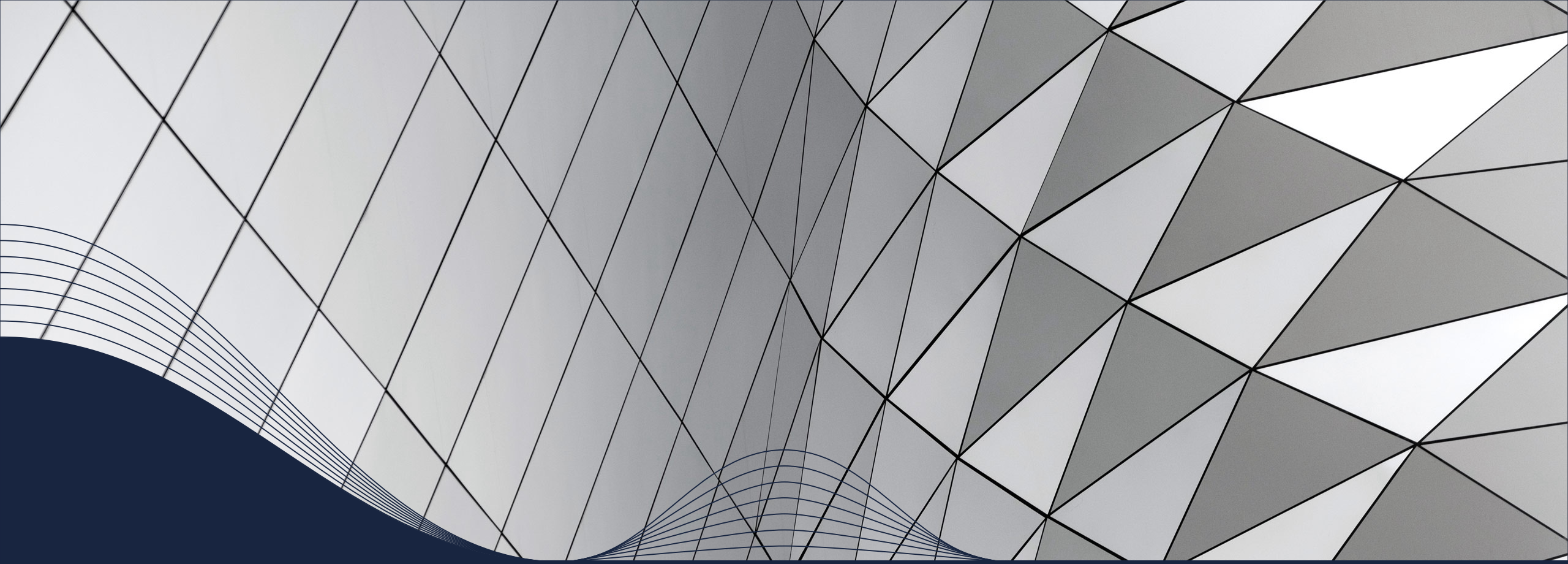


Legal IT Considerations and Challenges Facing Companies

By Ron Plesco

DLA PIPER

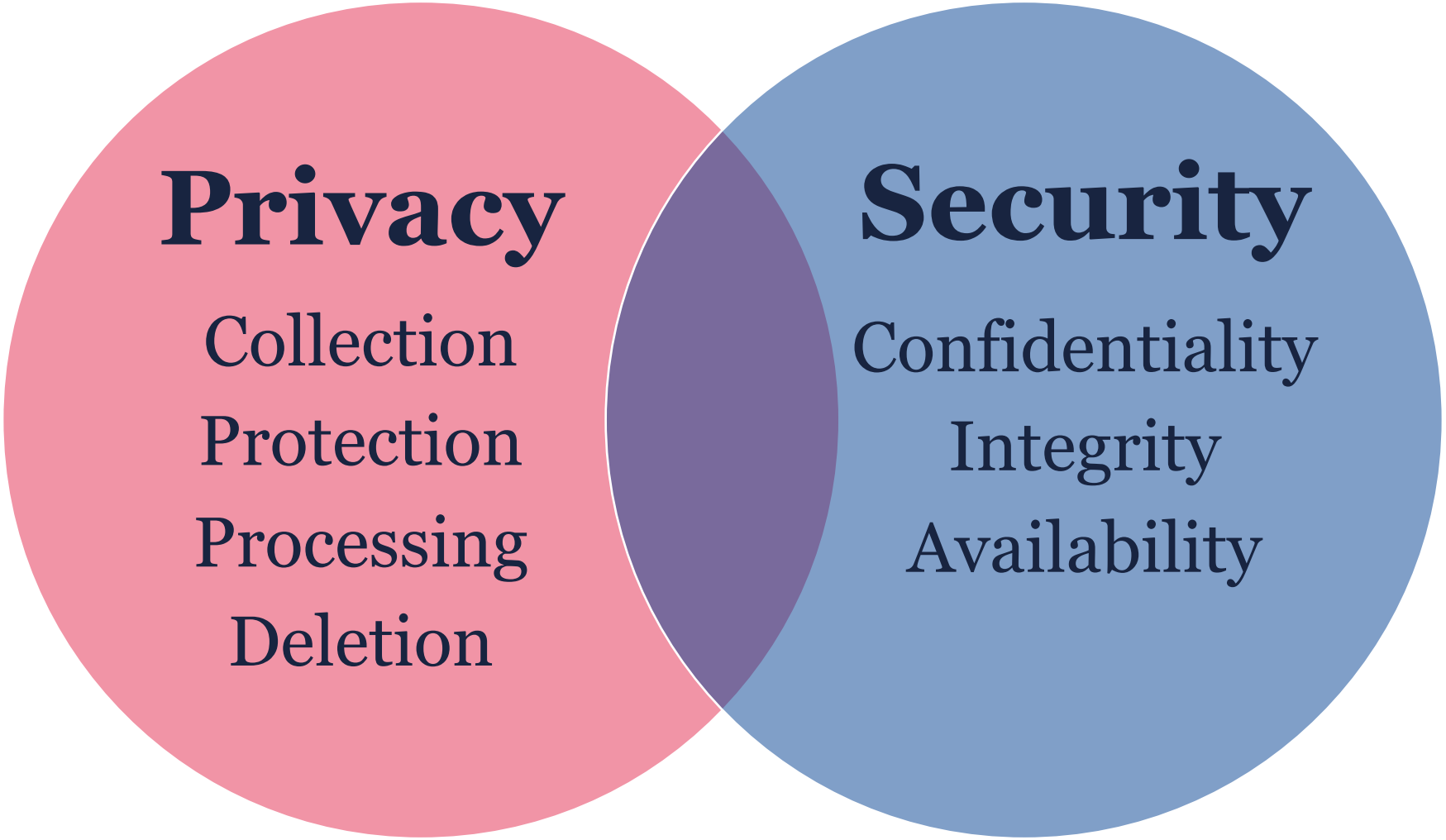
PA Chamber

IT Security Con.

May 5, 2022

Agenda

- Privacy v. Security
- Understanding the Cyber Threat and Cyber Risk Landscape
- Lessons Learned from Breaches
- Cyber Risk Tolerance
- NIST and Cyber Governance
  - Board and Management Roles
- Working with Law Enforcement
- Privilege Issues


Privacy
Collection
Protection
Processing
Deletion
Security
Confidentiality
Integrity
Availability

Key Definitions – Controller v Processor

Data controller

- The company that is responsible for processing because it determines the purposes and means of processing – it processes PI on its own behalf, for its own business purposes

Data processor

- Data controller's vendor/service provider that processes PI under the instruction and on behalf of the data controller

Common Legal Requirements Elements Across the Globe

Privacy

Privacy is a societal norm, sometimes contained in laws, that expresses limitations over the collection, protection, processing, and deletion of information regarding an individual.

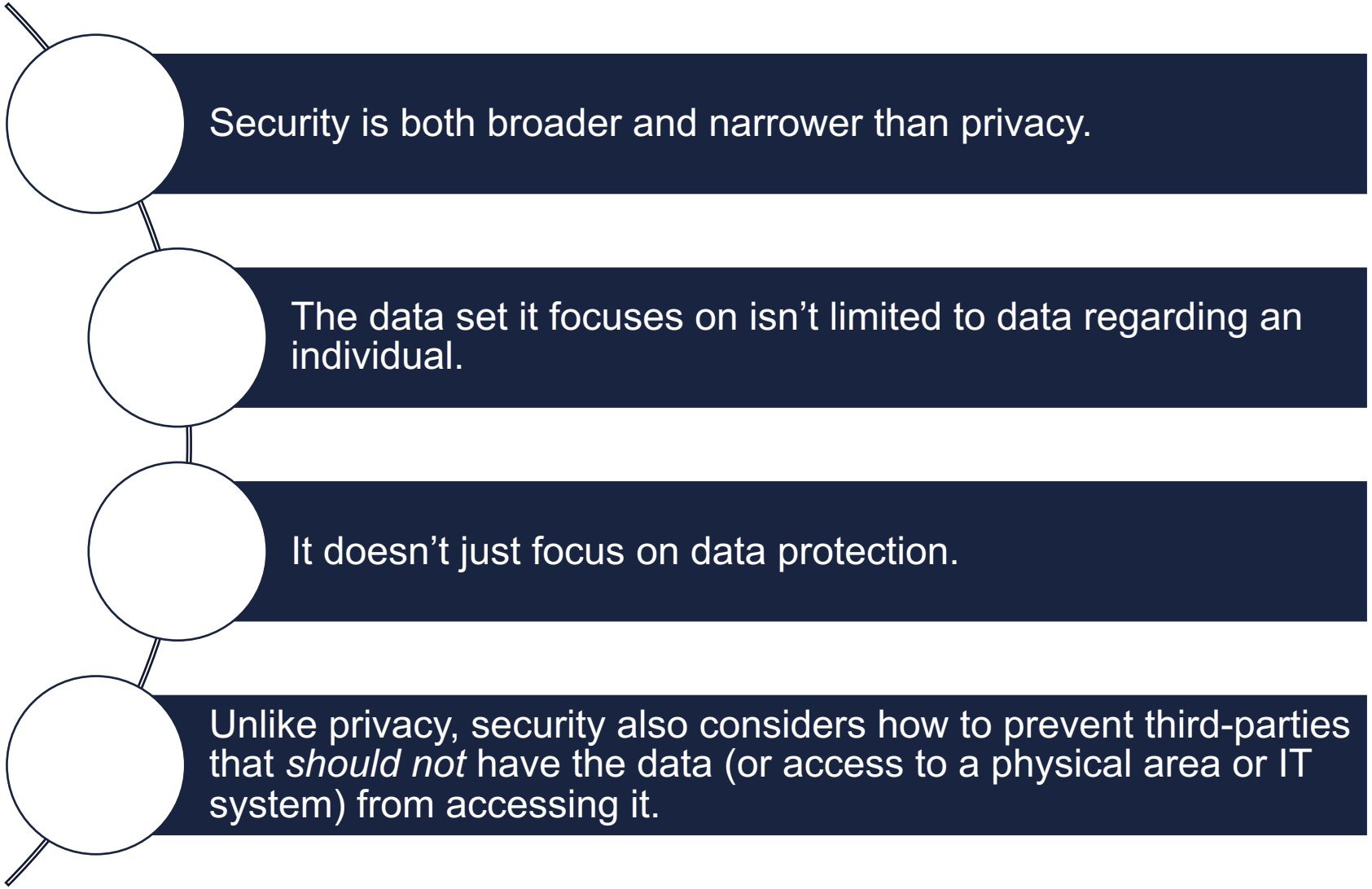
The primary focus is on what an authorized person or entity lawfully does with information regarding an individual.

An Example--Lawfulness of Processing

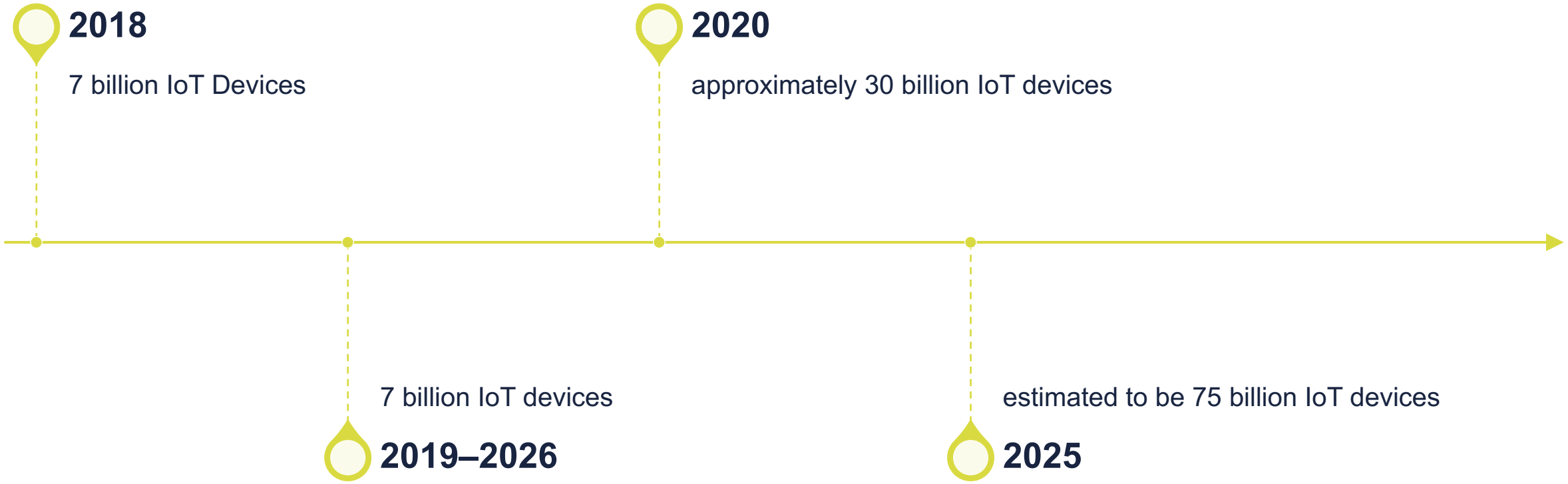
General principle (Art. 6)

- Company may process PI only if it has a specific legal basis:
  - If processing is necessary for execution agreement (“contractual necessity”)
  - Compliance with legal obligation
  - Legitimate interest of the controller
  - Consent of the individual
  - Protection of vital interest of individual

Security


Security is both broader and narrower than privacy.
The data set it focuses on isn’t limited to data regarding an individual.
It doesn’t just focus on data protection.
Unlike privacy, security also considers how to prevent third-parties that *should not* have the data (or access to a physical area or IT system) from accessing it.

The Ever-Expanding Surface Area



Understanding Security – Key Points

Security is more than just protecting data from theft

CIA

- Confidentiality.
- Integrity.
- Availability.

Understanding Security – Key Points

What are the key focus areas for security?

People, process, and technology

Understanding Security – Key Points

People:

- Training and education;
- Following good security practices;
- Insider threat;

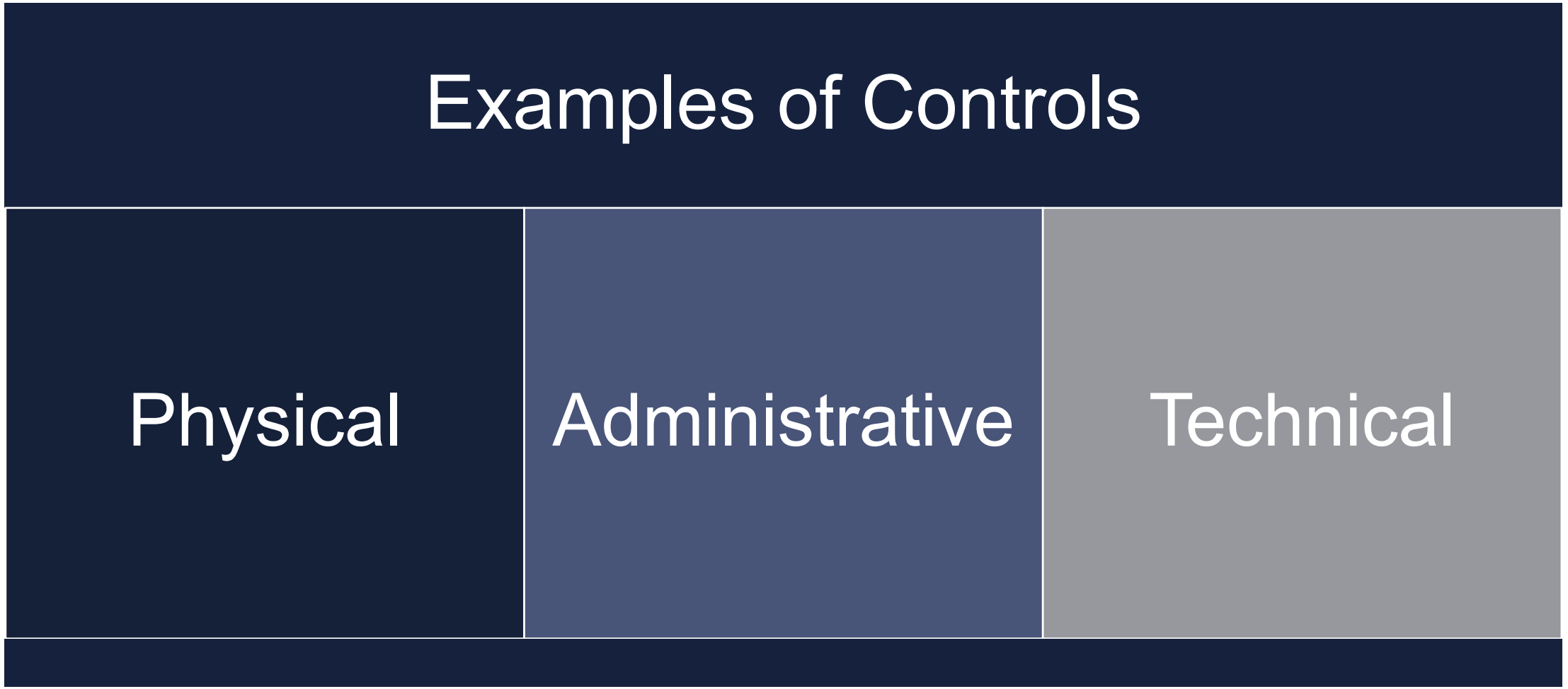
Process:

- Governance;
- Policies and procedures;
- Information sharing;

Technology:

- DLP;
- Pen testing.

Understanding Security – Key Points



What Has Been the Traditional Approach to Cyber?

- It was seen as the domain of SMEs with technical backgrounds.

How Has That Begun to Change?

- Cyber is beginning to become viewed as a broader enterprise risk that should be governed in more traditional ways.
- Boards have become involved, but not necessarily in the best way.

Understanding Cyber

Cyber is an asymmetric threat.

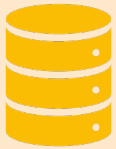
This means that the attackers may know more about your vulnerabilities than management does.

The Board will inherently know less about the vulnerabilities than management

Ultimately managing cyber risk is a governance issue, and to appropriately manage this risk the Board must understand the potential risks to the business.

Information Risk/Value. Information is an asset of the company, and the Board should ensure that it is appropriately protected, valued, and utilized for the benefit of the company.

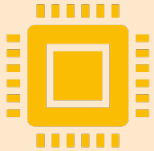
Why is it still a challenge for many companies?



Architecture issues.

The proliferation of digital storage and new devices.

Cybersecurity, more than most enterprise risks, cuts across numerous subject matter domains, and therefore requires companies to be coordinated in order to manage these risks.



Moreover, cyber is a risk that is newly being appreciated by many companies.

The Evolution of Threats

Yesterday

Isolated Criminals and Script Kiddies

- Identity Theft
- Self-promotion
- Theft of Content or Services

Today

Organized Criminals, Nation States, Hacktivists, and Insiders

- Intelligence Gathering
- Intellectual Property
- Financial Information
- Strategic Access/Destruction
- Terrorism

An Overview of Threats

Cyber Crime.

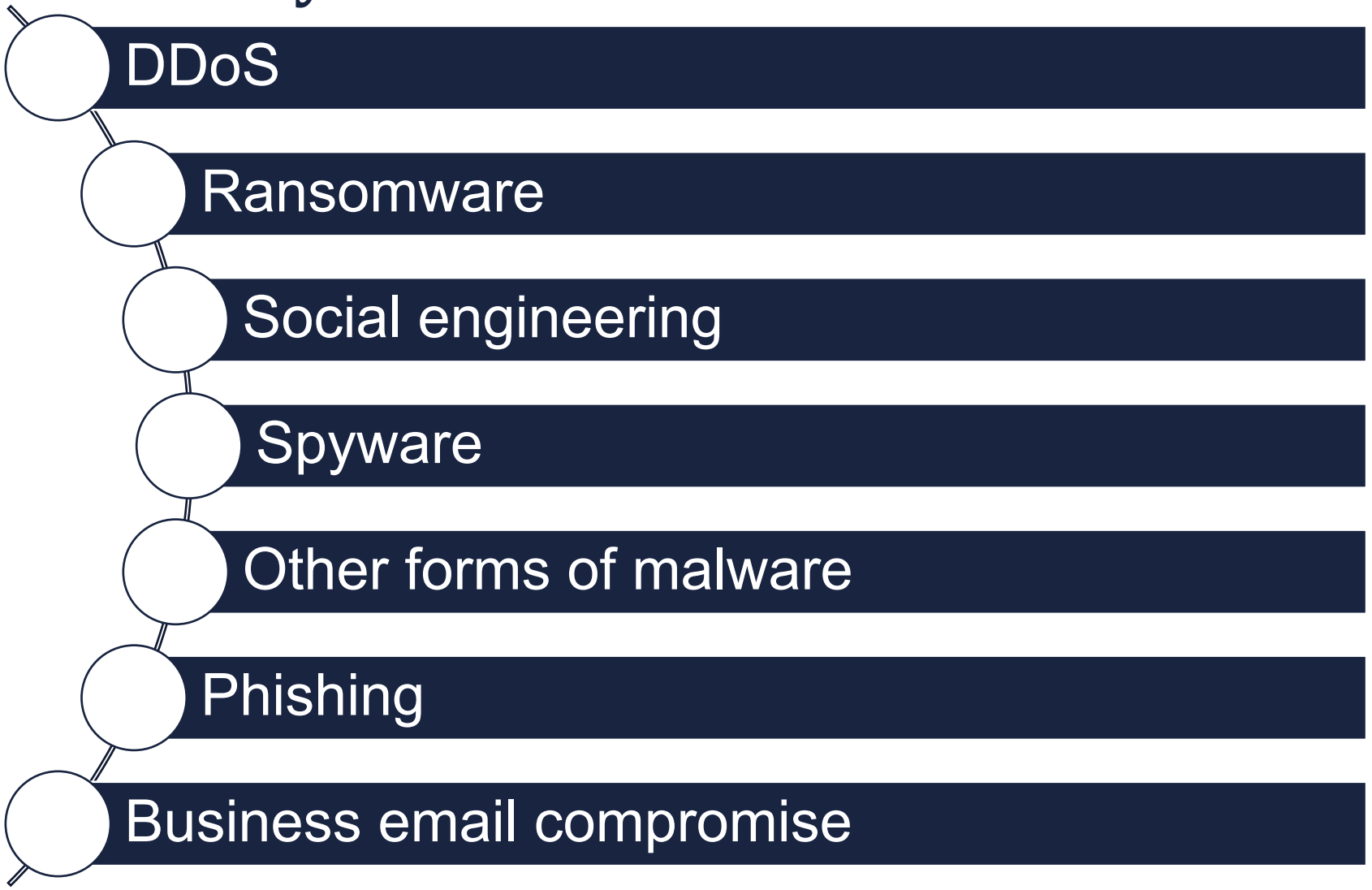
Cyber Vandalism.

Cyber Espionage.

Cyber War.

Cyber as a Threat Vector.

Other Forms of Cyber Issues



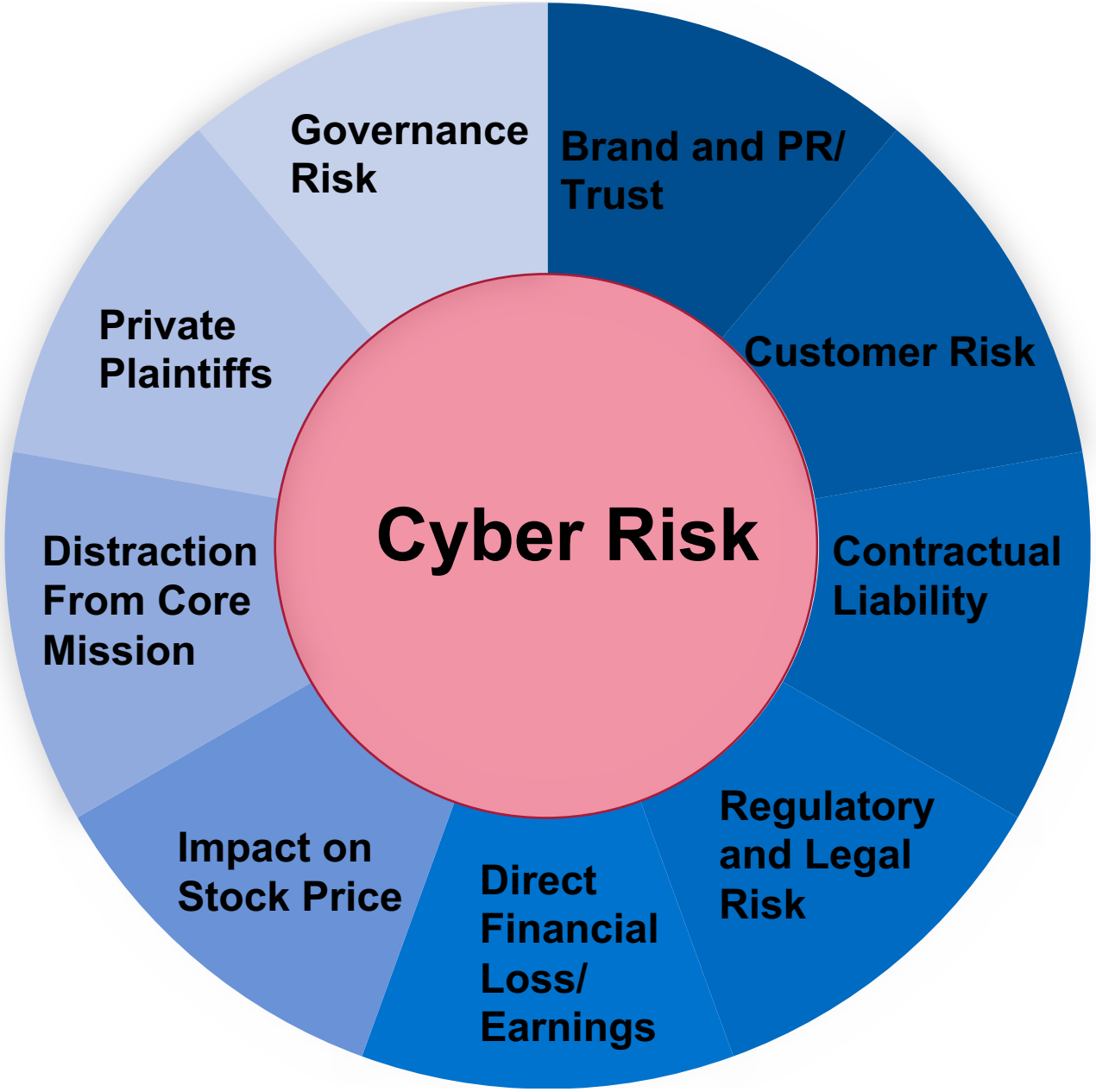
Systems of Value

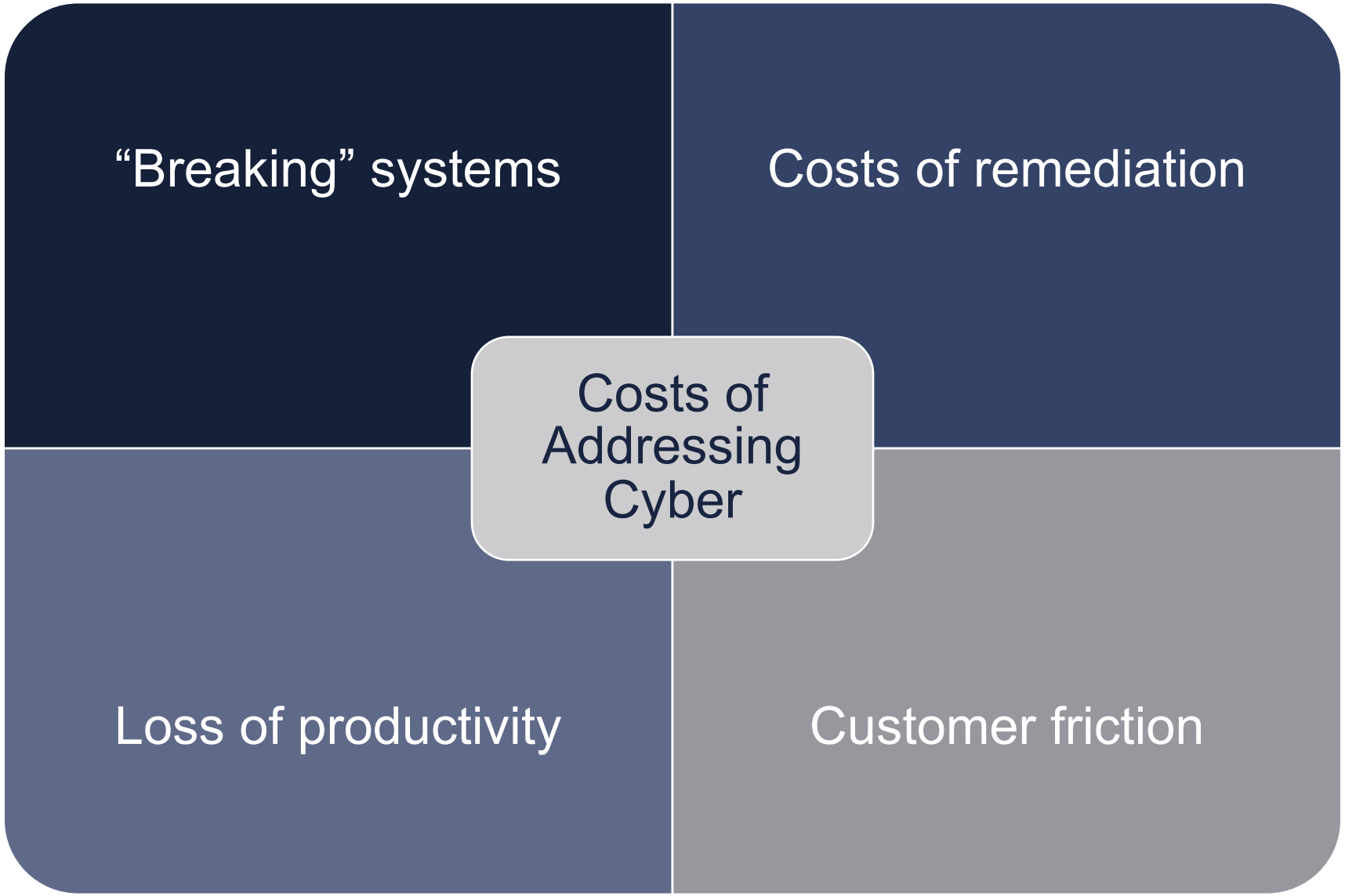
Theft of data isn’t the only issue

Denial of access to systems can be a concern for many companies

Have a Plan

- “Everyone has a plan, until they get punched in the mouth.” Mike Tyson.
- You need to have a plan for when you get punched in the mouth.


Governance Risk
Brand and PR/ Trust
Customer Risk
Contractual Liability
Regulatory and Legal Risk
Direct Financial Loss/ Earnings
Impact on Stock Price
Distraction From Core Mission
Private Plaintiffs
Cyber Risk


“Breaking” systems
Costs of remediation
Costs of Addressing Cyber
Loss of productivity
Customer friction

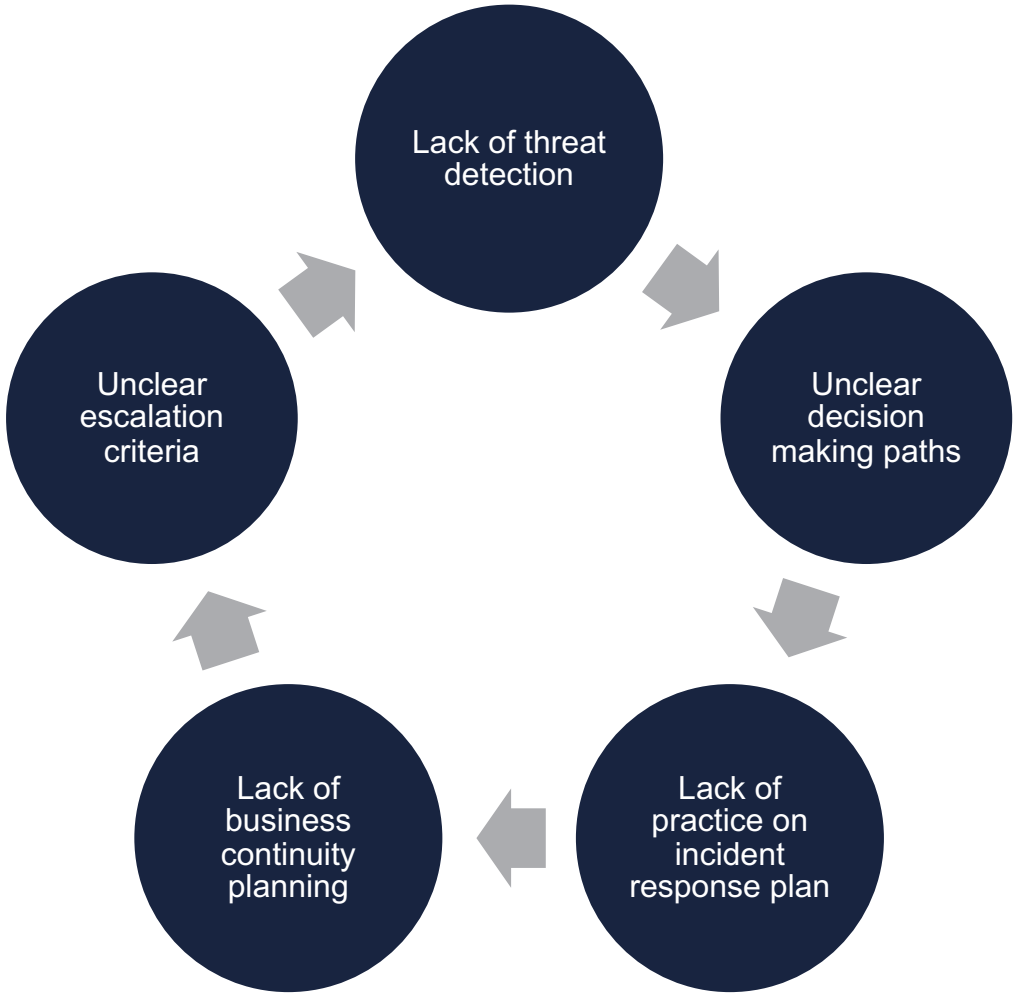
Balancing Risks and Costs

- Ultimately management must balance all of these risks and costs and determine what the appropriate risk governance strategy is.

What is Your Cyber Risk Tolerance?

- After examining the potential impact of a cyber event, management, with appropriate input from the Board, should determine what the company's risk tolerance is regarding cyber.
- Ultimately the Board needs to understand the earnings impact of the risk tolerance of the Company and ensure that it and management are aligned, and it must ensure, via its oversight responsibility, that Company management appropriately addresses cyber.

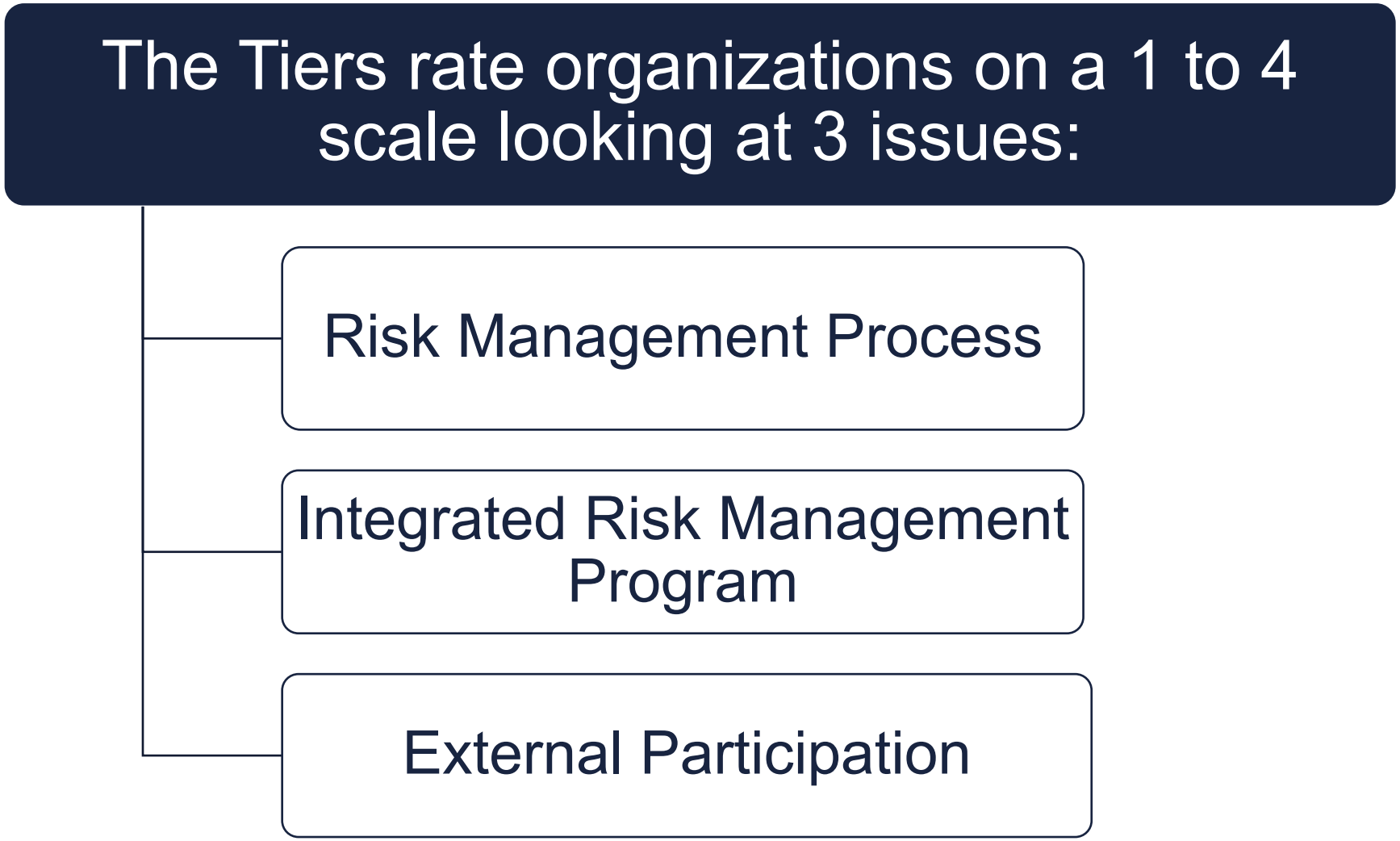
Lessons Learned from Breaches



NIST as a Program Reference Point

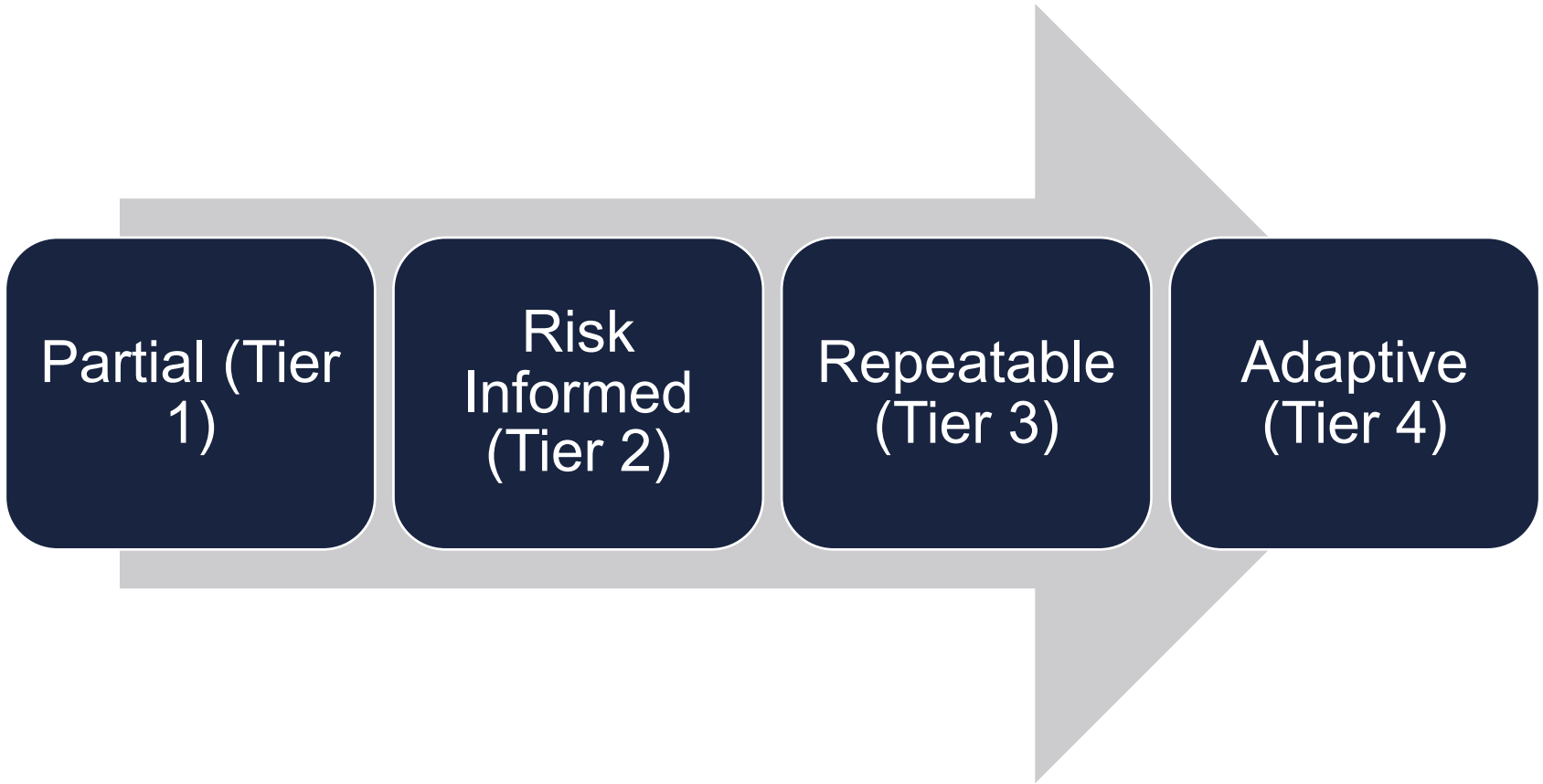
- Whether your company uses a NIST framework or not, the NIST Framework is a helpful reference point.

The NIST Tiers

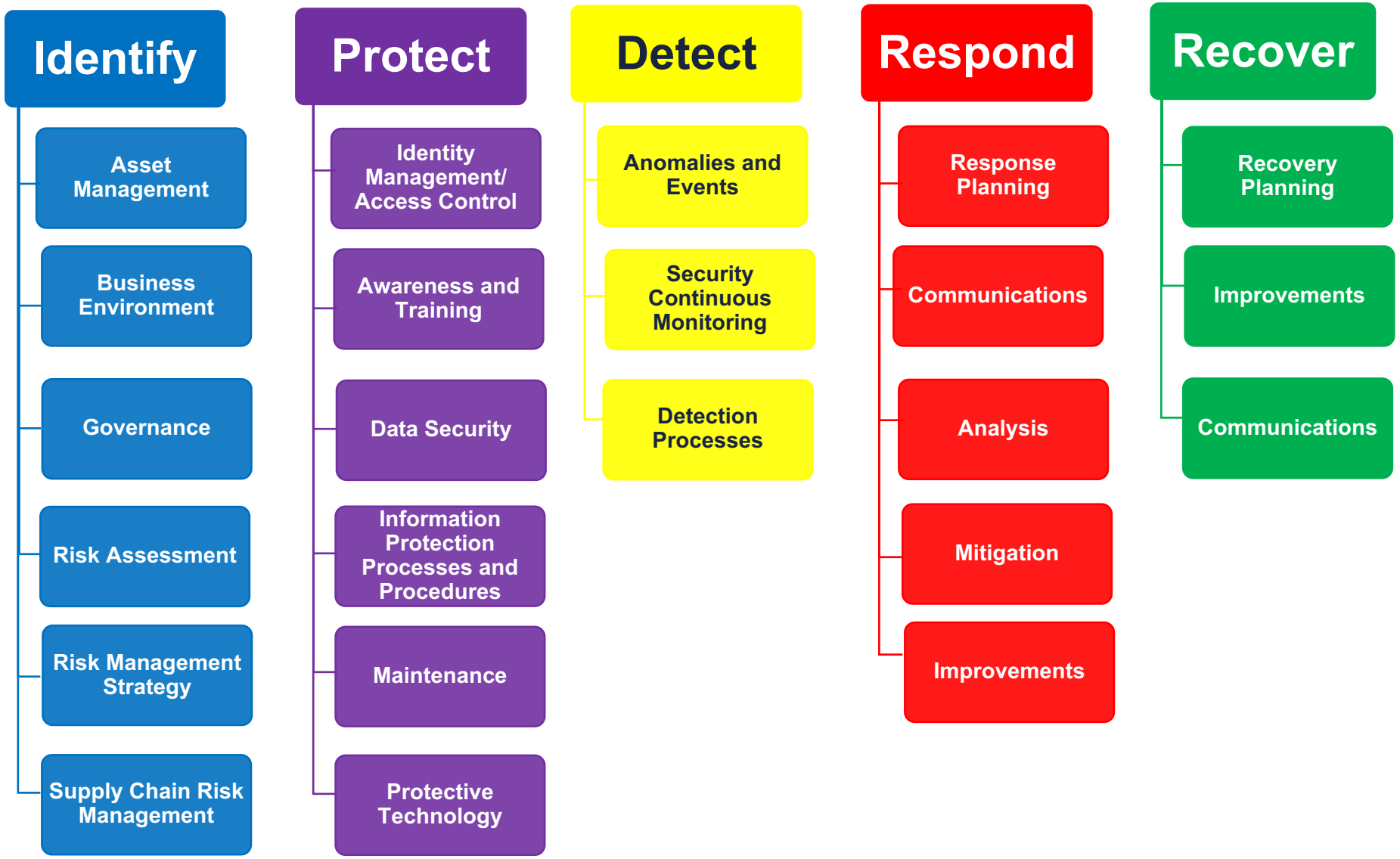


The NIST Tiers

The tiers range from:



The Framework – Updated Draft



Cyber and the Board

Understand the cyber risk profile of the Company by discussing this with management, and any appropriate third parties

Make sure that management has appropriate processes and programs to engage in appropriate risk assessment, which include identifying, assessing, and mitigating risk

Engage in appropriate oversight by:

- making sure that cyber is appropriately addressed by the Board, including through relevant committees;
- ensuring that risks are appropriately remediated; and
- the cyber risk program is otherwise functioning appropriately

Make sure that management appropriately communicates the risk

Do an appropriate, executive-level “table-top” exercise.

In Short—The Board Should

What Should Management Do?

Conduct an appropriate enterprise cyber risk assessment

Determine what your most critical systems and information are

Assist the Board with determining the Company's risk tolerance

Create as appropriate, cross-functional risk governance structure that continually assesses and improves cyber risk, including organizational, behavioral, and technical changes

Keep the Board appropriately informed of the Company's cyber risks

Make sure escalation criteria are clear

Align incentives for employees with the risk tolerance of the Company

Engage in appropriate business continuity planning

What Should Management Do?

Appropriately manage the company's cyber risks, via an appropriate cyber risk mitigation program, including appropriately remediating known cyber issues

Have a third-party evaluate your company (under privilege)

Test and train employees, as appropriate, on common attack vectors such as "phishing"

Examine risk shifting devices, such as insurance

Engage in appropriate information sharing

Develop appropriate relationships with law enforcement

Practice responding to a security incident

Engage the appropriate third-parties to help you with an incident before an incident happens

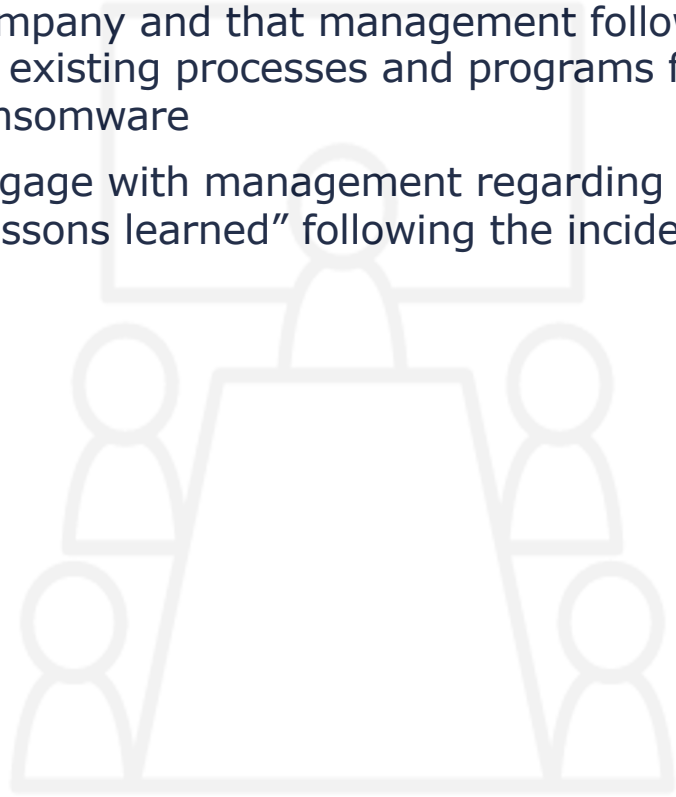
SUMMARY BOARD & MANAGEMENT ROLES DURING A CYBER INCIDENT

Management

- Execute containment and recovery plans, including assessment of the payment of the ransom
- Execute information sharing strategy (*e.g.*, critical partners)
- Preserve relevant documents, including forensic collection, if appropriate, with consideration of the application of the work-product doctrine
- Make the facts stand still
- Execute public relations plan based upon the nature and scope of the incident
- Fulfill notice, disclosure, and other legal obligations
- Execute on engagement strategy with law enforcement
- Conduct a "lessons learned" review following the incident

Board

- Engagement with management to ensure that the ransomware response is consistent with the risk tolerance for the company and that management follows its existing processes and programs for ransomware
- Engage with management regarding "lessons learned" following the incident



BOARD ENGAGEMENT MODEL – CYBER

The following is the working draft of a proposed framework for the levels of board engagement associated with ransomware incidents based on related impacts and ransom demands

	Periodic Board / Committee Reporting	Advise Lead Director and Relevant Chairs	Convene Board for Briefing
Minimal Impact to Operations	• Incorporate in regular board / committee reporting		
Moderate Impact to Operations	→	• Lead Director and relevant Chairs consulted in real time • Notification to full Board to follow within 24 hours	
Material / Critical Impact	→	→	• Lead Director and relevant Chairs consulted in real time • Board convened for briefing within 24 hours

Working With Law Enforcement

- How should companies think about these issues?
- When should companies call law enforcement?
- Who should they call?
- Privilege considerations

AN EXAMPLE--RANSOMWARE SHOT CLOCK ACTION ITEMS

Management / Third-Party Action Item	Timeframe
Engagement of Third Parties	
Engage legal counsel	24 hours
Engage technical experts (e.g., cybersecurity forensics investigation team)	24-48 hours
Engage payment facilitator	24-48 hours
Payment Facilitator Payment Process	
Identification of bank and contact to inquire about facilitating payment (potentially submit wire transfer from bank or payor agency)	1-12 hours for initial contact; certain banks may take up to 3 days to facilitate payment. Wires by 3pm for same day payment
Payment facilitator to engage with threat actors for additional information and potential negotiation of fee	24 hours
Determine identity of threat actors and attack vectors used to gain access to systems for OFAC guidance considerations	24 hours
Identify whether systems were backed up and time to engage back up	48 hours
Wire funds to payment facilitator	48 hours (1-24 hours after determination of whether payment will be made)
Identify data affected and whether exfiltrated	72 hours

AN EXAMPLE--RANSOMWARE SHOT CLOCK ACTION ITEMS (CONT.)

Management / Third-Party Action Item	Timeframe
Notification and Assessments Obligations	
Notify Board and keep Board informed	24 hours / Ongoing
Notify the Key Regulators	24 hours / Ongoing
Generate reactive press holding statement	24 hours
Notify insurance companies	24-48 hours
Evaluate insurance coverage	24-48 hours
Evaluate payment priorities and concerns	24-48 hours
Assess considerations of and potential notification to local FBI field office and other relevant regulators	48-72 hours
Consider whether communications regarding the incident will be made and enact communication plan	48-72 hours
Evaluate potential disclosure obligations	72 hours
Other Considerations	
Complete OFAC analysis	48 hours