MARSH

NAVIGATING THE CYBER SECURITY CONUNDRUM

BUILDING CYBER RESILIENCE

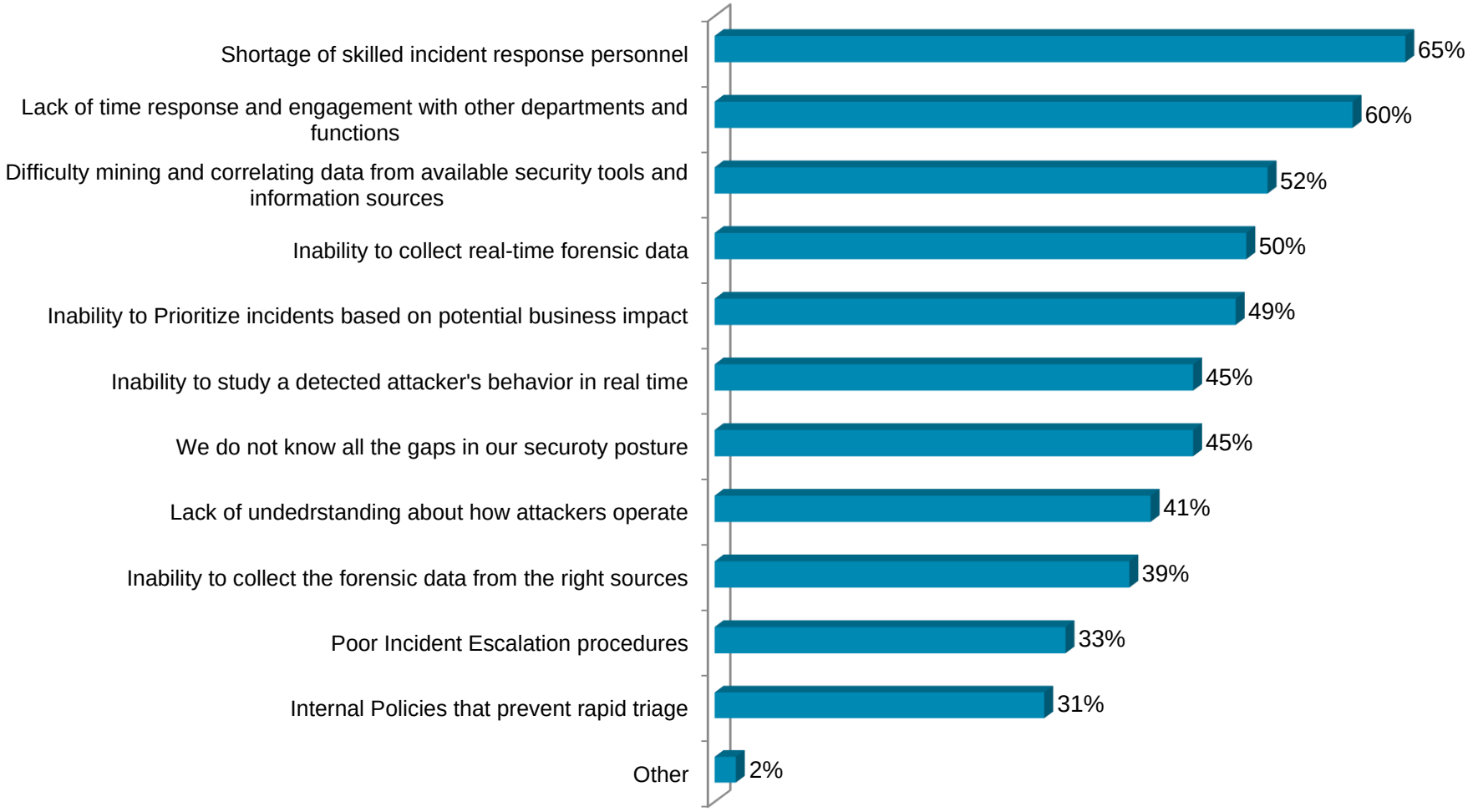
AUGUST 2019

Swabhiman Chhotray
Vice President, Cyber Risk
Marsh Risk Consulting, Asia

27% of healthcare organizations have reported to be a victim of a Cyber Attack in the past 12 months.

- Marsh-Microsoft Global Cyber Risk Perception Survey

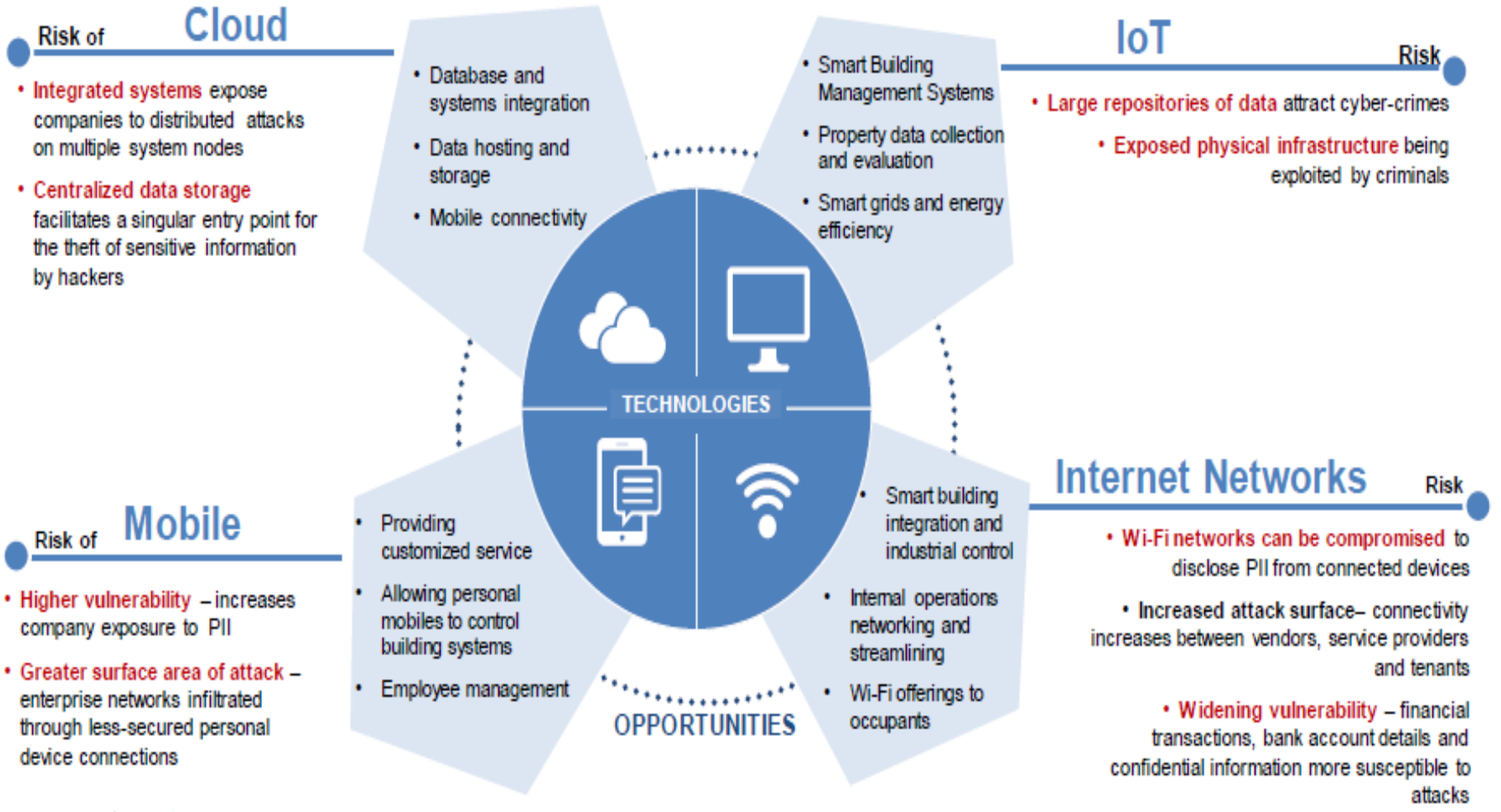
Obstacles to the ability of effectively responding to cyber attacks



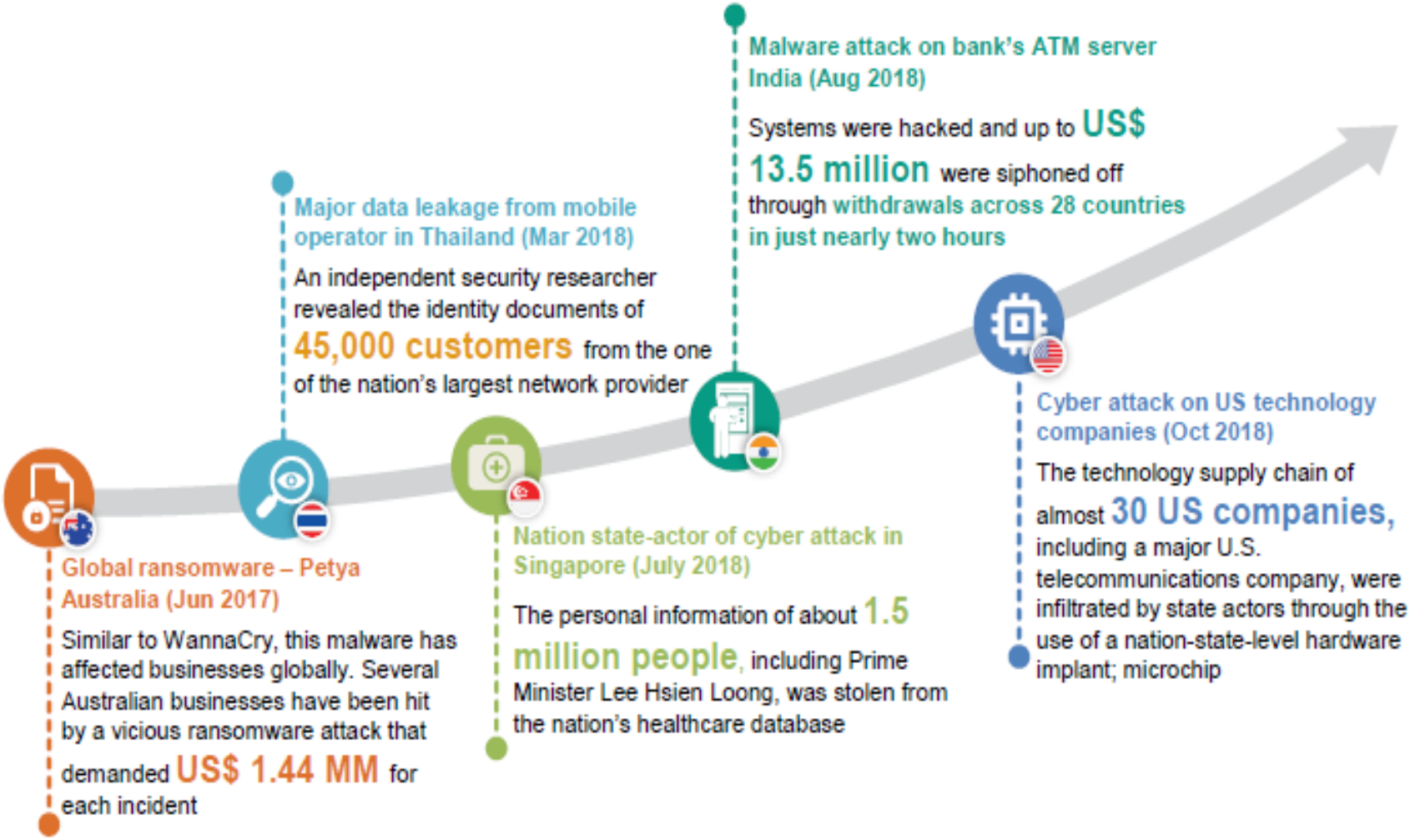
Source : Ponemon Institute

How do we formulate an adaptive framework to manage the Cyber Risk Management Lifecycle ?

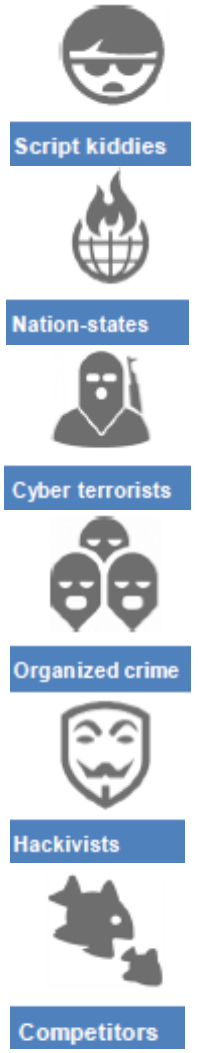
Growing Cyber vulnerabilities in adopting emerging technologies

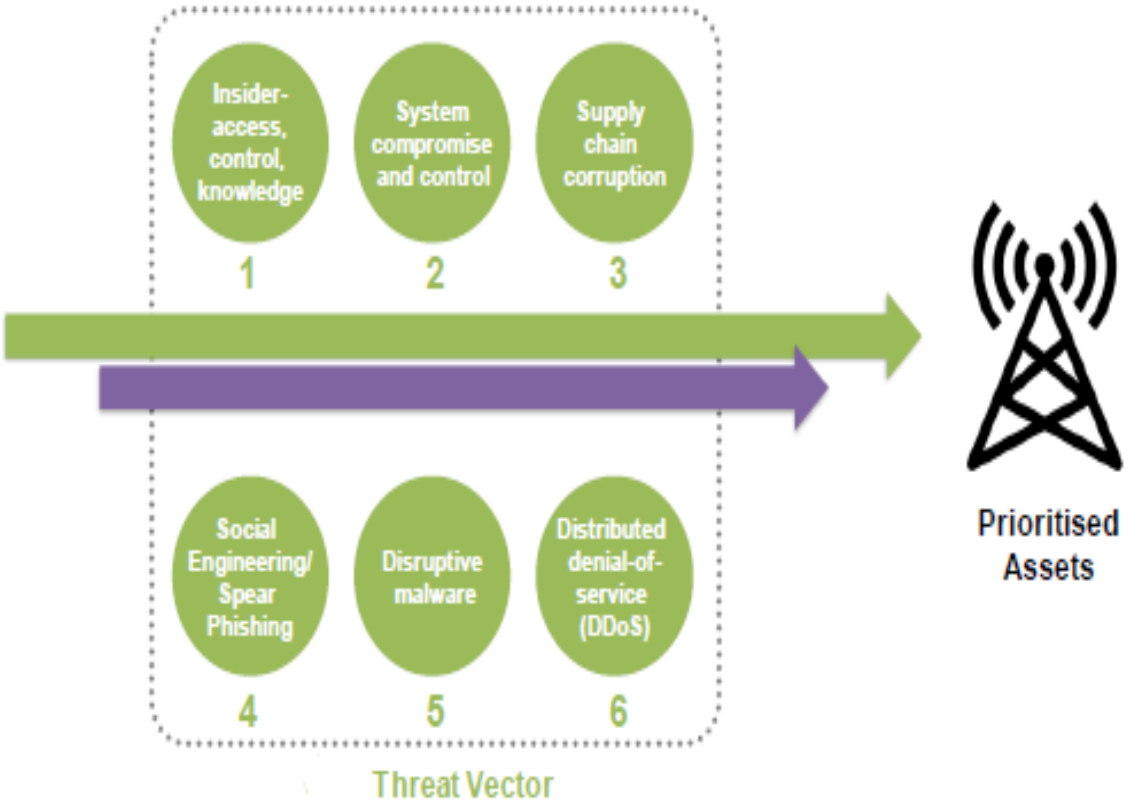


The frequency and materiality of cyber incidents are increasing >4,000 ransomware attacks daily (on average)



Common Threat Vectors





People, Process or Technology?

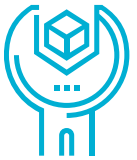
Cyber – A Complex Risk

Multiple stakeholders.

Limited historical data

Rapidly evolving threat landscape

Lack of talent

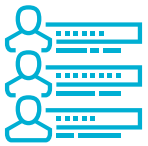


Lack of assimilation into the overall business strategy

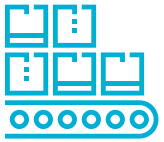
Lack of a common body of knowledge

Foundational Objectives for an organization looking to become resilient

An **in-depth understanding** of processes within the Information Security Function



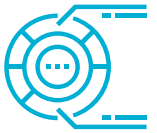
A Cyber Security Aware workforce as a strong 1st line of defense



Testing the **effectiveness of controls**

Identifying gaps in **policy**

Rank findings and potential events by relative likelihood and impact, and determine the residual risk



Identify action items to close gaps

Building Cyber Resilience

Three Strategic Imperatives to achieve Cyber Resilience

1.

KNOW THE THREATS

Grasp The Urgency

2.

KNOW YOURSELF

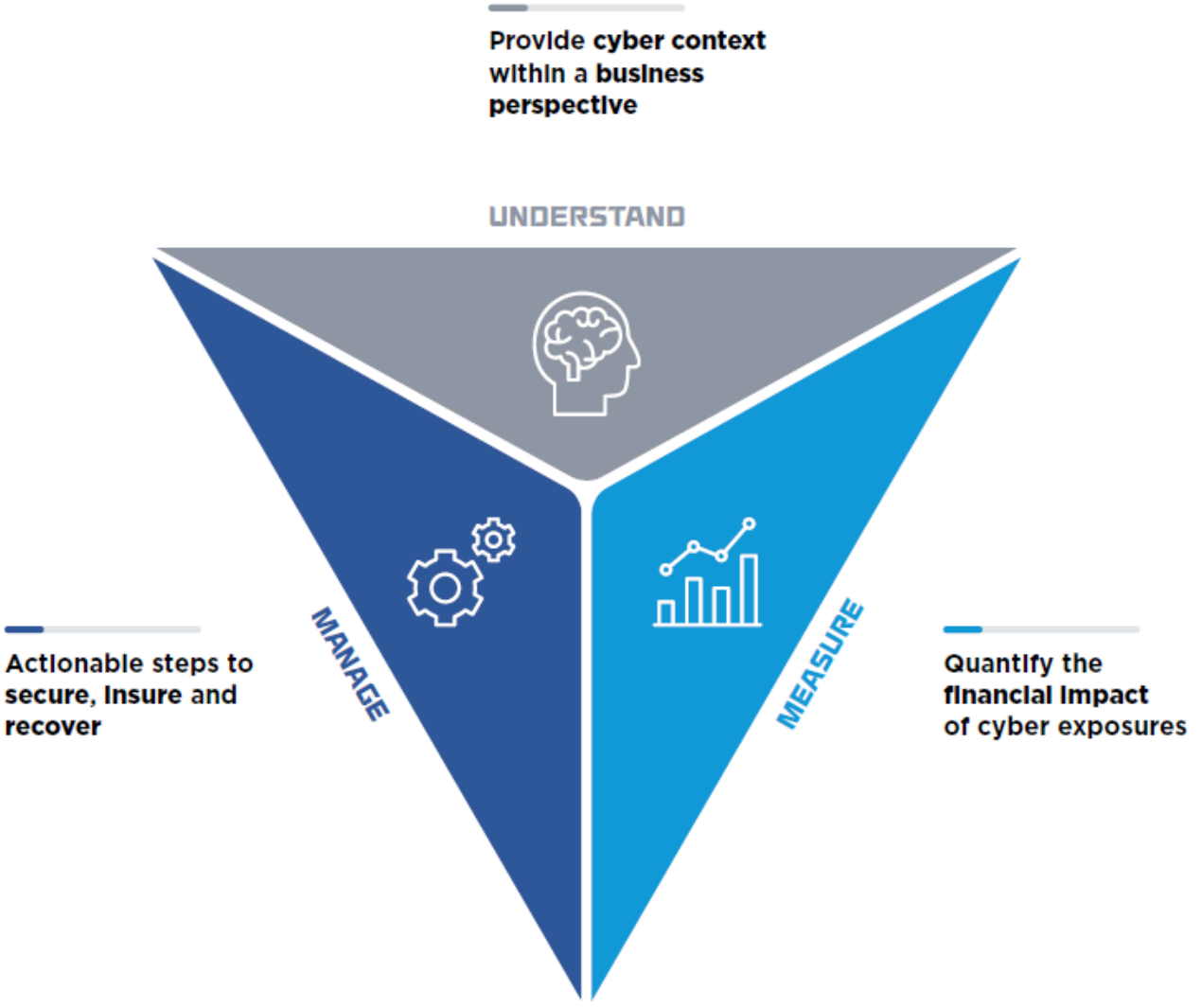
Evaluate Your Position

3.

KNOW WHAT YOU CAN DO

Prepare Your People

How to line up your Defense



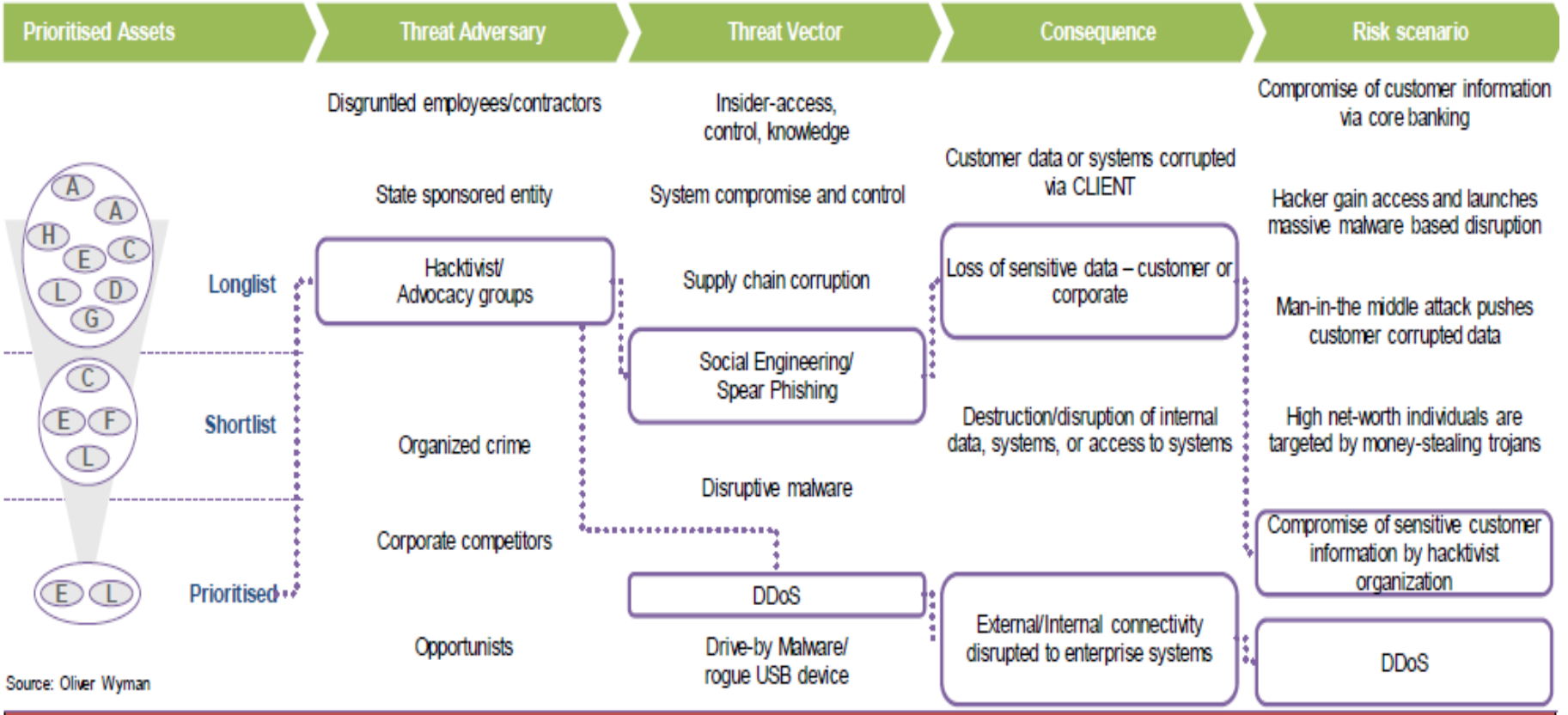
1. Know your Threats - Understand

1. Know Your Threats - Top Cyber Loss Scenarios with the largest perceived potential impact

1. Know your Threats - Cyber calls for more robust defense-and-response strategies which include cross-disciplinary considerations

Example of Risk-centric, inter-disciplinary process

Cyber intelligence & scenario planning



Threat and risk intelligence should feed security operations; risk reporting; cyber response planning; training development; security tech architecture; other cyber investments, and more

2. Know yourself – Understand & Measure

2. Know Yourself - A strategic Cyber Resiliency agenda is necessary to create momentum – this is a continuous journey

A **CYBER RISK STRATEGY**
Consistent view of current and target maturity model across cyber program categories

B **CYBER RISK ASSESSMENT**
Consistent assessment of Cyber Risks based on a comprehensive asset inventory and linked to impact on business outcomes

C **CYBER RISK APPETITE**
Clearly articulated top-of-the-house qualitative statements and quantitative metrics to define acceptable level of Cyber Risk

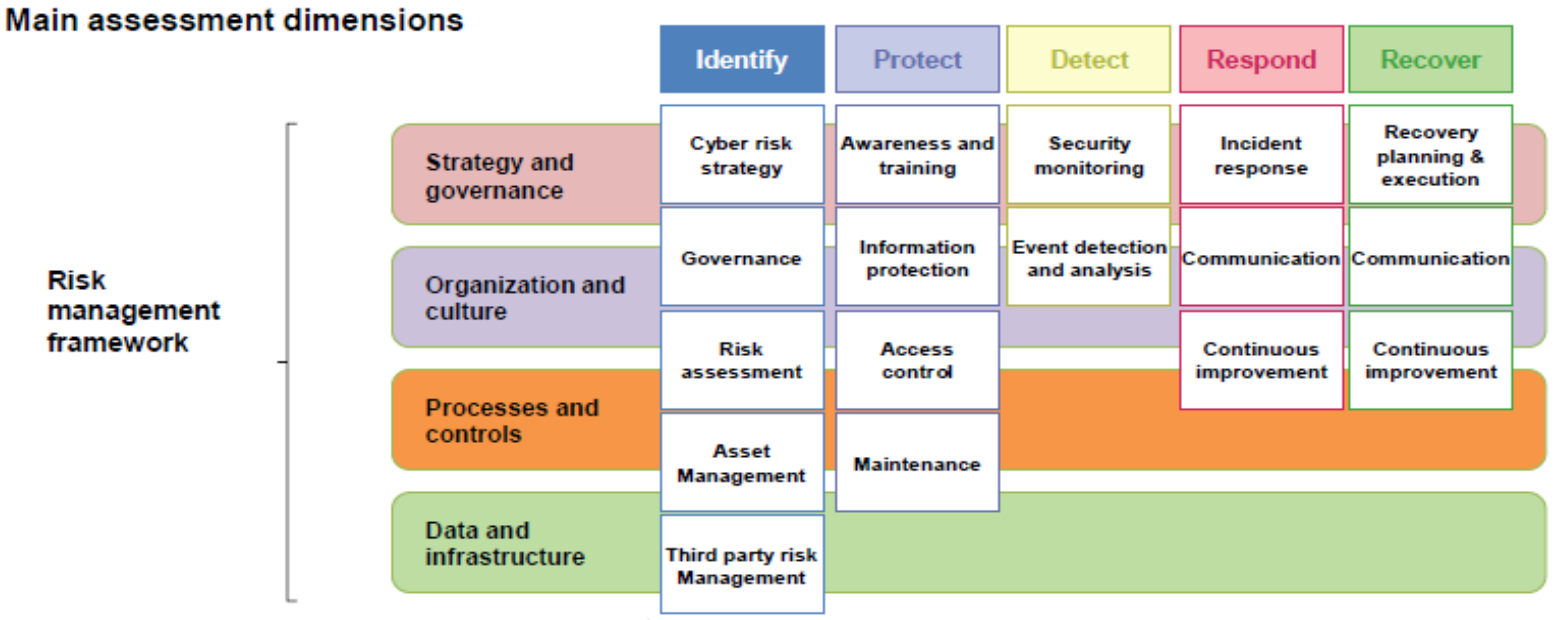
D **CYBER DASHBOARD**
Selection/Cascading of metrics, to enable monitoring, executive communication, and decision-making

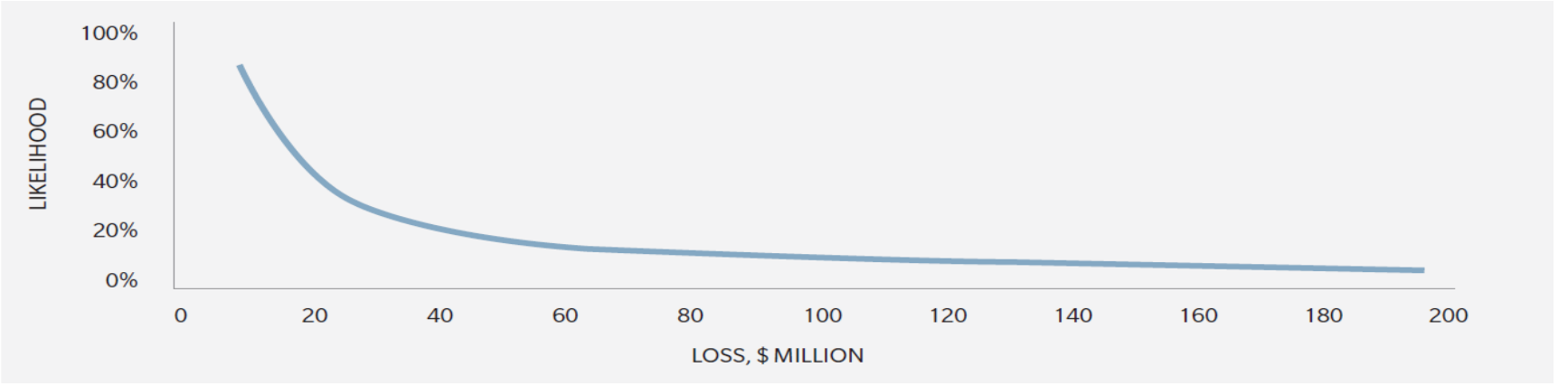
E **CYBER RISK QUANTIFICATION**
Approach to sizing the severity and likelihood of a cyber events or series of events in dollar terms

F **CYBER RISK OPERATING MODEL**
Clearly articulated roles and responsibilities for Cyber Risk management across the organization, its people and suppliers

G **CYBER RESPONSE PLAYBOOKS**
Comprehensive set of response mechanisms and governance for cyber incidents linked to risk identification

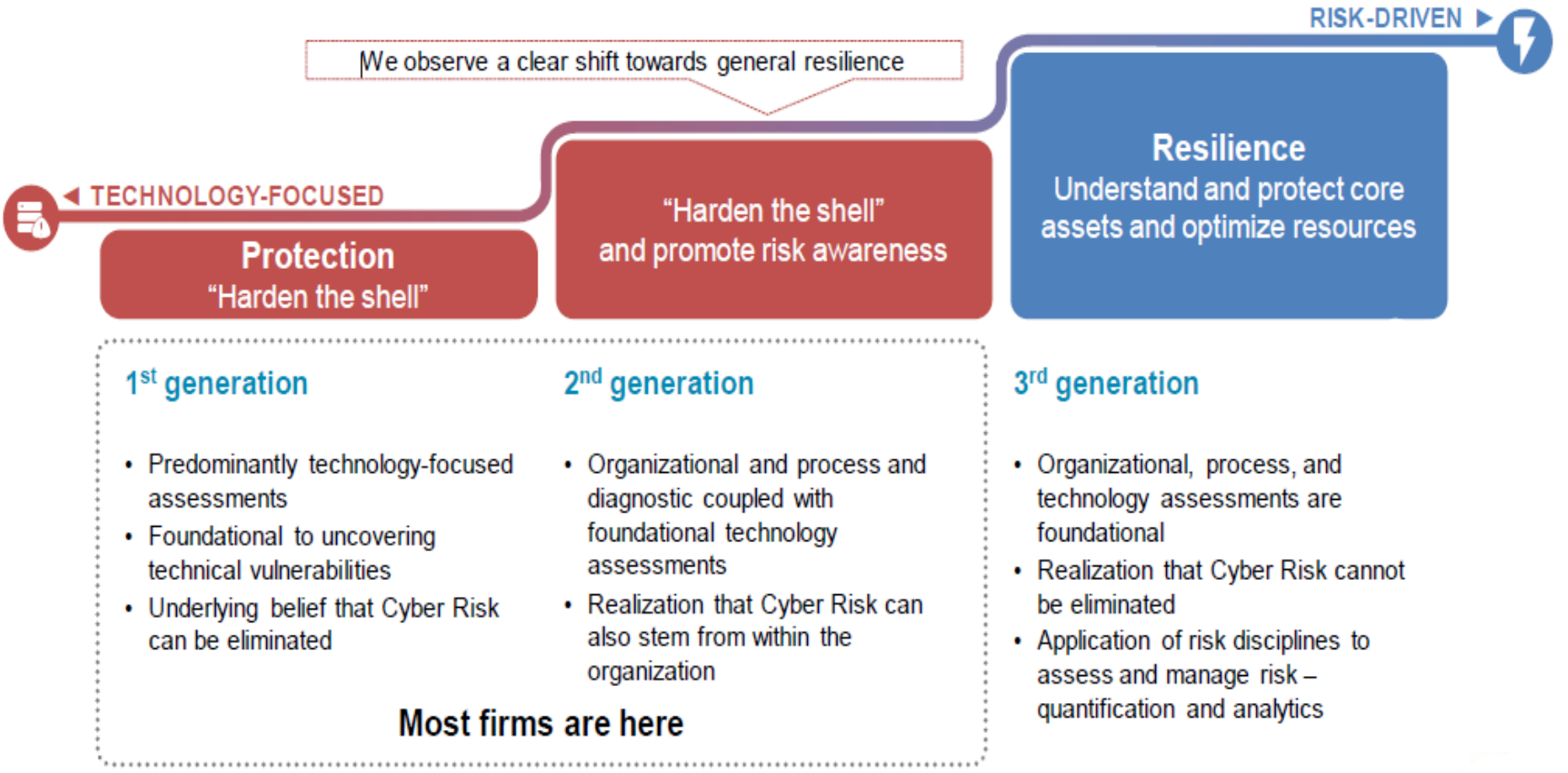
2. Know Yourself - Fact Finding – Main Dimensions for data gathering, Scenario Building and calculating the elusive cyber loss curve





3. Know what you can do - Manage

3. Know what you can do - Shift towards a risk-driven management discipline focuses on reinforcing a Cyber Risk-aware culture



3. Know what you can do – Build a Cyber-Secure culture as no security technology will be against human vulnerability

Key elements to build a Cyber Risk-aware culture

Cyber Resilience
Understand and protect core assets and optimize resources

Influence and promote cyber awareness **from the top-down** to build morale

- ✓ Foster collaboration to discuss and advocate cyber topics
- ✓ Elevate Cyber Risk oversight to visible senior leadership

Conduct **formal cyber trainings**, for all employees, on regular intervals

- ✓ Emphasize the desired cyber behaviours in new hire or other learning events
- ✓ Conduct creative non-traditional cyber learning experiences

Active communication to create accountability and commitments from individuals

- ✓ Address "how does it impact me" questions
- ✓ Offer two-way communication opportunities
- ✓ Connect through multiple channels to reach diverse colleagues

Link desired Cyber Risk behaviour to **performance management process**

- ✓ Distribute Cyber Risk metrics by business units
- ✓ Form team "cyber leader-boards" to foster recognition

3. Know what you can do - Cyber Insurance as a financial safeguard against costs associated with a cyber breach

1st Party Coverage

Digital Asset Rectification
- IT forensic investigations
- Data asset restoration

Business Interruption
- Loss of income
- Additional costs/ extra expense

Extortion
- Ransom payments
- Rewards

Notification Costs
- Call centre, mail, email notification
- Credit monitoring

Public Relations
- PR firm costs associated with the breach

3rd Party Coverage

Privacy & Data Breach
- Legal costs associated with losing personally identifiable/ corporate info

Network Liability
- Legal actions from spreading virus transferred from your infected network

Defence Costs
- Legal and regulatory advice costs

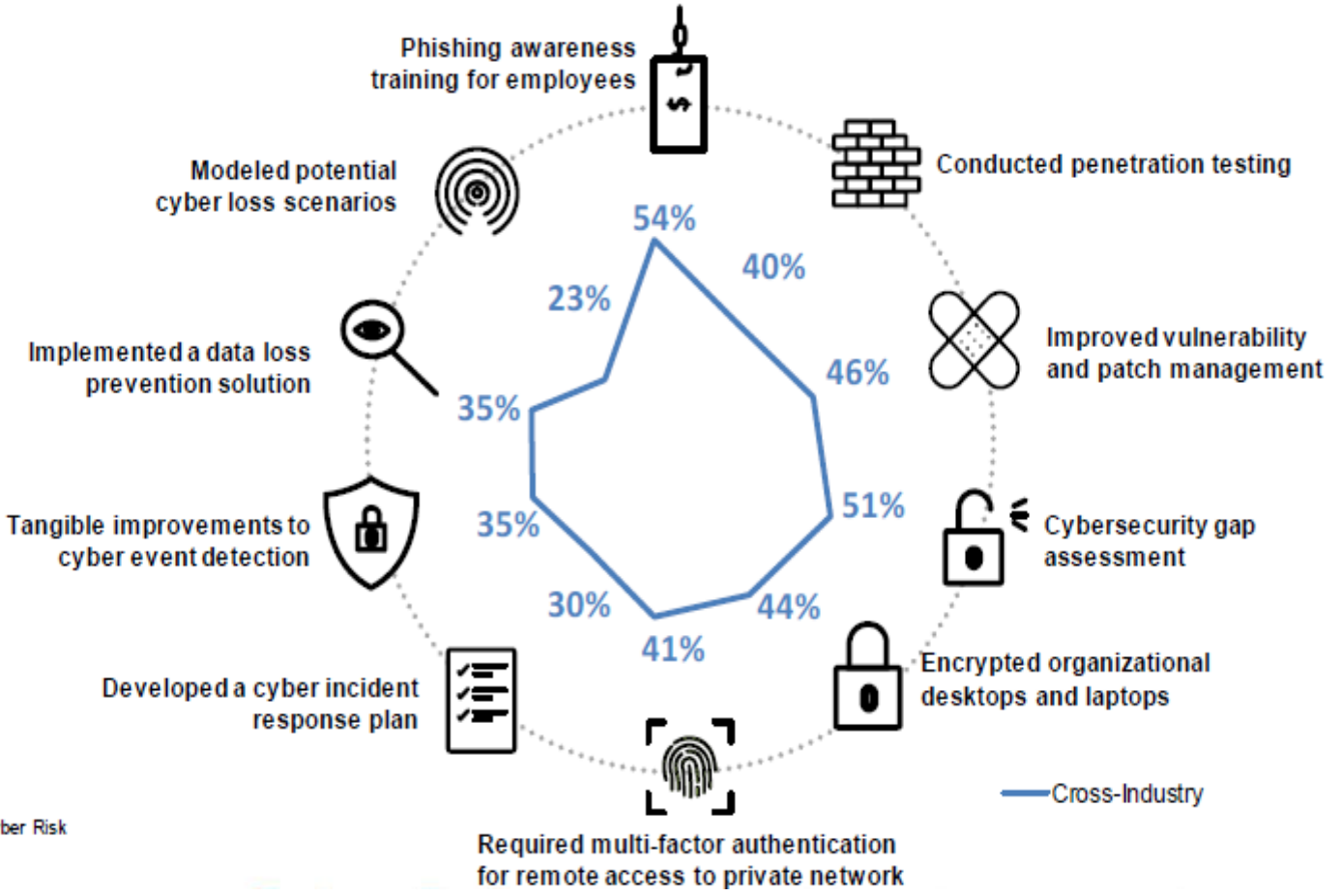
Damages
- Damages and settlements

Regulatory Fines
- Investigation costs
- Fines and penalties

Source: Marsh

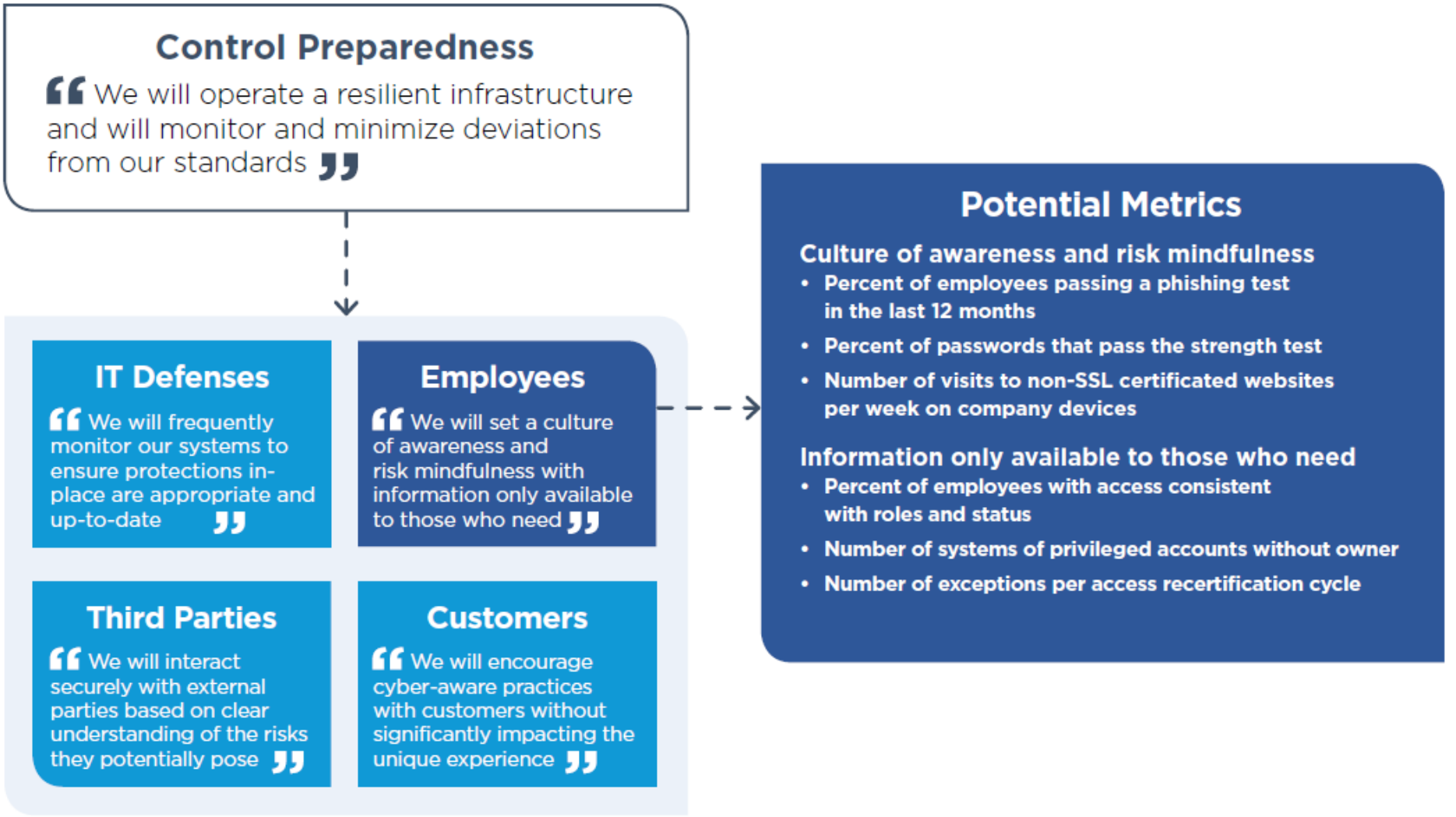
3. Know what you can do - Organizations across industry are making rapid progress in strengthening Cyber Resilience

Top 10 cyber risk-related actions taken by companies in the past 12–24 months



Source: Marsh Microsoft Global Cyber Risk Perception Survey 2017

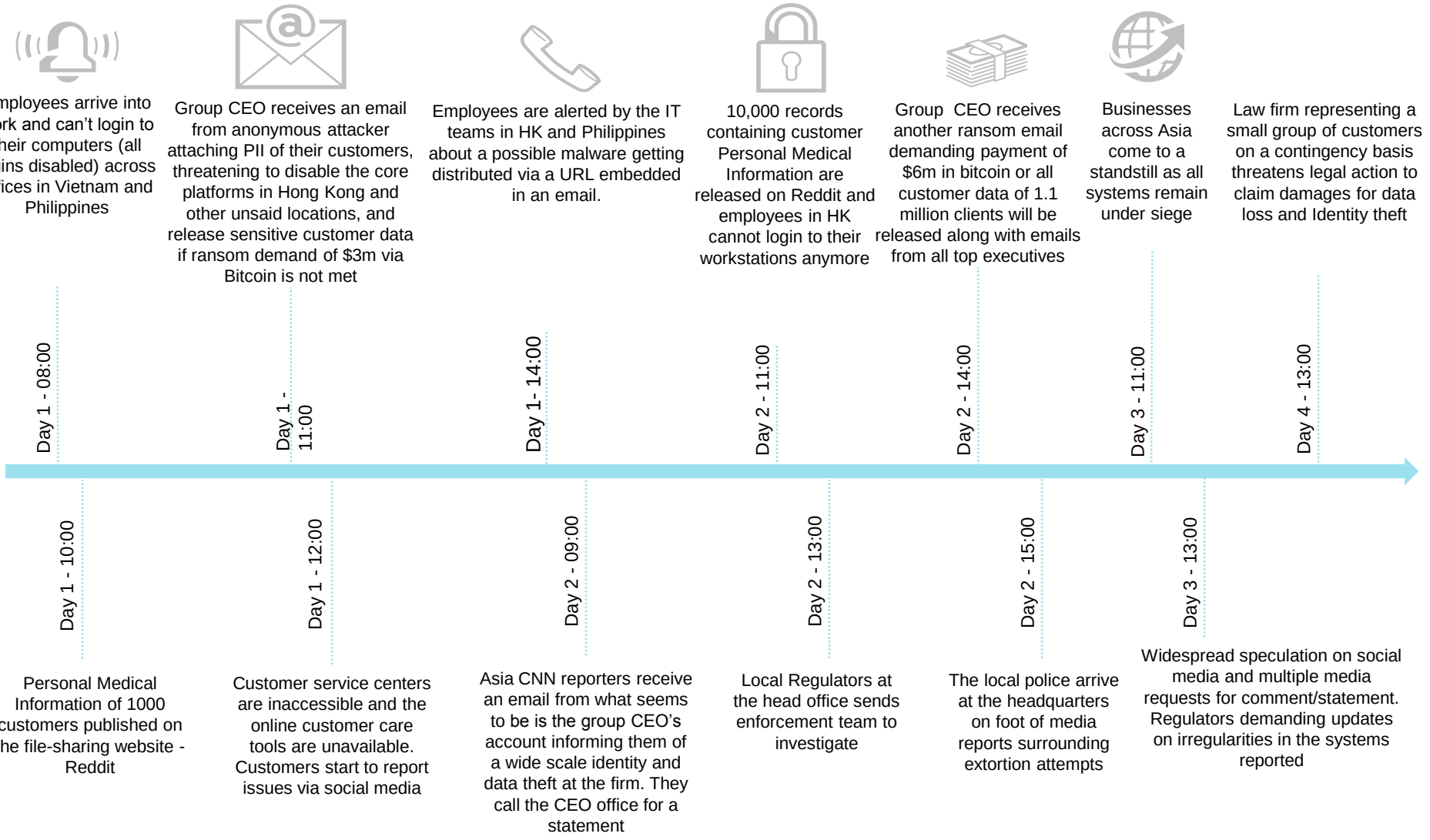
Cyber Resilience – A vision to help you with your mission



Stories

Lessons learnt the hard way

Destructive Malware spreads through unpatched servers causing outages and holding systems hostage



Investigating suspicious network activity

Background

Users of a large pharmaceutical company ABC complained of their screens freezing for times longer than usual. The network infrastructure team examined the situation and dismissed it as a bandwidth problem. But with more and more complains ABC's Information Security team became uncertain of the situation.

Objective

- Indicators of attack
- Indicators of compromise
- Potential policy violations
- Provide a status letter providing details of any qualifying indicators of compromise and other risks that have been identified

What we did – Tools and Methods

- Compared the traffic to signatures of known Indicators of Attack (IOAs), Indicators of Compromise (IOCs) and policy violations
- Processed all files with no known signature in a secure sandbox environment to determine whether they contain polymorphic malware or 0-day exploit code
- Performed statistical and behavioural analysis on the full traffic capture to locate instances of mass data exfiltration or legitimate seeming logins using stolen credentials
- Monitored endpoints activities, identify compromised systems and performing live forensic analysis of the infected machines

Network based

Installation of one (or more) appliance in order to monitor incoming and outgoing traffic

Host based

Deployment of agents on computers to detect suspicious activity on endpoints

Hybrid approach

Deployment of both network-based and host-based tools to monitor suspicious activity within the environment

From Aspiration to a call for Action

“In our current state of Cyber Security breaches are inevitable “

- The question is not whether you will be breached but how you will respond when there is a breach.

- Through a discussion of technical controls, compliance, and the financial impacts of cyber risks, more effective decisions on future cyber security investments can help mitigate cyber threats.

- Future progress depends on internal investments toward shaping mindsets and culture, strengthening technical expertise and managing human capital.

Thank You