey's purpose or structure, please contact:

Martin Boer (mboer@iif.com)

Merlina Manocaran (merlina_manocaran@mckinsey.com)

Soumya Banerjee (Soumya_Banerjee@mckinsey.com)

Claudia Sandoval Parra (Claudia_Sandoval_Parra@mckinsey.com)

www.mckinsey.com

@McKinsey

@McKinsey