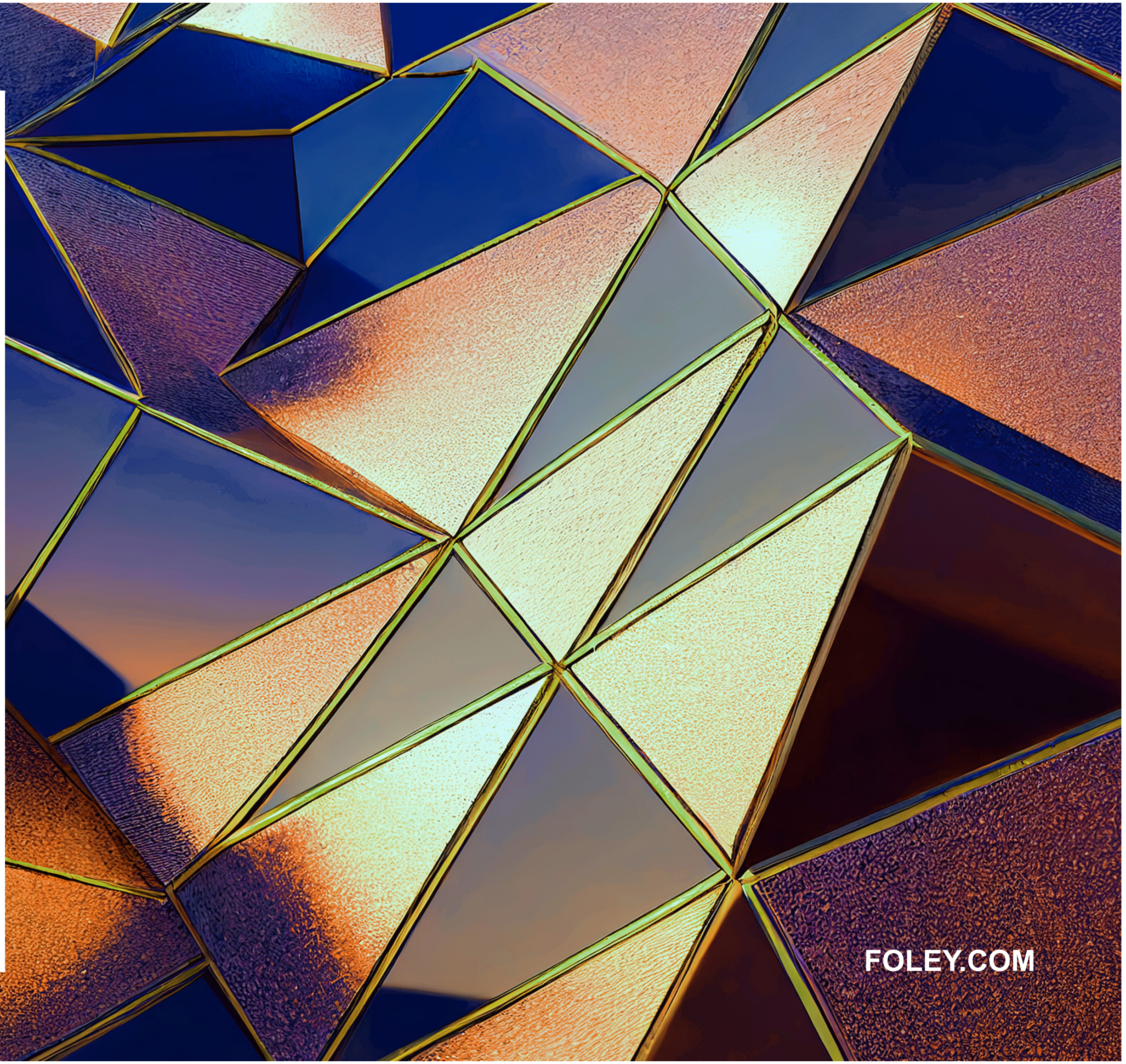
FOLEY

FOLEY & LARDNER LLP

Cybersecurity in Manufacturing and the Supply Chain

December 7, 2023

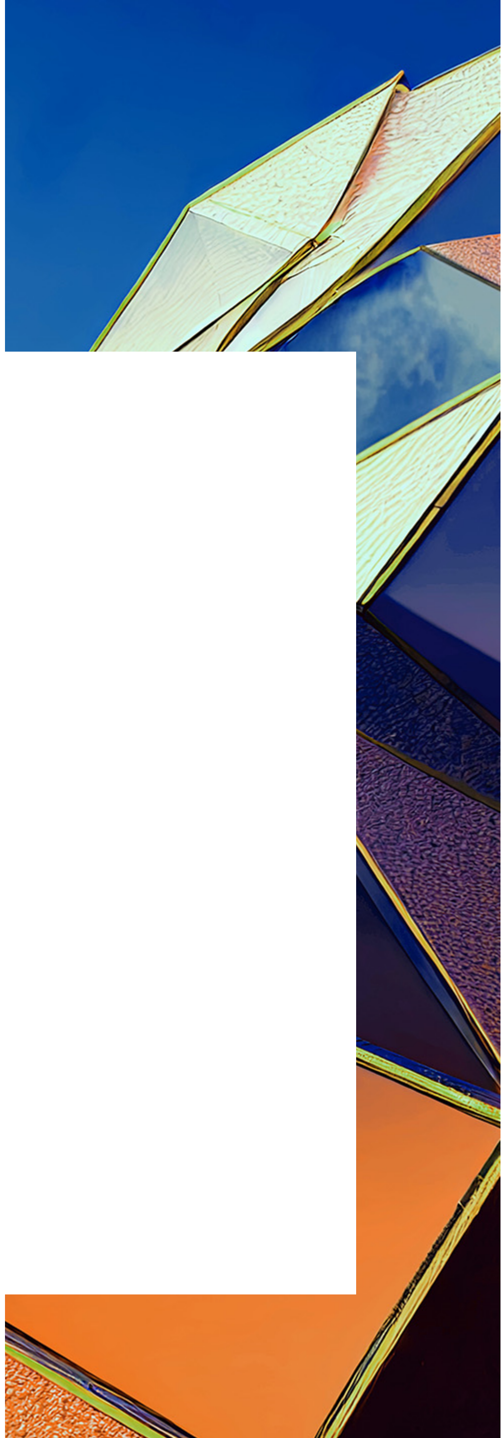


Presenters

Aaron Tantleff
Partner

T: 312.832.4367
E: atantleff@foley.com

Howard Grimes, Ph.D.
Chief Executive Officer
Cybersecurity Manufacturing Innovation Institute
T: 509.432.4652
E: Howard.Grimes@cymanii.org

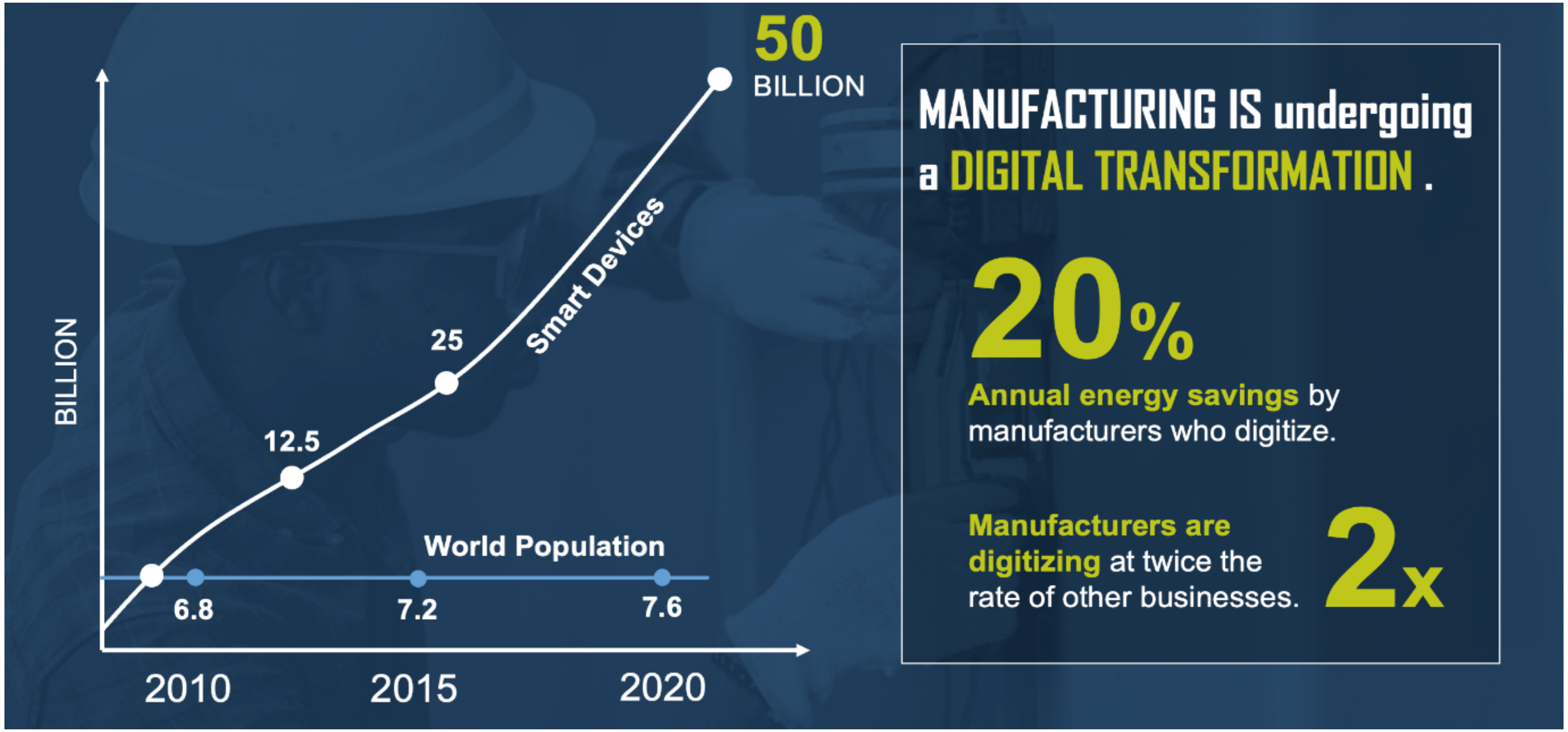


FOLEY

FOLEY & LARDNER LLP

How Did We Get Here?

Cyber Vulnerabilities are On the Rise – Exponentially



Contains trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.
Do not copy, cite, or distribute without permission of the author.

U.S. DEPARTMENT OF ENERGY

CYMANII

Bloomberg

US Edition

Live Now | Markets | Economics | Industries | Tech | AI | Politics | Wealth | Pursuits | Opinion | Businessweek

Opinion | Brooke Sutherland, Columnist

Manufacturers Move to the Front Line of Cyberattacks

The growing rate of hacks at industrial companies is an unpleasant byproduct of a surge of investment in digital connectivity.

November 8, 2023 at 11:35 AM CS

MANUFACTURING NET

VIDEO | ADVERTISE | NEWSLETTER SIGNUP | PODCAST

Aerospace Artificial Intelligence Automotive **Cybersecurity** Energy Industry 4.0 Operations Software Supply Chain

CYBERSECURITY

Manufacturing Segments that Face the Greatest Cyber Risks

Even as cybersecurity strategies improve each year, the sophistication of attacks and capabilities of hackers continue to rise.

By — Isla Sibanda

CYBERSCOOP

Ransomware attacks surge against US manufacturing plants

Cyberattacks against critical infrastructure continues to increase and some sectors, such as manufacturing, take the brunt of abuse.

BY CHRISTIAN VASQUEZ • FEBRUARY 14, 2023

#1 Trusted Cybersecurity News Platform

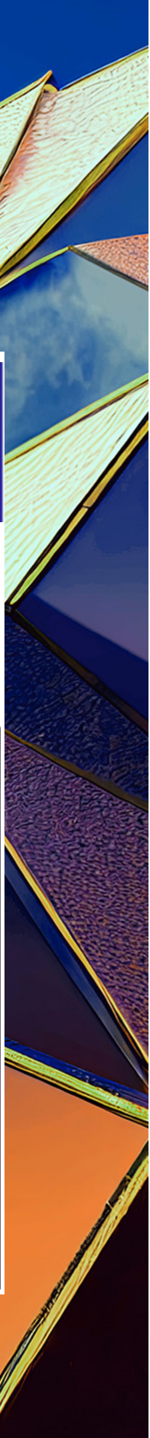
The Hacker News

Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023

Aug 02, 2023 | Newsroom

CVEs by CVSS Criticality, First Half of 2023

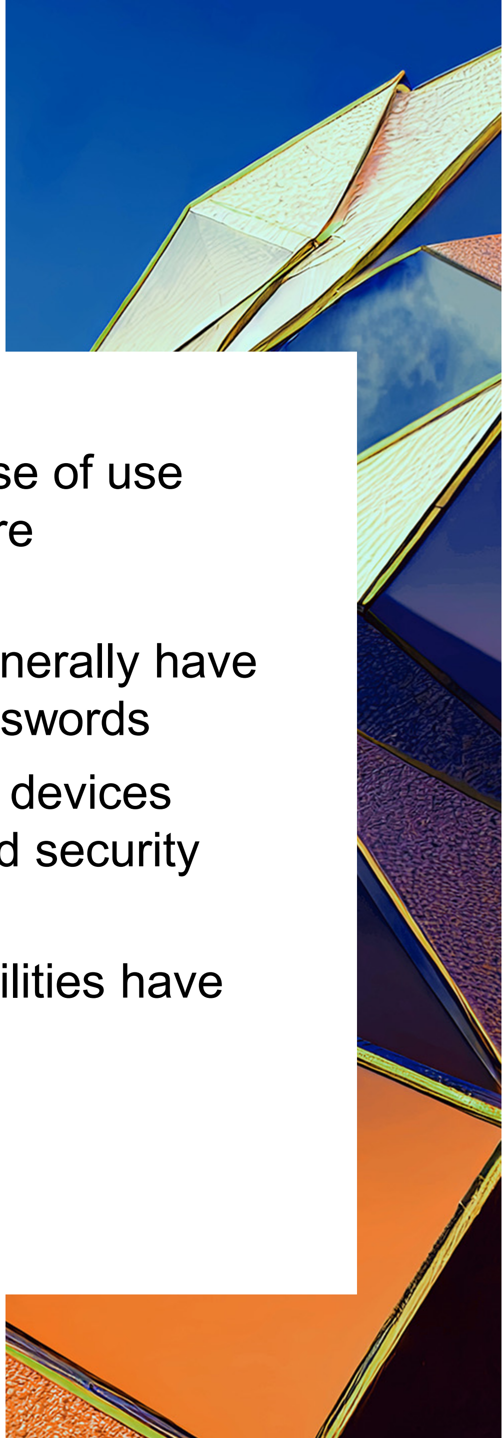
	1H 2023 Count	Percentage of Total (670)	1H 2022 Count	Percentage of Total (681)
Critical	88	13.1%	152	22.3%
High	349	52.1%	289	42.4%
Medium	215	32.1%	205	30.1%
Low	18	2.7%	35	5.1%
	High/Critical	65.2%	High/Critical	64.76%



IoT Cyber Attacks

- "Vulnerable by Design"
  - Systems not designed with security in mind
  - Increasing number of devices talking to each other creates a greater attack surface for cyber attackers to take advantage of
  - Hybrid and remote work environments, along with the proliferation of technology increases the risks posed by connecting or sharing data over improperly secured devices

- Many devices are designed for ease of use and convenience rather than secure operations
  - Consumer grade IoT devices generally have weak security protocols and passwords
  - Commercial/industrial grade IoT devices generally don't follow established security standards
  - Significant, well-known vulnerabilities have persisted for years



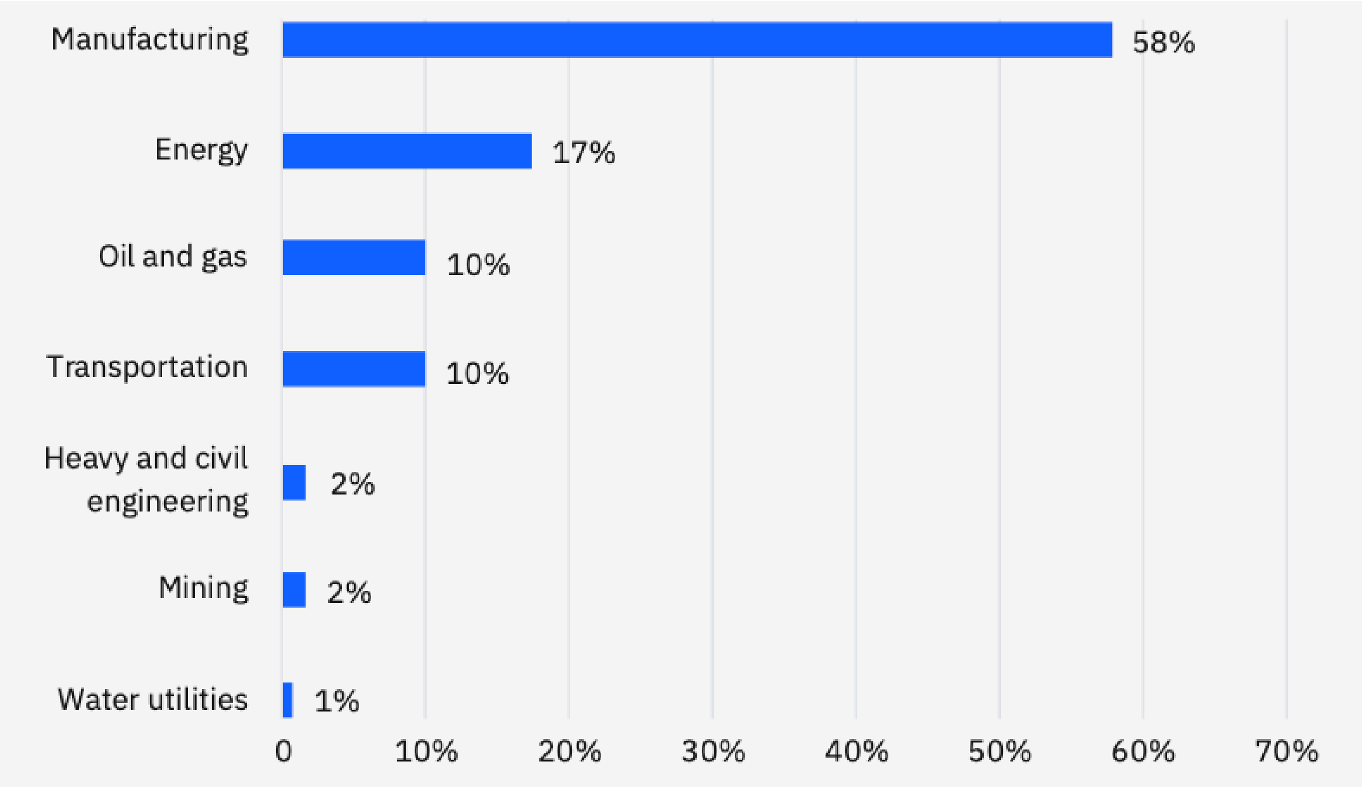
Rate of Ransomware Attacks in Manufacturing

2021	2022	2023
36%	55%	56%

In the last year, has your organization been hit by ransomware? Yes. n=363 (2023), 419 (2022), 438 (2021)

Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Threats to OT and industrial control systems



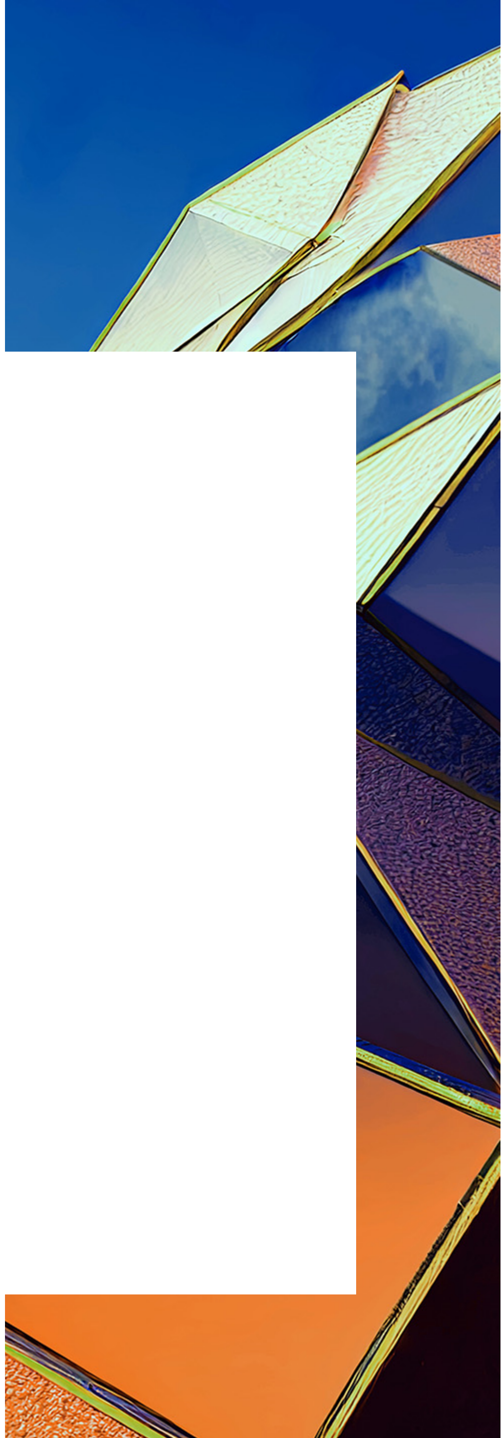
Source: X-Force Threat Intelligence Index 2023, IBM Security

* Proportion of IR cases by OT-related industry to which X-Force responded in 2022

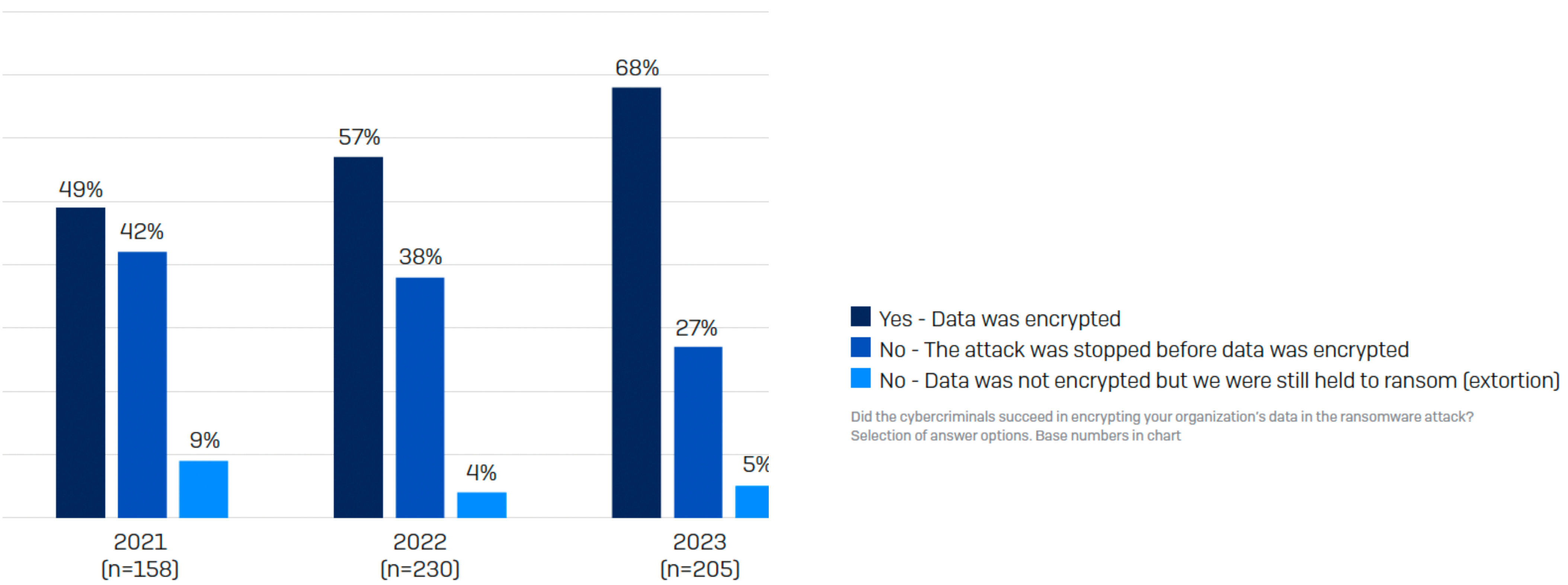
Root Causes of Ransomware Attacks in Manufacturing

	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Exploited vulnerability	24%	36%
Compromised credentials	27%	29%
Malicious email	21%	18%
Phishing	20%	13%
Brute force attack	5%	3%
Download	2%	1%

Source: The State of Ransomware in Manufacturing and Production 2023,
A Sophos Whitepaper. June 2023

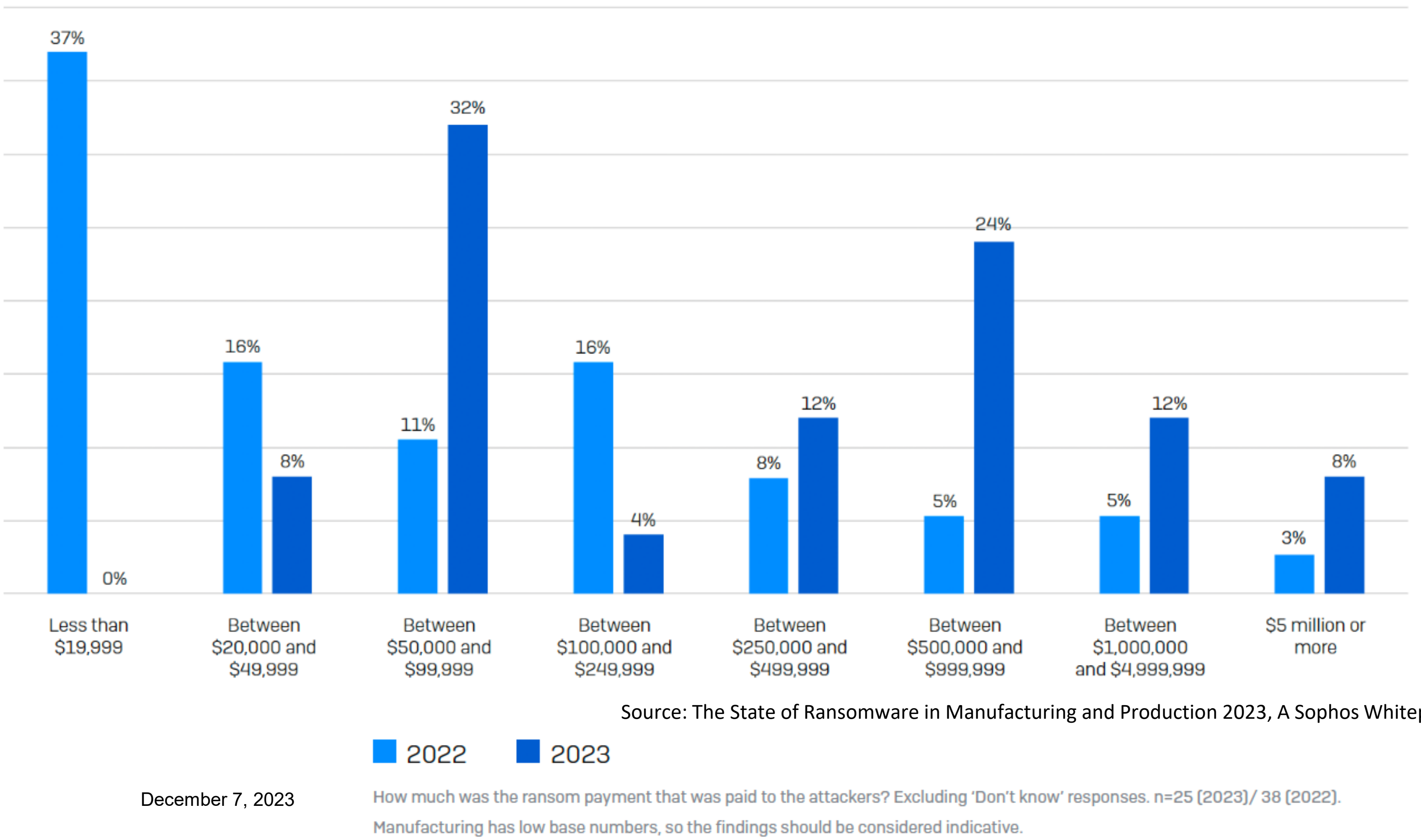


Rate of Data Encryption in Manufacturing



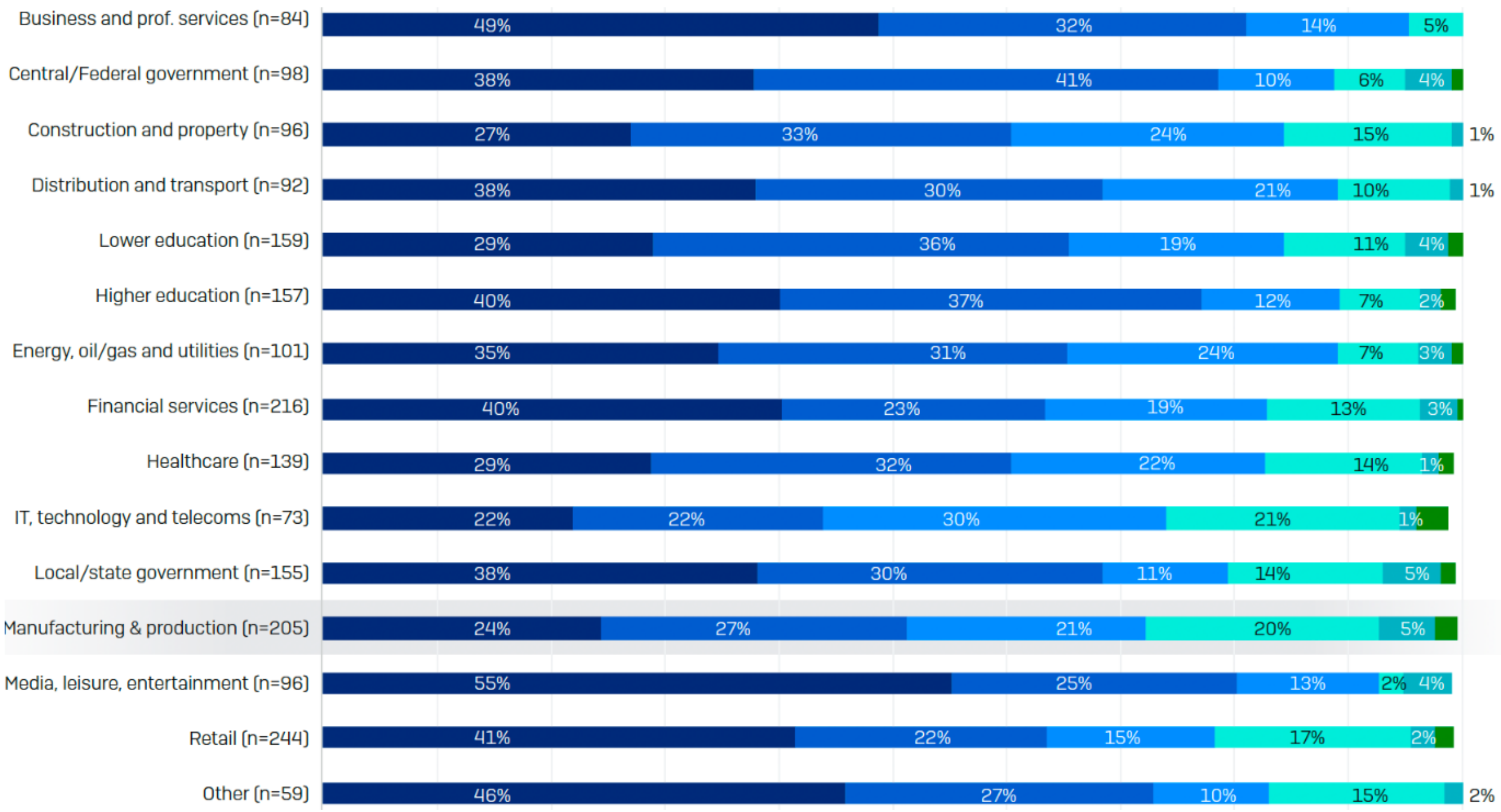
Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Ransom Payments by Manufacturing and Production: 2023 vs. 2022

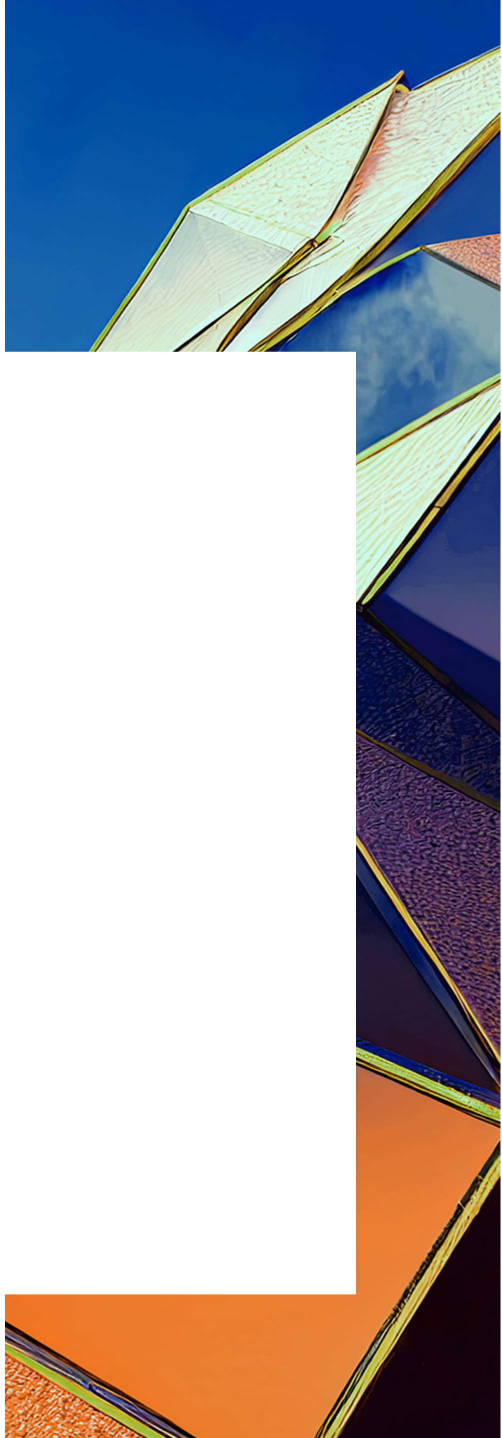


Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Root Cause of Attack by Industry

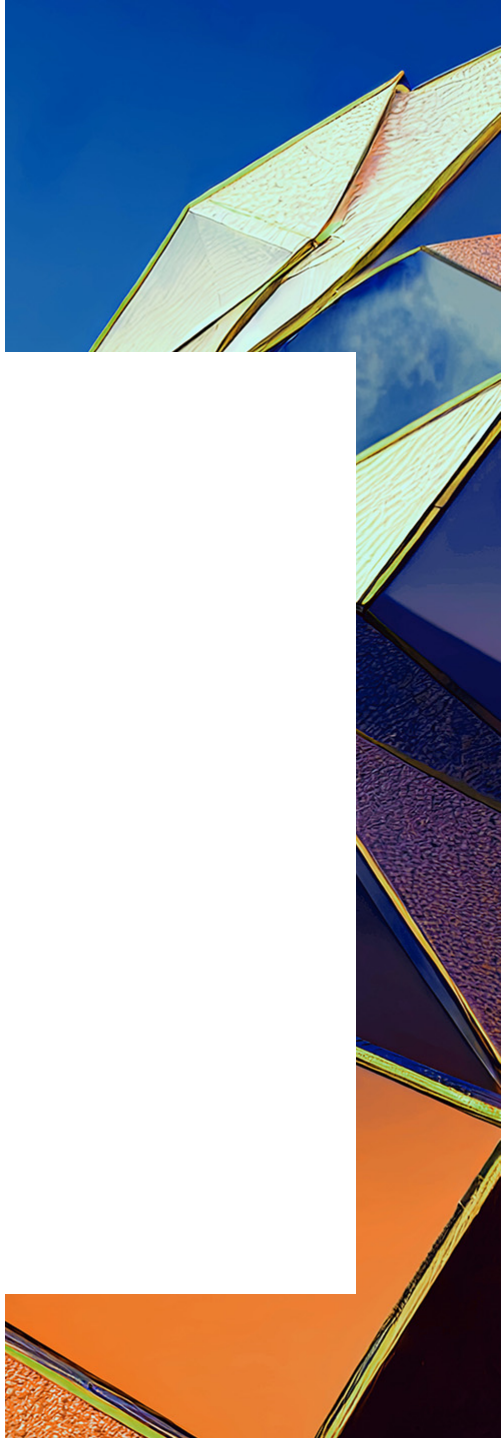


Source: The State of Ransomware in Manufacturing and Production 2023,
A Sophos Whitepaper. June 2023



Navigating the Complex Terrain of Cybersecurity Challenges Today

- A Shortage of Skilled Cybersecurity Professionals
- Supply Chain Vulnerabilities
- Bridging the IT-OT/ICS Gap
- Constantly Evolving Cyber Threat Landscape
- The Proliferation of Industrial Internet of Things (IIoT)
- Increased Sophistication and Funding of Adversaries



FOLEY

FOLEY & LARDNER LLP

Legal Implication, Obligations, and Liabilities

FOLEY

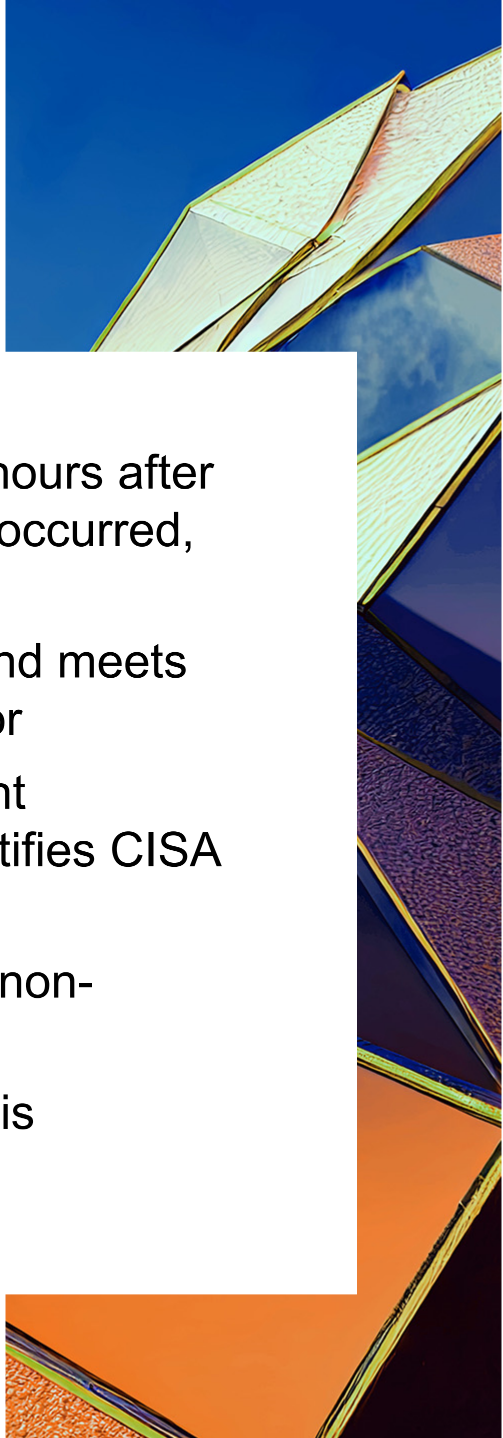
FOLEY & LARDNER LLP

Current Legislation and Legal Obligations

The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018

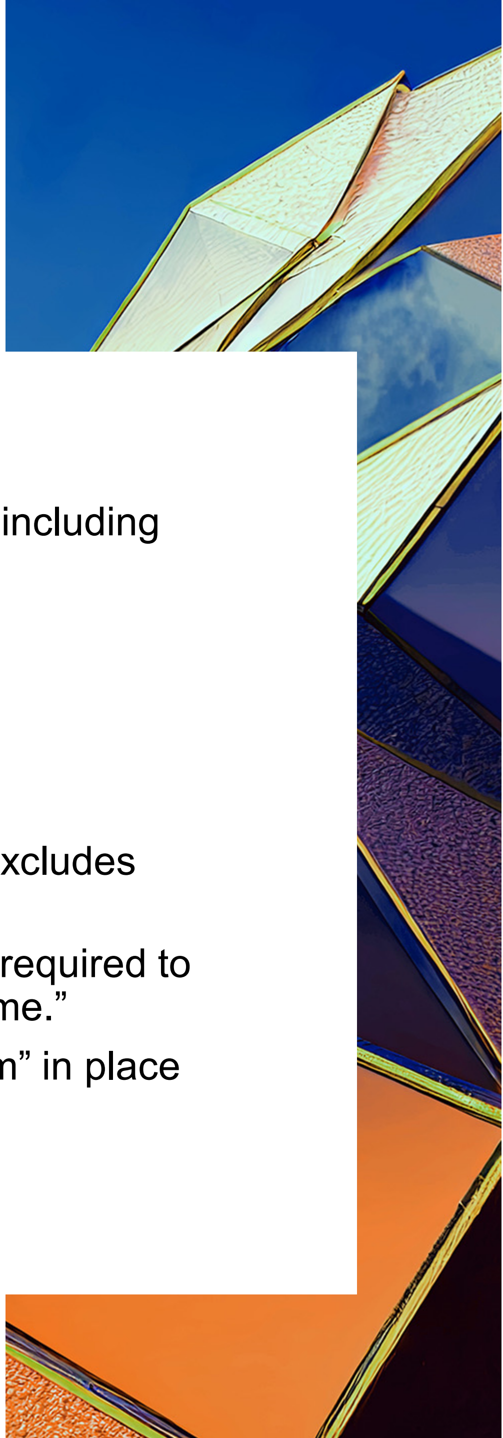
- Rapid Deployment
- Incident Analysis
- Threat Intelligence Sharing

- Report certain covered cyber incidents to CISA within 72 hours after the entity "reasonably believes" that such an incident has occurred, and ransomware payments within 24 hours
  - A "covered cyber incident" as one that is "substantial" and meets the "definition and criteria" to be set by the CISA Director
- Required to submit updates as "substantial new or different information becomes available" until the covered entity notifies CISA that the incident has been fully mitigated and resolved.
- Voluntary reporting of incidents and ransom payments by non-covered entities
- Voluntary provision of additional information beyond what is mandatory by covered entities



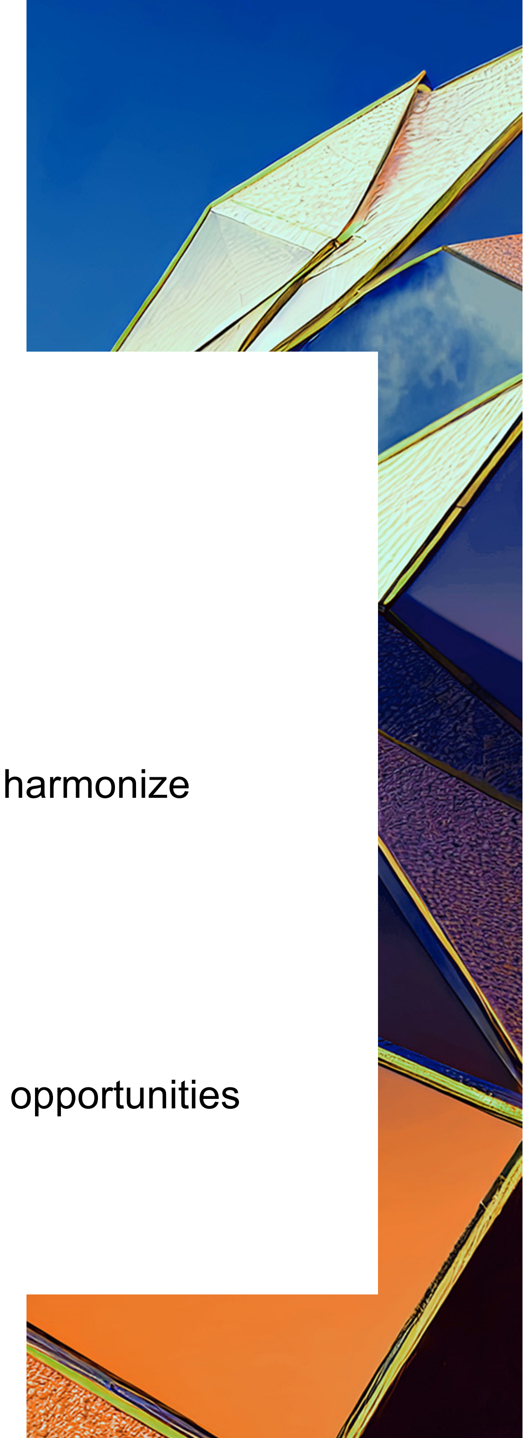
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

- Required and voluntary reporting will receive certain protections
  - Reports cannot be used by CISA, other federal agencies, or any state or local government to regulate, including through enforcement action, the activities of the covered entity that submitted the report;
  - Considered commercial, financial, and proprietary information if so designated;
  - Exempt from disclosure under freedom of information laws and similar disclosure laws;
  - Do not constitute a waiver of any applicable privilege or protection provided by law; and
  - Are not subject to a federal rule or judicial doctrine regarding *ex parte* communications
  - No cause of action based on the report (does not prevent litigation based on underlying incident), but excludes actions to enforce subpoena by federal government
  - But excludes reporting requirements covered entities that, “by law, regulation, or contract,” are already required to report “substantially similar information to another Federal agency within a substantially similar timeframe.”
    - Only available only if the relevant federal agency has an “agency agreement and sharing mechanism” in place with CISA
  - Reports to be available to Sector Risk Management Agencies and federal agencies within 24 hours



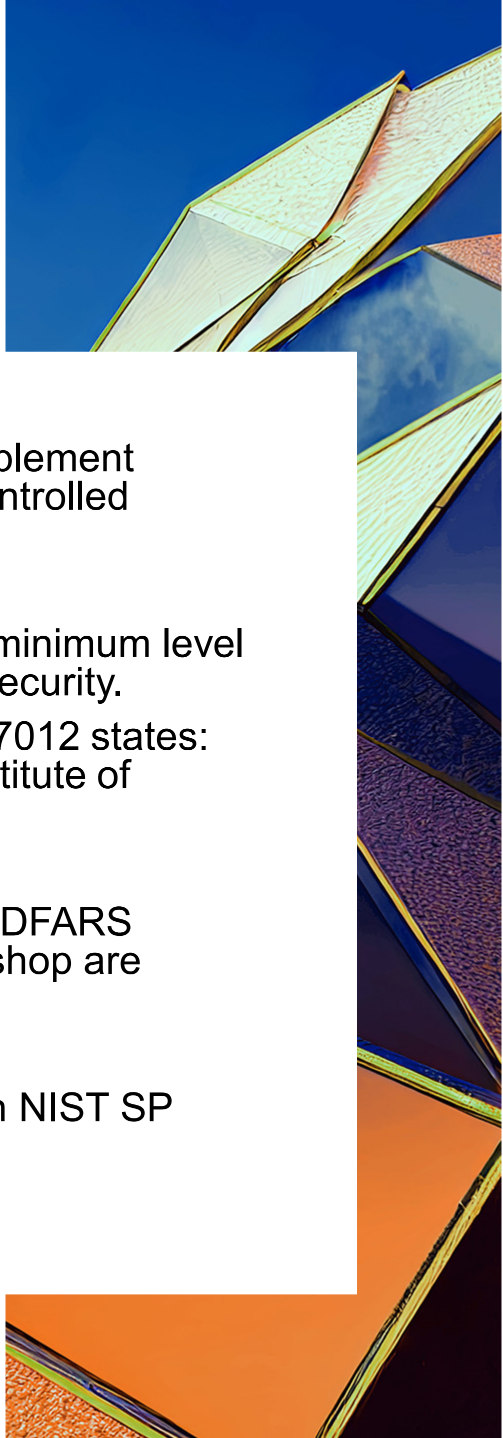
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

- Failure to submit a required report
  - CISA Director may issue a subpoena
  - Referral of the matter to the Department of Justice
  - Denied covered entities some of the protections for failure to comply
- Up Next
  - Cyber Incident Reporting Council
    - DHS to lead an intergovernmental Cyber Incident Reporting Council to “coordinate, deconflict, and harmonize Federal incident reporting requirements”
  - Ransomware Vulnerability Warning Pilot Program
    - Identify the most common security vulnerabilities in ransomware attacks
    - How to defend, mitigate, and contain the security vulnerabilities
  - Joint Ransomware Task Force
    - “coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.”



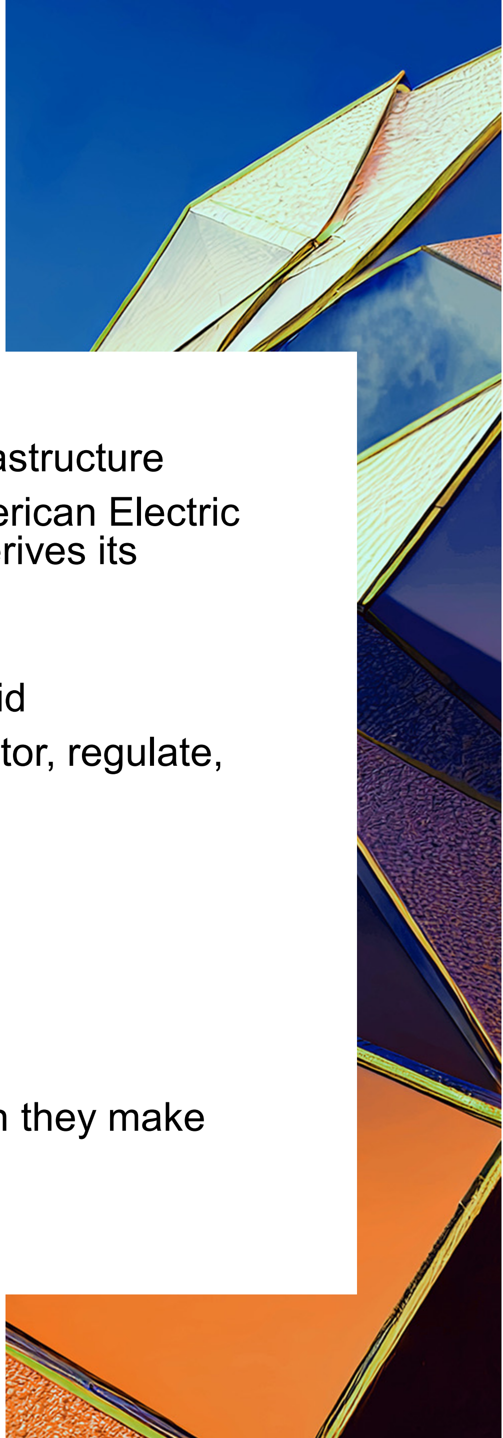
Defense Federal Acquisition Regulation Supplement (DFARS)

- All Department of Defense (DoD) contractors must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum cybersecurity standards or risk losing federal contracts. This includes safeguarding controlled unclassified information (CUI) and complying with the NIST Special Publication 800-171 standards.
- NIST 800-171
  - Cybersecurity standard rather than a regulatory requirement, but commonly understood to establish a minimum level of good cybersecurity practice/guidance akin to a requirement to meet DFARS requirements for cybersecurity.
  - DFARS is a DoD publication that sets the rules for participating in defense contracts. DFARS 252.204-7012 states: “the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171”
- Cybersecurity Maturity Model Certification (CMMC)
  - Unified cybersecurity standard that adds a verification component to the cybersecurity requirements in DFARS 252.204-7012. Establishes different levels so that the cybersecurity requirements for a small machine shop are simpler and easier to meet than those for a Tier 1 original equipment manufacturer (OEM).
  - All DoD contracts to ensure CMMC compliance by October 21, 2025
  - To be eligible for DoD contracts, a contractor must complete a self-assessment of their compliance with NIST SP 800-171
- Failure to meet these requirements can result in contract termination and legal consequences.



Federal Energy Regulatory Commission (FERC)

- FERC establishes cybersecurity standards for the energy sector to protect the nation's critical energy infrastructure
  - Cybersecurity standards for the bulk power system in the United States are governed by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards (NERC derives its authority from FERC)
  - Covers United States, Canada, and parts of Mexico
  - Failure to comply can result in penalties, loss of licenses, and damage to the reliability of the energy grid
- Framework of 14 ratified and proposed standards that outline recommended controls and policies to monitor, regulate, manage and maintain the security of critical infrastructure systems
  - CIP-003-9 Cyber Security – Security Management Controls.
  - CIP-004-6 Cyber Security -- Personnel and Training.
  - CIP-008-6 Cyber Security -- Incident Reporting and Response Planning.
  - CIP-013-1 Cyber Security -- Supply Chain Risk Management.
  - CIP-014-1 Physical Security.
- New voluntary cyber incentive framework allow utilities to apply for an incentive-based rate recovery when they make certain pre-qualified cybersecurity investments or join a threat information-sharing program



FOLEY

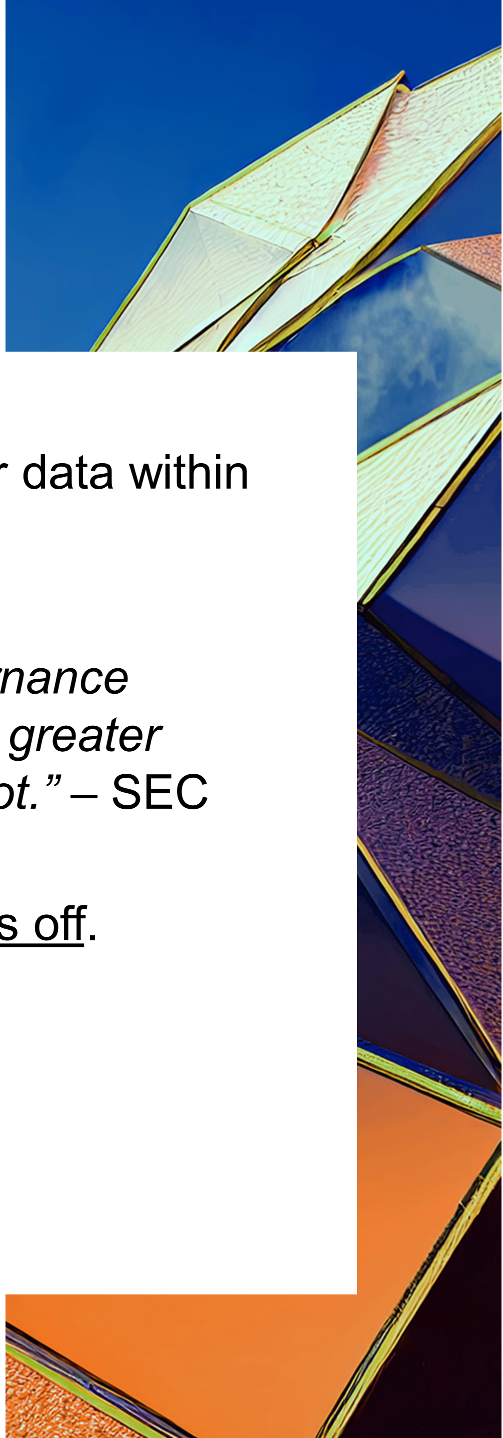
FOLEY & LARDNER LLP

The U.S. Securities and Exchange Commission (SEC)

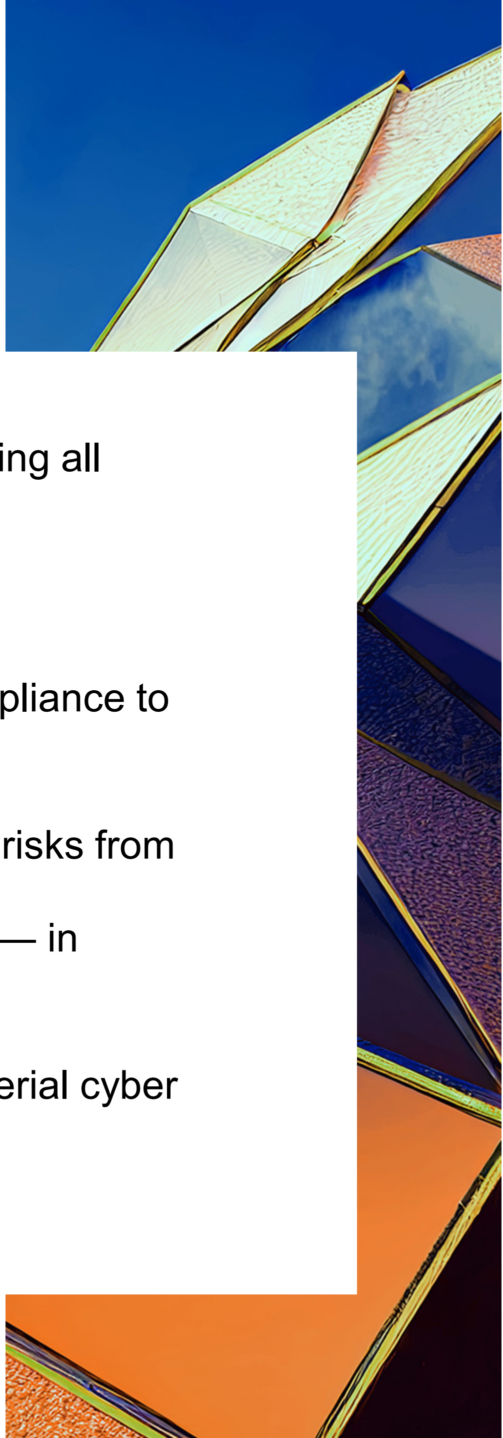
FOLEY.COM

Understanding the New SEC Cybersecurity Rules

- …they're calling your bluff. Be transparent about how you protect your systems and your data within them…with a focus on the interests of an informed, "reasonable investor."
- Any kind of cyber-related incident matters. This is not another "data breach" regulation.
- *"To the extent investors view strong cybersecurity risk management, strategy, and governance favorably, registrants disclosing more robust processes, more clearly, could benefit from greater interest from investors, leading to higher market liquidity relative to companies that do not."* – SEC Cybersecurity Risk Management Final Rule
- The SEC is creating a market condition where long-term planning and transparency pays off.



Final SEC Cybersecurity Disclosure Rules: Overview

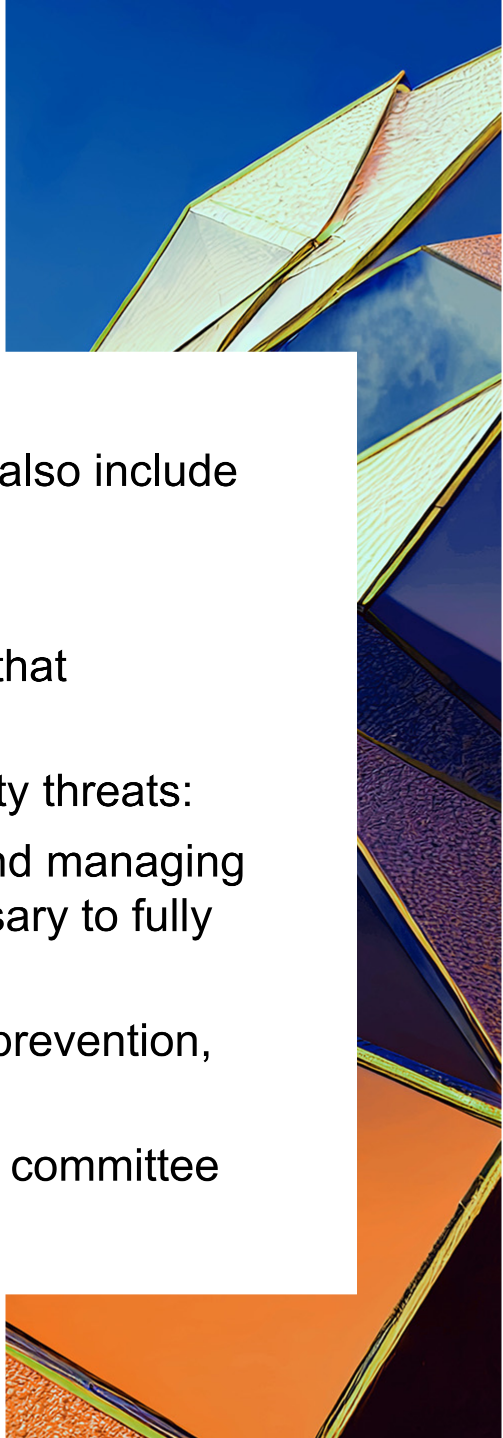


- Additional disclosure requirements for U.S. reporting companies, as well as foreign private issuers, including all companies with stock traded on U.S. stock exchanges (together, “public companies”)
- The final rule was effective on September 15, 2023, with compliance dates of:
  - Form 10-K disclosure: For all companies for the fiscal year ending on or after **December 15, 2023**, in upcoming annual reports
  - Incident reporting on Form 8-K: Beginning on December 18, 2023 (with an additional 180 days for compliance to June 15, 2024, for smaller reporting companies)
- Annually on Form 10-K:
  - Describe a company’s **risk management** processes for assessing, identifying, and managing material risks from cybersecurity threats
  - Discuss the **governance framework** — including the Board’s oversight role, and management’s roles — in assessing and managing material cybersecurity risk
- Current/incident reporting on Form 8-K:
  - Public reporting of material incidents within four business days of a determination that there was a material cyber incident occurring on a company’s IT system
  - Disclosure of any material updates on an ongoing basis

SEC Annual Reporting on Form 10-K: Disclosure Items

- In each Form 10-K, filed publicly via the SEC's EDGAR system, a public company must now include **cyber risk management** disclosures
- Description of processes for assessing, identifying, and managing material risks for cybersecurity threats in sufficient detail for a reasonable investor to understand, such as:
  - Whether and how any such processes have been integrated into the company's overall risk management system or processes;
  - Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
  - Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider
- Explanation of whether (and, if so, how) any risks from cybersecurity threats, including previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition
  - SEC provides examples of risks, including disruption to business operations, theft of IP, harm to customers or employees, reputational harm, legal risks

SEC Annual Reporting on Form 10-K: Disclosure Items (cont'd.)

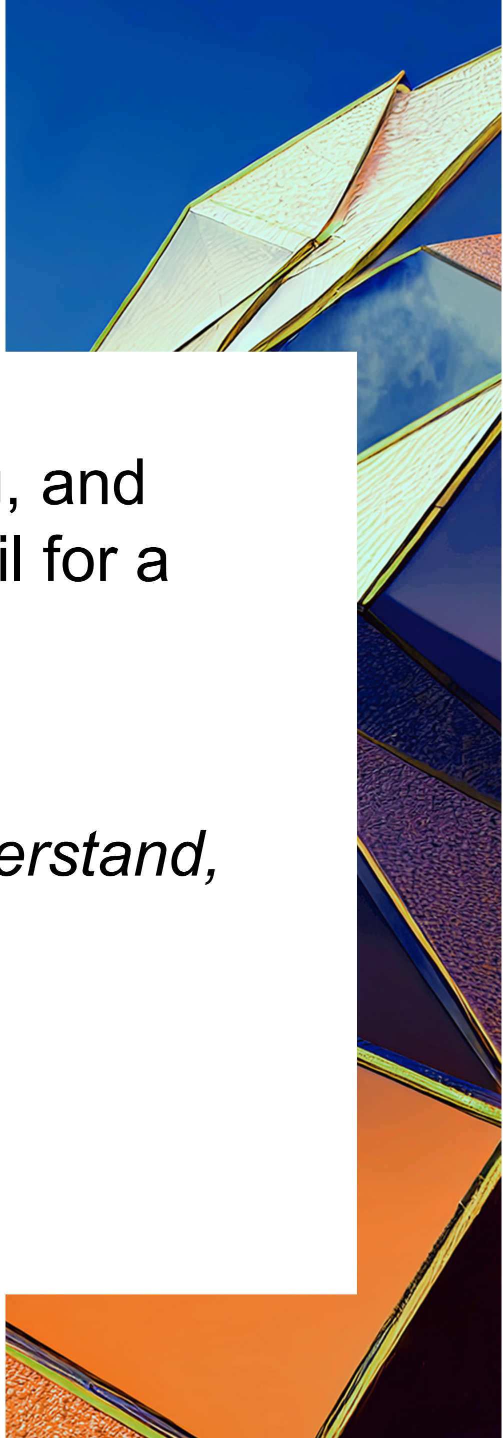


- In each Form 10-K, filed publicly via the SEC's EDGAR system, a public company must now also include **cyber governance** disclosures
- The Board's oversight of risks from cybersecurity threats
  - What Board committee, if any, is responsible for cyber risk oversight; a description of how that committee is informed of risks
- Management's role in assessing and managing the company's material risk from cybersecurity threats:
  - Whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
  - The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
  - Whether such persons or committees report information about such risks to the Board or a committee or subcommittee of the Board

Form 10-K Disclosure Requirement: Processes

Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes

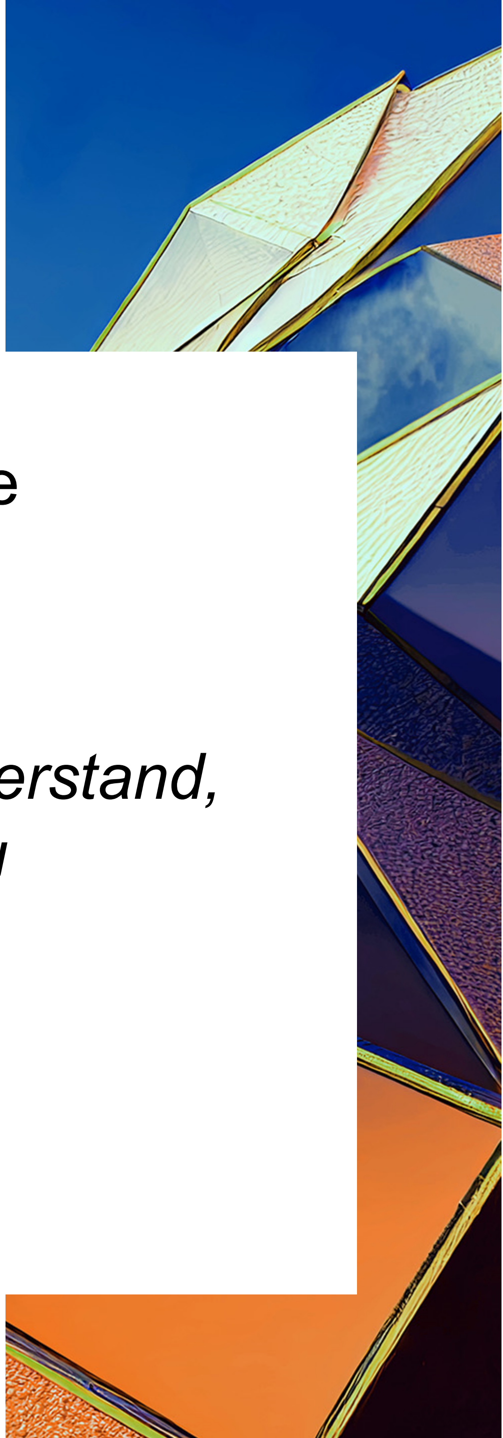
The market sees this: *"Please tell investors, in a way they will understand, how you manage the cybersecurity risks that may hurt them."*



Form 10-K Disclosure Requirement: Processes (cont’d.)

Whether and how any such processes have been integrated into the registrant’s overall risk management system or processes

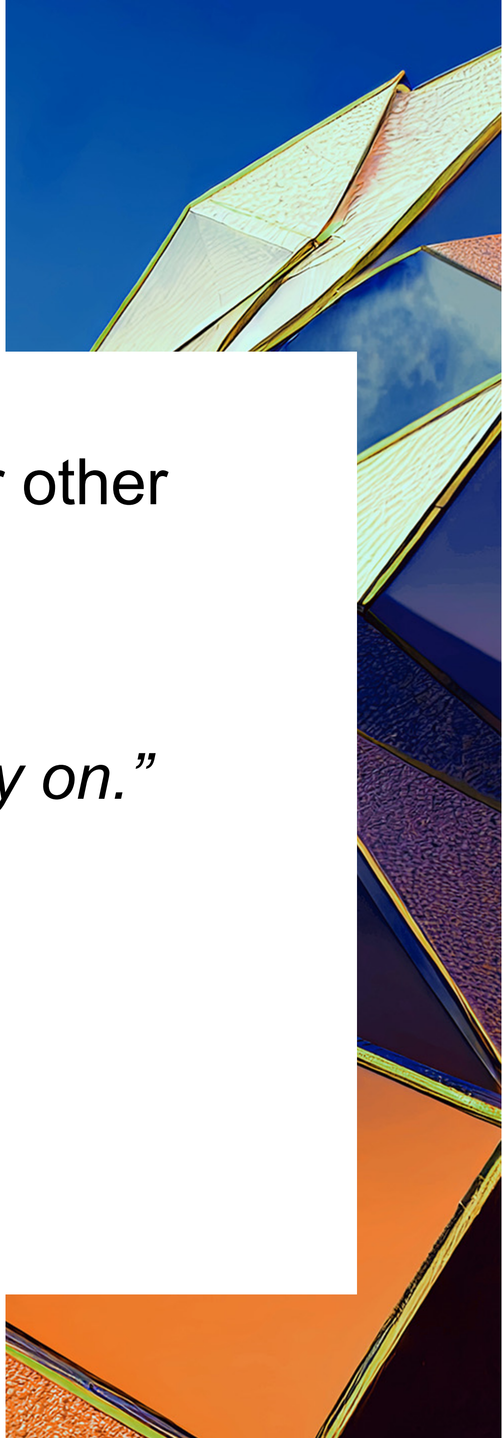
The market sees this: *“Please tell investors, in a way they will understand, how you make cybersecurity risk as important as the other risks you manage.”*



Form 10-K Disclosure Requirement: Processes (cont’d.)

Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes

The market sees this: *“Please tell investors what expertise you rely on.”*



Form 10-K Disclosure Requirement: Processes (cont'd.)

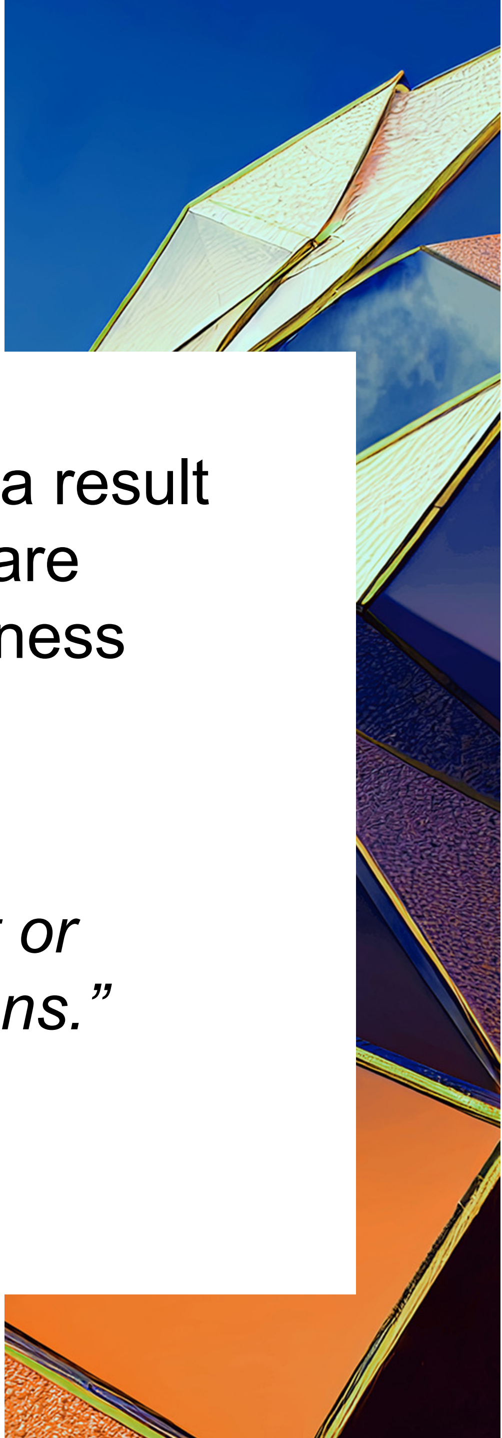
Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider

The market sees this: *"Please tell investors whether you consider third parties who pose risks to you as a risk to your investors."*

Form 10-K Disclosure Requirement: Risks

Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how

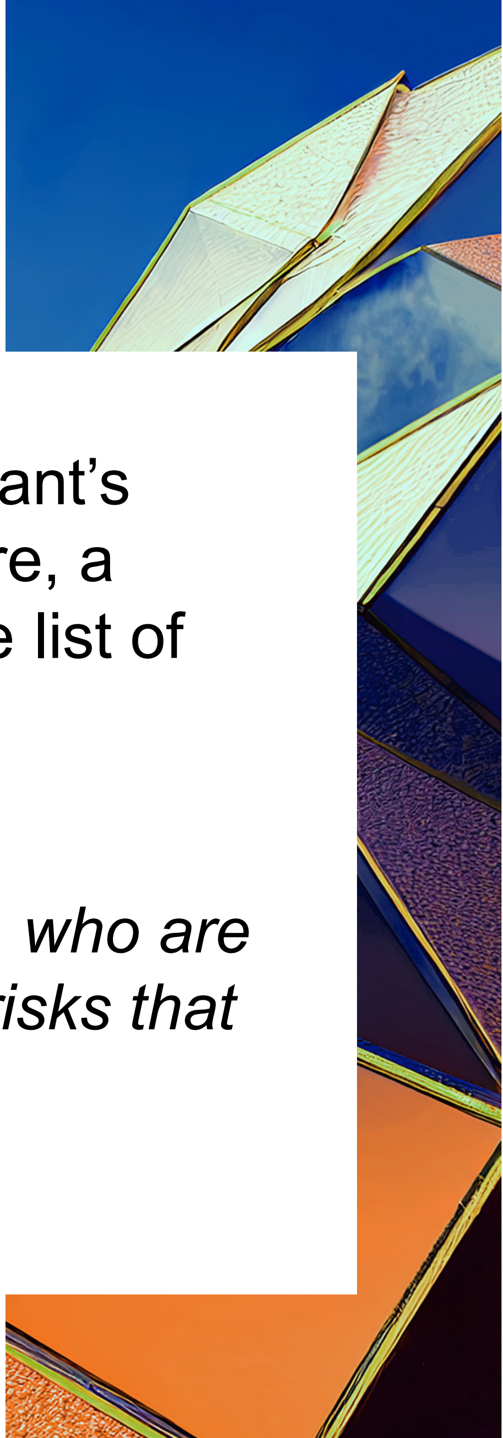
The market sees this: *"Please tell investors about how any current or previous incidents should inform their voting and investment decisions."*



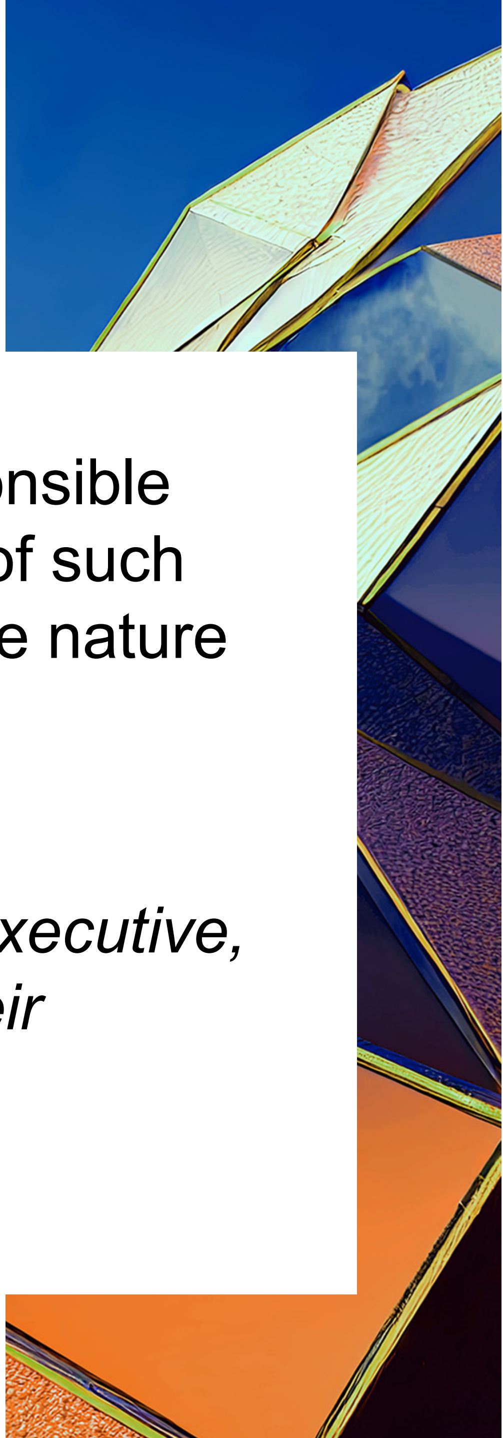
Form 10-K Disclosure Requirement: Risks (cont'd.)

Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

The market sees this: *"Please tell investors whether management, who are responsible for running the company, are involved in cybersecurity risks that pose a risk of harm to investors."*



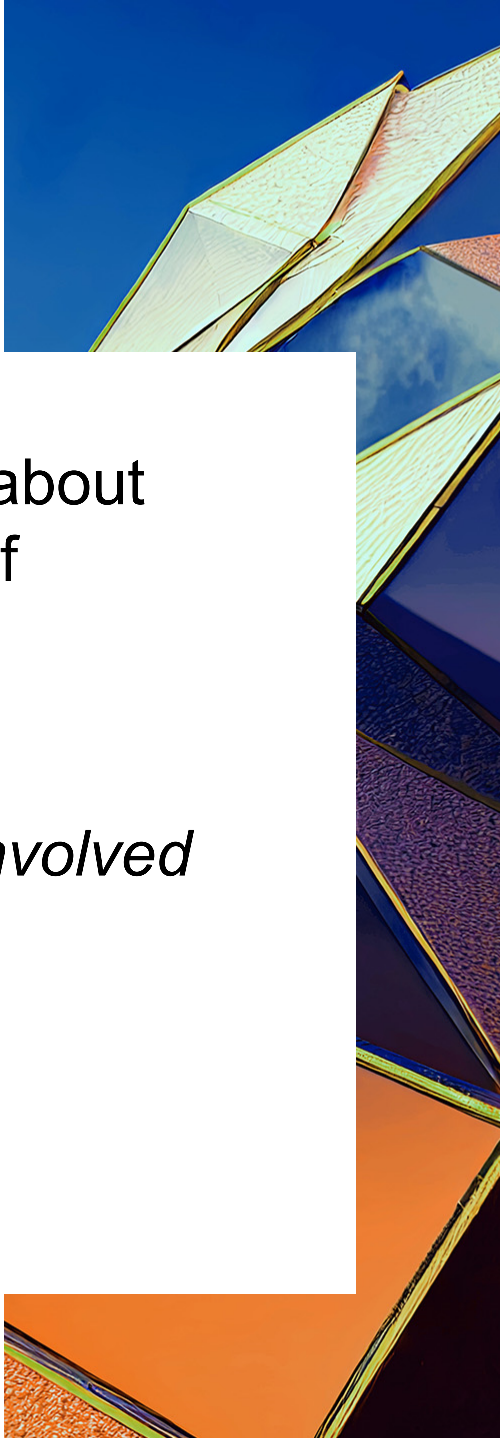
Form 10-K Disclosure Requirement: Governance



Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise

The market sees this: *"Please tell investors which management, executive, or director positions are involved in cybersecurity risks and what their expertise is."*

Form 10-K Disclosure Requirement: Governance (cont'd.)



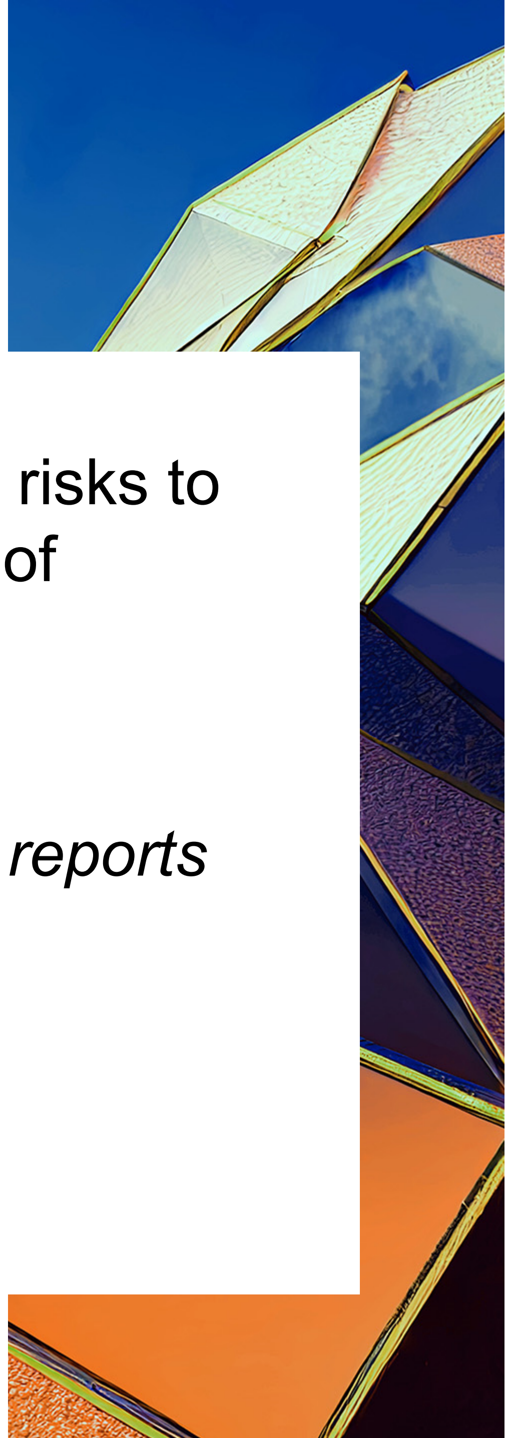
The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents

The market sees this: *"Please tell investors how management is involved in cybersecurity incident management."*

Form 10-K Disclosure Requirement: Governance (cont'd.)

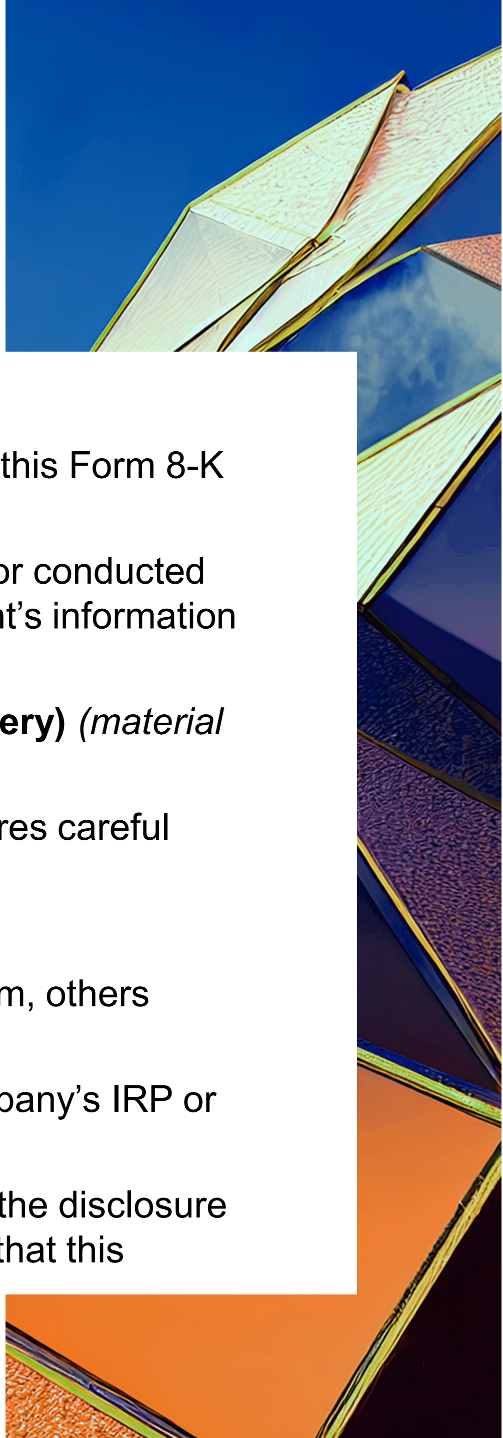
Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors

The market sees this: *"Please tell investors whether management reports incidents to investors."*



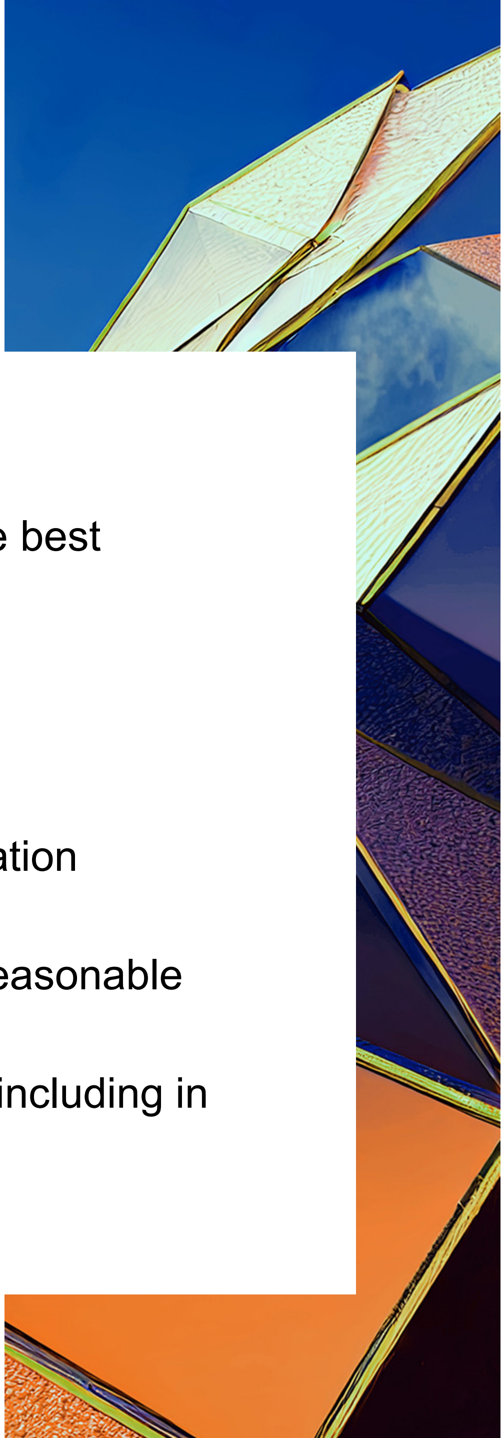
SEC Material Event Reporting on Form 8-K: Required Disclosure of Material Cybersecurity Incidents

- The SEC's rule established a new item 1.05 to Form 8-K requiring disclosure of a material cybersecurity incident; this Form 8-K filing is made via the SEC's EDGAR system and is publicly available to all
- "Cybersecurity incident" means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein
- Reporting is **required within four business days** of a determination of **materiality (<u>not</u> date of incident discovery)** *(material updates to be made on subsequent Form 8-K amendments)*
  - Determination of materiality may not occur for a substantial period of time after an incident is discovered; requires careful documentation of process
  - Important to be diligent in evaluating incidents to make materiality determinations without unreasonable delay
    - Appropriate personnel at company must be involved: legal, CISO, disclosure committee, Board, finance team, others involved with IRP
  - May be necessary to re-evaluate materiality if an incident is re-classified to a higher classification under a company's IRP or significant new facts become known
  - Rule allows a company to delay disclosure for up to 30 days if the U.S. Attorney General notifies the SEC that the disclosure would pose a substantial risk to national security or public safety; will be in only "extraordinary circumstances" that this exemption will arise

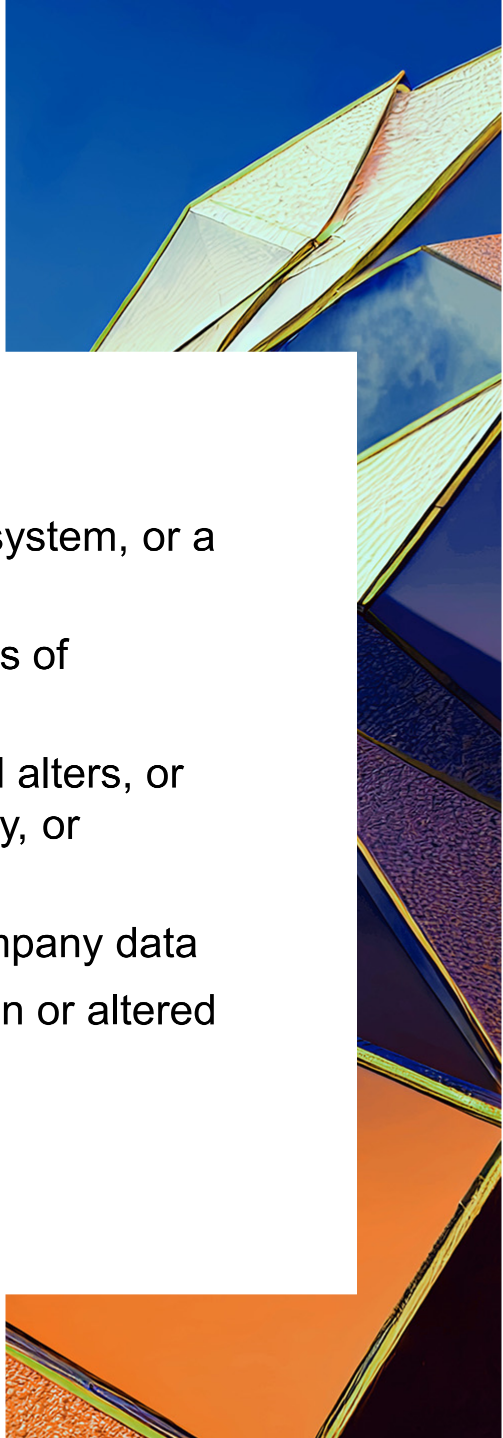


When is an Incident “Material” for Purposes of Form 8-K Reporting?

- Materiality is a legal determination based on the "facts and circumstances" of the matter
- The SEC has declined to identify what it believes to be material, stating that each company is in the best position to know what is material to its own investors
  - Factors to be considered include:
    - The nature, extent, and potential magnitude of the risk/incident
    - The range of potential harms to various stakeholders
    - Whether there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision
    - If not disclosed, whether disclosure of the omitted information would have been viewed by a reasonable investor as having significantly altered the total mix of information available
  - Consider intersection with other materiality determinations made for financial reporting reasons, including in periodic reporting and financial statement footnotes, though other contexts not determinative

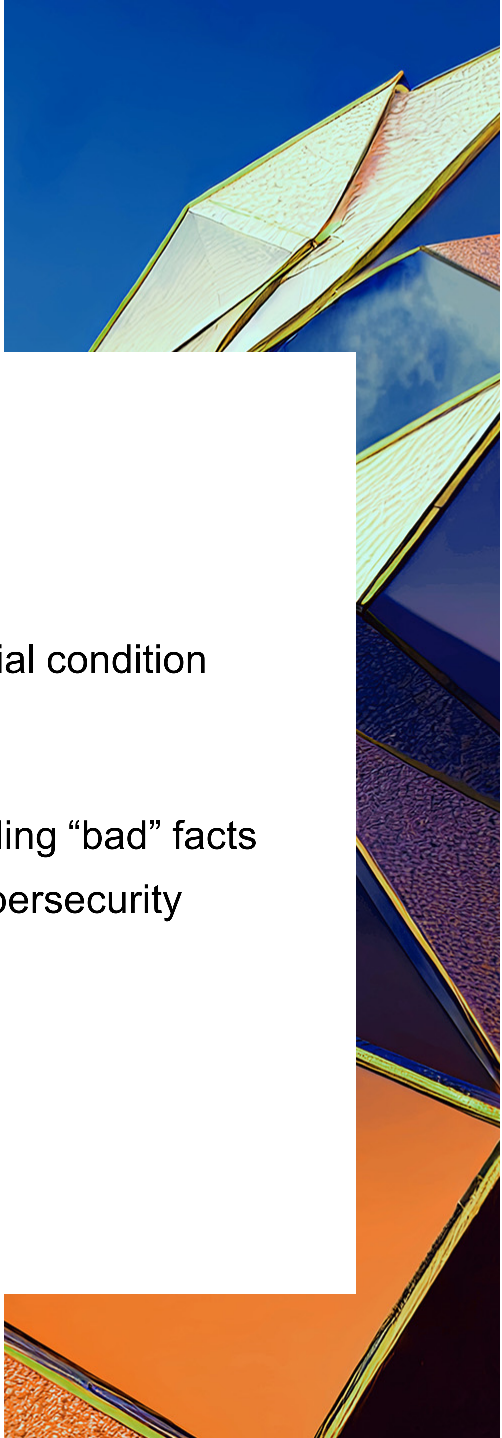


When is an Incident "Material" for Purposes of Form 8-K Reporting? (cont'd.)



- **Examples from the SEC's final release of incidents that may be material include:**
  - An unauthorized incident that compromises the confidentiality, integrity, or availability of data, a system, or a network, or violates the company's security policies or procedures
  - An unauthorized incident that causes degradation, interruption, loss of control, damage to, or loss of operational technology systems
  - An incident in which an unauthorized party accesses (or a party exceeds authorized access) and alters, or has stolen, sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the company
  - An incident in which a malicious actor offers to sell or threatens to publicly disclose sensitive company data
  - An incident in which a malicious actor demands payment to restore company data that was stolen or altered

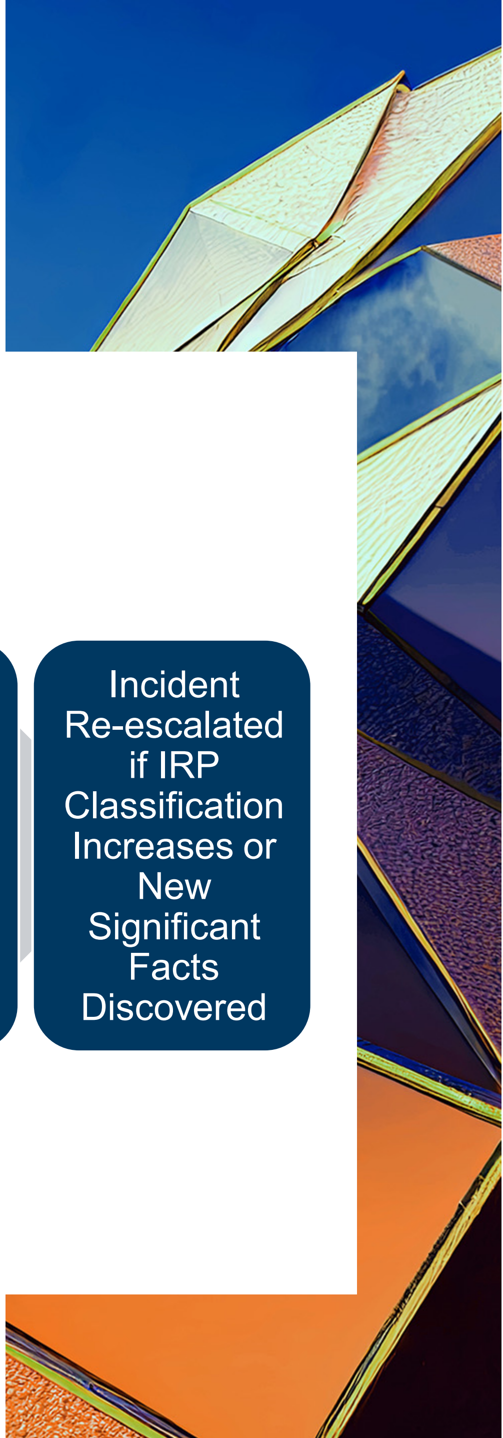
Content of Form 8-K: Disclosure of Material Incidents



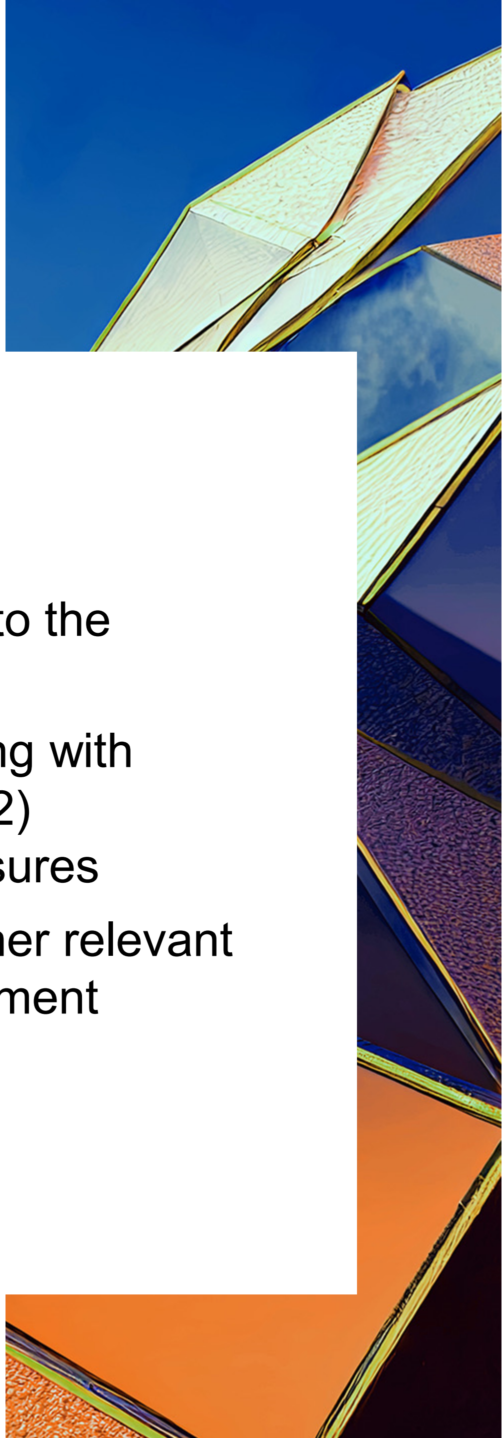
- **Disclosures should be information relevant to investors, not a road map for hackers!**
- Required disclosure content, if known, includes:
  - Material aspects of the nature, scope, and timing of the incident
  - Material impact (or reasonably likely material impact) of the incident on the company, e.g., on its financial condition and results of operations
  - Additional material information may be added as it becomes available on a Form 8-K/A
  - All disclosure must be materially accurate and complete; cannot share “good” facts and not corresponding “bad” facts
  - Do not need to disclose technical information about a planned response to the incident or impacted cybersecurity systems, related networks and devices, or potential system vulnerabilities
- Legal, CISO, financial reporting, etc., will work together to:
  - Disclose sufficient information to satisfy reporting requirements
  - Avoid disclosing information that may compromise the company’s security or remediation efforts
  - Ensure appropriate people across the organization have had the chance to review

Example: Incident Reporting Process Overview

1. Incident Occurs
2. Activate IRP
3. Classify Incident Per IRP
4. Incidents Classified Medium & Above Are Escalated
5. Who Determines if Incident is Material
6. Material Incidents Publicly Disclosed on Form 8-K Within Four Days
7. Incident Updates As Necessary on Amended Form 8-K
8. Incident Re-escalated if IRP Classification Increases or New Significant Facts Discovered



Examples of CISO Involvement in the New Disclosures

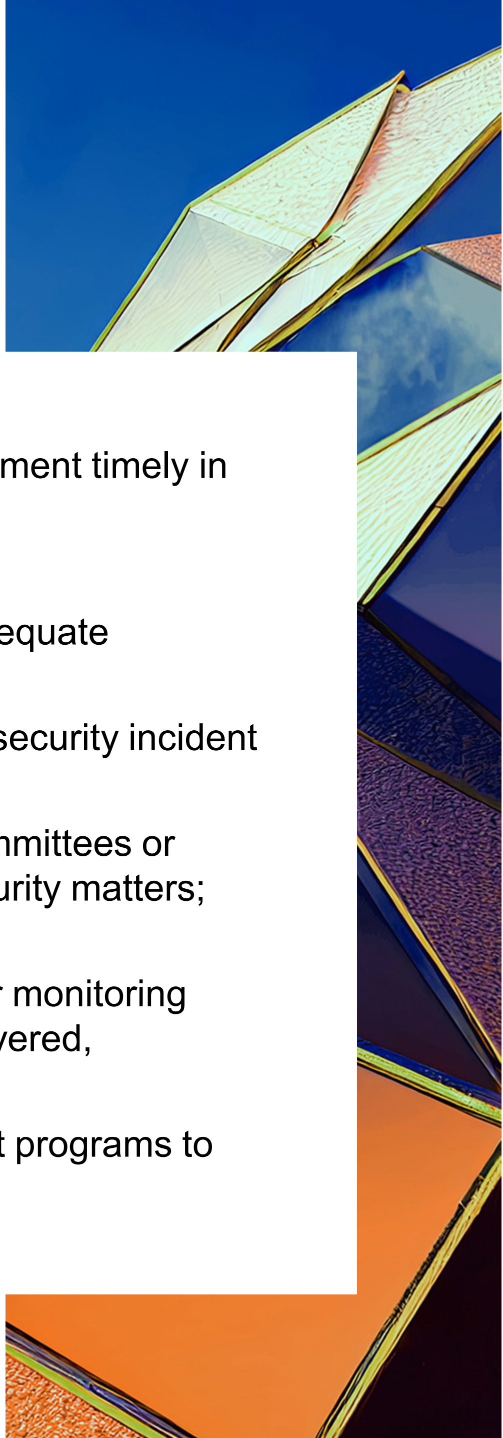


CISO involvement will be needed for:

- Accurately describing the new disclosures required in the Form 10-K
- Creating a materiality framework that may form a basis for decision-making with regard to the materiality of any future cyber incidents; prepare the framework on a “clear day”
- Assisting with (1) determining the materiality of a cyber incident to inform decision-making with regard to potential Form 8-K reporting and, once an incident is deemed to be material; (2) describing material incidents for inclusion in a Form 8-K and later, ongoing public disclosures
- Preparing a regular presentation to the Audit Committee of the Board of Directors (or other relevant committee) about potential cyber risks, cyber incidents, and the company’s risk management processes
- Advising the Board of Directors on strategies for mitigating cyber risks

Process Considerations to Support New Disclosures

- Evaluate cyber incident reporting disclosure controls and procedures to ensure information is elevated to management timely in light of the four business-day requirement to file an Item 1.05 Form 8-K
- Review and test IRPs to ensure incidents are appropriately reported throughout the organization
- IRPs should be regularly reviewed and tested, ideally through mock tabletop exercises, to ensure a timely and adequate response
- Consider delineating within the IRP or otherwise the personnel/team responsible for determining whether a cybersecurity incident is material as well as specific decision-making and documentation processes
- Boards should still be cognizant of which directors have expertise or experience with cybersecurity and which committees or subcommittees, if any, are responsible, or should be responsible, for providing oversight with respect to cybersecurity matters; amend governance documents accordingly
- To prepare for disclosure: Identify and document, if not already clear under current policies, who is responsible for monitoring risks from cybersecurity threats, how cybersecurity risks are identified, and how cybersecurity incidents are discovered, mitigated, and remedied
- There will be increased pressure for registrants to develop comprehensive, risk-based cybersecurity management programs to monitor the evolving risks to their companies



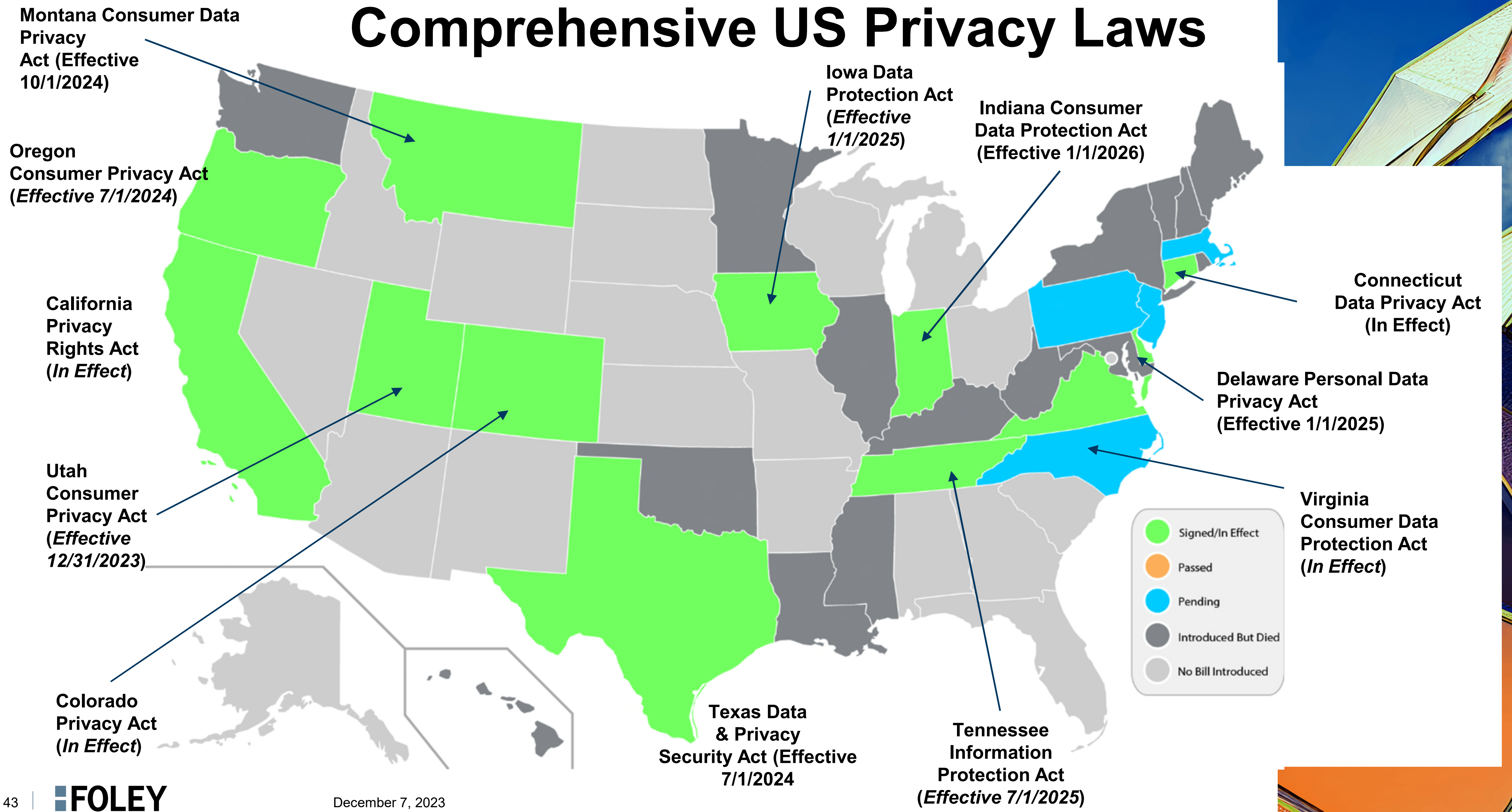
FOLEY

FOLEY & LARDNER LLP

Emerging State and Federal Legislation

FOLEY.COM

Comprehensive US Privacy Laws



Additional Legislation

- Federal Trade Commission (FTC) under § 5(a) of the FTC Act
- Securities and Exchange Commission (SEC)
- Gramm-Leach-Bliley Act (GLBA) and its implementing regulations
- Health Insurance Portability and Accountability Act (HIPAA)
- New York’s SHIELD Act
- California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)
- All 50 U.S. states plus Washington, D.C. and three federal territories have in place data breach notification laws
- Cybersecurity Information Sharing Act (CISA)
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

FOLEY

FOLEY & LARDNER LLP

Potential Legal Liabilities

FOLEY.COM

Sources of Corporate Liability After a Security or Privacy Incident

FTC ENFORCEMENT ACTIONS

These actions often lead to settlement or a consent decree, including fines and ongoing monitoring. Wyndham has challenged the Federal Trade Commission’s (FTC) authority to enforce a company’s cybersecurity practices

FCC ENFORCEMENT ACTIONS

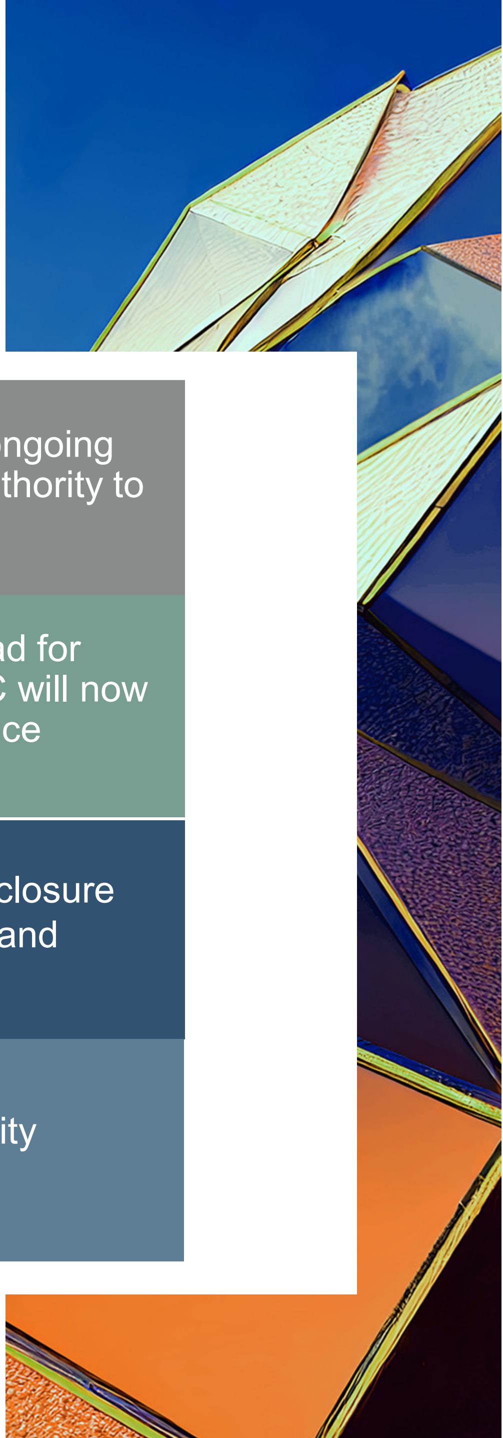
The Federal Communications Commission (FCC) generally follows the FTC’s lead for telecommunication companies and other companies within its authority. The FCC will now regulate broadband providers under the new FCC ruling that brings internet service providers under Title II of the Communications Act

SEC ENFORCEMENT ACTIONS

There have been no enforcement actions yet, but the SEC has indicated that disclosure requirements for public companies also include disclosure of cybersecurity risks and cybersecurity incidents

STATE ATTORNEYS GENERAL

State attorneys general enforce state privacy, breach notification, and data security laws (when applicable)



Cybersecurity Due Diligence for Directors and Officers

1. What are the greatest cyber security threats and risks to the company's highest-value intangible assets, and the most sensitive company and customer information? Does the company's risk management and assessment deal with protecting those assets and that information?

2. What is the company's volume of cyber security incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? How much time and cost is incurred to respond to those incidents?

3. What would the worst-case cyber incident cost the company in terms of lost business, system downtime, and reputational damage?

4. What is the company's specific cyber security breach response and crisis management plan, and how will it respond to customers, clients, vendors, the media, regulators, law enforcement, and shareholders, traditional and social media, NGOs, bloggers? Have the plans been practiced in mock situations?

5. What cyber security training does the company include in its compliance program?

6. What due diligence does the company perform with respect to its third-party service providers?

7. What cyber security due diligence is done as part of any acquisition?

8. Has the company performed a cyber security IT audit of the company's systems, services and products to analyze potential vulnerabilities that could be exploited by hackers?

9. What infrastructure enhancements have been adopted to show affirmative action to protect the company's IP, intangible assets, sensitive data and customer data and personal information?

Board of Directors Risks Assessment Questions

1 Where is the company's data stored geographically, and in what data centers? Has the General Counsel examined the legal issues in each jurisdiction?

2 What is the computer architecture structure of the company's computer centers and data centers, are they accessible to company employees, customers and vendors and suppliers, and how? Are they accessible to mobile users and how? What computer and data centers are outsourced, and how? How much data has been placed into a cloud computing environment, in what architecture, and are the clouds being used private, public, or a hybrid? Given all the retail data breaches, does the company utilize point of sale terminals and are they being updated? Does the company use mobile payment hardware and software?

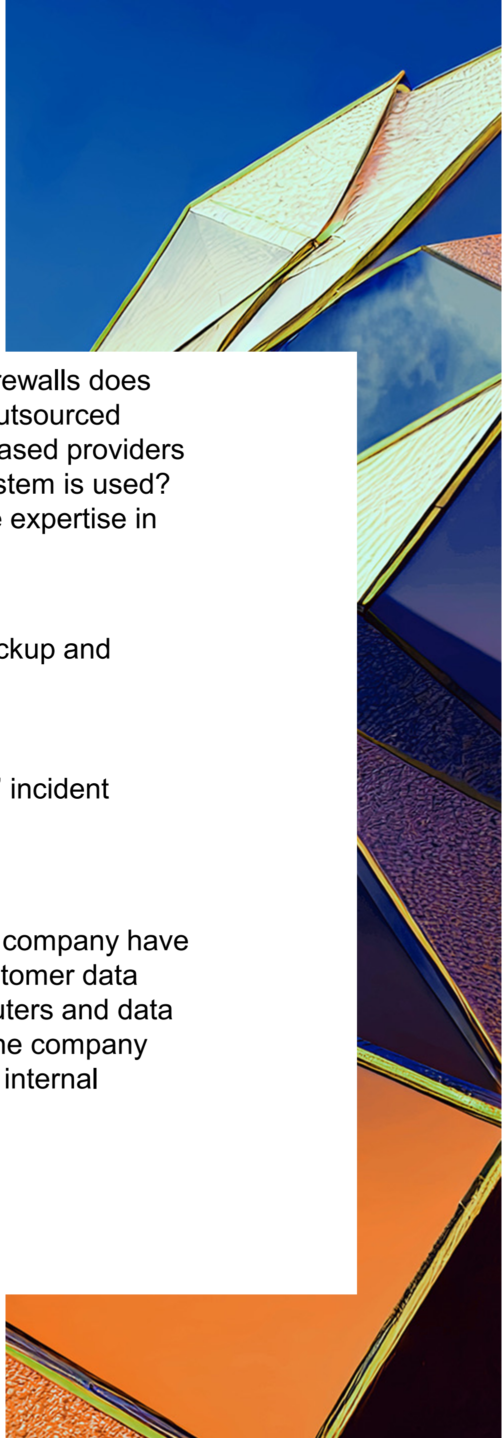
3 Are company and customer and competitor data being commingled in databases or on servers or in the same cloud environment or kept separate and is either customer or company data exposed to competitors, vendors, suppliers or other parties? If so, what types of security measures or confidentiality agreements been implemented?

4 What level and type of encryption and firewalls does the computer and data onsite centers, outsourced computer and data vendors and cloud-based providers use? What type of perimeter security system is used? Does the IT team or its consultants have expertise in these systems?

5 What are the company's and vendors' backup and disaster recovery plans?

6 What are the company's and the vendors' incident response and notification plans?

7 What speed and level of access does the company have to security information on its data and customer data stored in company and outsourced computers and data centers and cloud locations in the event the company needs to respond to a regulatory request, internal investigation or litigation?

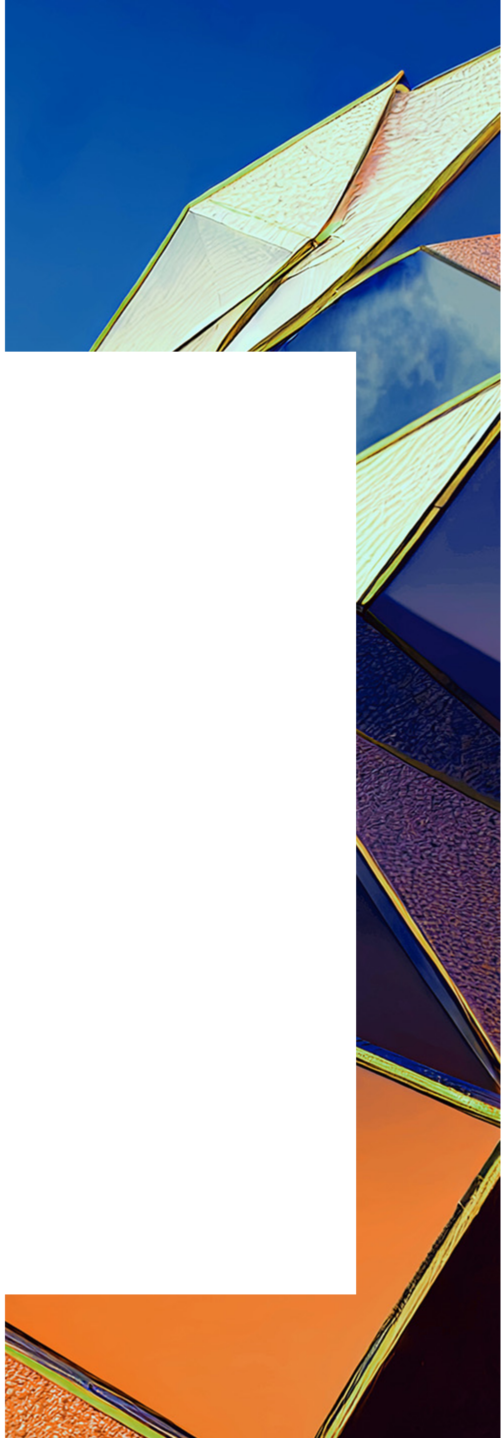


Board of Directors Risks Assessment Questions

8 How transparent are the vendor and cloud providers' own security systems? What access can the company get to the cloud provider's data center and personnel to ensure the security system is in place and functioning, while also making sure it can make a risk assessment and design a response plan?

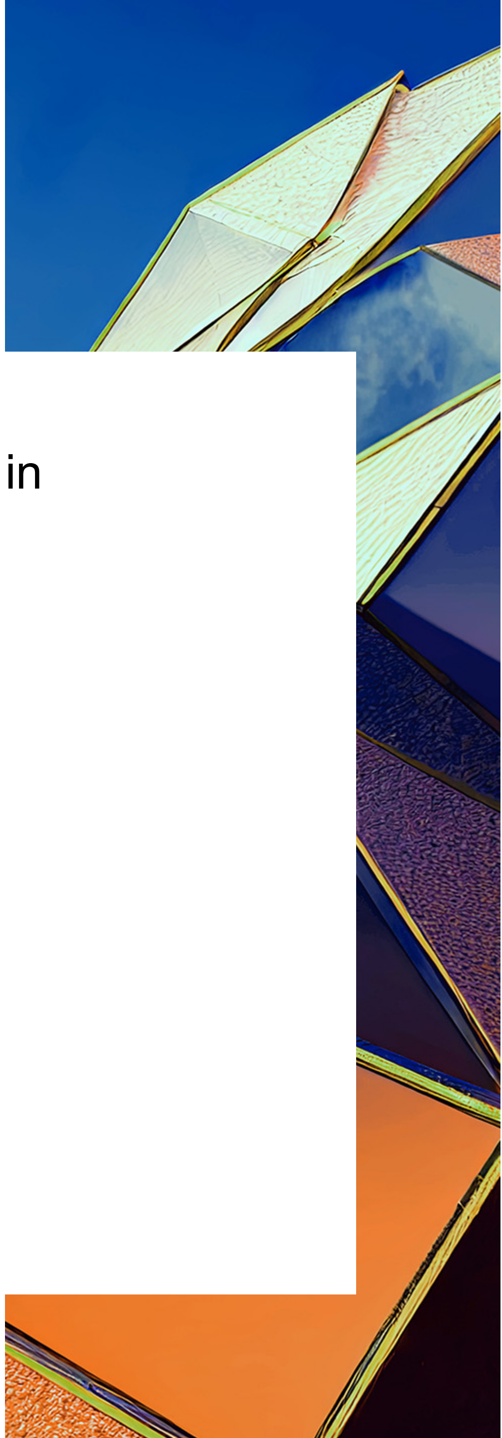
9 What are the vendor and cloud servicers' responsibilities to update their security systems as technology and sophistication evolves?

10 What are the company, computer and data vendors, and cloud providers' ability to continuously monitor, detect, and respond to security incidents, and what logging information is kept in order to potentially detect suspicious activity?



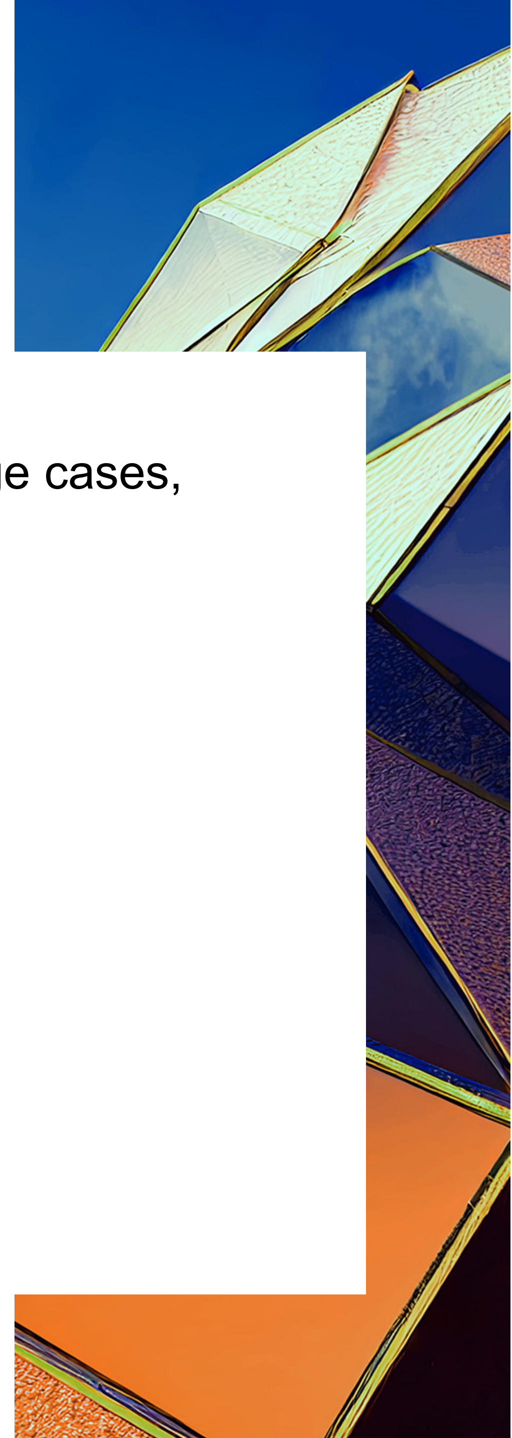
Director and Officer Liability

- Shareholders also may file lawsuits alleging that negligence of the directors and officers in addressing cybersecurity risks resulted in financial loss



Intellectual Property (IP) Implications

- Cybersecurity incidents involving IP loss or disclosure, particularly in industrial espionage cases, can lead to costly legal liabilities.



Contractual Obligations

- Manufacturers could be held liable for breach of contract if a cybersecurity attack disrupts their ability to fulfill contractual obligations. Contracts often contain clauses related to required data protection and cybersecurity, and failure to meet these contractual obligations can lead to various legal consequences.

Cyber Insurance Considerations

- Combating the increase in cyber threats and compliance with the growing legal requirements can be costly. Cyber insurance plays a crucial role in mitigating financial risks associated with cyber threats. Manufacturers should carefully consider the various aspects of cyber insurance. These policies typically consist of two main components:
  - First-Party Coverage: This aspect of the policy addresses the direct costs incurred by the manufacturer as a result of a cyber incident. It includes coverage for data breach response, business interruption, and data restoration expenses. For example, if a ransomware attack disrupts operations, the business interruption coverage may help compensate for lost revenue during the downtime.
  - Third-Party Coverage: Third-party coverage deals with liability issues arising from a cyber incident. It encompasses protection against legal costs, such as those associated with defending against lawsuits due to data breaches, privacy violations, and intellectual property theft. Manufacturers may also be covered for regulatory fines and penalties.

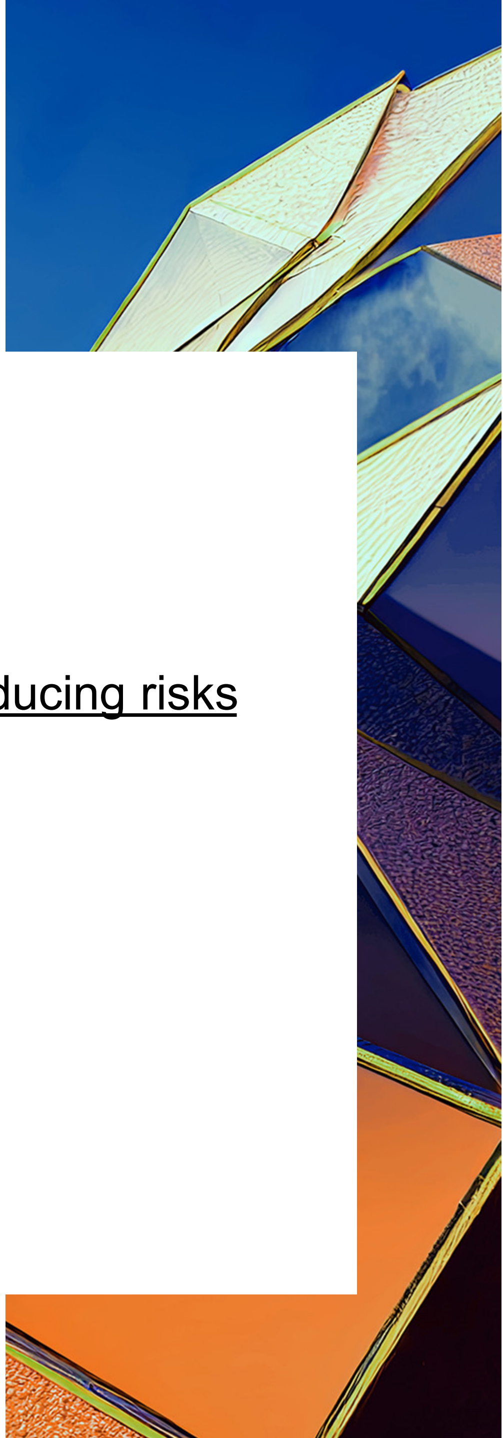
FOLEY

FOLEY & LARDNER LLP

Managing Cyber Risks Today

What is Cybersecurity Strategy?

- How your organization reduces your risks
- Use a standard of practice *to measure risk*, addressing risks to others and yourself
  - Duty of Care Risk Analysis (DoCRA), CIS RAM, ISO 27005, NIST 800-30
- Use a standard of practice to determine roles, responsibilities, processes, metrics for reducing risks
  - ISO 27001, NIST Risk Management Framework
- Ensure that risk measurement, reduction, and reporting are integrated into the business

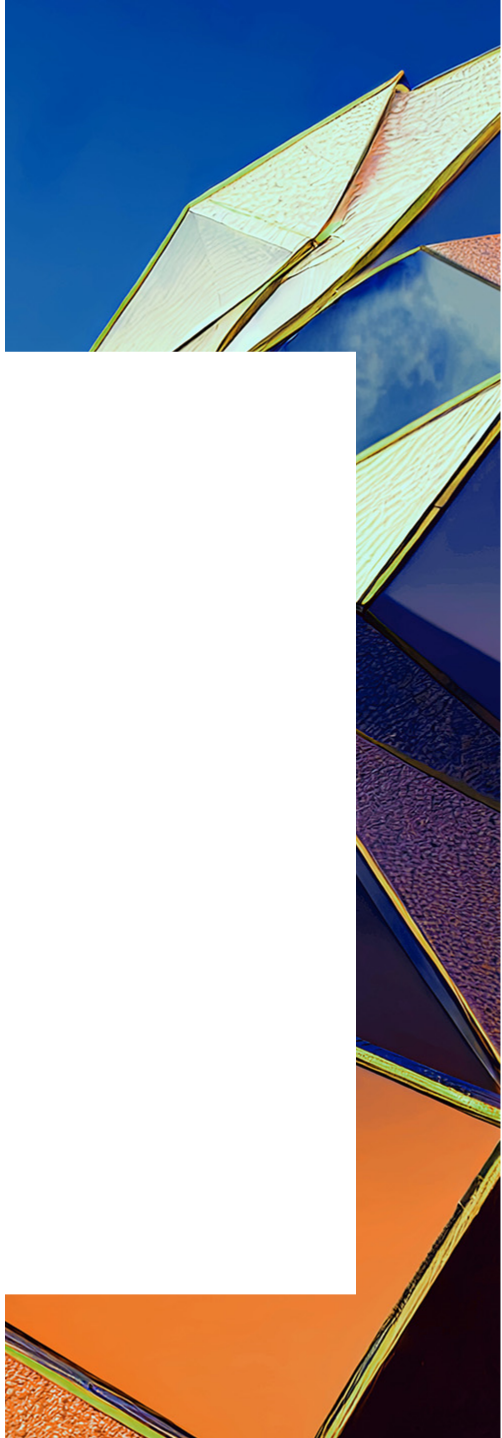


What is Governance?

- <u>Responsibilities for cybersecurity are at the level of management whose role is necessary to effectively manage the risk</u>.
  - Executives:
    - Gather and communicate responsibilities; contracts, regulations, and business expectations.
    - Ensure that resources, prioritization, and collaboration are sufficient for meeting commitments.
  - Management:
    - Communicate expectations to personnel. Communicate status and needs to executives.
    - Ensure that teams, projects, and systems meet commitments.
  - Personnel:
    - Implement and manage controls according to commitments.
    - Report status and security concerns.

Why is Governance Rising as a Cybersecurity Issue?

- In breach case after breach case, we see cybersecurity teams unable to communicate with executives
- Executives don't know what they should know
- Executives do not understand cybersecurity personnel
- Management does not feel comfortable being honest about risks
- Management does not know how to conduct risk analysis in business and legal terms
- Good governance would fix this
- Good governance is good for cybersecurity



The Rise of Governance

SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule

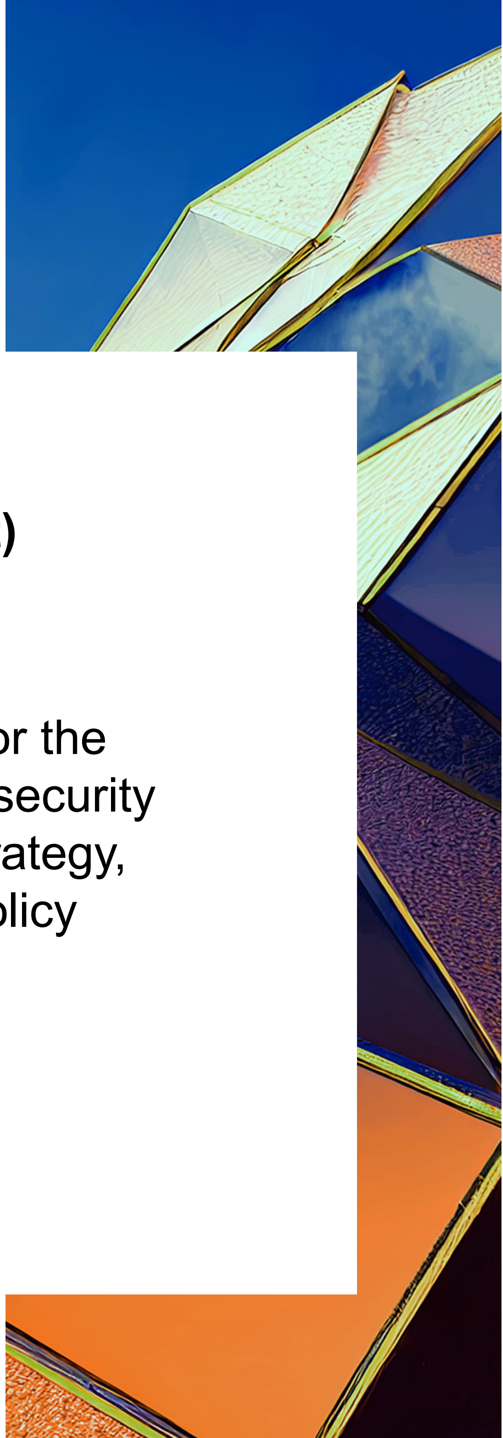
- Disclose what your risk management, strategy, and governance methods are

23 NYCRR Part 500

- Operate a data governance program

NIST Cybersecurity Framework 2.0 (Draft)

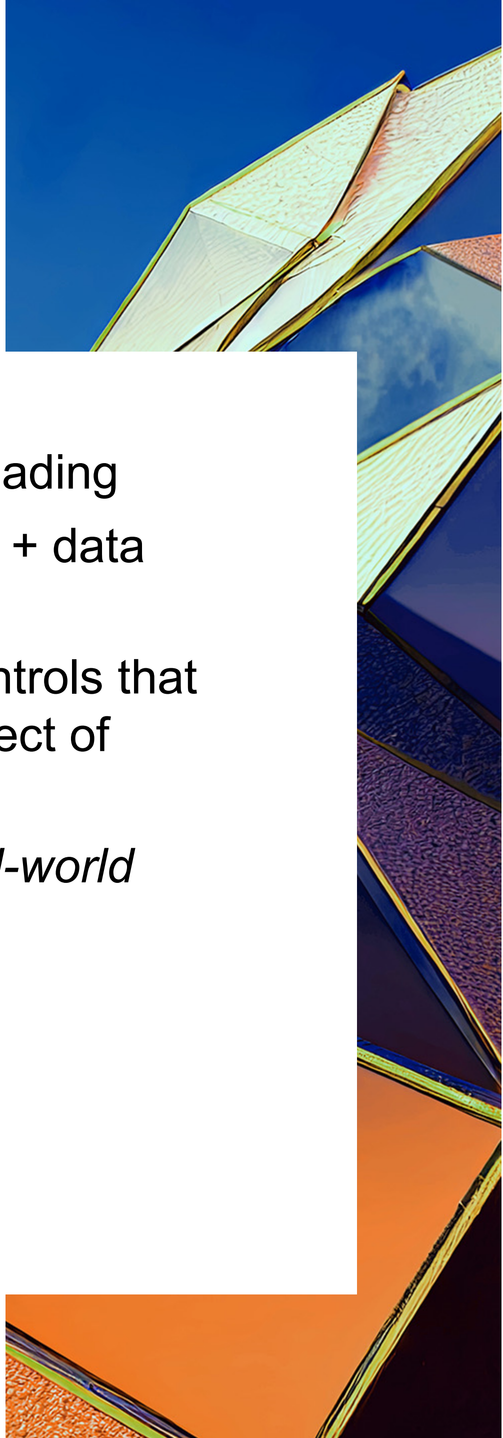
- Establish and monitor the organization’s cybersecurity risk management strategy, expectations, and policy



“Secure" Architecture

- Somewhat effective tools exist.
- However:
  - These primarily focus on preventing intruders from accessing the network (“keep the bad actors out” or “perimeter defense”)
    - Include firewalls, intrusion detection and prevention systems, secure access control, and air gapping
  - Controlling access to the network, manufacturers can reduce the likelihood of a breach.

- “Secure Architecture” can be misleading
  - Conjoining of perimeter defense + data security;
  - Involves inadequate security controls that are applied only to a limited aspect of operations or a supply chain;
  - *Little or no consideration for real-world physical consequences*;
  - Aligned solely with compliance requirements.



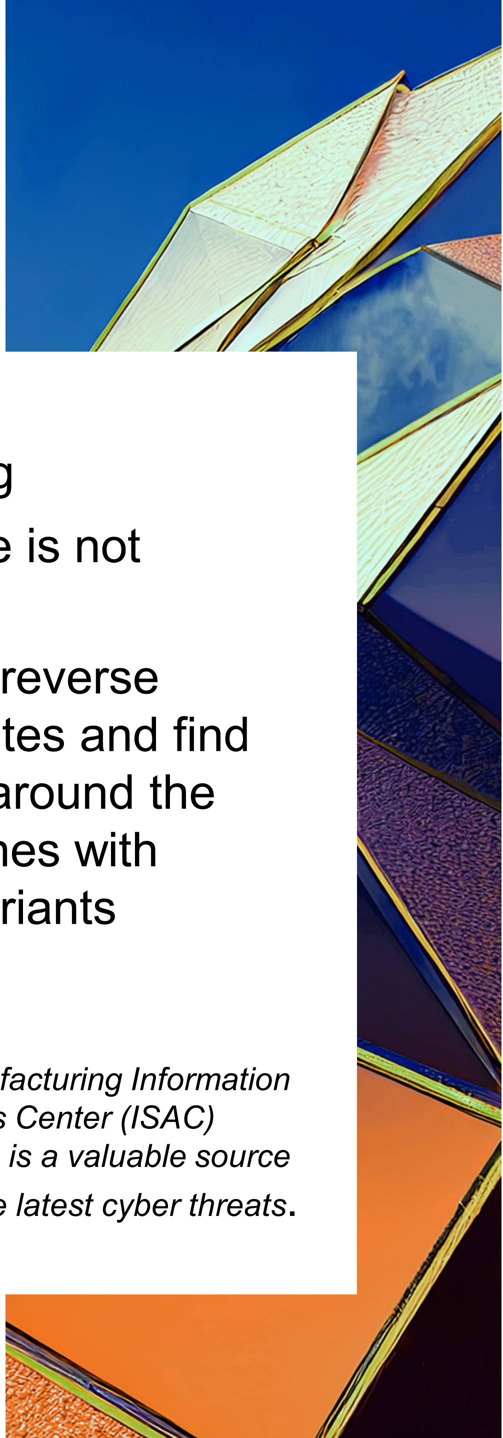
Multi-Faceted Approach to Cybersecurity

- Investing in employee cybersecurity training and awareness
  - Human element represents the single biggest cybersecurity risk
  - First line of defense against cyber threats

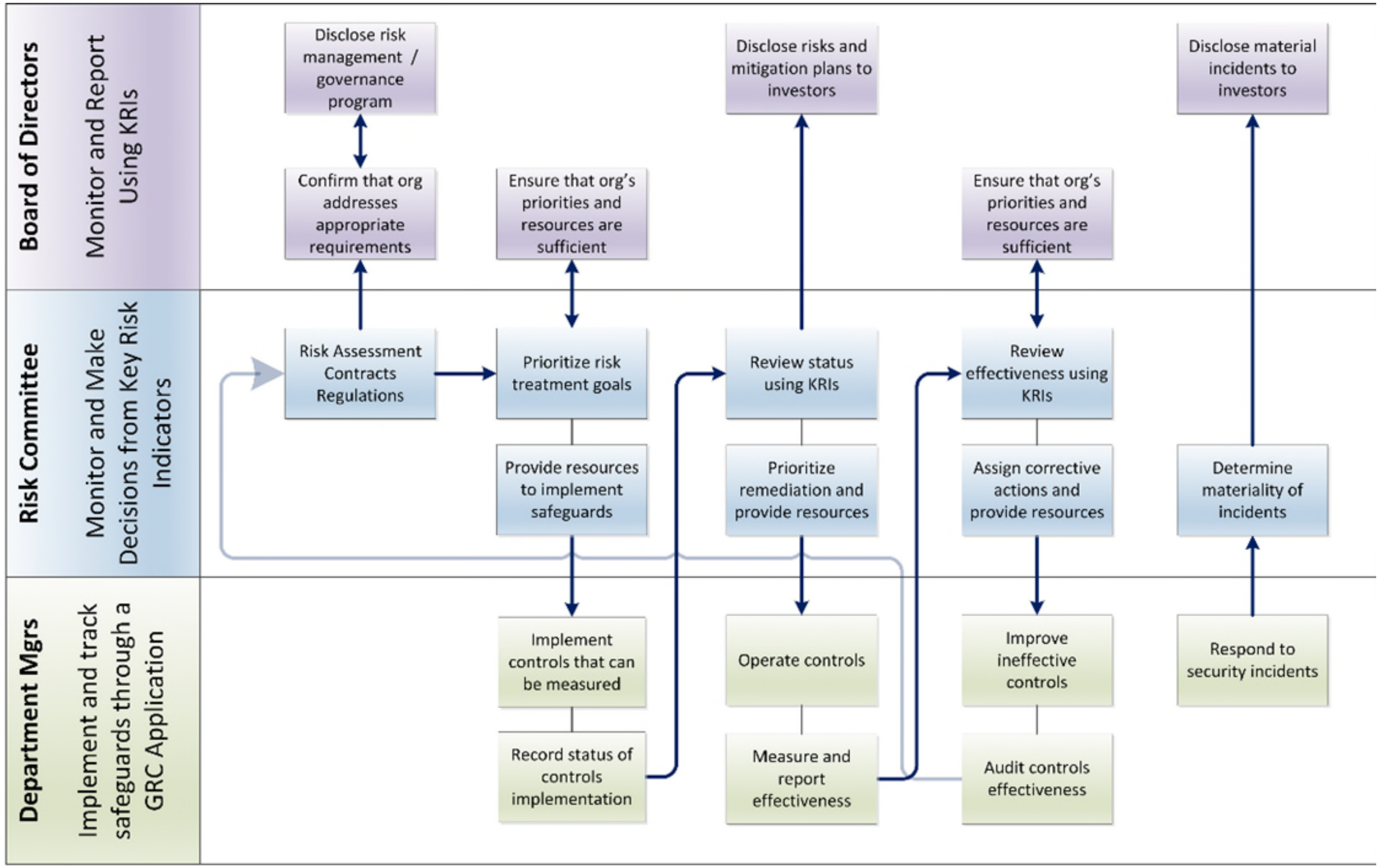
- Regular software updates
  - Updates often secure against known vulnerabilities
  - Threat actors target older software vulnerabilities - low-cost compromise
  - Vulnerabilities are old, patches available for years
  - Outdated software harbors thousands of vulnerabilities that cybercriminals exploit

- Active monitoring
  - Patching alone is not enough
  - Attackers can reverse engineer updates and find ways to work around the released patches with new exploit variants

A recently launched Manufacturing Information Sharing and Analysis Center (ISAC) (https://www.mfgisac.org/) is a valuable source of public information on the latest cyber threats.



Information Flow for Good Governance



HALOCKSecurityLabs
Purpose Driven Security

FOLEY

FOLEY & LARDNER LLP

Proactively Addressing Cyber Risks While Increasing Productivity and Energy Efficiency

CyManII's Vision

- To secure U.S. manufacturers as they digitize by fortifying their physical systems with embedded cybersecurity and energy-efficient solutions.

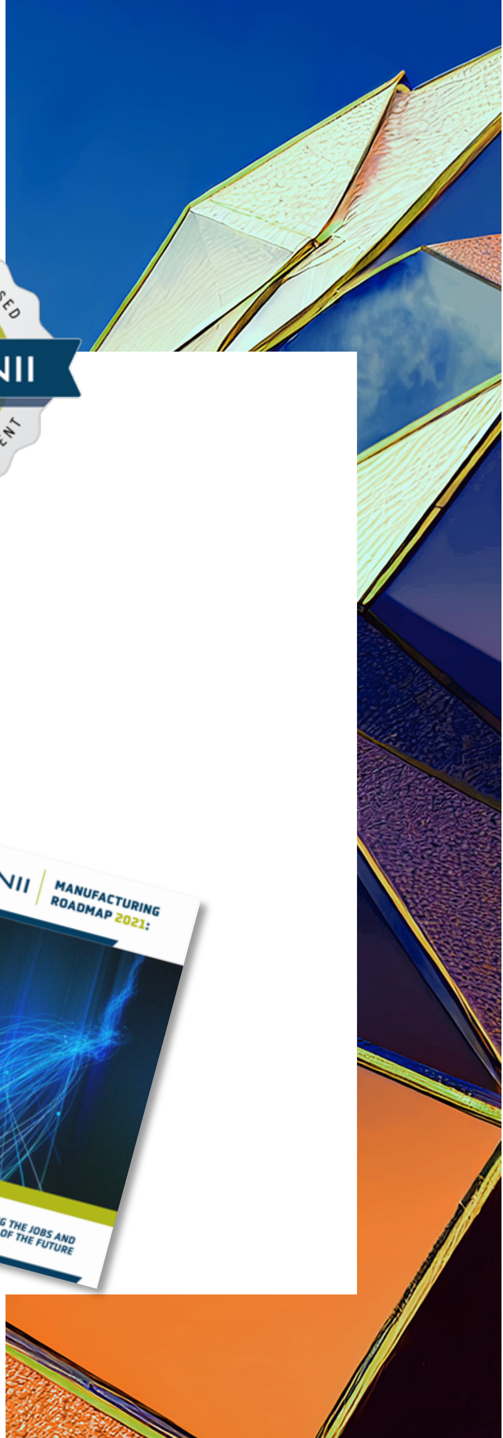
Core Pillars

ε-PURE

Innovate	Inspire	Inform
Secure the digital thread	**Secure. *TOGETHER***	**Create a cyber-informed workforce**
• Build defensible architectures • Create identify-centric cyber-physical passports • Secure a decarbonized ecosystem	• Partner across industry's supply chain • Cooperate across Govt stakeholders • Focus on: Manufacturing Sectors Critical Energy Infrastructure Data and beyond…	• Focus on OT / ICS security • Leadership on CIE • Empower current workers • Expand emerging workforce (students)

CYMANII the cybersecurity manufacturing innovation institute

OFFICIALLY ENDORSED CYMANII EDUCATIONAL CONTENT

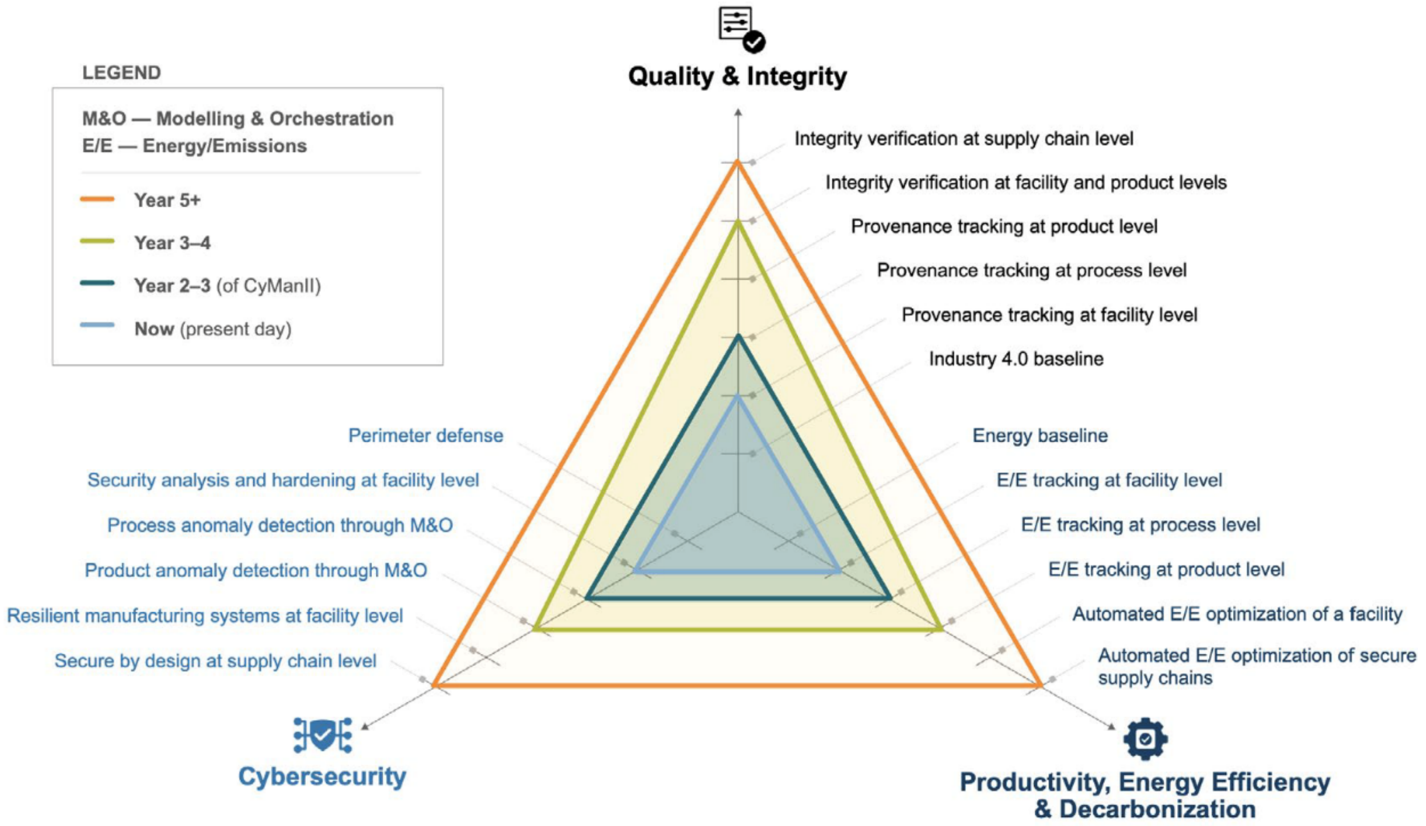


CYMANII the cybersecurity manufacturing innovation institute

U.S. DEPARTMENT OF ENERGY

December 7, 2023

Innovations Needed to Fundamentally Cyber Secure IT/OT/ICS and Physical Systems While Moving from Cyber Investments as a Cost Center to a Profit Center

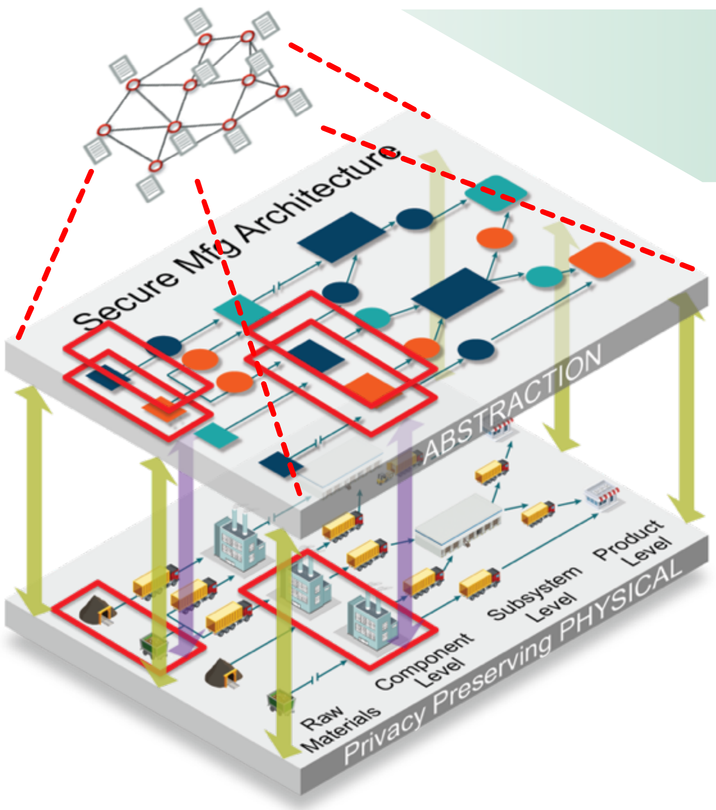


December 7, 2023

CyManII's Secure Defensible Architectures

- The Digital Engineering Lifecycle must be addressed across the entire supply chain
  - Every operation, machine, and person is a "node" in this digital design (supply chain is seamless with operations)
  - Every node is captured in a cyber-physical identity (passport) that is used for:
    - Guarantees of physical functions
    - Linkage of security to product quality and energy / emissions efficiency (embodied energy)
  - Verifiable security properties that are extensible to multiple domains
- Cyber-Physical Passport: makes your supply chains "born qualified" and "rooted in trust"

Secure Defensible Architectures (SDA)



Analysis
Modeling
Optimization

- Maximize E&E Efficiency
- Maximize Production
- Minimize Risk

Integrated Model of Automation & Supply Chain

- Perimeter defenses insufficient in modern **digital design lifecycle**
- We treat **Automation as nodes in Supply Chain** network

Framework for Security & Efficiency Across "Sectors"

- Digital **identity** = physical + cyber + energy (Cyber-Physical Passport)
- Automation **activities** validated across supply chain

Agile, Adequate, & Consequential Formalism to Validation

- **Targeted formal methods** and evidential basis for design & implementation
- Continuous Integration/Deployment (**CI/CD**) in manufacturing context

Unify security across the digital thread of design, build, deliver for industries of all sizes

CYMANII
U.S. DEPARTMENT OF ENERGY

Cyber-Physical Passport

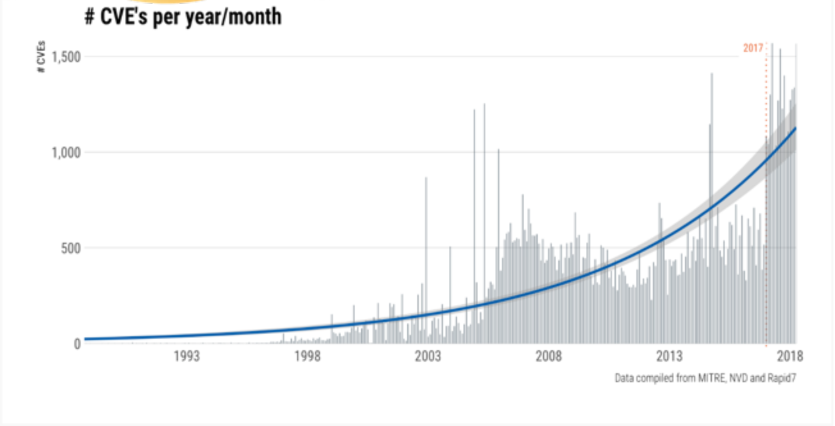
- Enables digital provenance tracking through *verifiable security guarantees*.
- Traceability across supplier boundaries.
  - Using a global ledger as well as physical and virtual watermarks, the CPP follows a product through its value chain, crossing suppliers and staying with the end product.
- Verification of the digital thread.
  - Formal verification methods are used to continually assess the critical code along the product's lifecycle for accuracy and evidence of compromise.
- Tamper-proof ledger.
  - The data captured in the CPP is protected and anonymized with use of a unique hash and permissioned blockchain where entities logging transactions are first authenticated.
- Improved protection & system hardening.
  - A secure manufacturing architecture along with a multi-physics digital twin provide enhanced cyber protection and high-fidelity monitoring.

OPERATIONAL
Resilience

OPERATIONAL
Efficiency

How to Address Cyber Vulnerabilities “At Scale”

- Challenge:
  - Vulnerability trends significantly favor the attackers, present systems are not ”defensible”.
  - If we continue to reactively chase and patch vulnerabilities, we will “lose the war” for national & economic security.
- New Approach:
  - Identify Cyber Weakness Enumerations that capture thousands of vulnerabilities at a time (1:10,000+)
  - Create methods and tools that can systematically identify and eliminate/mitigate weaknesses
  - Address these CWE’s in a priority fashion to cyber secure US Manufacturing
- Current defenses are orders of magnitude behind:
  - 10’s days vuln-to-exploit, 100+ days to patch, 200+ days to detect
  - 10’s active vulnerability instances / device, 100-1000 latent vulnerabilities
  - 100x the cost to fix in implementation vs design



4/2018   100k CVEs, ~600 CWEs
4/2023   214k CVEs,   933 CWEs

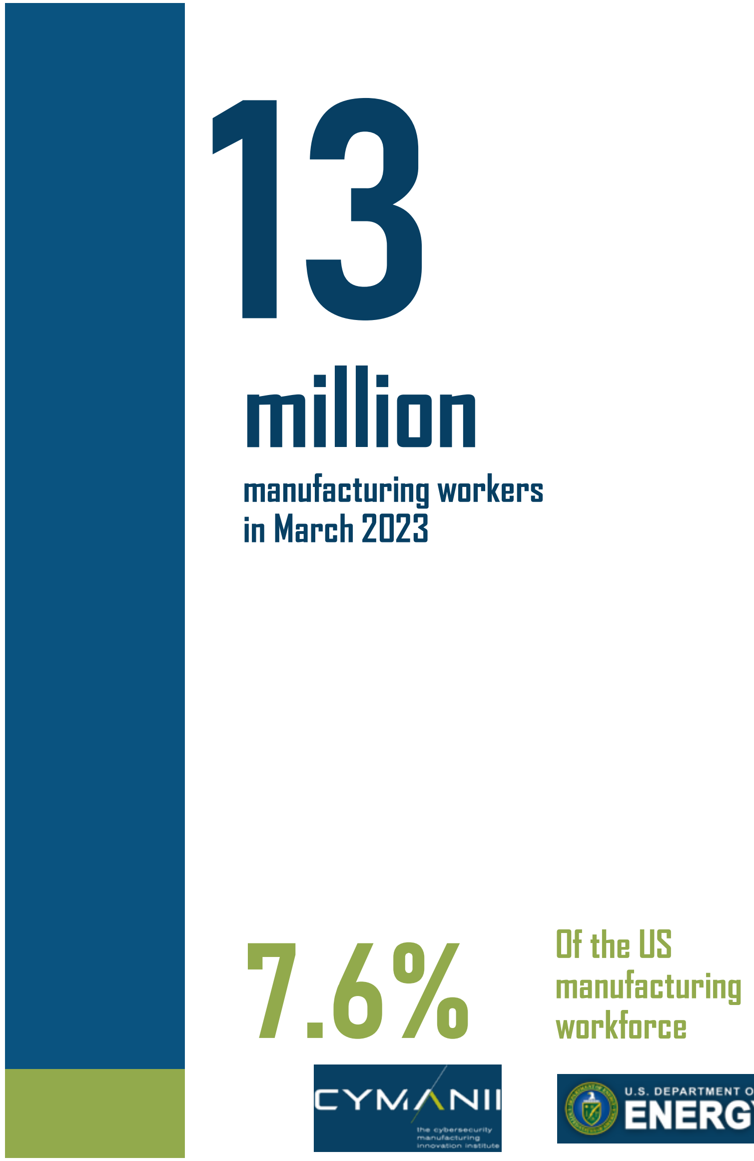
Across 1,063,482 platforms

100s to 1000s : 1 of CVEs-to-CWEs

December 7, 2023

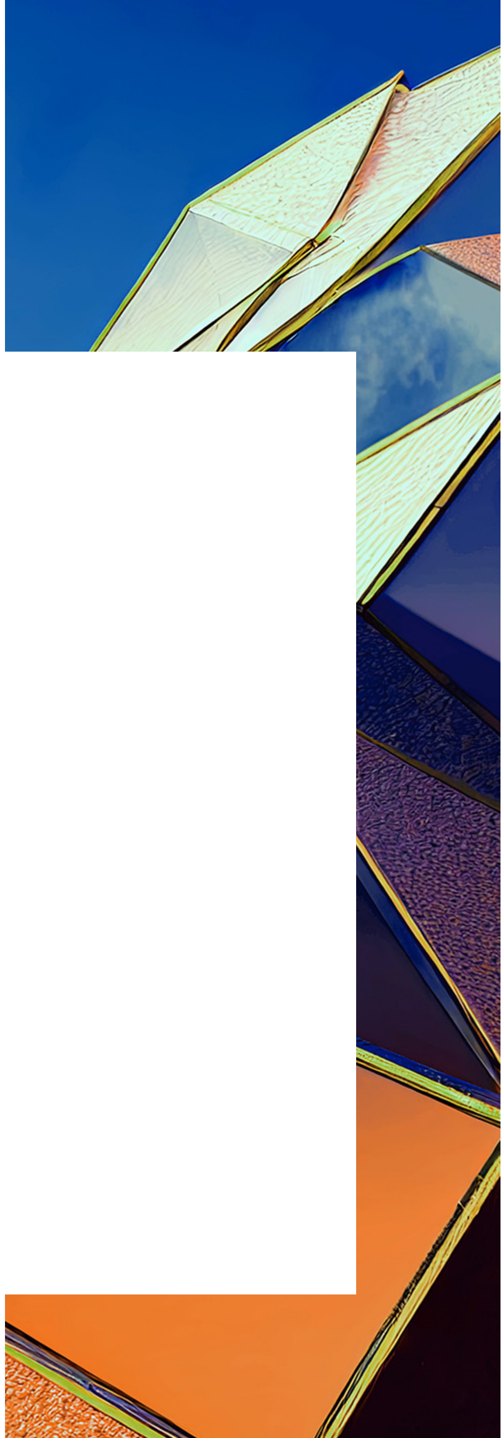
Workforce Development

- Why 1 million workers?
- We must aggressively reach the growing workforce with training that scales.



CYMANII the cybersecurity manufacturing innovation institute

U.S. DEPARTMENT OF ENERGY



Workforce Development

CYBER READINESS INSTITUTE

TOOLINGU | sme

PORT SAN ANTONIO

Networking Academy

1

LEADERSHIP & AWARENESS TRAINING

Manufacturing leaders & stakeholders

2

CORPORATE ONLINE CYBER TRAINING FOR ALL WORKERS

All manufacturing workers

3

HANDS-ON COMPLIANCE TRAINING

Information security team & leaders

4

ONLINE AUTHENICATED TECHNICAL TRAINING

Skilled IT/OT security & maintenance professionals

5

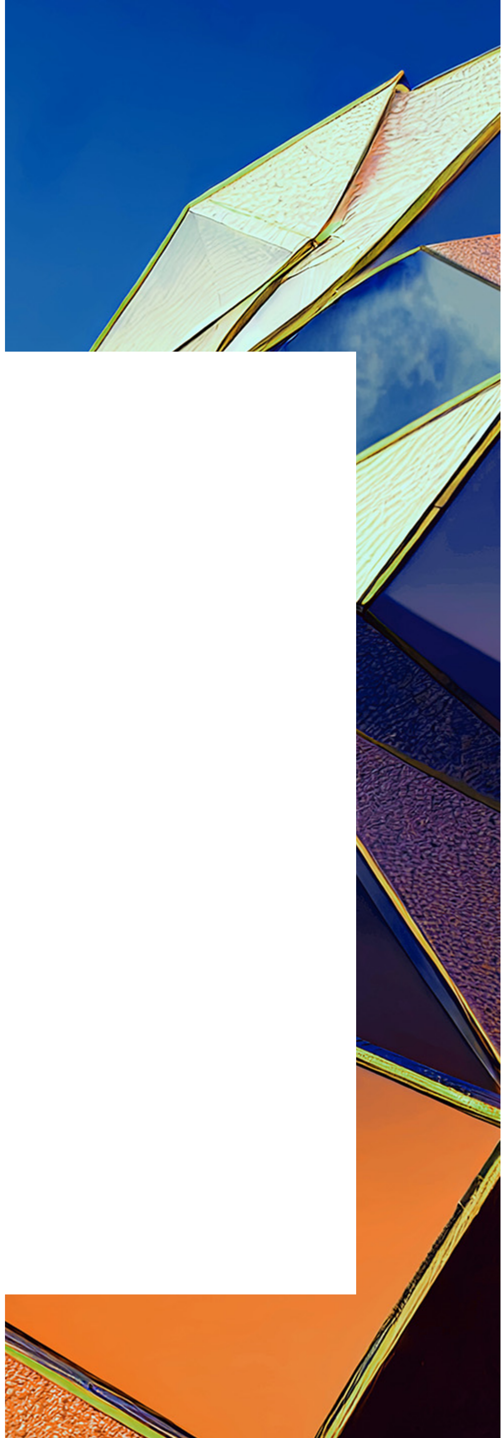
DEGREE AND CERTFCATE SEEKING STUDENTS AND PROFESSIONALS

Online degree & certificate seeking students and professionals.

December 7, 2023

Thank You

- Questions?



About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM