

CYBER RISK MANAGEMENT: RESPONSE AND RECOVERY

JULY 2018

Jessica So and Keri Lee

MMC Global Risk Center worked with WomenCorporateDirectors and Marsh to identify emerging trends in cyber risk governance and the role of cyber insurance

About this report

- The research tapped into the insights of the global membership of WomenCorporateDirectors and the global Marsh teams.
- Focuses on emerging issues in cyber risk management and the role of the board in cyber risk governance.
- Includes a particular focus on evolving cyber insurance and what directors need to know about the role of cyber insurance in a comprehensive cyber risk management framework.



“

One of the most critical emerging risks weighing on directors' minds is the area of cybersecurity. Today, every single industry is digital, which means that we're all vulnerable to breaches, data loss, and ransomware attacks.

”

Susan Stautberg

WomanCorporateDirectors (WCD)
Chair Emeritus and Co-Founder

Susan C. Keating

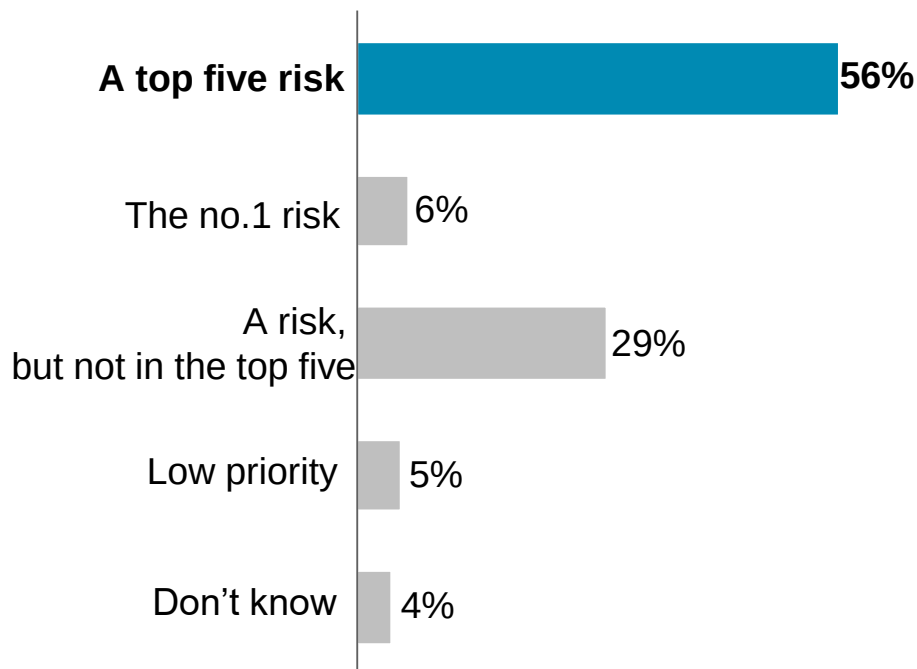
WomanCorporateDirectors (WCD)
Chief Executive Officer

Background

Cybersecurity is ranked as a leading risk but many boards are not confident about current mitigation and response strategies

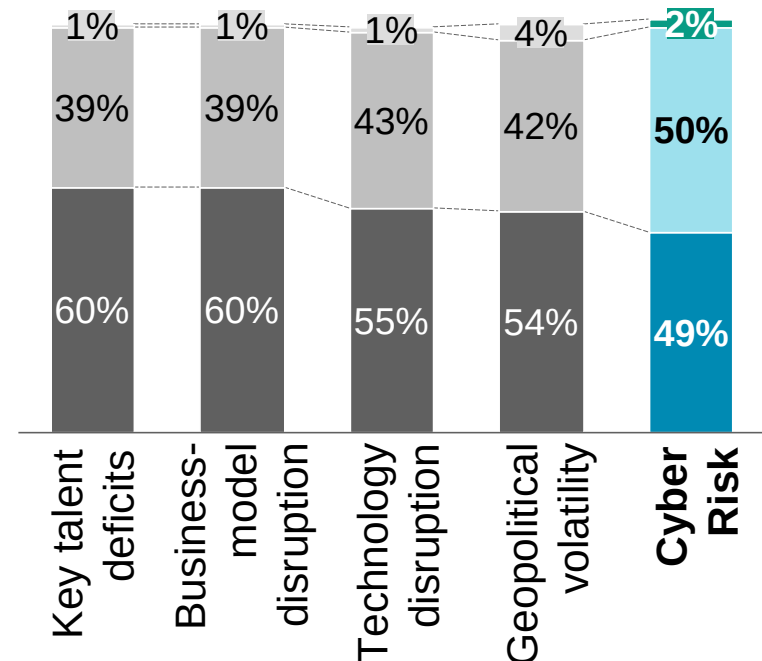
Ranking of cybersecurity - % of total respondents

(Source: Marsh/Microsoft Cyber Risk Perception survey 2018)



Board confidence in managing key risks - % of total

(Source: NACD public company governance survey 2017-2018)

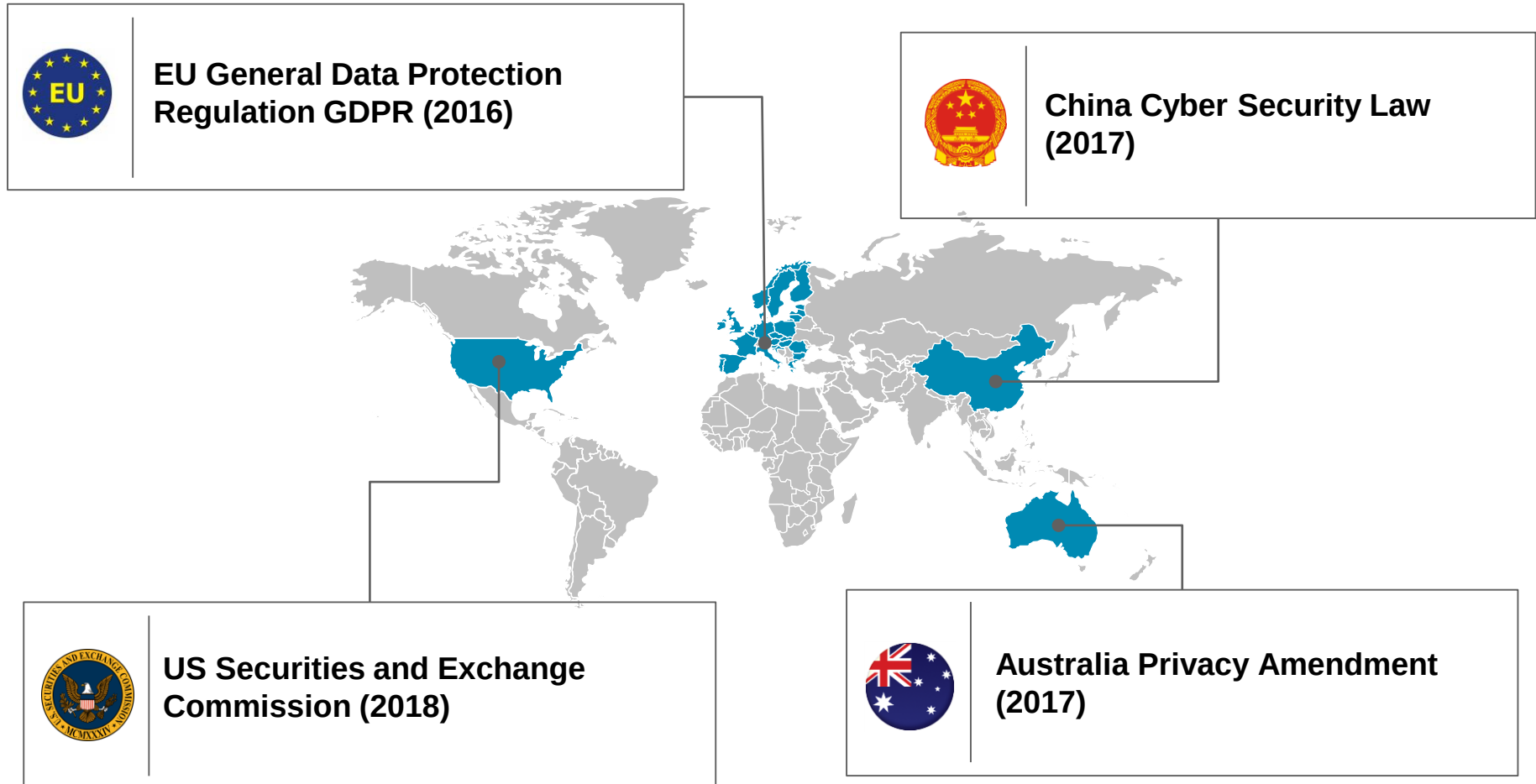


■ % Not at all confident ■ % Confident/very confident
■ % Slightly/moderately confident

Regulatory response

Tightening regulatory requirements for cybersecurity and breach notification are raising the importance of effective cyber risk management

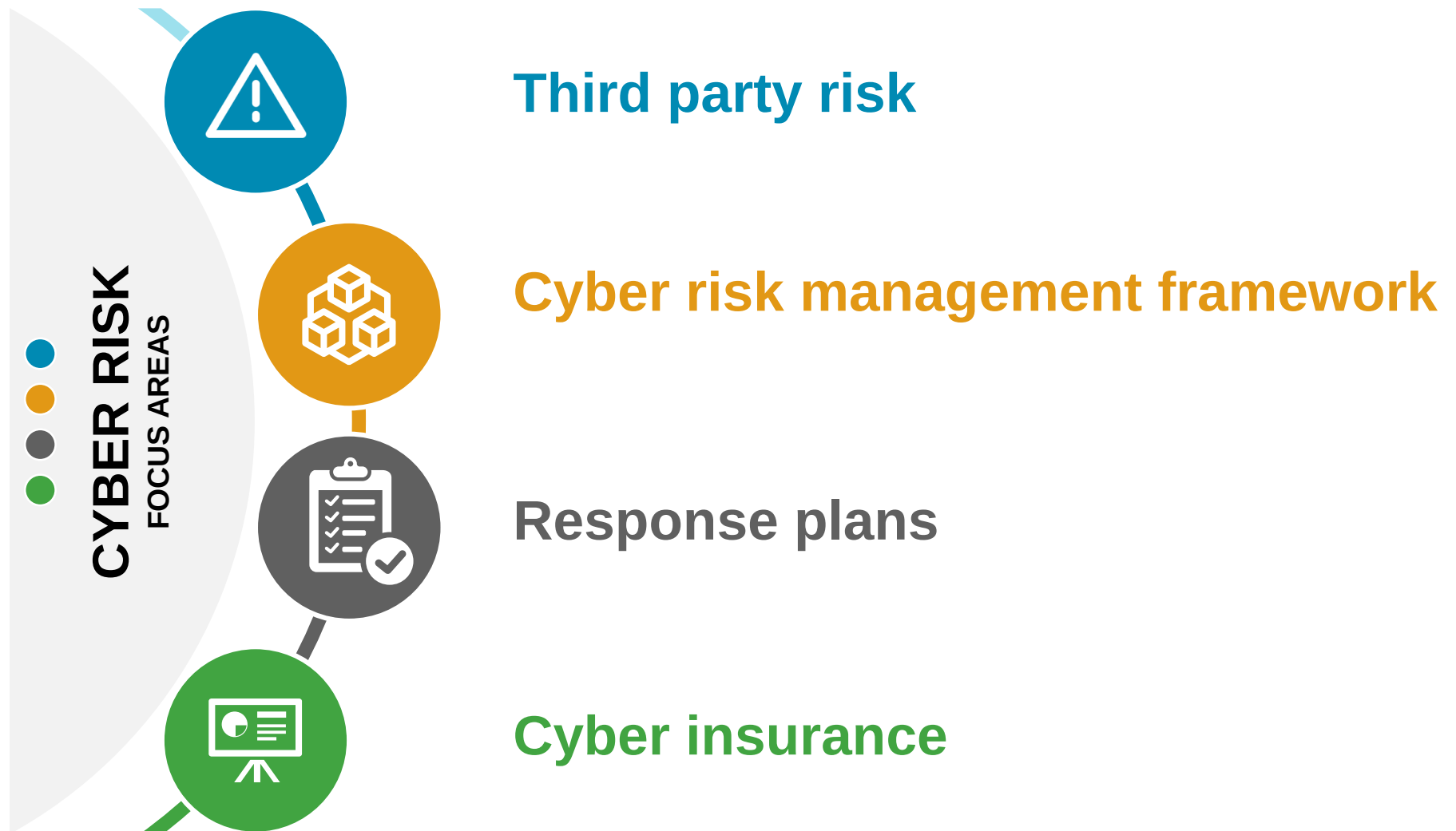
Sample of regulatory requirements for cybersecurity and breach notification



Source: EU General Data Protection Regulation (2018), The Diplomat (2017), Security and Exchange Commission (2018)

Focus areas of cyber risk

With rising impacts of cyber risk, directors are increasingly focused on effective risk management and response to increase cyber resilience



Source: MMC/ WCD; Cyber Risk Management – Response and Recovery (2018)

Third party risk – a growing concern

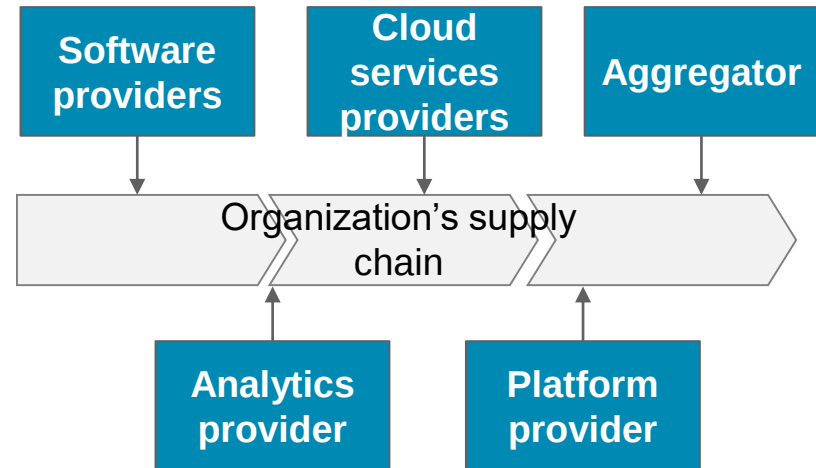
Third parties pose risks beyond an organization's control and increase the focus on IT security throughout the supply chain

Risk assessments on third-party suppliers are not being performed by many organizations



1 in 3
organizations do
not assess the
cyber risk of
vendors and
suppliers

Third parties are increasingly embedded in value chains and their risk exposure should be assessed



“

Much mission-critical data is housed by third-parties and it raises questions about how we can determine whether they are properly managing this information – or even our recourse if the information is mishandled across international borders.

”

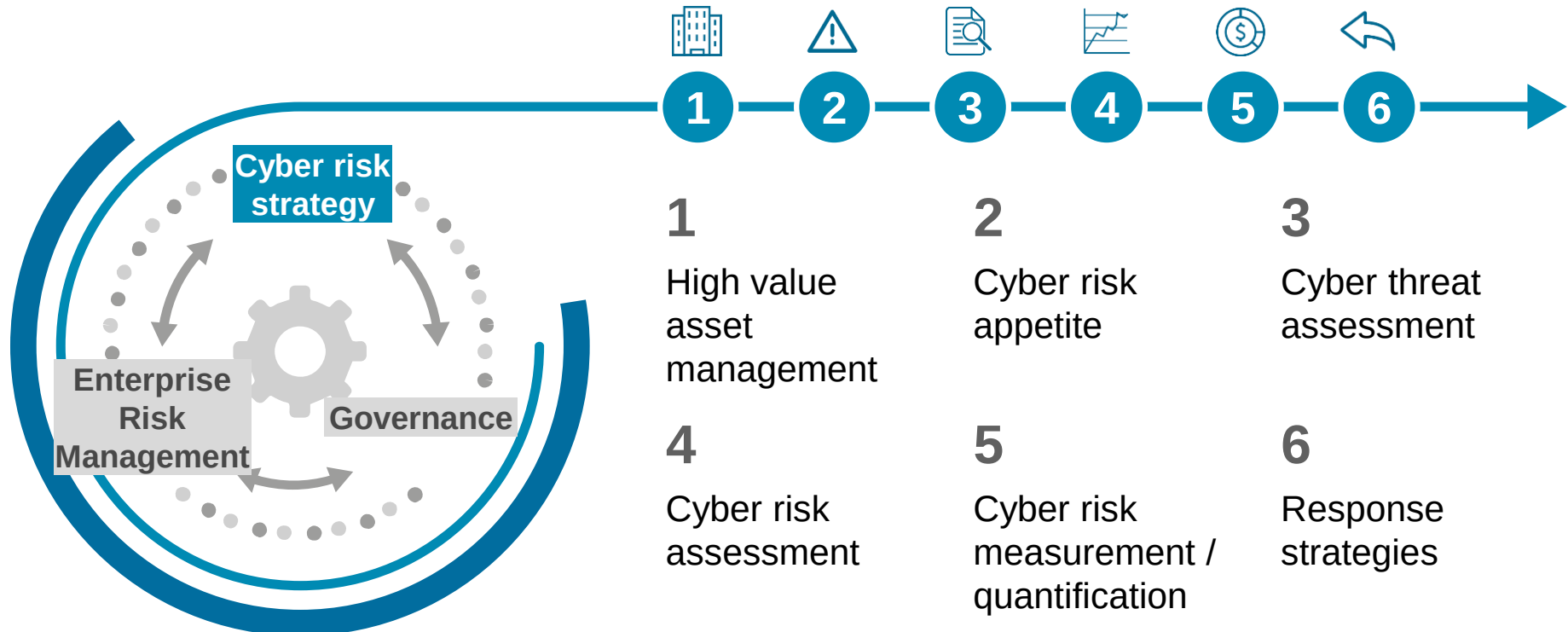
Suzan Bayzait

Co-Chair, Toplum, Gönüllüleri Vakfı

Cyber risk management

A comprehensive cyber risk management framework enables an organization to maximize their return on cyber spending and lower total cost of risk

Focus areas of a comprehensive cyber risk management process



Source: MMC; Cyber Risk Management – Response and Recovery (2018); See also, “Deploying A Cyber Risk Strategy: Five key moves beyond regulatory compliance,” Paul Mee and James Morgan, Oliver Wyman, 2017



A rising focus on response planning

With a recognition of “when” not “if” for cyber-attacks, it is critical for organizations to develop a cyber risk response plan

Many boards need to increase their focus on their organization’s cyber incident response plans

30% of companies have a cyber response plan

60% of boards have reviewed their breach response plan in the last 12 months

Response planning: Three key lessons identified by directors

- 1** Development of preliminary drafts of communications to all stakeholders
- 2** Consideration of legal requirements around timelines to report breaches to minimize financial penalties
- 3** Consideration that normal methods of communications may be casualties of the breach

“

There is a definite trend by boards to think more about preparedness, recovery and resilience because there is an assumption their organizations will be hacked. It is about how soon you can be back up and operating.

”

Catherine Allen

*Director, Synovus Financial Corporation,
El Paso Electric Company, Analytics Pros*

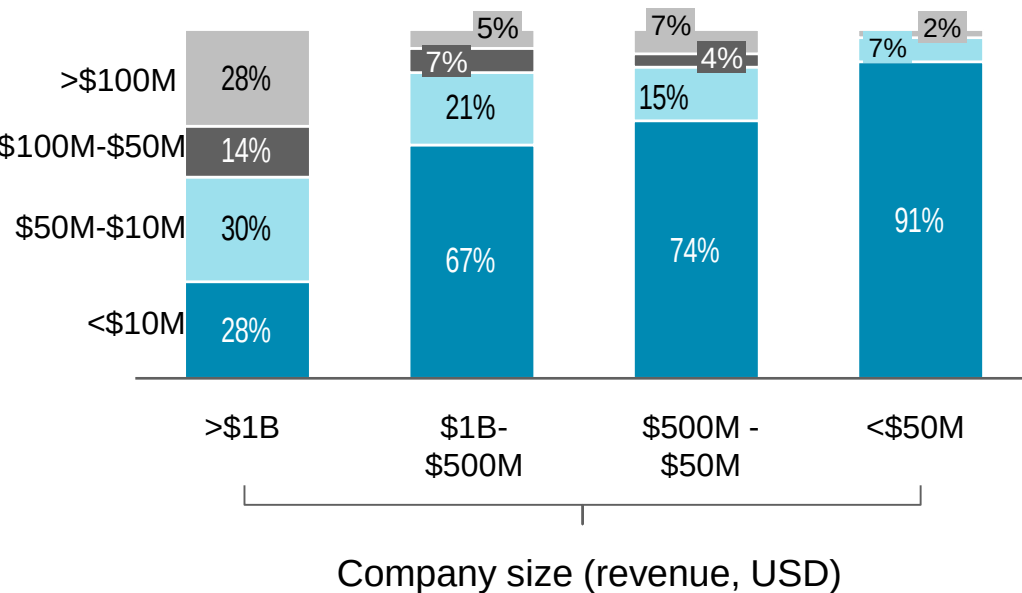


Cyber insurance – a critical element in response and recovery

Cyber insurance is an increasingly important element in limiting an organization's financial damage from costs of cyber attacks

Companies can face significant direct and indirect costs after a cyberattack

Estimated financial impact of a cyber event - % of total



First-party costs and expenses



Business interruption



Theft and extortion



Incident response



Recovery expenses

Third-party liability and defense costs



Breach of privacy



Regulatory fines



Misuse of data



Defamation or slander

Cyber insurance

Insurers are responding to evolving cyber threats and costs by providing expanded standalone coverage options for organizations

TRADITIONAL INSURANCE



Property



Casualty



Crime



Errors & omissions



Kidnap and ransom

Management teams should work with insurance brokers to conduct a comprehensive gap analysis

Insurers are increasingly excluding cyber coverage under existing policies



This places a growing focus on the need and value of standalone policies

STANDALONE CYBER INSURANCE¹



Data confidentiality



Operational technology malfunction



Network outage



Inadvertent disruption of 3rd party system



Deletion or corruption of data



Encryption of data



Cyber Fraud/Theft

Management should undertake a detailed analysis of their digital assets, exposures and overall cyber risk appetite

1. Refer to the appendix for further details on cyber insurance policies
Source: MMC/ WCD; Cyber Risk Management – Response and Recovery (2018)

Path forward

Management should be questioned about their organization's current cyber readiness

Ten questions to ask management about the organization's cyber readiness

- 1 What cyber risk management framework does the organization use to assess and benchmark our approach and risk profile (e.g., NIST)?

 - 2 Given management's assessment of our cyber risks and mitigating procedures, where are our most significant residual vulnerabilities?

 - 3 Where do we rank in cyber preparedness compared to relevant peers and how frequently does management perform cyber scenario testing/war games? How do we benchmark our performance?

 - 4 Which leaders across the organization have accountabilities for cyber risks within IT, functions, business and operational areas, etc.? How do we ensure we have enough resources dedicated to each?

 - 5 How are our business continuity/resiliency plans adapting in response to dynamically evolving cyber threats? For example, what company policy and protections are in place regarding ransomware threats and related payments? Do these plans consider local laws?
-

-
- 6** Have we quantified and assessed the potential financial impact of an interruption caused by a cyber event?
-
- 7** Do we have a dedicated cyber insurance policy, or are we relying on add-on products or blended coverages? What exposures does our cyber insurance coverage address and what risks have we elected not to insure?
-
- 8** What are the limits of liability of cyber insurance that we have available, and how can we determine if they are sufficient?
-
- 9** How often will the board be updated on the status of cyber risk management and cyber insurance coverage, and what will be the format of that report?
-
- 10** How have we compared our cyber insurance program to our fundamental risk profile, as well as to similarly-situated peers in our industry, or those with similar risk/threat profiles?
-

Cyber Risk Quantification Process

Assess cyber risk through a structured scenario approach

Why this approach?

- 1 Organisations lack own historical data
- 2 Threat environment is rapidly changing
- 3 Cyber attack outcomes are not always comparable

Combines quantitative and qualitative techniques focusing on the mechanisms that lead to losses to quantify the potential loss exposure



Step One: Identify Organisation-wide High-value Assets

Business, risk, and information technology personnel should identify assets from all business and functional units (e.g., HR) potentially subject to cyber attacks

List out digital assets and physical assets

Digital Assets

Such as critical data that should be protected or operational services that can be disrupted

Physical Assets

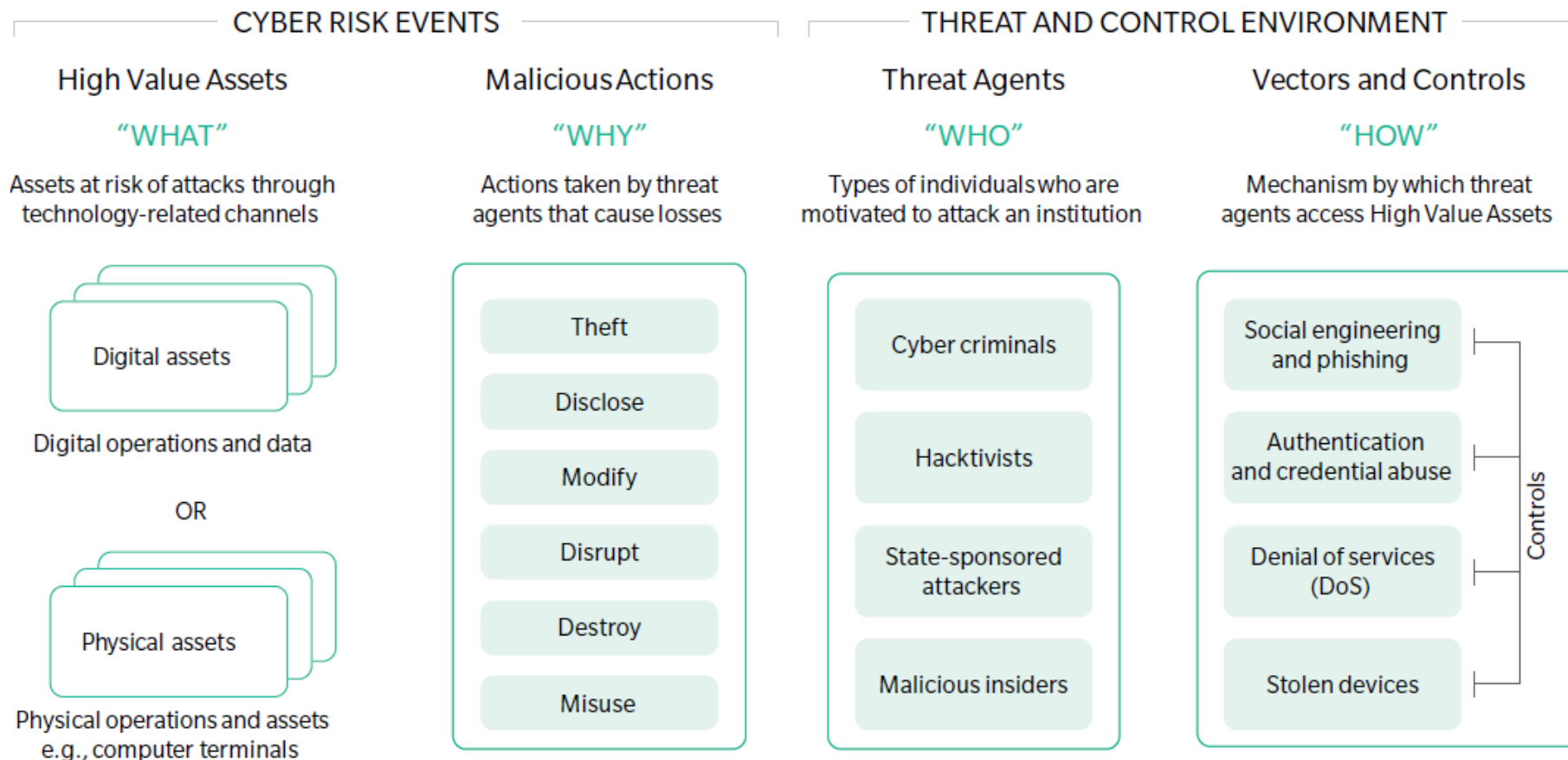
Including computing hardware and connected infrastructure that can be damaged or destroyed

Assess the materiality of each cyber-relevant asset based on inputs from each business and functional unit



Step Two: Identify Risks To High-value Assets

Develop cyber risk scenarios by identifying each potential malicious action to which each high-value asset could be subject



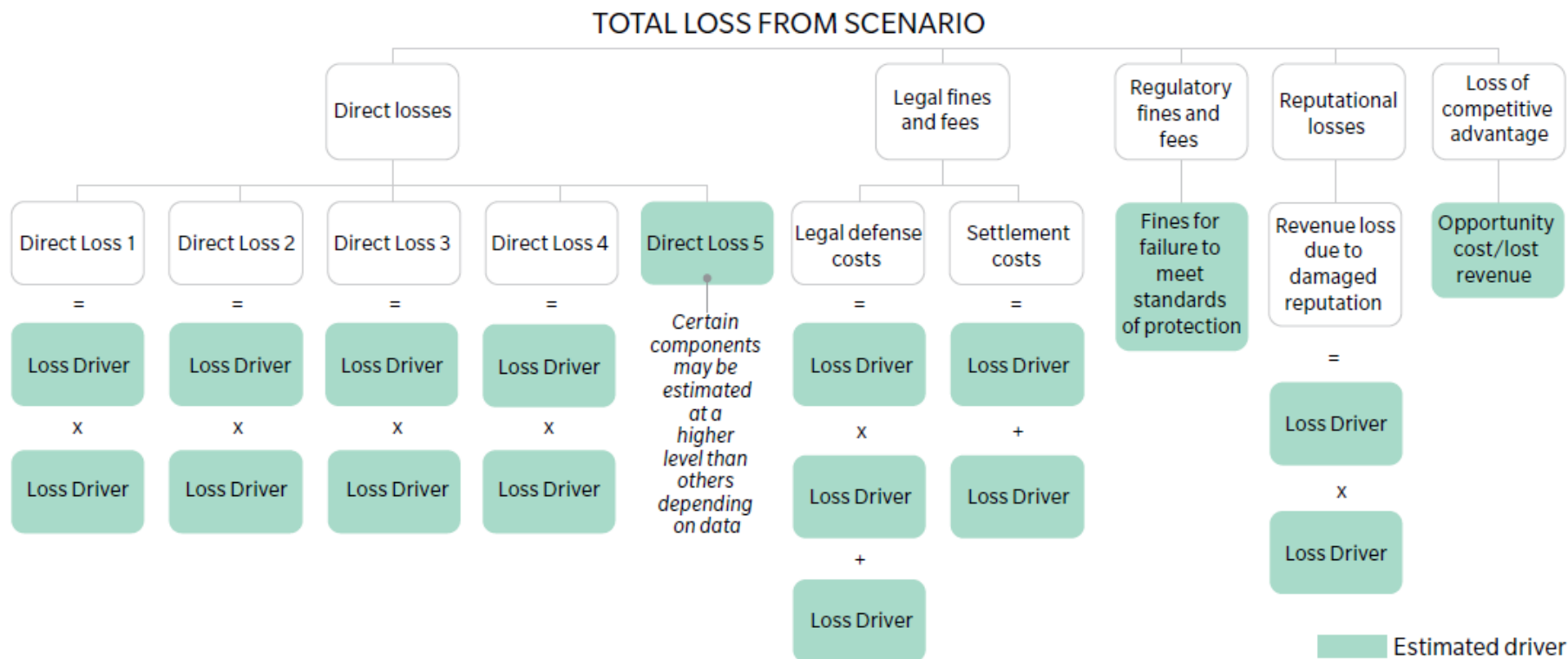
Step Three: Estimate Frequency Of Cyber Risk Events

Hard to estimate

- Industry resources exist to help calculate the frequency of various types of cyber attacks on various sorts of systems in a given time frame
- Expert opinion
- Focus on severity

Step Four: Estimate Severity Of Cyber Risk Events

Discuss scenarios in a series of table-top exercises/workshops with key stakeholders from the business, risk, and information technology units



Managing Risk For Today And Tomorrow

The objective of risk quantification is to use the output to allow for more informed business decisions and improved cyber risk management

RISK MANAGEMENT



Better understand Cyber Risk exposure and the underlying drivers of the losses, and improve response to attacks

INVESTMENTS



Prioritize investments across the Cyber Risk mitigation spectrum and relative to competing investment demands

INSURANCE



Determine Cyber coverage strategy and the nature/extent of premiums

EXECUTIVE OVERSIGHT



Understand Cyber Risk exposure status, trends/outlook and impact of investments over time

Thank you!



Jessica So

DID: +65 6922 8103

Email: jessica.so@marsh.com



Keri Lee

DID: +65 6922 8117

Email: keri.lee@marsh.com



MARSH & MCLENNAN
COMPANIES