59 Dingledeny
Olney,
Bucks MK46 5ES
United Kingdom

Tel: +44 1234 713233

www.i-riskgroup.com

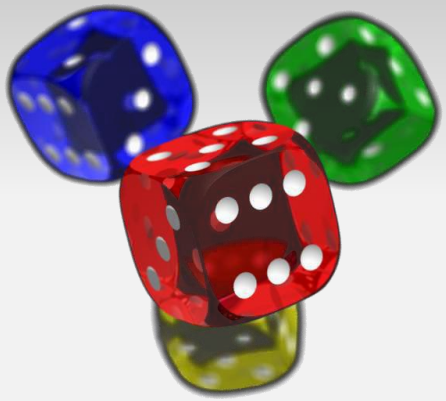
Cyber Risk Governance: The Role of the Board

2nd International BSEC Conference – Risk Management in Energy, Istanbul, 27 & 28 May 2019

Creating Strategic Value for Global Enterprises

Contents

- What is Cyber Risk?
- Cyber risk in the Energy Sector
- Cyber risk governance – the role of the Board
- From Cyber Risk to Resilience



What is Cyber Risk?

Cyber risks can come from:

- **Internal malicious or unintentional activity**
- **External malicious or unintentional activity**

The International Organization for Standardization defines cybersecurity or cyberspace security (cyber risk management) as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

What is Cyber Risk?

Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems

The potential of loss or harm related to technical infrastructure or the use of technology within an organization and beyond

Cyber risks can come from:

- **Internal malicious or unintentional activity**
- **External malicious or unintentional activity**

What is Cyber Risk?

Examples

What is Cyber Risk?

Cybersecurity (the management of cyber risk) is not only an IT problem, it is an enterprise-wide problem that requires an interdisciplinary approach, and a comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cybersecurity practices

Cyber Risk in the Energy Sector

Is energy different from any other sector in respect to cyber risk management? What are the unique cyber risk challenges in the energy sector to be addressed?

Cyber Risk in the Energy Sector

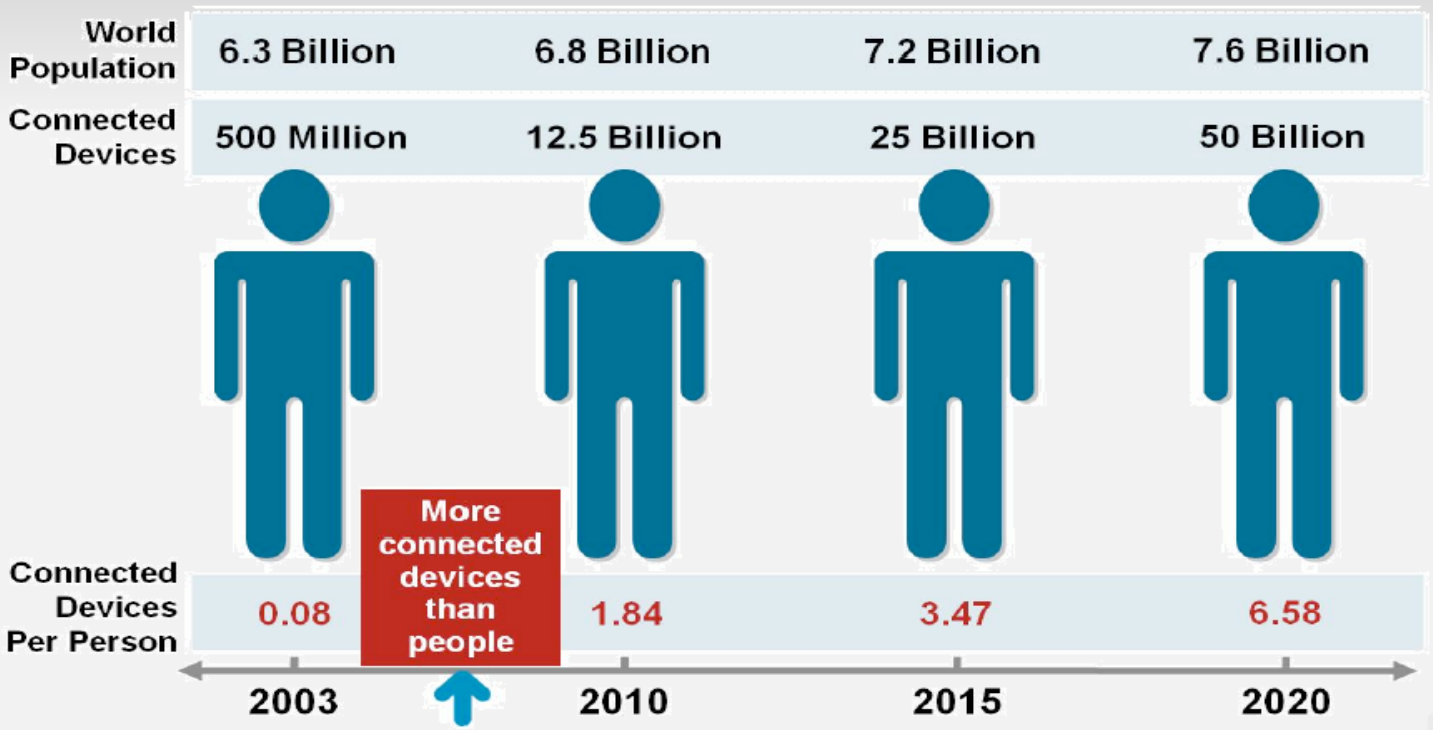
Digital technologies, devices and media have brought us great benefits and offer enormous opportunities but their use also exposes us to increased exposure to cyber risk

This is not specific to the Energy Sector

Cyber Risk in the Energy Sector

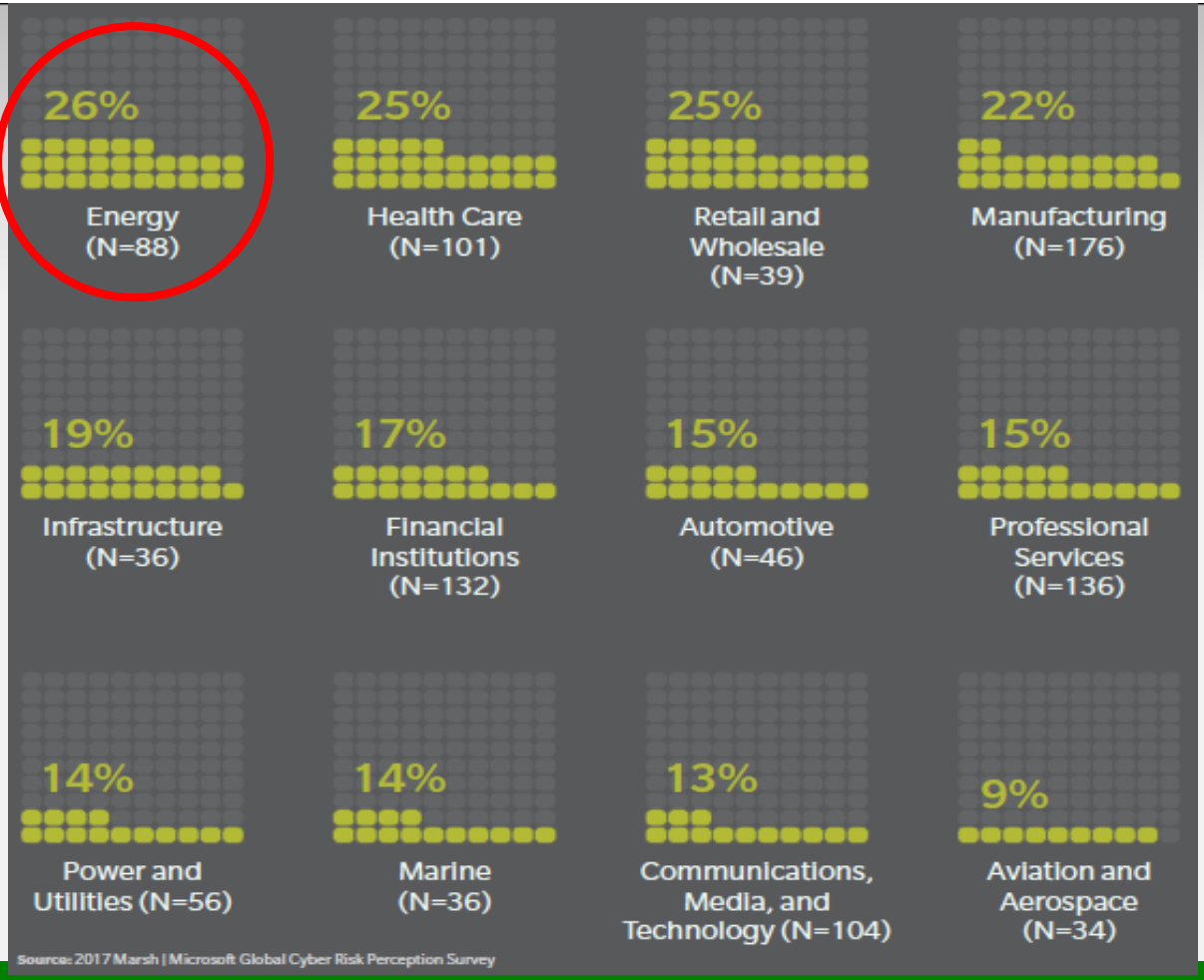
Example IOT - Proliferation of Connectivity – all sectors

Figure 1. The Internet of Things Was "Born" Between 2008 and 2009



Source: Cisco IBSG, April 2011

Cyber Risk in the Energy Sector

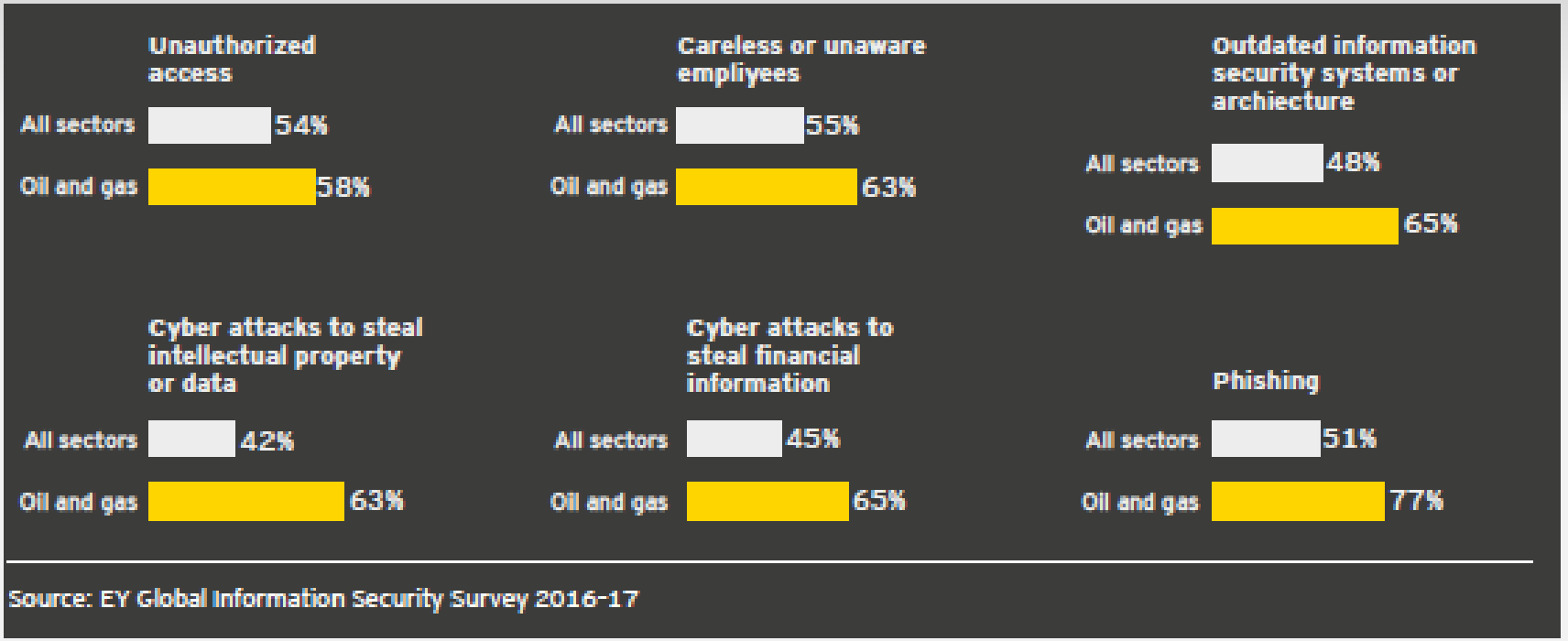


BUT - Energy one of the key industries impacted by Cyber Attacks

Cyber risk in energy = convergence of the virtual and physical world

Cyber Risk in the Energy Sector

Further example - Cyber threats faced by Oil and Gas Sector compared to other industrial sectors



Cyber Risk in the Energy Sector

Unique cyber risk challenges in the energy sector

Challenge	Electricity	Oil	Gas	Nuclear
Grid stability in a cross-border interconnected energy network.	x		x	x
Protection concepts reflecting current threats and risks.	x	x	x	x
Handling of cyber attacks within the EU.	x	x	x	x
Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility	x			x
Introduction of new highly interconnected technologies and services.	x		x	
Outsourcing of infrastructures and services.	x		x	x
Integrity of components used in energy systems.	x		x	x
Increased interdependency among market players.	x			
Availability of human resources and their competences.	x	x	x	x
Constraints imposed by cyber security measures in contrast to real-time/availability requirements.	x		x	x

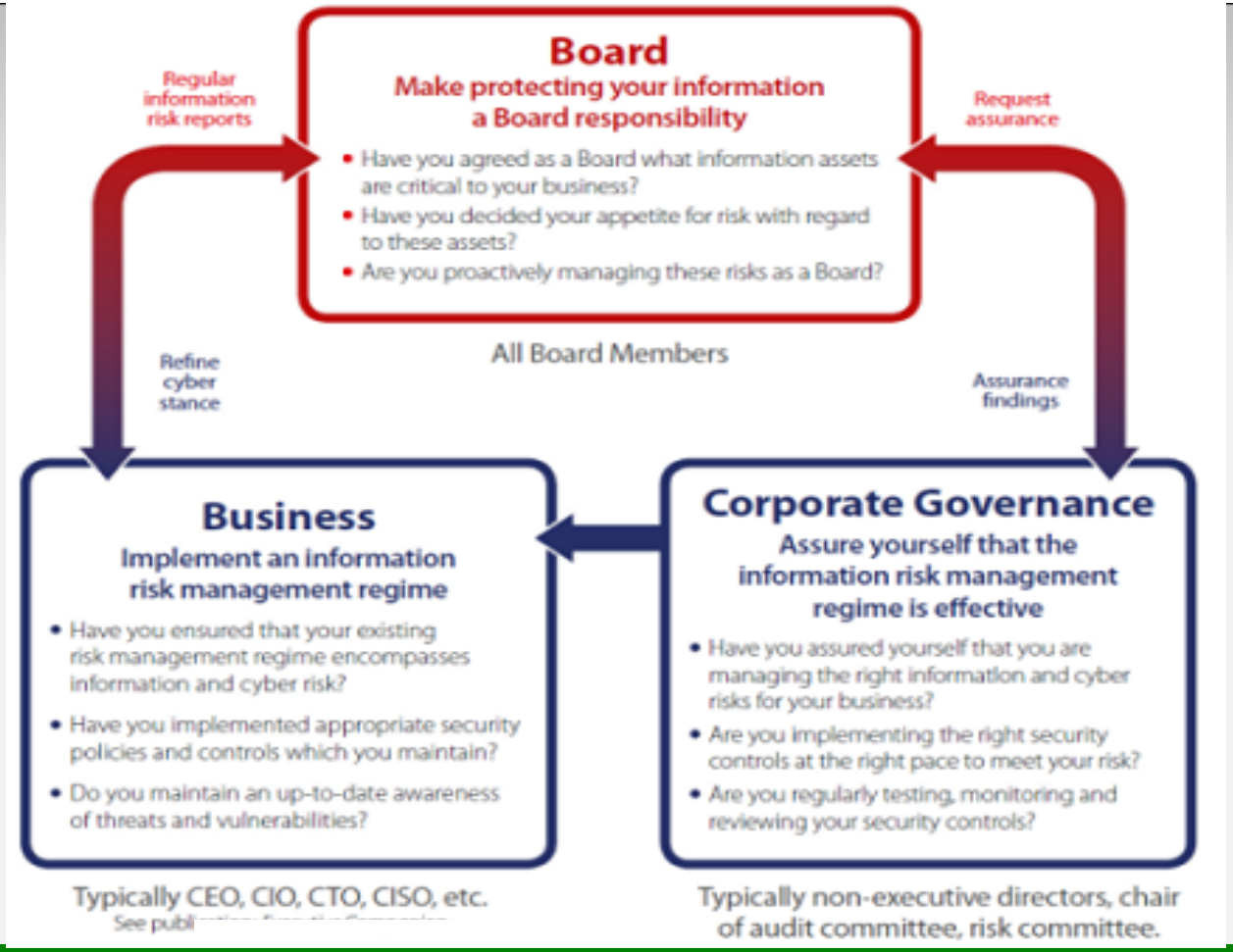
Source: Cyber Security in the Energy Sector, EECSP Report February 2017

Cyber Risk Governance – the role of the Board

It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to digital assets. But meeting these requirements has had its limitations:

- A crowded agenda Cybersecurity is just one of many pressing issues demanding board-level engagement, particularly in a time of ongoing economic volatility.
- The IT silo Cyber risk seen as an IT issue rather than part of broader enterprise risk framework and protection of the strategic value of the information itself.
- “Not our problem” Cybersecurity has been seen as a significant problem only in select sectors.
- Difficult to gauge and model
- Invisible pay-off In the face of competing demands for scarce resources,
- Wrong priorities Organizations have overinvested in preventative controls at the expense of detect/ response capability

Cyber Risk Governance – the role of the Board



Cyber risk management and oversight addresses the board's development and implementation of an effective enterprise wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

Source: http://www.powernetamerica.com/cybersecurity/governance

Cyber Risk Governance – the role of the Board

THE BOARD SHOULD VIEW CYBERSECURITY AS AN IMPORTANT ELEMENT OF ENTERPRISE RISK THAT THEY MUST OVERSEE.

- Identify the organization's essential assets that may be vulnerable to cyber attack.
- Identify which cyber risks to avoid, which to accept, and which to mitigate.
- Develop specific plans associated with each approach.

THE BOARD SHOULD VIEW CYBERSECURITY AS A STRATEGIC AND MANAGERIAL ISSUE

- Management should be accountable for reporting their actions and cyber breaches.
- Promoting employee awareness and training is crucial.
- Third party testing of cyber vulnerabilities can provide a high degree of deterrence.
- Boards should maintain an external team of professionals that are available for training and in crisis situation.

Cyber Risk Governance – the role of the Board

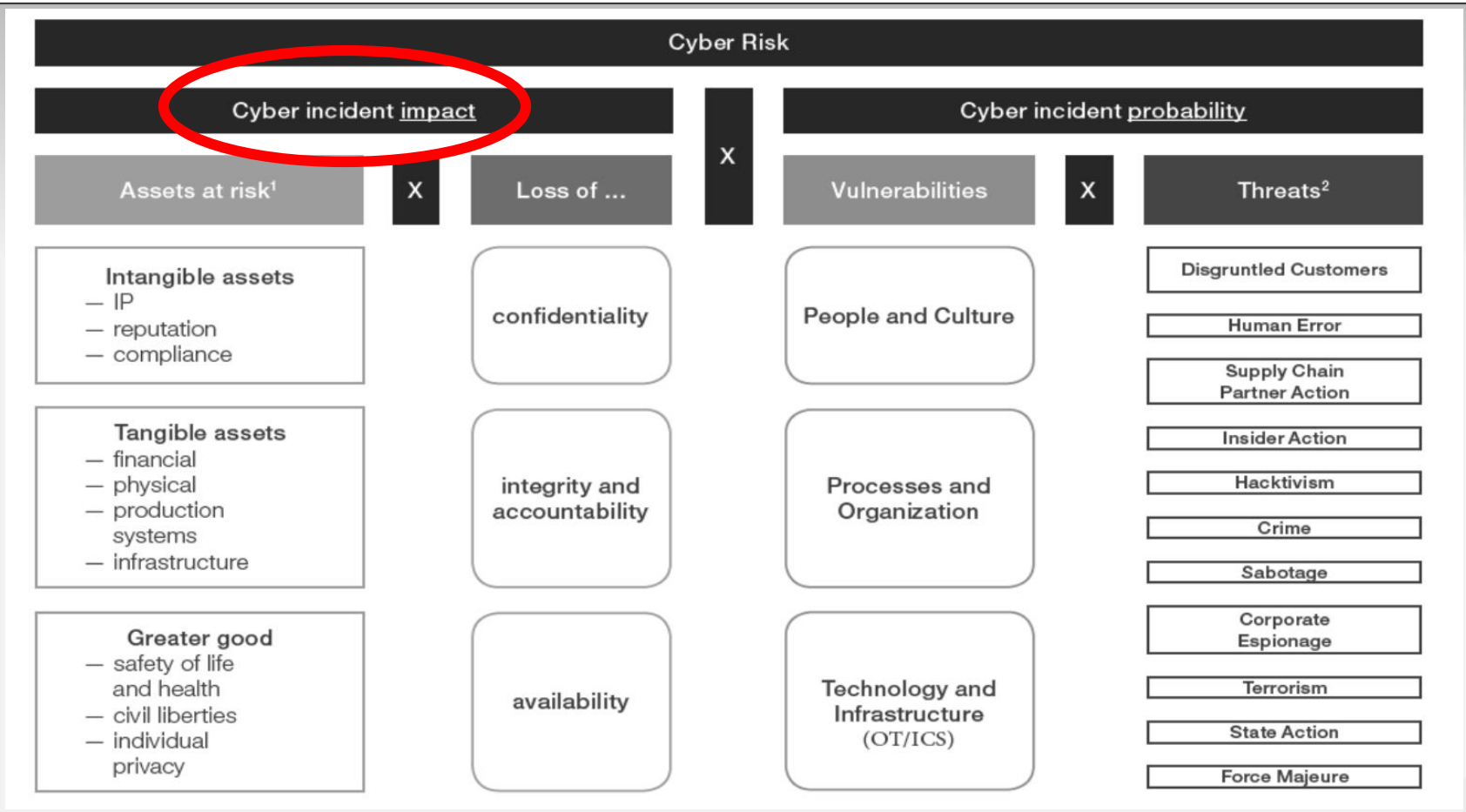
THE BOARD SHOULD BE GUIDED BY TWO BROAD CONCEPTS OF CYBERSECURITY:

- Ensure that cybersecurity is managed within three lines of defense, and
- That cybersecurity is managed based on constantly reacting to gathering intelligence and promoting adaptation to the changing risk environment

THE BOARD SHOULD UNDERSTAND THE COMPANY'S EXPOSURE TO THIRD PARTYS

THE BOARD SHOULD DEFINE AND SUPPORT A CYBER RISK CULTURE

From Cyber Risk to Resilience



I-Risk Group

Creating Strategic Value for Global Enterprises

Supplementary - Regulatory Expectations (Common)

CATEGORY	NOTABLE EXPANSION OF REGULATORY EXPECTATION	SOURCE FFIEC	ECRM	NYDFS
Scope breadth and depth	• Scope of Non Public Information (NPI) still unclear, but can be interpreted as significantly broader than Non Public Personal Information			●
Strategy and governance	• Integration of Information Security into risk culture and decision-making	●		
	• Prescriptive governance document requirements	●		●
	• Board-approved, enterprise-wide cyber risk appetite and risk tolerances		●	
	• Board-approved, written, enterprise-wide cyber risk management strategy		●	
	• Annual Board certification of compliance and annual Board reporting			●
Framework	• Integration of Information Security into third party risk management program	●		
	• Integration of Information Security into the Lines of Business (LoBs) and support functions	●		
	• Integration of Information Security into enterprise risk management framework	●	●	
	• Specific testing/assessment requirements (e.g., bi-annual vulnerability assessment)			●
Operating model	• Responsibility for cyber risk management across three independent functions		●	
	• Mandated Chief Information Security Officer (CISO) role			●
	• Specific guidelines to be included in policies governing third-party cybersecurity			●
Infrastructure and capabilities	• Two-hour recovery time objective for sector-critical systems		●	
	• Quantification and aggregation of cyber risk with consistent, repeatable methodology		●	
	• Specific data protection requirements (e.g., multi-factor authentication)			●
	• Maintenance of five-year audit trail for material financial transactions			●

Source: Oliver Wyman analysis