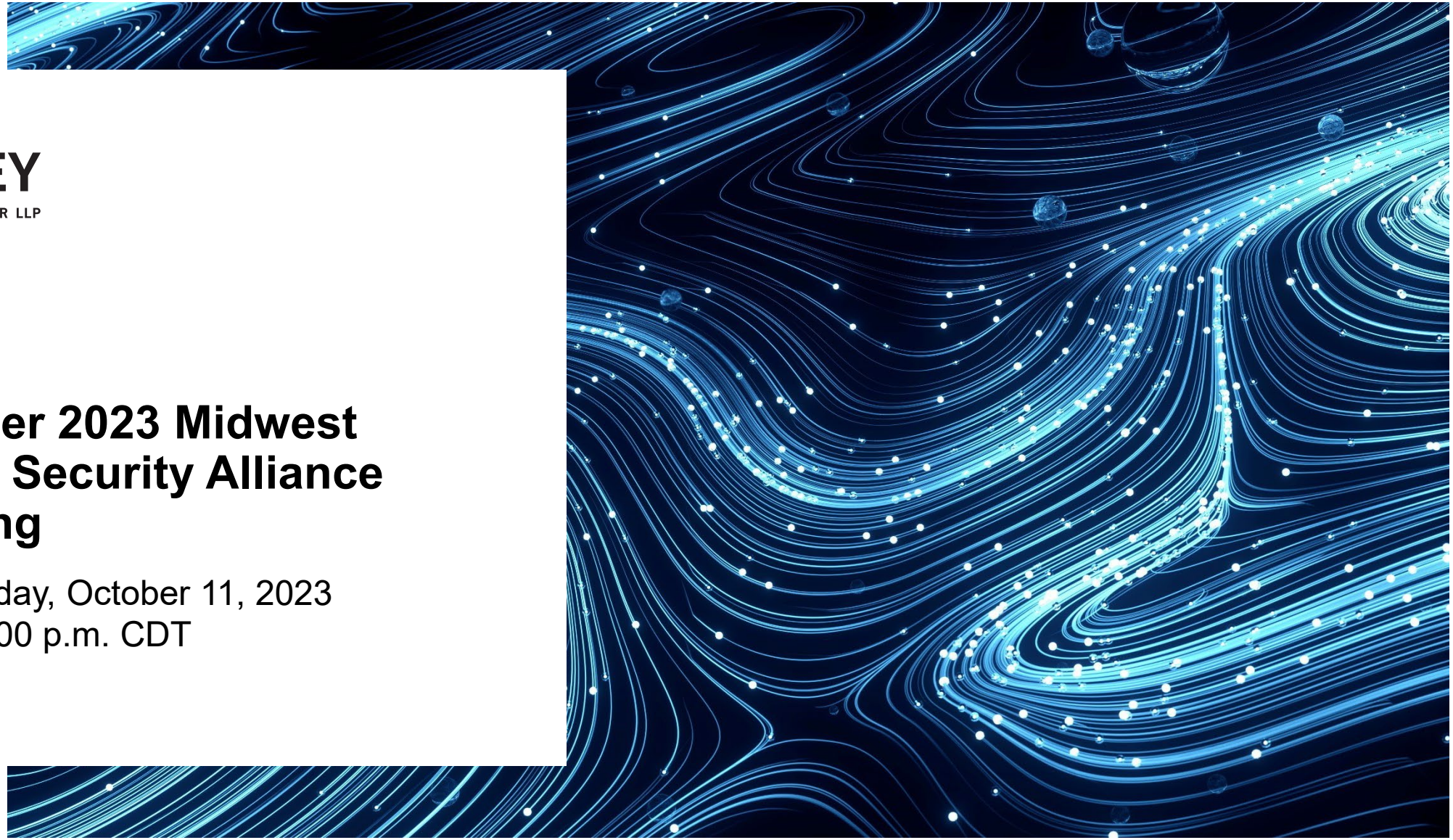
FOLEY

FOLEY & LARDNER LLP



October 2023 Midwest Cyber Security Alliance Meeting

Wednesday, October 11, 2023
5:30 - 7:00 p.m. CDT

Agenda

- Welcome to MCSA
- Midwest Cyber Security Alliance Scholarship and Sponsorship Information
- Housekeeping and Continuing Education Credit
- Today’s Topic: Understanding the Impact of the SEC Cybersecurity Rules from a Legal and IT Firm Perspective
- Q&A

MCSA Scholarship Program

- To support cyber security education, MCSA is offering partial scholarships to Milwaukee School of Engineering (MSOE) and University of Wisconsin, Milwaukee students in a cyber security discipline with a 3.0 GPA
- MCSA participation is desired
- Opportunities to connect students and corporations for internships, mentoring, and hands-on facility tours

MCSA Corporate Sponsorship Opportunities

- Sponsorship levels
  - Midwest Cyber Corporate Partner: $5,000
    - Exclusive benefits, MCSA website and social media promotion, $1,000 goes to scholarships
  - Midwest Cyber Corporate Ambassador: $2,500
    - Exclusive benefits, MCSA website and social media promotion, $500 goes to scholarships
  - Midwest Cyber Vendor: $3,000
    - One presentation opportunity for qualified vendor, $500 goes to scholarships

Visit www.midwestcyber.org/sign-up to join today and receive communications about other MCSA news and events, plus access to members-only content.

Continuing Legal Education Credit: CLE

Applications for accreditation will be submitted to CO, FL, NY, and WI (50-minute hour); and CA, IL, TX, UT, and VA (60-minute hour) for up to 1.50 credit hours. Uniform Certificates of Attendance will be provided to attendees seeking credit in other jurisdictions. Foley & Lardner is an approved MCLE provider in California, Colorado, Illinois, New York, Texas, and Utah. Certificates of Attendance will be distributed to eligible participants approximately eight weeks after the program via email.

In-person participants

- Complete the attorney affirmation form and return it to the registration table as you leave. **For those seeking New York or New Jersey credit**, please have a Foley staff member note time in/time out and initial your form.

Webinar participants

- You will need to be logged into the meeting for the full duration of the live event.
- Your first and last names must also be entered upon joining the meeting and displayed throughout the program.
- **Please listen carefully for the CLE COURSE code(s) announcement:** You will need to record one or more CLE course codes that will be announced during the program, complete an Attorney Affirmation form (available in the chat window), and return it to Lisa Frymark (lfrymark@foley.com) following the program, but no later than June 22.

Continuing Education Credit: CPE

This program may be eligible for continuing privacy education (CPE) credit toward CISA, CISM, CGEIT, and/or CRISC certifications and maintenance. Please visit the ISACA website to review the specific CPE requirements for your certification and verify whether the topic(s) addressed in this program align with one or more of your certification's job practice areas.

In-person participants

- Please see a Foley staff member for a verification form to complete for self-reporting purposes.

Webinar participants

- If determined to be eligible, download the ISACA Verification of Attendance Form from the chat box in MS Teams for self-reporting purposes.

Continuing education questions: Contact Lisa Frymark at lfrymark@foley.com.

Thank You to Our Sponsor

Presenters

Moderator

Jennifer Urban, CIPP/US
Partner, Cybersecurity Practice
Foley & Lardner LLP

Speakers

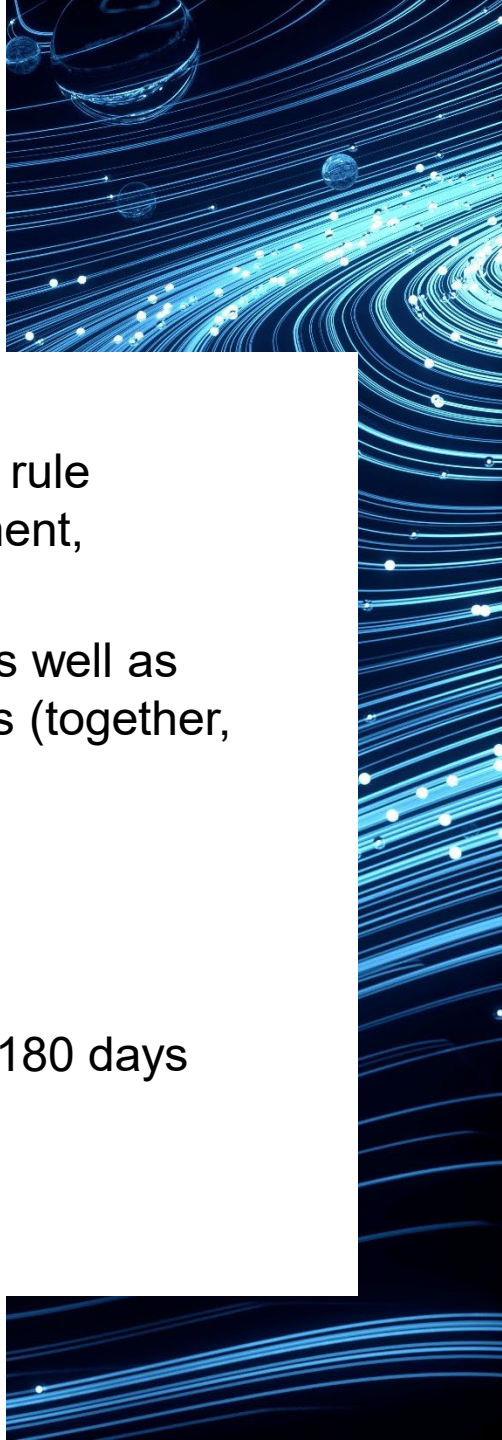
Terry Kurzynski, CISSP, CISA, PCI QSA, ISO 27001 Auditor
Senior Partner
HALOCK Security Labs

Chris Cronin, ISO 27001 Auditor
Partner
HALOCK Security Labs

Jessica Lochmann
Partner, Transactions Practice
Foley & Lardner LLP

SEC Final Cybersecurity Disclosure Rules: Foley Perspective

Final SEC Cybersecurity Disclosure Rules: Overview



- In July 2023, the U.S. Securities and Exchange Commission (the "SEC") adopted a final rule intended to augment and standardize disclosures regarding cybersecurity risk management, governance, and incident reporting
- The new rule imposes additional disclosure requirements for US reporting companies, as well as foreign private issuers, including all companies with stock traded on US 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)

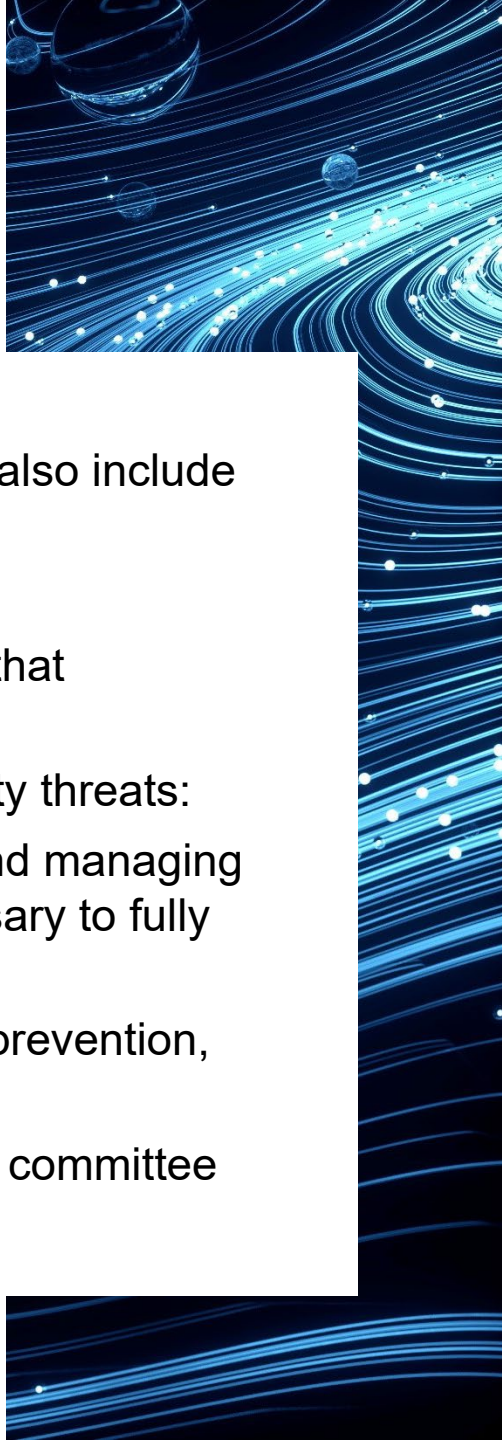
Final SEC Cybersecurity Disclosure Rules: Overview (cont'd.)

- The new rule includes new disclosure requirements for public companies to be made both annually and on a current basis
- 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

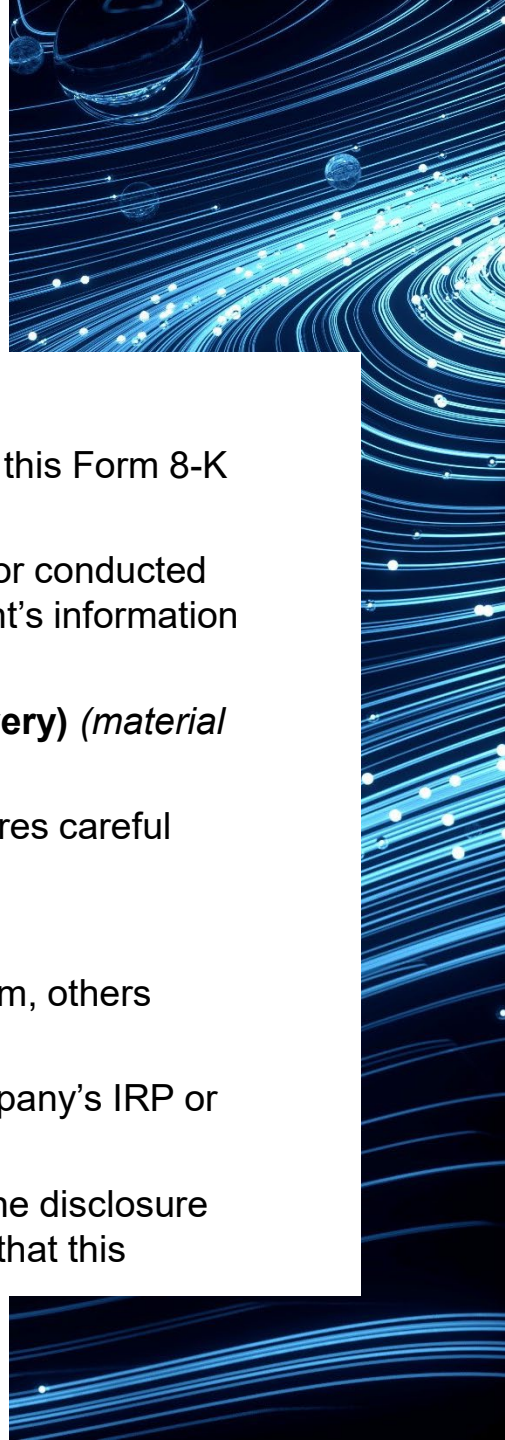
- In each Form 10-K, filed publicly via the SEC's EDGAR system, a public company must now include **cyber risk management** disclosures:
- Description of processes any, for assessing, identifying, and managing material risks for cybersecurity threats in sufficient detail for a reasonable investor to 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

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 (not 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 US 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

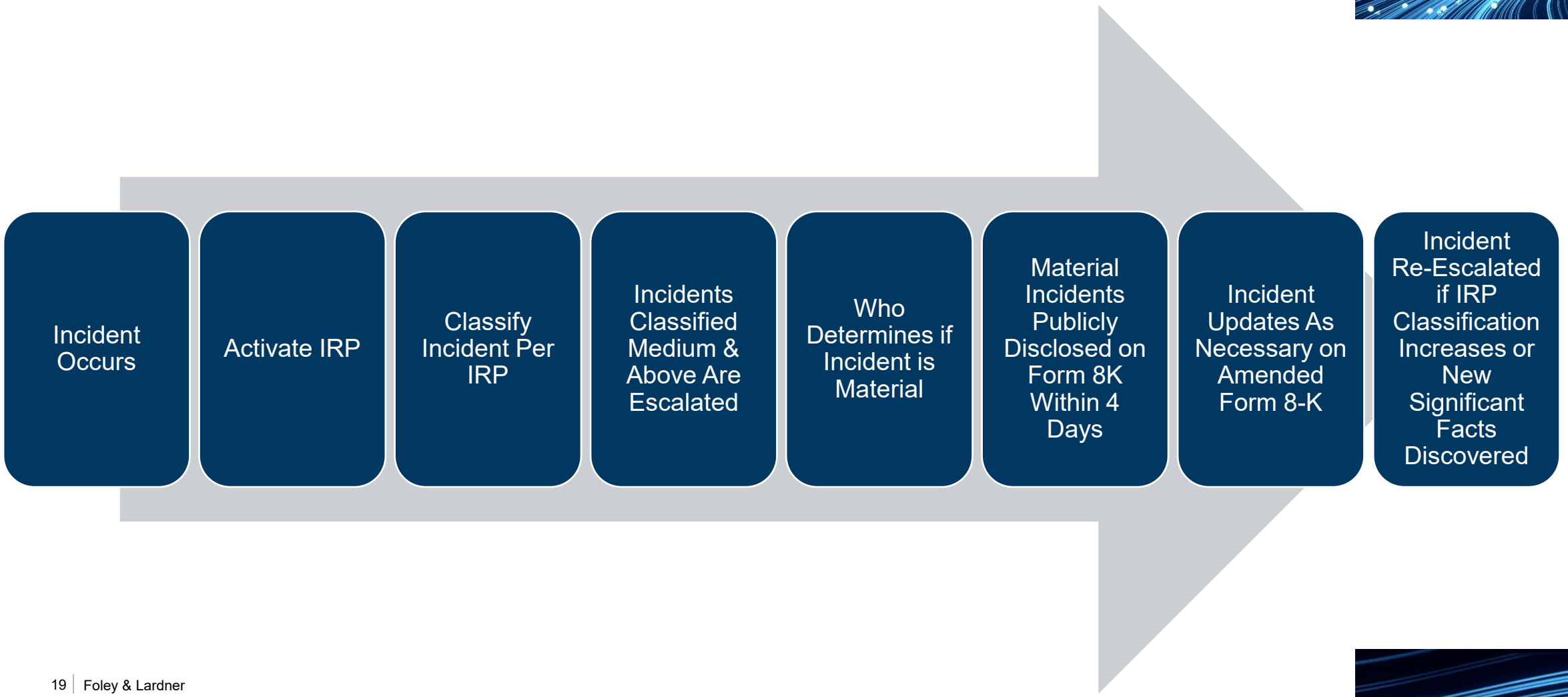
When is an Incident "Material" for Purposes of Form 8-K Reporting? (cont'd.)

- **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

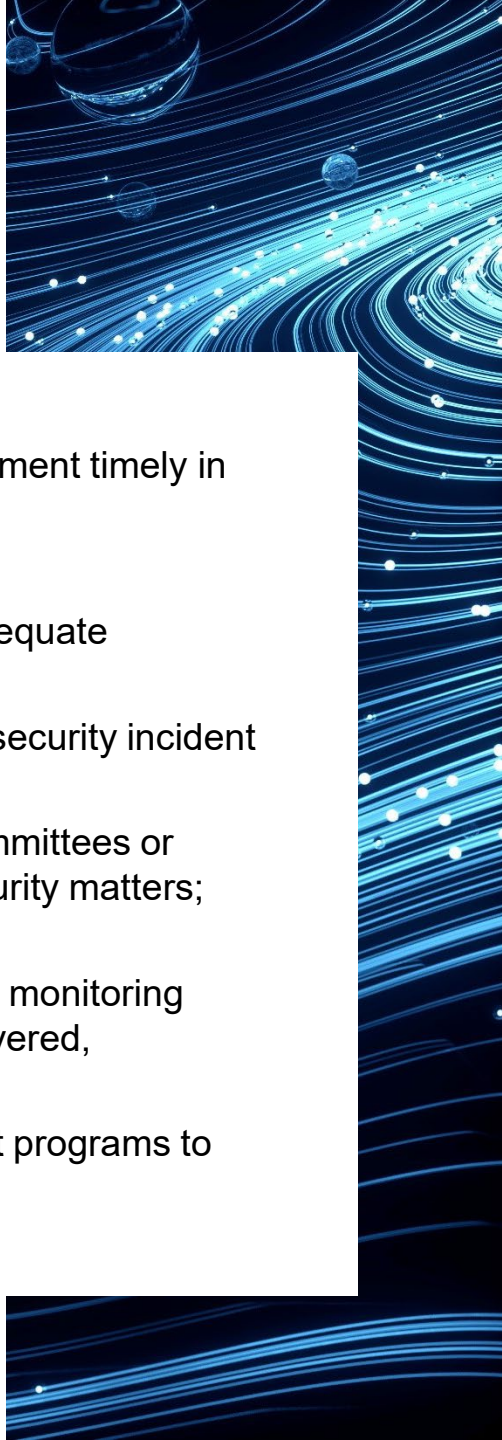


Examples of CISO Involvement in the New Disclosures

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

CLE Code Announcement No. 1 for Webinar Attendees

Please listen carefully for the first CLE code announcement. Record the code on your Affirmation Form and return it to Lisa Frymark at lfrymark@foley.com following the program.


FOLEY
FOLEY & LARDNER LLP
Understanding the Impact of the SEC Cybersecurity Rules: HALOCK Perspective
HALOCK®
Purpose Driven Security

Discussion Topics

- SEC Raised the Bar
  - *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* Rule
- The Rise of Governance
  - What is it, and what does the rise in governance mean?
- How to Prepare
  - One consistent reasonableness story

The SEC Just Raised the Bar

- Not telling you how to secure systems and data
- Requiring that your organization tells the public how your organization secures systems, so you prevent harm to others...
- …what everyone's roll is or isn't (from Board of Directors down) to secure systems and data…
- …and how you disclose material incidents

HALOCK® Purpose Driven Security

What is Cybersecurity Risk Management?

- Knowing your current risks
- Knowing your risk goals
- Planning safeguards that reduce current risks toward risk goals
- Providing the right resources, priorities, and collaboration to reduce current goals
- Reporting progress and concerns toward risk goals

- **Risk = Impact x Likelihood**
- *This is not maturity assessments*
- *This is not compliance assessments*

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?

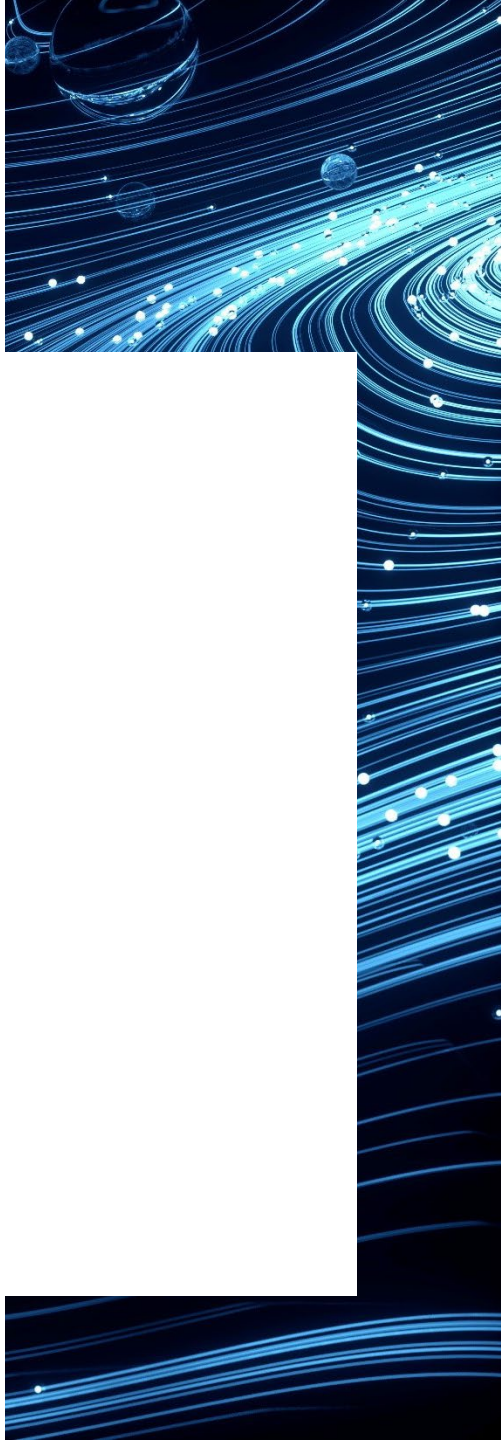
- Responsibilities for cybersecurity are at the level of management whose role is necessary to effectively manage the risk.
  - Executives:
    - Gather and communicate responsibilities; contracts, regulations, and business expectations.
    - Ensure that resources, prioritization, and collaboration 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

Who Might Come After You?

- Regulators
- Shareholders
- Customers, employees, the public



The Rise of Governance

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

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

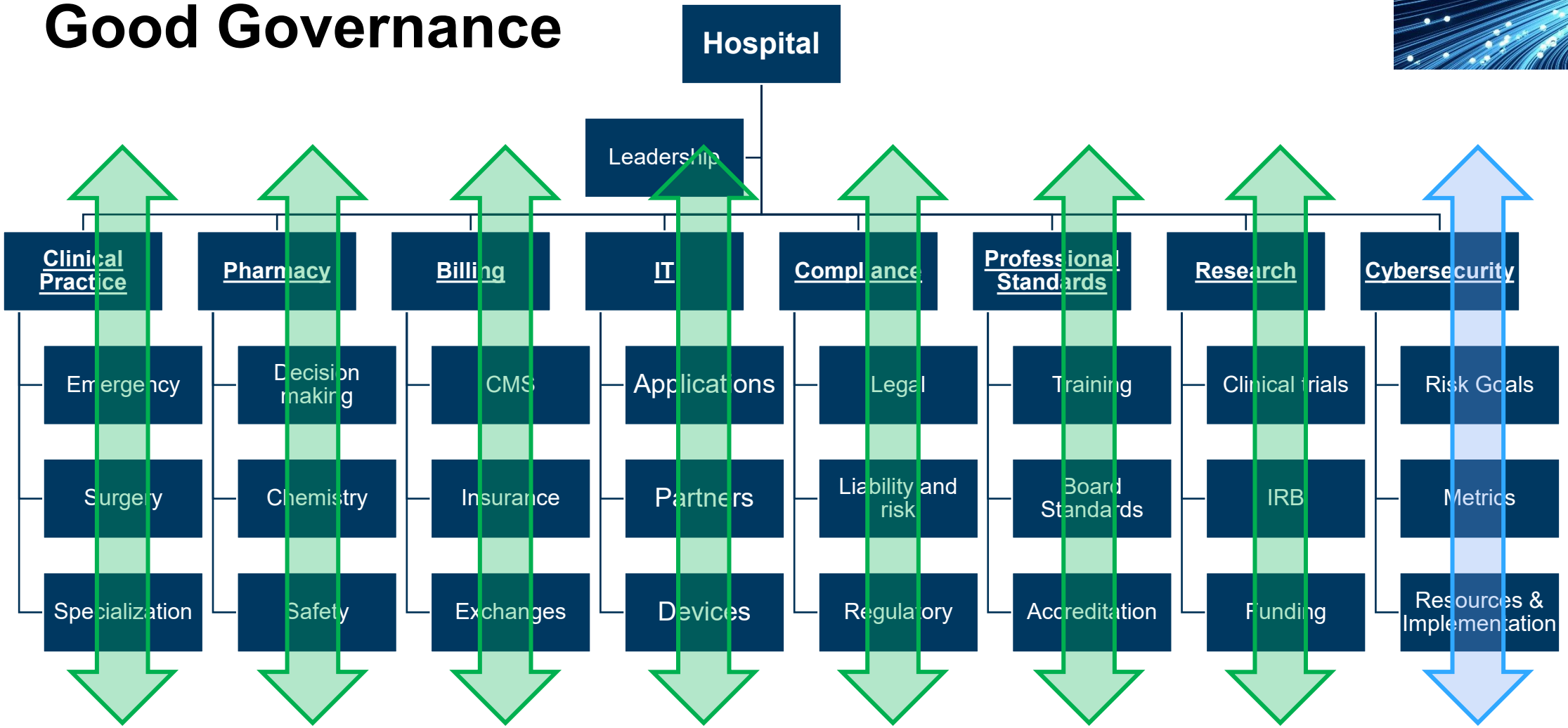
23 NYCRR Part 500

- Operate a data governance program.

NIST Cybersecurity Framework 2.0 (Draft)

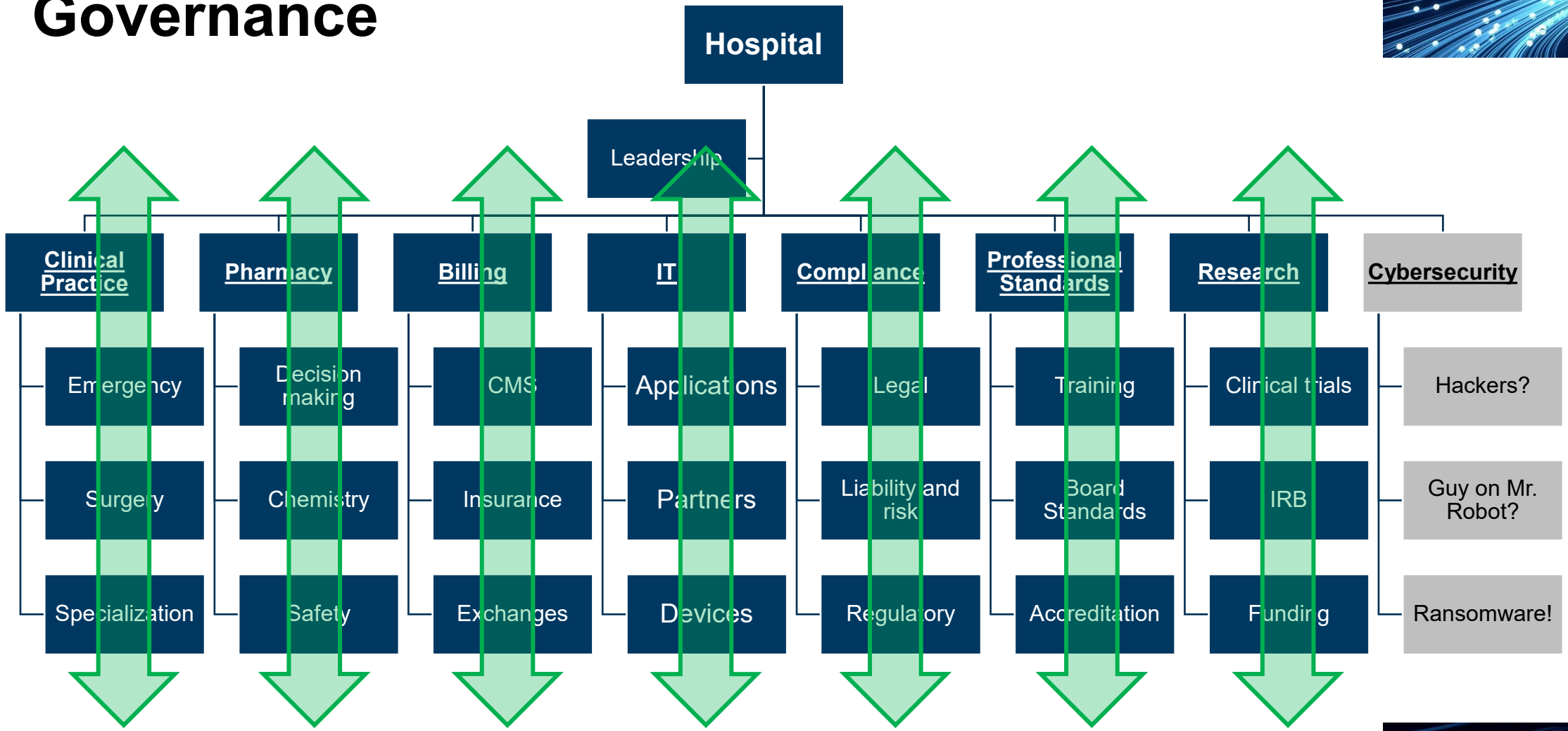
- Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.

Good Governance



HALOCK® Purpose Driven Security

Not Sufficient Governance



HALOCK® Purpose Driven Security

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.

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;

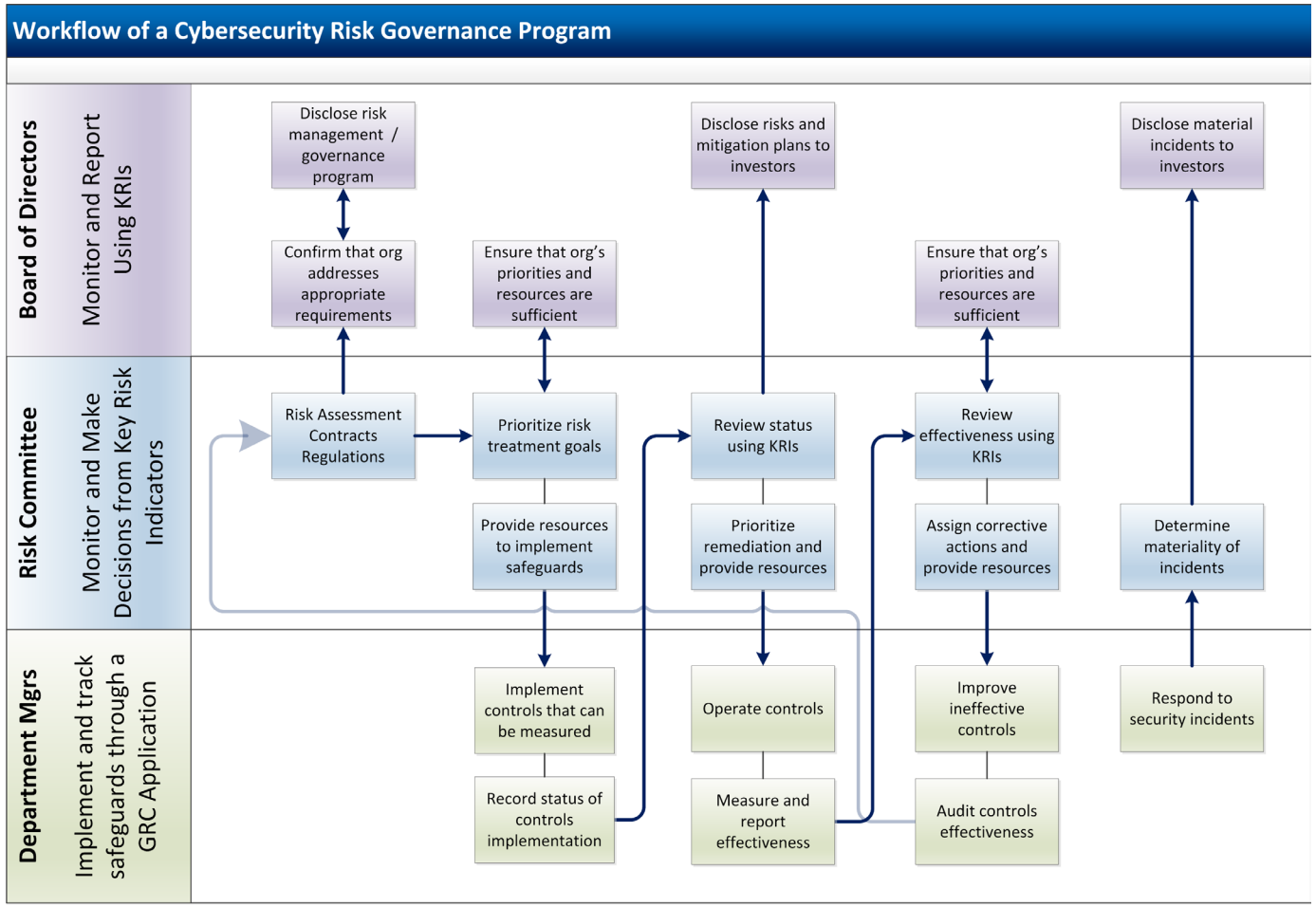
The market sees this: *"Please tell investors how management are involved in cybersecurity incident management."*

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

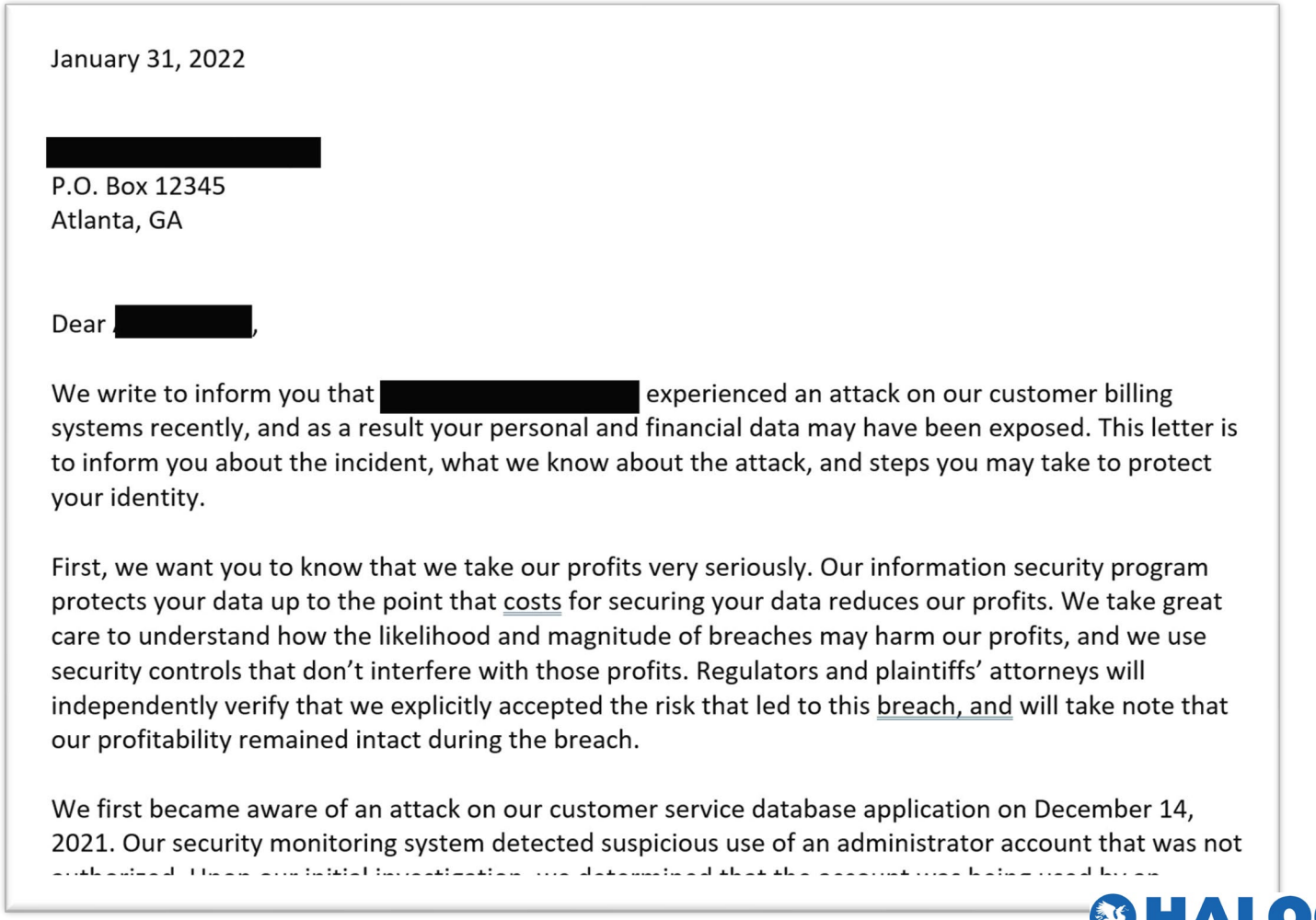
Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors

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

Information Flow for Good Governance



An Indicator of Bad Governance



January 31, 2022

[redacted]
P.O. Box 12345
Atlanta, GA

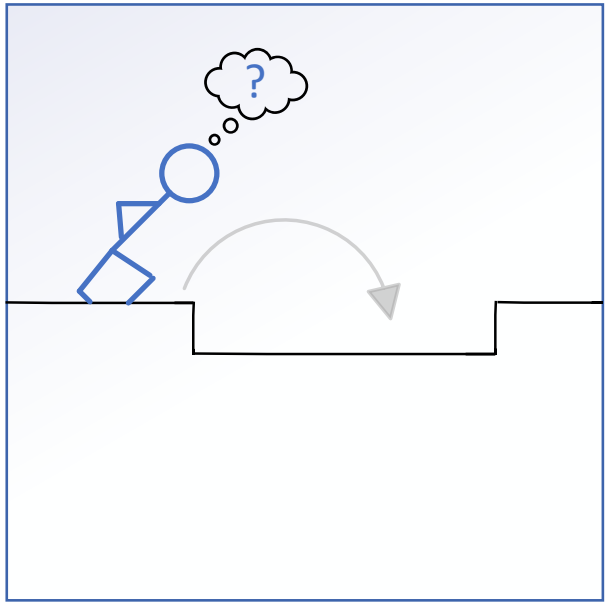
Dear [redacted],

We write to inform you that [redacted] experienced an attack on our customer billing systems recently, and as a result your personal and financial data may have been exposed. This letter is to inform you about the incident, what we know about the attack, and steps you may take to protect your identity.

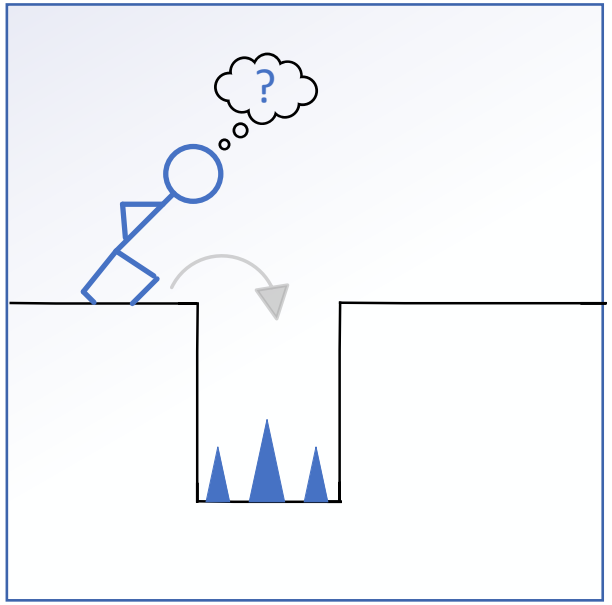
First, we want you to know that we take our profits very seriously. Our information security program protects your data up to the point that costs for securing your data reduces our profits. We take great care to understand how the likelihood and magnitude of breaches may harm our profits, and we use security controls that don't interfere with those profits. Regulators and plaintiffs' attorneys will independently verify that we explicitly accepted the risk that led to this breach, and will take note that our profitability remained intact during the breach.

We first became aware of an attack on our customer service database application on December 14, 2021. Our security monitoring system detected suspicious use of an administrator account that was not

Another Way to Say It…

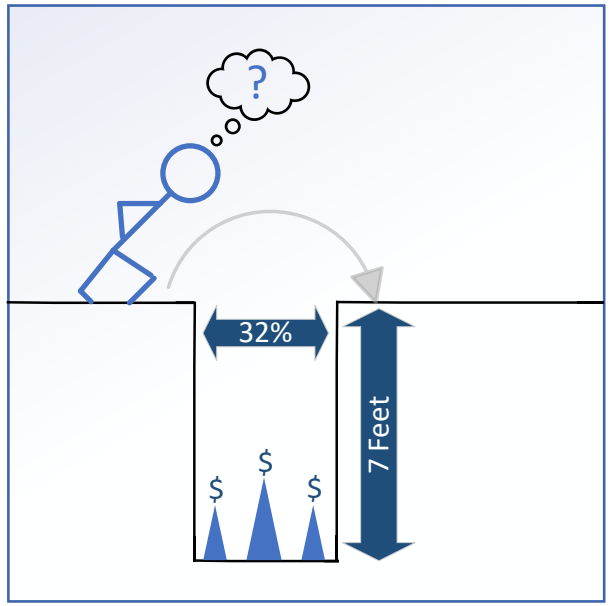


Risk analysis is about likelihoods ...

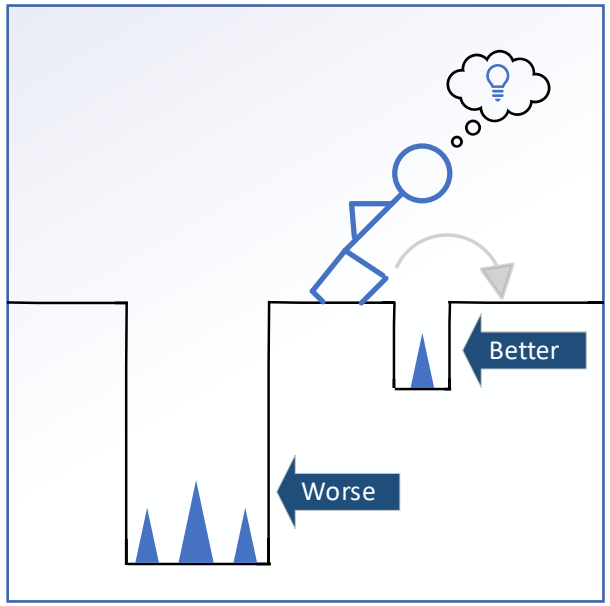


… and it's about impacts

Another Way to Say It…

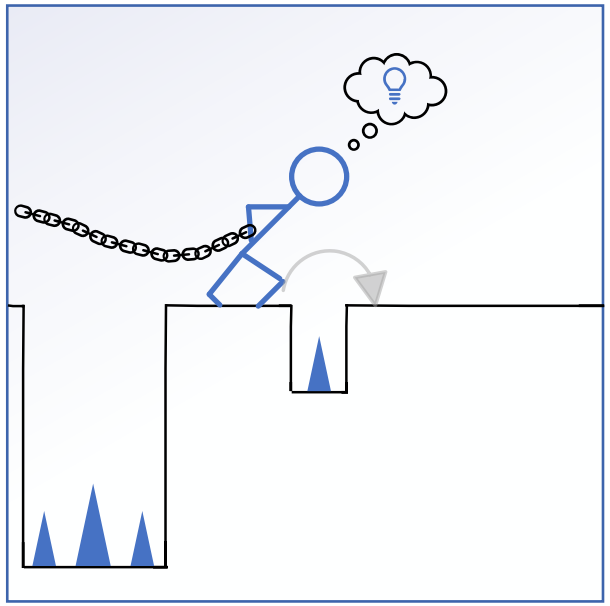


Some risk analysis is quantitative

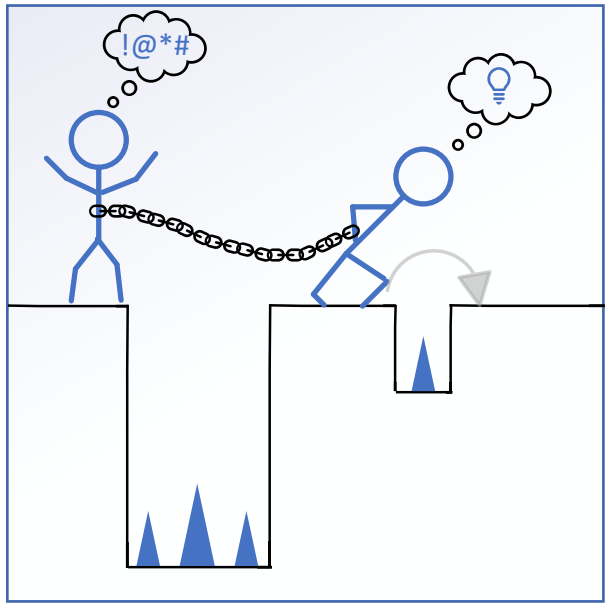


Some risk analysis is qualitative

Another Way to Say It…



But cyber risk analysis misses the point …



… if you forget the risks you impose on others.

HALOCK® Purpose Driven Security

CLE Code Announcement No. 2 for Webinar Attendees

Please listen carefully for the second CLE code announcement. Record the code on your Affirmation Form and return it to Lisa Frymark at lfrymark@foley.com following the program.

Using Risk to Define Reasonable and Material

Objectives Impact	Mission Impact	Obligations Impact	x	Likelihood
"Profit"	*"User health"*	*"User Privacy"*		
1. On plan	*1. Significant results*	*1. No harm*		*1. Not possible*
2. Within variance	*2. Few flat results*	*2. Concern*		*2. Rare, if at all*
3. Out of variance	*3. Significant misses*	*3. Few embarrassed*		*3. Occasional*
4. < 3 yrs profit loss	*4. Majority misses*	*4. Many exploited*		*4. Common*
5. Out of business	*5. Cannot help users*	*5. Millions exploited*		*5. Frequent*

Impact we would invest in to prevent		Likelihood of impact we would invest in to prevent		Risk we would invest in to prevent		Acceptable Risk
3	*x*	*3*	*=*	*9*	*<*	*9*

Adoption of DoCRA for Reasonableness

2021	Pennsylvania uses DoCRA and CIS RAM to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v. Earl Enterprises*
2022	Pennsylvania uses DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v. Hanna Andersson*
2022	Seven states use DoCRA's principles as a test for reasonable security in a data breach lawsuit. *Pennsylvania v. Wawa*. These states include Pennsylvania, New Jersey, Delaware, Maryland, Washington D.C., Virginia, and Florida.
2022	Two states (Pennsylvania and New York) use DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v. Herff Jones*
2023	Various commentators proposed incorporating the test into draft regulations interpreting the Colorado Privacy Act's requirement of "reasonable" security measures for personal information.
2023	Two states (Pennsylvania and Ohio) use DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v. DNA Diagnostics Center, Inc.*

Why You Really, Really Want to Define Reasonableness and Materiality for Yourself

1. Regulations are vague because regulators cannot be more specific than the law allows.
2. Vagueness can be used to your advantage.
3. Base your definitions for reasonableness and materiality in law and standards of practice.
   - DoCRA has done this for you.
   - CIS RAM is a great place to start. It's free and comes with instructions.
   - The SEC will not define material for you; generally, something is material if a reasonable person would consider it important when making an investment decision, or if it would significantly affect existing publicly available information about a company.
4. When held to account, your definitions will likely prevail.
   - See Item 1.
5. If you do not define reasonable and material, regulators will see this and hold it against you.

DoCRA View – 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.

DoCRA users say this: *"Our risk analysis evaluates potential impacts to three factors, our business objectives, our mission, our obligations to prevent harm to customers, employees, investors. We invest in safeguards that are no more burdensome to us than the risk reduction they create for others. Our risk management plan targets risks that would not require repair to any party."*

DoCRA View – Form 10-K Disclosure Requirement: Governance

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:

DoCRA users say this: *"The Executive Committee evaluates the materiality of cybersecurity incidents in part by determining whether the incident causes an unacceptable impact, as defined by our risk assessment criteria (our mission, our objectives, our obligations)."*

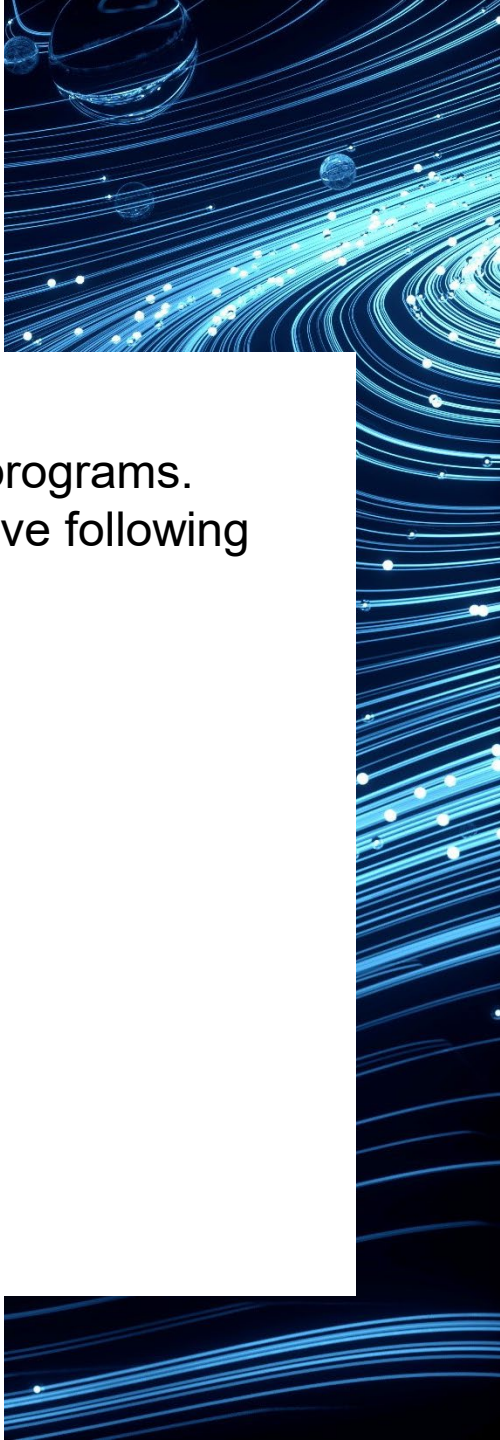
DoCRA View – Form 10-K Disclosure Requirement: Governance (cont'd.)

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

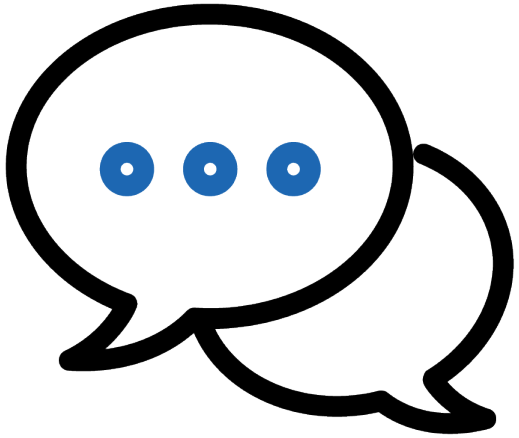
DoCRA users say this: *"The Executive Committee sets criteria and goals for reasonable risk using the three impact criteria (our mission, our objectives, our obligations). They provide resources and prioritization for reducing those risks with improved safeguards and processes. They receive non-technical updates about the progress of risk-reducing activities, and issues that must be addressed. They alter plans, resources, and priorities to ensure that they we meet our risk goals."*

We Value Your Feedback

We would greatly appreciate your thoughts and suggestions to help us improve for future programs. Please take a moment to complete the brief, optional feedback questionnaire you will receive following the program.



Questions?



Presenters

FOR MORE INFORMATION, PLEASE CONTACT US:

Jennifer Urban, CIPP/US
Partner, Cybersecurity Practice
Foley & Lardner LLP
jurban@foley.com

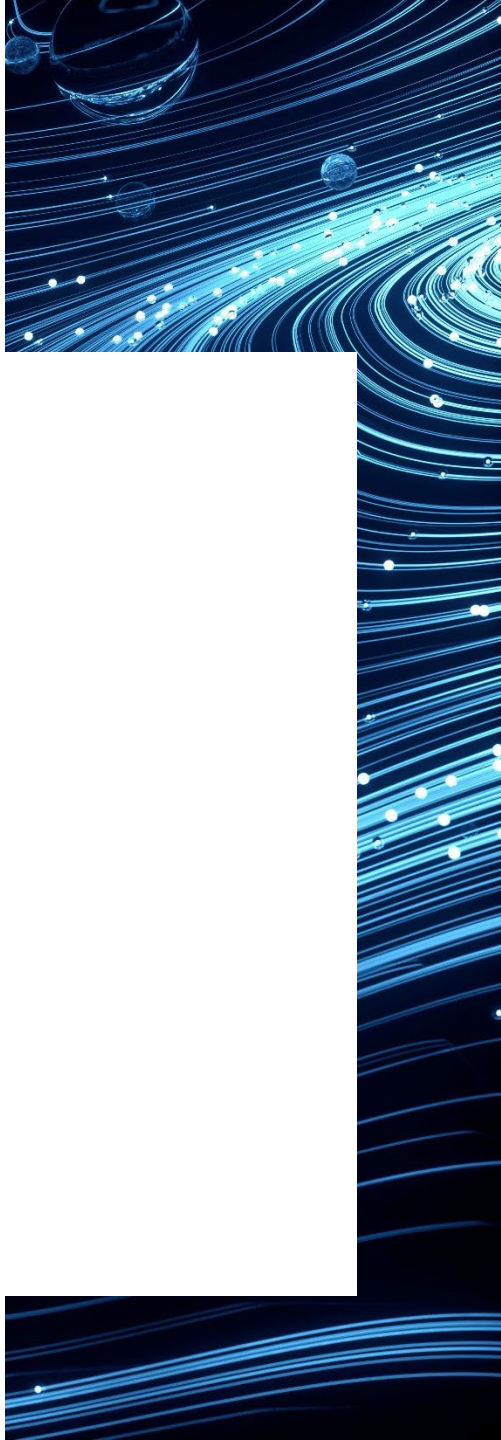
Terry Kurzynski, CISSP, CISA, PCI QSA, ISO 27001 Auditor
Senior Partner
HALOCK Security Labs
terryk@halock.com

Chris Cronin, ISO 27001 Auditor
Partner
HALOCK Security Labs
ccronin@halock.com

Jessica Lochmann
Partner, Transactions Practice
Foley & Lardner LLP
jlochmann@foley.com

About Foley

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With over 1,100 lawyers in 25 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical and beneficial to their businesses.



FOLEY

FOLEY & LARDNER LLP

FOLEY.COM