MARSH OLIVER WYMAN

CYBER RESILIENCE FOR THE ENERGY SECTOR
US ENERGY ASSOCIATION PUBLIC BRIEFING

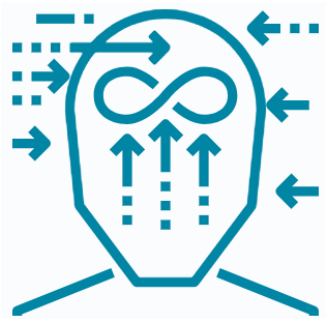
SEPTEMBER 27, 2018

Presented by: Paul Mee and Matthew McCabe

MARSH & McLENNAN COMPANIES

Three strategic imperatives to achieve cyber resilience

Assume you will be breached



Understand your position and prepare

Develop the right partnerships

Section I

ASSUME YOU WILL BE BREACHED

In our interconnected and digitized world, cyber risk is increasing and evolving rapidly

Drivers of increased cyber risk

Digitized world
Our lives are becoming more digitized every day

Pace of innovation
Companies are innovating more and more rapidly

Technology complexity
Technology is getting more intelligent, sophisticated, and pervasive

Data sharing and interchange
Growing interconnectedness combined with massive increase in velocity, volume, and variety of data

Attack sophistication
Actors are increasingly organized, sophisticated, and devious

The key components of cyber risk

Threat

- **Actor:** Nation-state sponsored, hacktivists, cyber criminals, insiders
- **Motivation:** Theft, disruption, destruction
- **Means:** Technical/electronic e.g. zero-day exploit, DDOS, or process/human, e.g. social engineering, phishing)

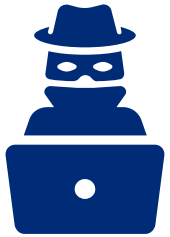
Vulnerability

- **Workers:** e.g. control systems access
- **IT defenses:** e.g. application security
- **Customers:** e.g. password handling
- **Third-parties:** e.g. data transfer

Impact

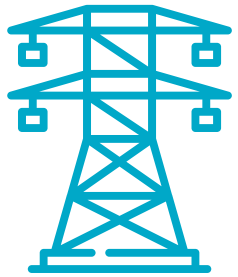
Breach of…

- **Confidentiality:** Disclosure or misuse of information
- **Integrity:** Modification, deletion or misuse assets
- **Availability:** Disruption of an entity's ability to perform its operations

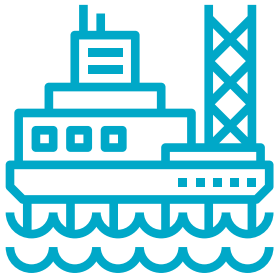


Possibility of a **negative impact** due to a **threat driven by malicious intention** focused on **exploiting vulnerabilities** in processes that leverage technology

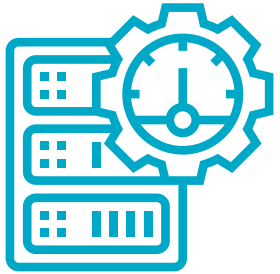
The energy sector attack surface is growing due to digitization



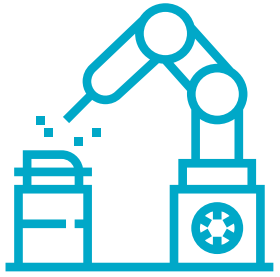
Electric transmission companies depend on automated controls to run their networks



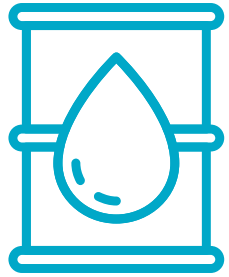
Oil and gas companies depend on data networks to manage facilities and interpret operating conditions



Utilities rely on data networks to manage the grid and to analyze their customers' needs



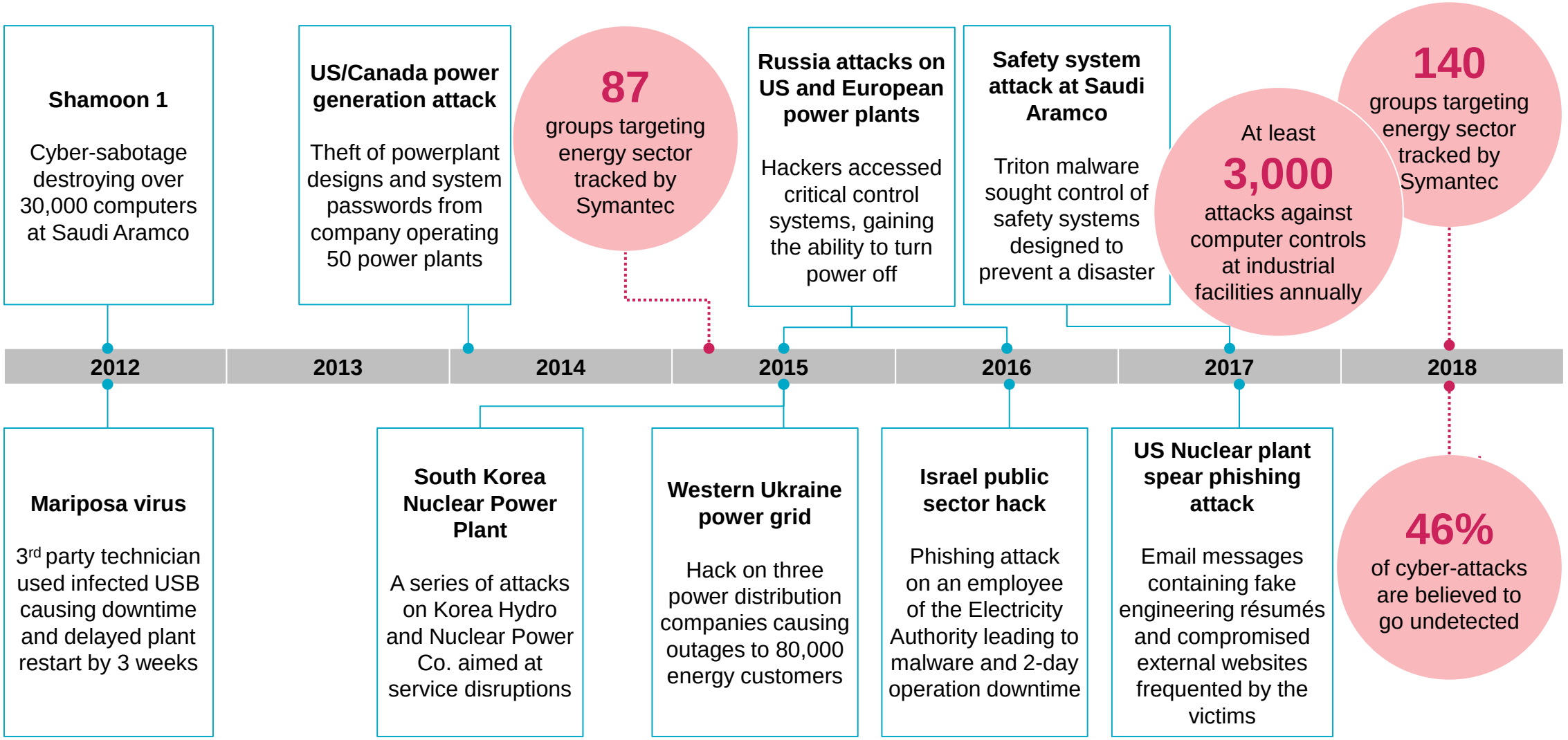
Upstream companies use digital technologies for reservoir modelling, drilling resource dispatching, production optimization and others



Downstream companies use supply-demand matching smart grids and new approaches to networking operational systems

Source: World Energy Perspectives: the Road to Resilience, MMC and Swiss Re (2016)

The frequency and materiality of cyber incidents is increasing



Sources: The State of Cybersecurity in the Oil & Gas Industry: United States Sponsored by Siemens, independently conducted by Ponemon Institute LLC (2017); Cyber Attacks And The Energy Sector, Navigant Consulting, Inc. (2017); Five months after energy cyber attack, U.S. pushes collaboration, World Oil (2018)

The impact of cyber-attacks can be significant

NotPetya

Encrypted computer files then demanded **$300 Bitcoin ransom** – but ransom feature not functional, effectively disabling data.

- June 27, 2017: "NotPetya" malware hits Ukraine government and businesses, exploiting vulnerability in an OS
- Similar to earlier ransomware "WannaCry" – But more lateral, moving across networks and **capturing passwords and administrator rights**
- Serious disruptions to government systems, critical infrastructure and multiple global businesses, resulting in over **$1 billion aggregate losses**

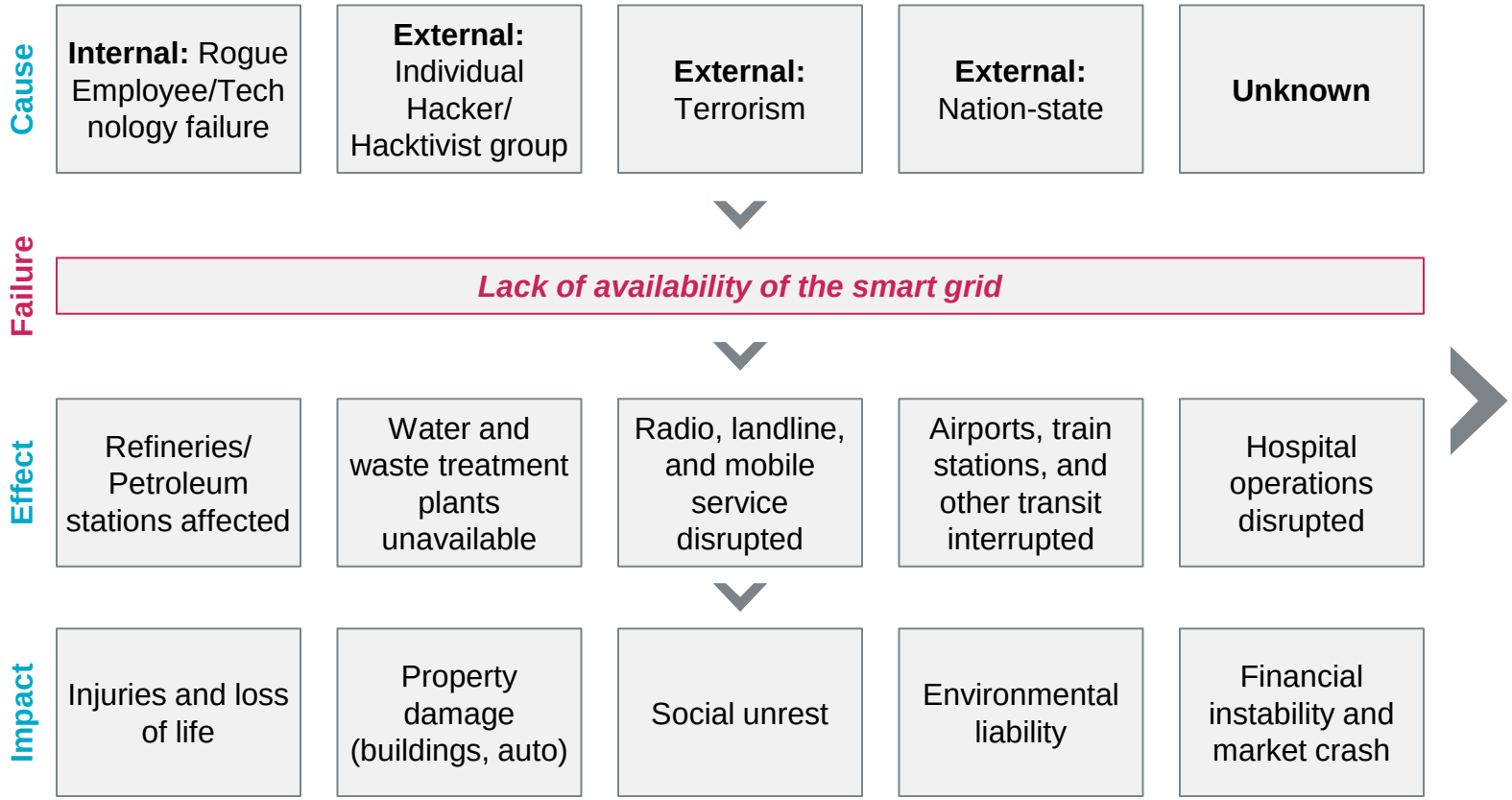
Losses Revenues

Reckitt Benckiser	Mondelēz International	MAERSK	FedEx	SAINT-GOBAIN	MERCK
$142 MM ($13.4 BN, 2016)	**$188 MM** ($25.9 BN, 2017)	**$250 MM+** ($30.9 BN, 2017)	**$300 MM** ($60.3 BN, 2017)	**$387 MM** ($51.9 BN, 2016)	**$600 MM+** ($39.8 BN, 2016)

Note: All loss data is from public sources. Logos link to relevant financial filings and articles

Cyber risks can be catastrophic

The failure of the smart grid



Lloyd's estimates a cyber blackout could cost up to

$71 BN

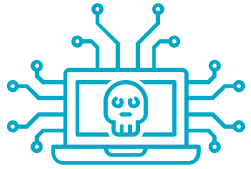
to insurers and up to

$1 TN

to the broader economy

Source: WEF Mitigating Risks in the Innovation Economy report (2017); Lloyd's Emerging Risk Report (2015); In this scenario, Power is restored to some areas within 24h, while others remain without electricity for weeks as the blackout plunges 15 US states into darkness and leaves 93 mm people without power

A perfect storm of cyber risk threatens the energy sector



Conflict in cyberspace, including nation state activity, continues to shift from reconnaissance to operational disruption

The rapid adoption of technology for control and monitoring increasingly opens the door to vulnerabilities

Even with the recent increase in spending and coordination, industry still cannot fend off the most sophisticated and persistent threats

Without pivoting to a stronger strategy to address this complex cyber threat, the United States could experience catastrophic consequences within the next decade.

- Matt McCabe, Cyber Risk Adviser, Marsh

Source: Marsh

Section II

UNDERSTAND YOUR POSITION AND PREPAREDNESS

Energy organizations need to be cyber resilient

Cyber-related strategic objectives

Ensure cyber risk is **comprehensively managed** across the organization and **elevated to the Board**

Monitor threat landscape and cyber risk exposure status

Be prepared to **respond quickly** and in a structured way to a cyber attack

Prioritize investments across the cyber risk mitigation spectrum and relative to other investment demands

Understand cyber risk exposure and the underlying drivers of losses

Determine **cyber insurance coverage** strategy and the nature/extent of premiums

A strategic cyber resiliency agenda

1 CYBER RISK STRATEGY

Consistent view of current and target maturity model across cyber program categories

2 CYBER RISK ASSESSMENT

Consistent assessment of cyber risks based on a comprehensive asset inventory and linked to impact on business outcomes

3 CYBER RISK APPETITE

Clearly articulated top-of-the-house qualitative statements and quantitative metrics to define acceptable level of cyber risk

4 CYBER DASHBOARD

Selection/Cascading of metrics, to enable monitoring, executive communication, and decision-making

5 CYBER RISK QUANTIFICATION

Approach to sizing the severity and likelihood of a cyber events or series of events in dollar terms

6 CYBER RISK OPERATING MODEL

Clearly articulated roles and responsibilities for cyber risk management across the organization, its people and suppliers

7 CYBER RISK PLAYBOOKS

Comprehensive set of response mechanisms and governance for cyber incidents linked to risk identification

The following pages focus on a subset of these elements

2 Cyber risk assessment

Cyber heat-map example

Function	Category	Documentation	Oversight and Org'	Process	Infrastructure	Overall
I. Identify	A. Cyber risk strategy	3	3	3		3
	B. Governance	1	2	3	1	2
	C. Risk assessment	2	2	3	3	2
	D. Asset management	2	2	1	1	1
	E. Third party risk management	3	2	2	2	2
II. Protect	A. Access control	3	2	2	1	2
	B. Awareness and training	3	3	3	3	3
	C. Information protection	2	2	4	3	3
	D. Maintenance	3	3	3	3	3
III. Detect	A. Security monitoring	2	3	5	4	4
	B. Event detection and analysis	2	2	5	4	3
IV. Respond	A. Incident Response	2	3	5	3	3
	B. Communications	2	3	3		3
	C. Continuous Improvement	1	3	2		2
V. Recover	A. Recovery planning and execution	2	2	2	2	2
	B. Communications	1	3	3		2
	C. Continuous improvement	3	3	3		3

Not applicable Lagging practice 1 2 3 4 5 Leading practice

Aggregate output
The heat-map summarizes the assessment output for each category and risk management framework component

Rating
The scoring indicates a maturity level which is linked to detailed criteria in the assessment catalogue

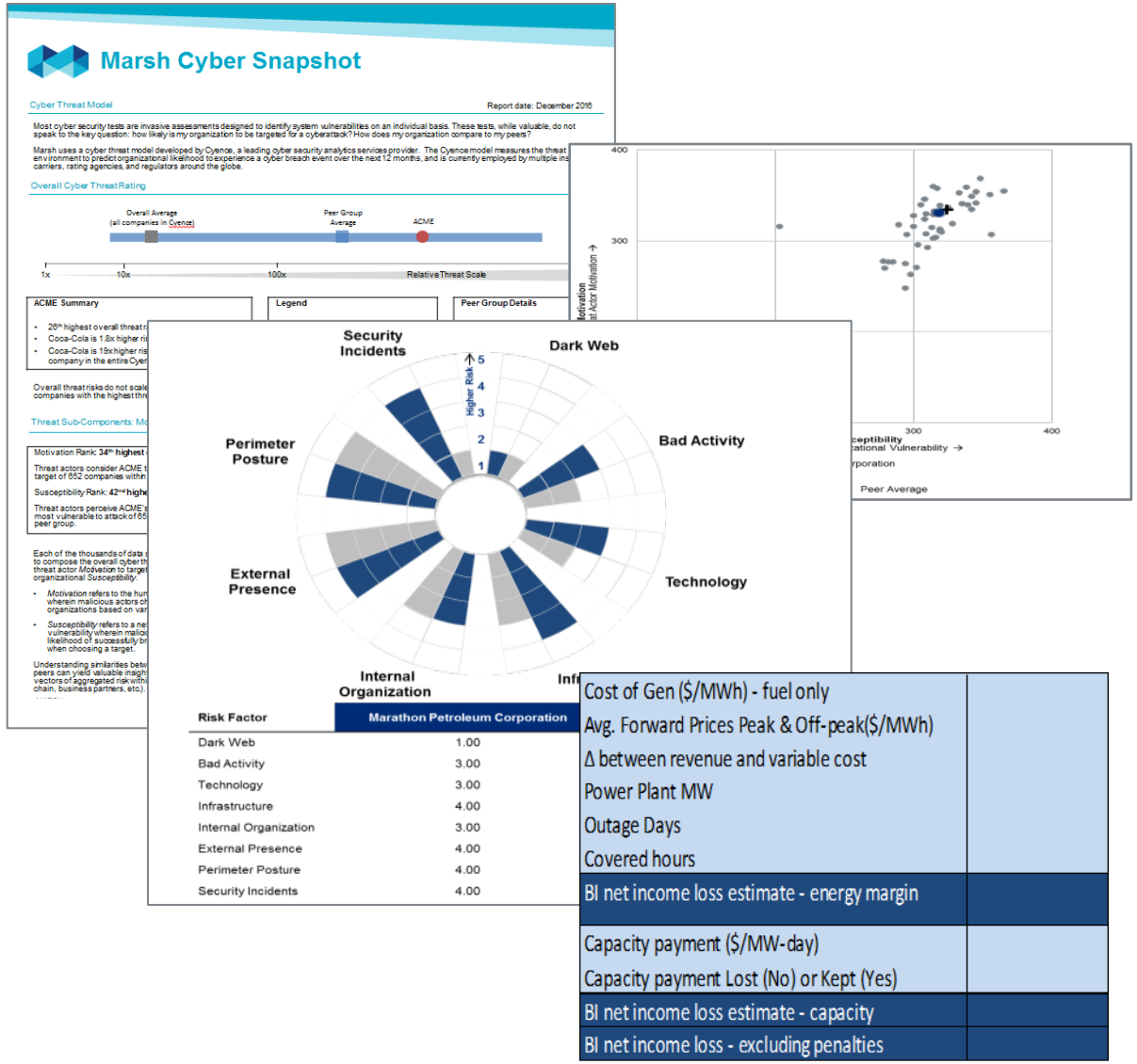
Fact-base fully supports the assessment
For each aggregate score detailed evidence is gathered and fact-based observations are made

1 – Lagging	2	3 – Developing	4	5 – Leading
Behind standard observed practice		*In line with standard observed practice*		*"Best of breed" among large organizations*

2 Cyber analytics

Use cyber threat analytics to understand posture relative to peers

- Identify cyber risks germane to your organization
- Model the threats and your susceptibility
- Understand the motivation of bad actors
- Benchmark against peers
- **Understand the potential impact**
  - Scenarios may be industry or company specific
  - Considers factors related to power outage, including impact on revenue, net fuel, or energy margin basis
  - May also consider megawatt capability analysis, capacity payments, peak vs off peak, and other sector specific analysis



2 SEC guidance on assessing impact of a cyber incident

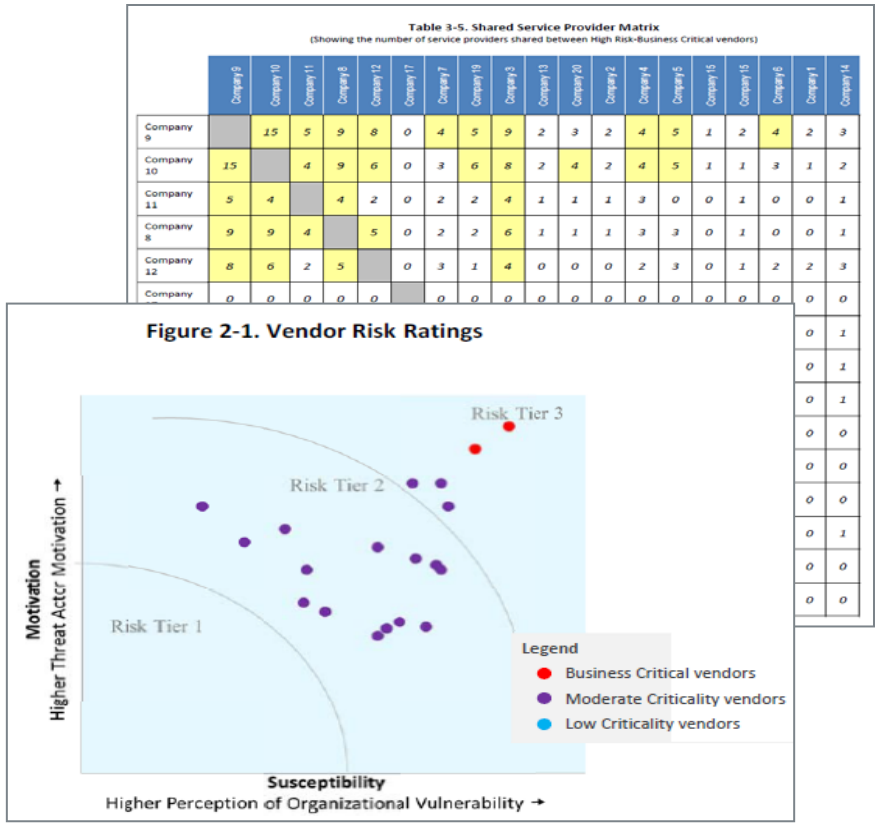
Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.

Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures, dated Feb. 26, 2018.

2 Getting third parties in line

“A firm's level of cybersecurity is only as good as the cybersecurity at its vendors.”
– Benjamin Lawsky, Superintendent of Financial Services, New York State, after JPM Chase breach

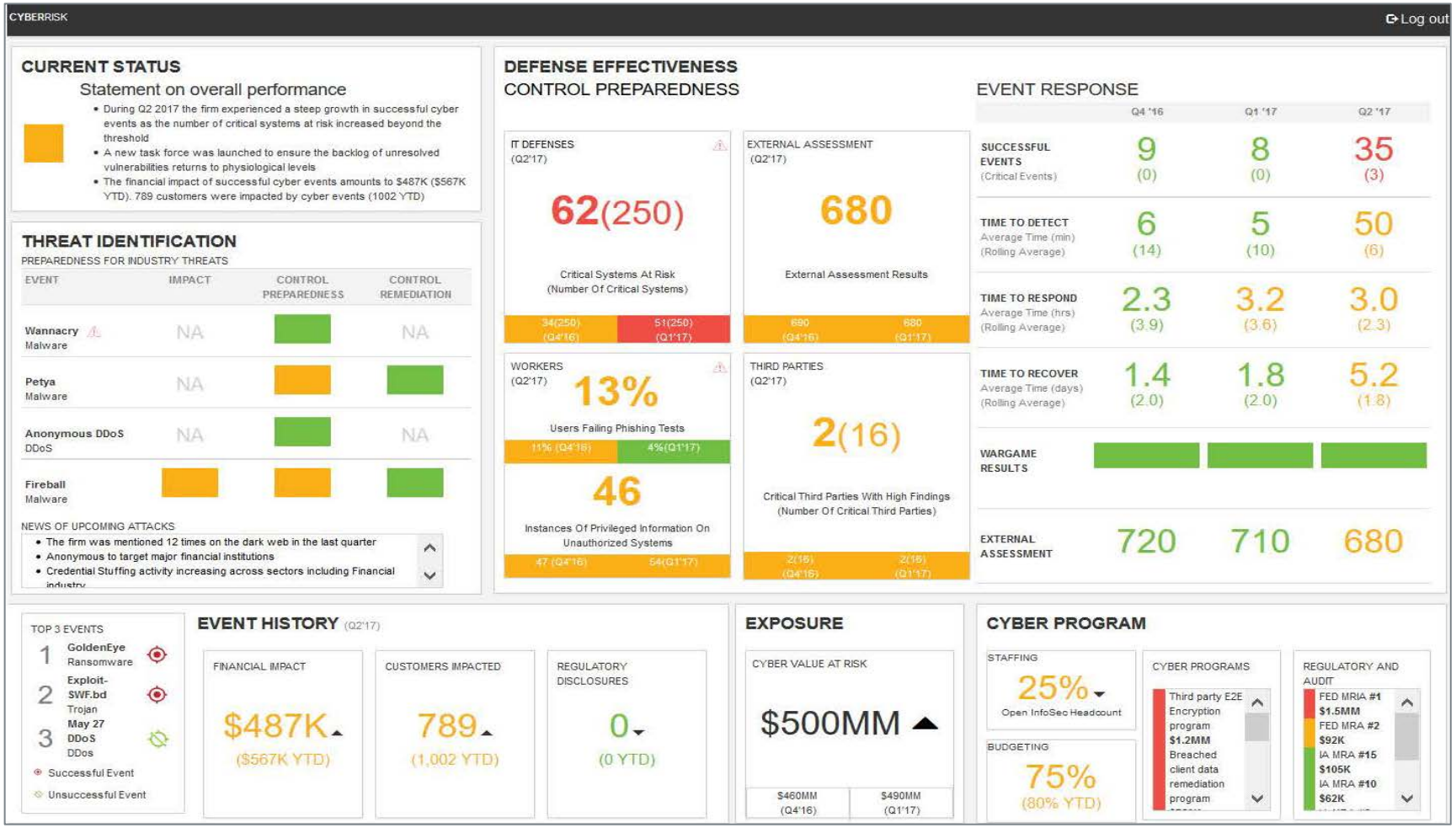
- Identify the full extent of your third party ecosystem
- Assess third party materiality from a cyber risk perspective (taking into account confidentiality, integrity, and availability)
- Assess the cybersecurity posture of your third parties and measure associated risk
  - “Primary” risk
  - Concentration risk
- Implement additional controls, risk accept, or terminate relationships



4 Ensure management understands their cyber risks, posture, and preparedness

Digital cyber dashboard - example

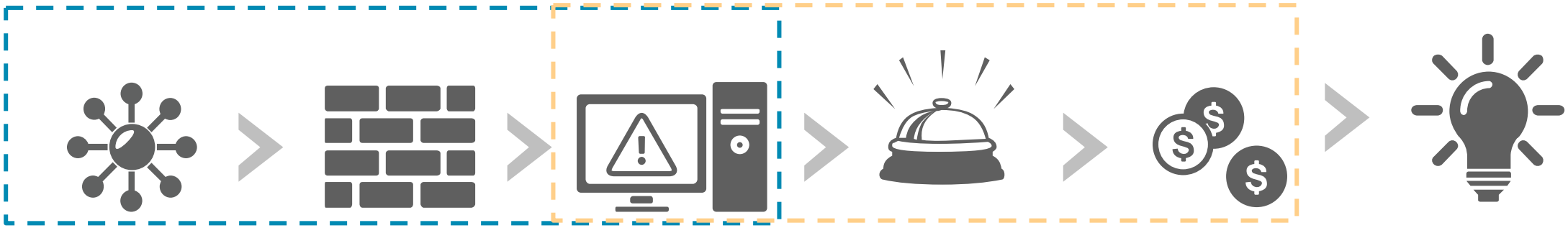
Disguised client example



Illustrative

5 Quantify cyber risk in actionable terms

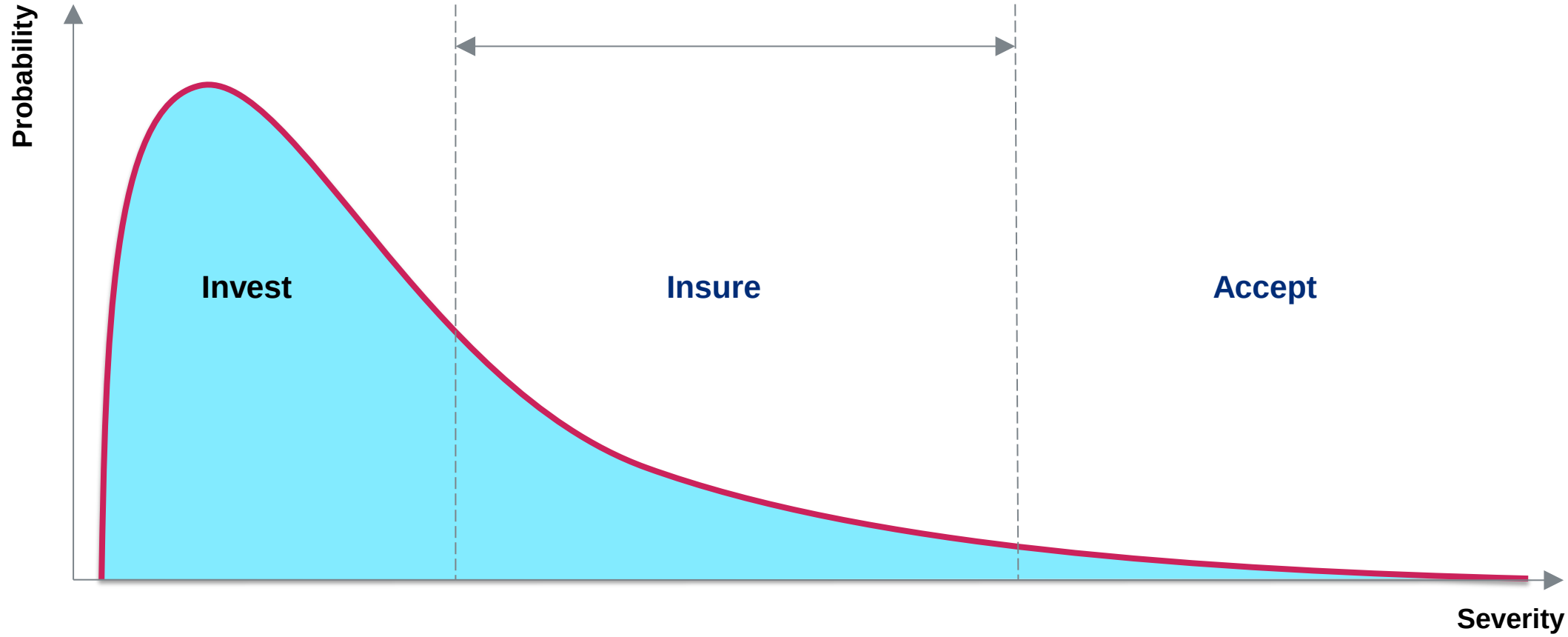
Vectors	Preventative Controls	Loss-driving activity	Responsive Controls	Losses	Strategic Response
Mechanism by which threat agents access high value assets	*Precautions taken to prevent access to high value assets*	*Malicious actions conducted on high value assets*	*Measures taken to detect and mitigate damage once high value assets have been accessed*	*Financial impact on firm as a result of malicious actions*	*Action plans developed after post-attack forensics to improve controls and mitigate future losses*



Frequency of cyber risk event

Severity of cyber risk event

5 Determine where best to invest, insure against and accept cyber risks



Frequency	High	Low	Very Low
Severity	Low	Medium-High	Existential

Section III

DEVELOP THE RIGHT PARTNERSHIPS

Cultivating the right relationships is critical to becoming cyber resilient

Peers

Strategic partners

Government & law enforcement

Operating at the intersection of risk, strategy, and people, Marsh & McLennan Companies delivers innovative solutions to address our clients' most complex challenges

That's **THE MMC ADVANTAGE**

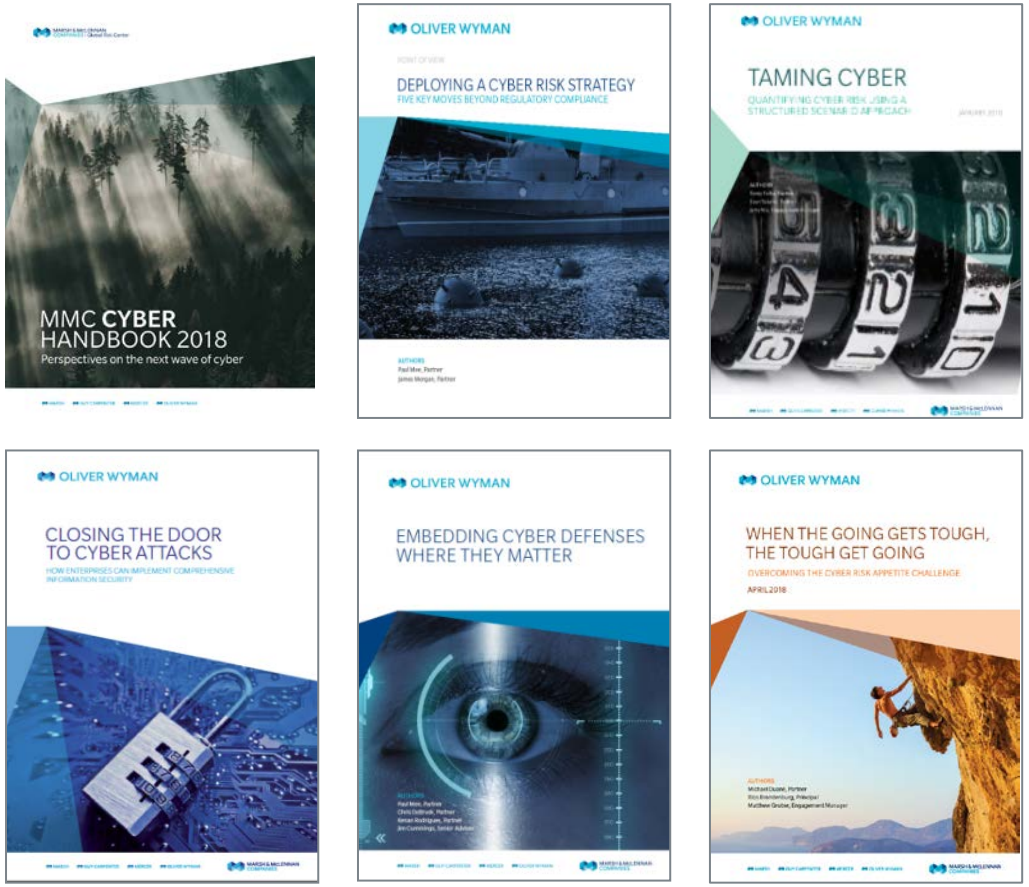
- Cyber risk security strategy and risk management/transfer
- Strategic risk management and risk transfer optimization
- Operational and organizational effectiveness and change management
- Business and organization transformation
- Brand strategy, activation, and employee alignment
- Project planning and risk management

Marsh & McLennan Companies: The Cyber Experts

Marsh & McLennan brings unique capabilities to the table…

1. **Leading cyber risk management practice**
2. **Deep knowledge of the energy sector**
3. **Change excellence**
4. **Strength of execution**

…Alongside specific experience and expertise on this topic



Contact Us

Matthew McCabe
Matthew.P.Mccabe@marsh.com
Senior VP and Cyber Risk Adviser
Marsh

Julia McGillis
Julia.L.Mcgillis@mmc.com
Managing Director
Marsh & McLennan Strategic Solutions Group

Paul Mee
Paul.Mee@oliverwyman.com
Partner, Americas Cyber Lead
Oliver Wyman

Victoria Shirazi
Victoria.Shirazi@mmc.com
Associate Director
Marsh & McLennan Strategic Solutions Group

Gerry Yurkevicz
Gerry.Yurkevicz@oliverwyman.com
Partner
Oliver Wyman Energy, Utilities and Infrastructure Practice

CONFIDENTIALITY

Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.

QUALIFICATIONS, ASSUMPTIONS AND LIMITING CONDITIONS

This report is for the exclusive use of the Oliver Wyman client named herein. This report is not intended for general circulation or publication, nor is it to be reproduced, quoted or distributed for any purpose without the prior written permission of Oliver Wyman. There are no third party beneficiaries with respect to this report, and Oliver Wyman does not accept any liability to any third party.

Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information. The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. Oliver Wyman accepts no responsibility for actual results or future events.

The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the client. This report does not represent investment advice nor does it provide an opinion regarding the fairness of any transaction to any and all parties.