CYBERSECURITY CURRENT PERSPECTIVES FOR BOARDS

ARAVIND SWAMINATHAN, PARTNER

January 16, 2024

orrick

LEGAL LANDSCAPE

orrick

U.S. "Cybersecurity Law"

Laws imposing civil or criminal liability for **hacking**

Laws implementation of **security** measures

Laws requiring **notification** of security breaches

Contractual duties re: security and/or breach notification

Regulator enforcement **consent decrees**, and related requirements

Regulator and industry **standards, guidelines, and frameworks**

Industry Standards

- **Key Points:**
  - Not legal requirements
  - Can be required by contract
  - Some can be a safe harbor

U.S. State Breach Notification Laws

50 state breach notification and data security laws

Information Covered

- Name combined with SSN, driver's license or state ID, financial account numbers, etc.
- Some states include tax information, medical and health insurance information, or biometric information
- Usernames with passwords

Exemptions

- GLBA, HIPAA, other regulatory regime, written policies

Exceptions

- No Risk of Harm to the Individual
- Good Faith Acquisition by and Employee/Agent
- Non-Electronic Data (only hard copies)
- Encryption (without the key)
- Publicly available

"Data Breach"

- Triggered by **unauthorized acquisition / access / loss / use of** PI that compromises the confidentiality, integrity or security of data in electronic or hard copy.

Consequences

- **Notification to:**
  - **Individuals**
  - **States Attorneys General**
- **Timing:** varies, as short as 10 days from determination of breach

Health Insurance Portability and Accountability Act

Breach Notification Rule

Protected Health Information ("PHI")

Information that is (1) individually identifiable, (2) created or received by a Covered Entity ("CE") or Business Associate ("BA") and (3) relates to the:

- Physical or mental health or condition of an individual,
- Provision of health care to an individual, or
- Payment for health care provided to an individual

Exceptions

- Financial Transaction
- Low probability PHI compromised
- Unintentional workforce acquisition, access, or use (good faith and within scope of authority)
- Inadvertent disclosure within CE or BA
- Good faith belief no retention of information

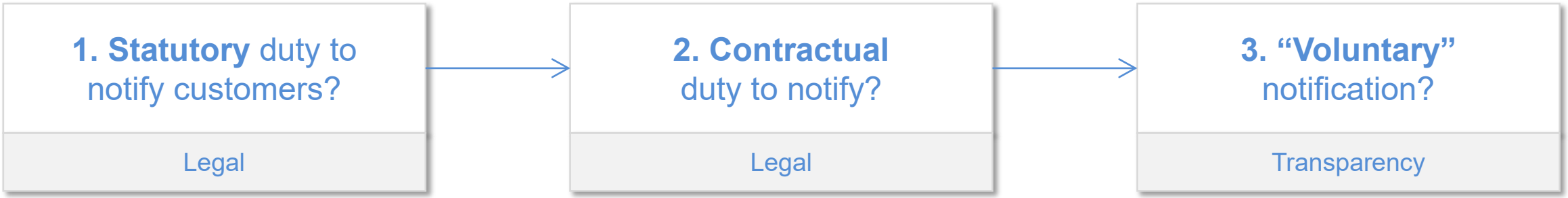
"Breach of Security"

- **Unauthorized acquisition, access, use, or disclosure of** PHI that compromises the privacy or security of PHI.

Consequences

- **Notice to OCR:** If 500 or more individuals are affected, CEs must notify OCR without unreasonable delay and in no case later than **60 calendar days** after discovery of breach. CEs can notify HHS-OCR annually if fewer than 500 individuals are affected.
- **Notice to individuals and the media:** Individuals must be notified without unreasonable delay and in no case later than **60 calendar days** after discovery of breach. If more than 500 individuals in a single state or jurisdiction, the media must be notified.
- **OCR Investigation:** OCR must investigate breaches with 500 or more affected individuals.

Legal Framework: Obligation to Notify



- Generally trigger on unauthorized "access" or "acquisition" of personal information, plus exceptions
- 50+ separate U.S. state laws + territories
- FTC ACT Notice
- Rest-of-world

- Differs by customer re: definitions and duties
- Contractual duties unaffected by statute

- Forensics are often inconclusive, which leads to a multi-factor decision tree
- Voluntary notice scenarios based on facts, risk mitigation and ethical concerns

What is your North Star?

Legal Framework

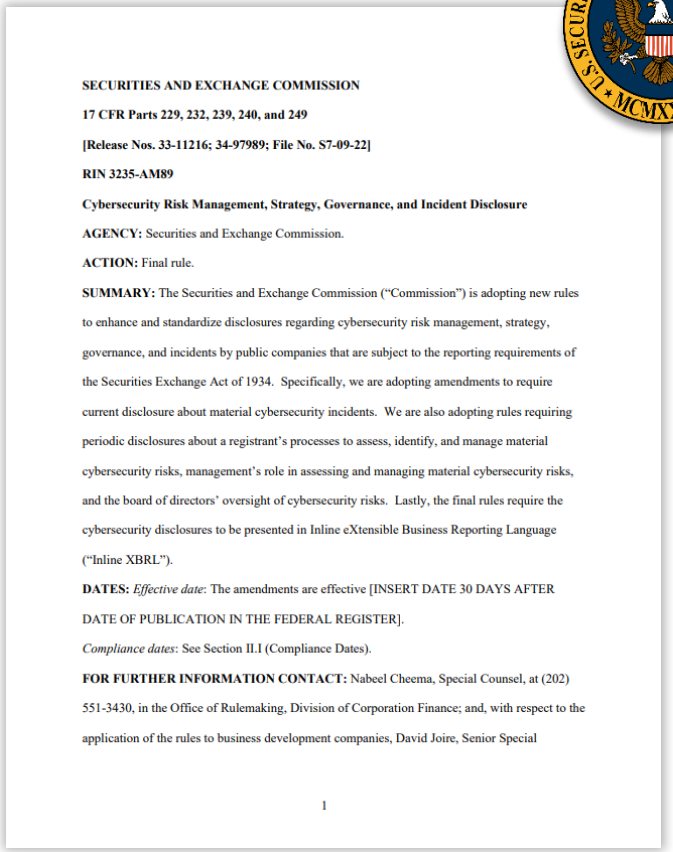
- **Obligation to conduct a "reasonable" investigation**
  - State Breach Notification Statutes
  - FTC Act
  - Industry-specific Requirements
    - GLBA Guidance
  - GDPR (and, increasingly, other international regimes, e.g., China, Turkey, Brazil)
  - Contracts
- **What is a reasonable investigation?**
  - Balance of factors including volume and sensitivity of data, type of attack, burden of investigation, and industry custom
  - Practical concerns

Third-Party Risk Management

- Conduct diligence on security
- Consider contractual provisions
  - Statutory requirements (reasonable security)
  - Breach notification
  - Liability provisions
- Ongoing review and assessment to verify compliance

SEC Finalizes Cybersecurity Disclosure Rules

- Effective December 18, 2023, companies must disclose material cybersecurity incidents, including certain third-party incidents, on a Form 8-K.
- The materiality determination must be made "*without unreasonable delay*," a slight softening from the proposal.
  - Disclosure must describe the incident's nature, scope, timing and effect, less detail than the proposal.
- There is a limited exception for delay if requested by the United States Attorney General.
- Governance disclosures focus on board and management processes for cyber risk, and apply starting with 10-K filings for fiscal years ending on or after December 15, 2023.
- Companies do not have to disclose director cyber expertise, or how the board considers cybersecurity in company strategy.



SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11216; 34-97989; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks. Lastly, the final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL").

DATES: *Effective date*: The amendments are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Compliance dates: See Section II.I (Compliance Dates).

FOR FURTHER INFORMATION CONTACT: Nabeel Cheema, Special Counsel, at (202) 551-3430, in the Office of Rulemaking, Division of Corporation Finance; and, with respect to the application of the rules to business development companies, David Joire, Senior Special

1

SEC Rulemaking: Themes and Trends

"*A registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.*"

"*[I]dentify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risk*"

- Increased SEC focus on **process disclosure**
- SEC increasingly seeking disclosure of **specific uniform data**, regardless of whether material to the issuer
- SEC seeking detailed **board governance disclosures** – personnel, processes, and views
- SEC seeking detailed **disclosure about management-level governance** – personnel, processes, and views
- SEC focused on **risk management programs** and related disclosures

SPECIAL CONSIDERATIONS FOR BOARDS

Trending: Focus on Executives and Boards

Business

Yahoo Shareholder Sues Company For Delaying Data Breach Disclosures

A Yahoo shareholder has sued the company's directors in Santa Clara County Superior Court for allegedly violating their fiduciary duties.

By Norcal Patch (Patch Staff) - March 10, 2017 11:53 am ET

Like 0

RISK MANAGEMENT

Shareholder sues Wendy's over data breach

Judy Greenwald

12/21/2016 2:42:00 PM

SHARE

A Wendy's Co. shareholder has filed a derivative lawsuit against the company and

Jonathan Weiss/Shutterstock.com

Sell In May & Walk

LAW360 A LexisNexis® Company

News, cases, companies, firms

7 Target Board Members In ISS' Over Data Breach

By Linda Chiem

TECH

SEC sues SolarWinds over massive cyberattack, alleging fraud and weak controls

PUBLISHED TUE, OCT 31 2023•10:48

Rohan Goswami

MAY 5, 2014 @ 08:20 AM

Target CEO Gregg Steinhafel Resigns In Data Breach Fallout

TECH

FTC seeks to hold Drizly CEO accountable for alleged security failures, even if he moves to anotl company

PUBLISHED MON, OCT 24 2022•3:53 PM EDT

Lauren Feiner
@LAUREN_FEINER

SHARE

05-07-2014 | 07:32 AM | Author: Kevin M. LaCroix

Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit

Typical Post-Breach Claims Against Officers & Directors

Failure to:

- ☒ Implement and monitor effective cybersecurity program;
- ☒ Protect company assets and business by recklessly disregarding cybersecurity risks and ignoring “red flags”;
- ☒ Implement and maintain internal controls to protect customer or employee personal and financial information;
- ☒ Take reasonable steps to timely notify individuals that company’s information security system was breached; and/or
- ☒ Implement controls or oversee cybersecurity program, resulting in a waste of corporate assets.

Caused or allowed company to:

- ☒ Disseminate materially false and misleading statements to shareholders regarding incident; and/or
- ☒ Make false or misleading cyber-risk disclosures in public filings

Key Questions for Execs / Board Members To Consider

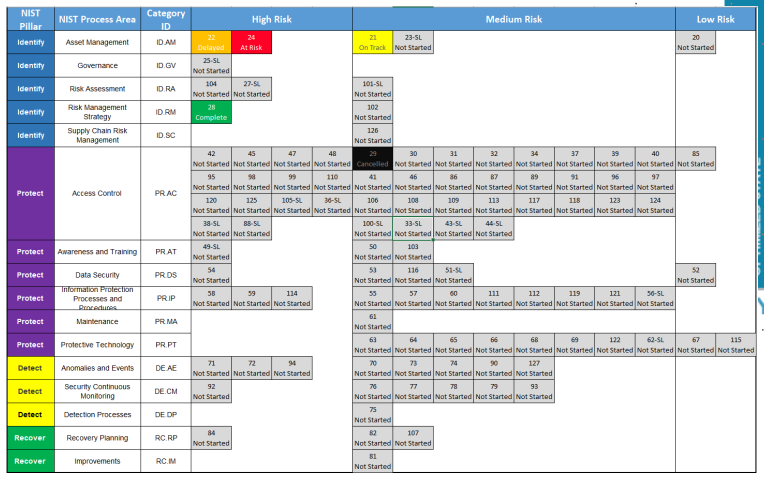
- **Top Cybersecurity Risks**: What are our top cybersecurity risks, and what is the residual risk the business is accepting?
- **Risk Ownership**: Who in management has primary ownership of cybersecurity risk?
- **Security Framework**: Do we use a security framework, such as National Institute for Standards and Technology (NIST) Cybersecurity Framework, and how has our maturity evolved over time?
- **Considering External and Internal Threats**: Are both external and internal threats considered when planning cybersecurity program activities?
- **Periodic Assessments**: Do we conduct periodic technical and risk assessments? Do we base remediation and security improvements on identified risks?
- **Auditing**: Do we audit and test our security controls, practices and procedures, to ensure we are following them, and they are working effectively?
- **Vulnerability Management Program**: Do we have a vulnerability management program and standardized SLAs for addressing / mitigating / remediating vulnerabilities?
- **Business Continuity and Disaster Recovery**: Do we have a BC/DR strategy? Is it integrated into our incident response process? Do we test it regularly?

Key Questions for Execs / Board Members To Consider

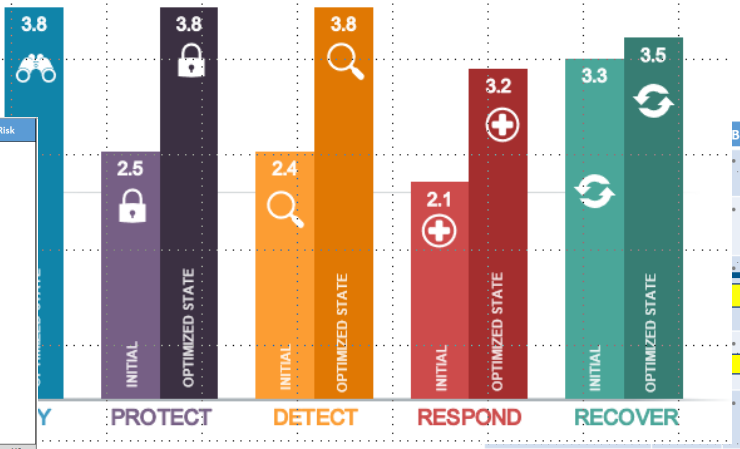
- **Vendors**: Do we require vendors to have a minimum level of security, and test them regularly?
- **Threat Intelligence**: Do we have a structured and comprehensive approach to obtaining threat intelligence, including participating in threat intelligence sharing forums to develop understanding of threat landscape (*e.g.*, FS-ISAC)?
- **Employees**: Are employees trained and made aware of their role related to cybersecurity? Does every employee receive some basic cybersecurity awareness training? Do we offer remedial training for those who need it?
- **Inventory of Data and Assets**: Do we have an inventory of data and assets that might be subject to compromise (e.g., data map or network map)?
- **Encryption**: Do we use encryption to protect data in transit and at rest?
- **Incident Response Plan**: In the event of a cyberattack, has management developed a robust incident response plan? Do we have outside resources that may be necessary if there's an attack?
- **Cyber Insurance**: Do we have cyber liability or other insurance to cover costs of forensic analysis, legal services, public relations, credit monitoring, litigation defense, etc.?

Regular Board Briefings by Company Security Team

- Establishing baseline of the current cybersecurity program
- Cybersecurity roadmap development and progress to goals



NIST Pillar	NIST Process Area	Category ID	High Risk	Medium Risk	Low Risk
Identify	Asset Management	ID.AM	22 Delayed; 24 At Risk	21 On Track; 23-SL Not Started	20 Not Started
Identify	Governance	ID.GV	25-SL Not Started		
Identify	Risk Assessment	ID.RA	104 Not Started; 27-SL Not Started	101-SL Not Started	
Identify	Risk Management Strategy	ID.RM	28 Complete	102 Not Started	
Identify	Supply Chain Risk Management	ID.SC		126 Not Started	
Protect	Access Control	PR.AC	42 Not Started; 45 Not Started; 47 Not Started; 48 Not Started; 95 Not Started; 98 Not Started; 99 Not Started; 110 Not Started; 120 Not Started; 125 Not Started; 105-SL Not Started; 36-SL Not Started; 38-SL Not Started; 88-SL Not Started	29 Cancelled; 30 Not Started; 31 Not Started; 32 Not Started; 34 Not Started; 37 Not Started; 39 Not Started; 40 Not Started; 41 Not Started; 46 Not Started; 86 Not Started; 87 Not Started; 89 Not Started; 91 Not Started; 96 Not Started; 97 Not Started; 106 Not Started; 108 Not Started; 109 Not Started; 113 Not Started; 117 Not Started; 118 Not Started; 123 Not Started; 124 Not Started; 100-SL Not Started; 33-SL Not Started; 43-SL Not Started; 44-SL Not Started	85 Not Started
Protect	Awareness and Training	PR.AT	49-SL Not Started	50 Not Started; 103 Not Started	
Protect	Data Security	PR.DS	54 Not Started	53 Not Started; 116 Not Started; 51-SL Not Started	52 Not Started
Protect	Information Protection Processes and Procedures	PR.IP	58 Not Started; 59 Not Started; 114 Not Started	55 Not Started; 57 Not Started; 60 Not Started; 111 Not Started; 112 Not Started; 119 Not Started; 121 Not Started; 56-SL Not Started	
Protect	Maintenance	PR.MA		61 Not Started	
Protect	Protective Technology	PR.PT		63 Not Started; 64 Not Started; 65 Not Started; 66 Not Started; 68 Not Started; 69 Not Started; 122 Not Started; 62-SL Not Started	67 Not Started; 115 Not Started
Detect	Anomalies and Events	DE.AE	71 Not Started; 72 Not Started; 94 Not Started	70 Not Started; 73 Not Started; 74 Not Started; 90 Not Started; 127 Not Started	
Detect	Security Continuous Monitoring	DE.CM	92 Not Started	76 Not Started; 77 Not Started; 78 Not Started; 79 Not Started; 93 Not Started	
Detect	Detection Processes	DE.DP		75 Not Started	
Recover	Recovery Planning	RC.RP	84 Not Started	82 Not Started; 107 Not Started	
Recover	Improvements	RC.IM		81 Not Started	



		Basic	Intermediate	Advanced	Optimized
		External p… protected			• Integrated processes into risk management framework
		• Basic tools	• < 24 hours to detect nefarious • Federated SIEM	• < 2 hours to detect nefarious activity	• Near real-time detection • Integration into Microsoft PAC
		• Basic playbook • SDLC and Operations	• Integrated crisis management • Forensics Compliant	• Red Team drills • Ransomware Settlement Service	• Destructive testing • 3rd party IR Integration • Hardened Backups
		• Onboarding & Off- No Change	• Dormant Account Controls • Role Based Provisioning	• Privileged Account Management • Service Account Controls	• Minimal access rights • Dark Web scans • Advanced authentication
		• OWASP best practices leveraged	• Tools used for targeted risk areas • Coding Standards Defined	• SDLC gates leveraging CI/CD • All developers trained in OWASP	• DevSecOps framework and team • Software Quality Visualization
Risk Management	Adhoc	• Known risks are prioritized for remedia…	• Published risk registry • Processes to identify adversaries, • Integration into ISAC organizations	• NIST Compliance • Risk Management integrated into disciplines	• 3rd Party Risk Management to understand supply chain and service risks • ISO 27K accredited ISMS
Red Team	Adhoc	• Occasional penetration	• Dedicated Red Team to threat hunt	• Mature Red Team and process	• Red Team leverage for 3rd party relationships • Team quality control
Security Culture	Adhoc	• Occasional awareness messaging	• Managed security awareness testing	• Awareness program tailored based on job function and risks	• Integrated into performance management and access constricted based on risk

- Key (15) questions for Board members

QUESTIONS?