

Managing Cybersecurity and CISO Risk— SolarWinds and New SEC Rule Implications

Thursday, Jan. 11, 2024

1:00-2:00 PM EST

10:00-11:00 AM PST

19:00-20:00 Europe

Welcome and Introductions

Panelists



Corey M. Dennis
Senior Director, Counsel,
Info. Sec & Privacy
Eli Lilly and Company



Ed McNicholas
Partner
Ropes & Gray



Caitlin Sarian
CEO
Cybersecurity Girl LLC



Judy Selby
Partner
Kennedys LLP







Cybersecurity Threat Landscape

- Costs to companies of cybersecurity incidents rising quickly
- Large cybersecurity attacks pose systemic economic risk and serious concerns for critical infrastructure and national security
- Most significant common cyber attacks:
 - Ransomware
 - Business Email Compromise
 - Insider threats
- SEC current guidance requires disclosures of cybersecurity risks
- Post-breach litigation and enforcement often alleges securities fraud based on statements about extent of cybersecurity protections as well as failures to effectively govern cybersecurity risks.

New SEC Cybersecurity Requirements

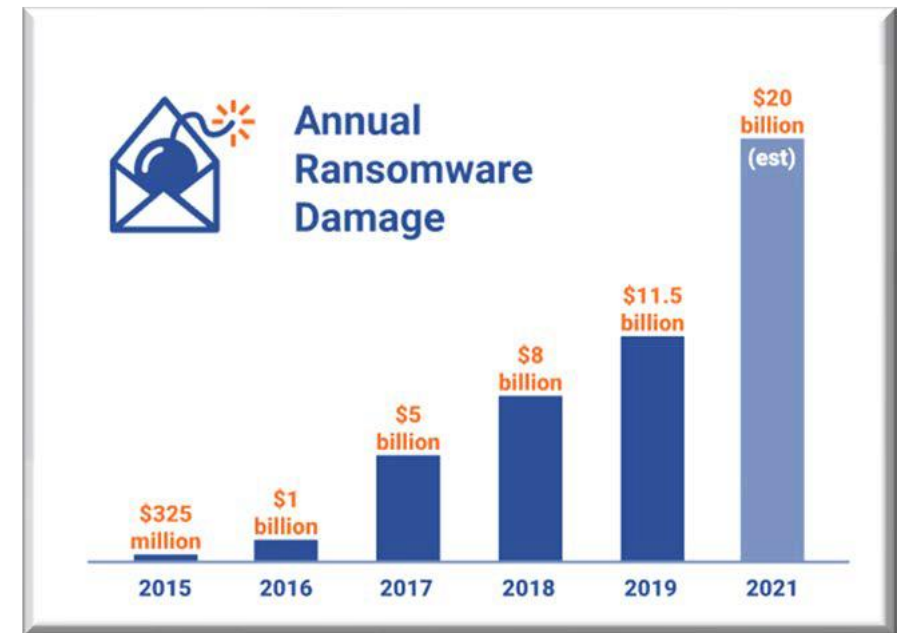
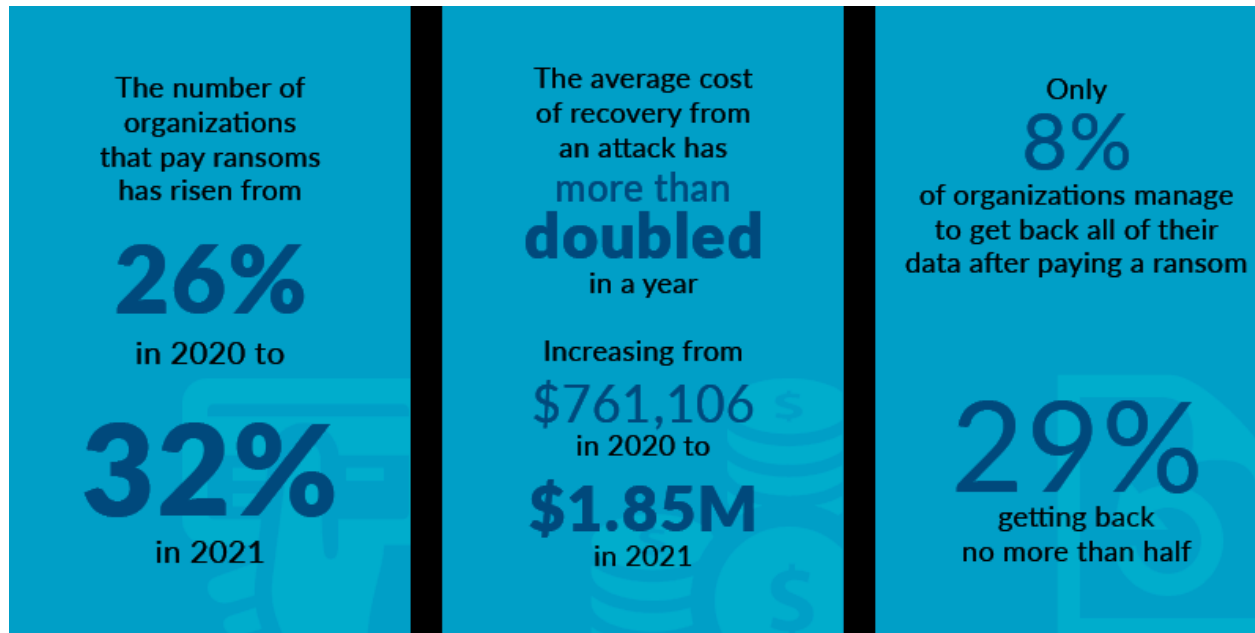
- 8-K disclosure within **four business days** after the registrant determines that it has experienced a material cybersecurity incident
- Further disclosures of cybersecurity risks including 10-K disclosures of
 - Policies and procedures for identifying and managing cybersecurity risks;
 - Cybersecurity governance processes,
 - Expressly including the board of directors' oversight role regarding cybersecurity risks; and
 - Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing policies, procedures, and strategies.

Understanding cyber attackers

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hactivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Cyber Threats Dramatically Increasing

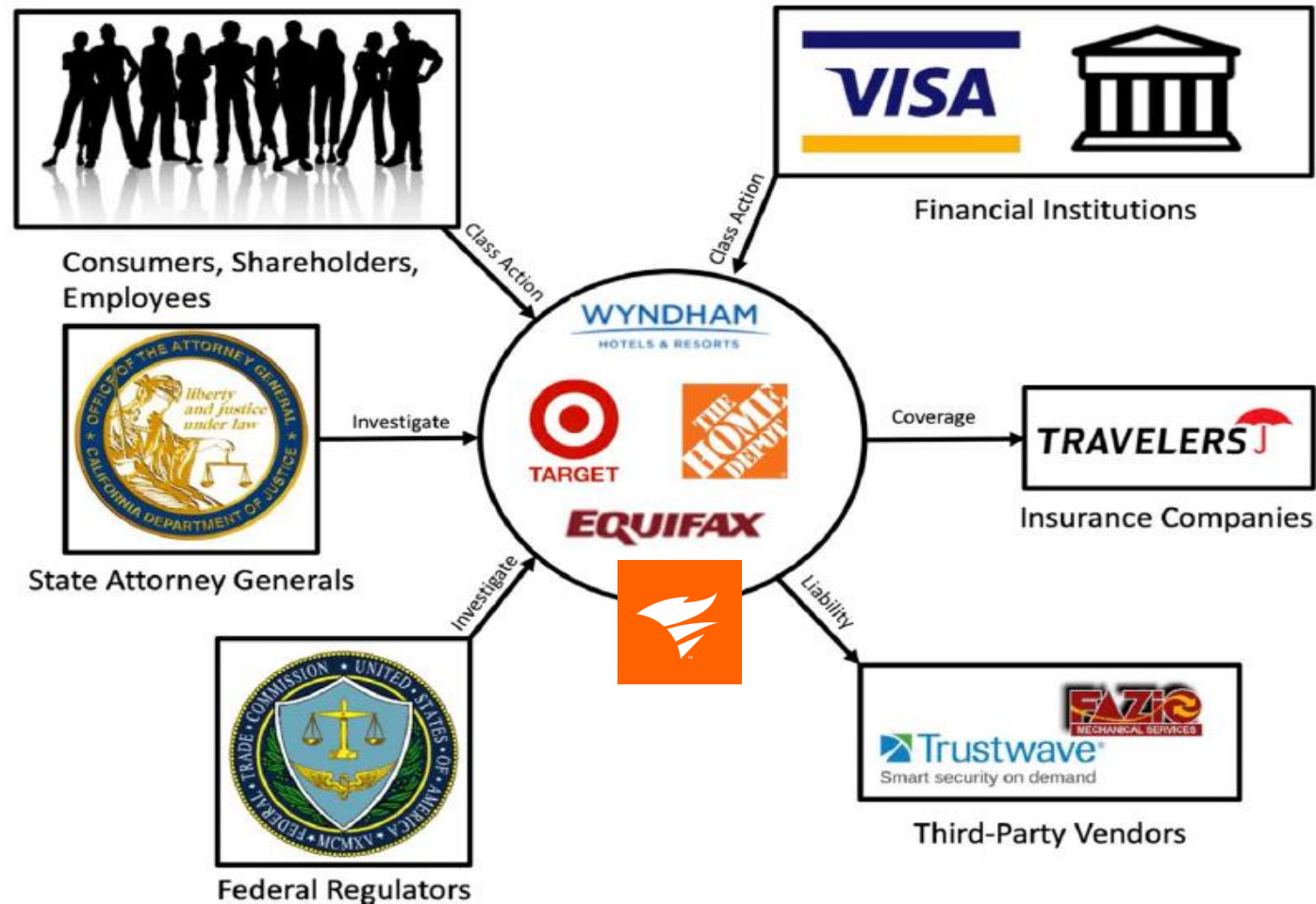
- In 2022, the FBI received 800,944 cyber-incident complaints
- \$26 billion in losses reported to the FBI between 2016 and 2019 from business email compromise, a/k/a "Phishing."



Sometimes Complex and Slow: Anatomy of APT

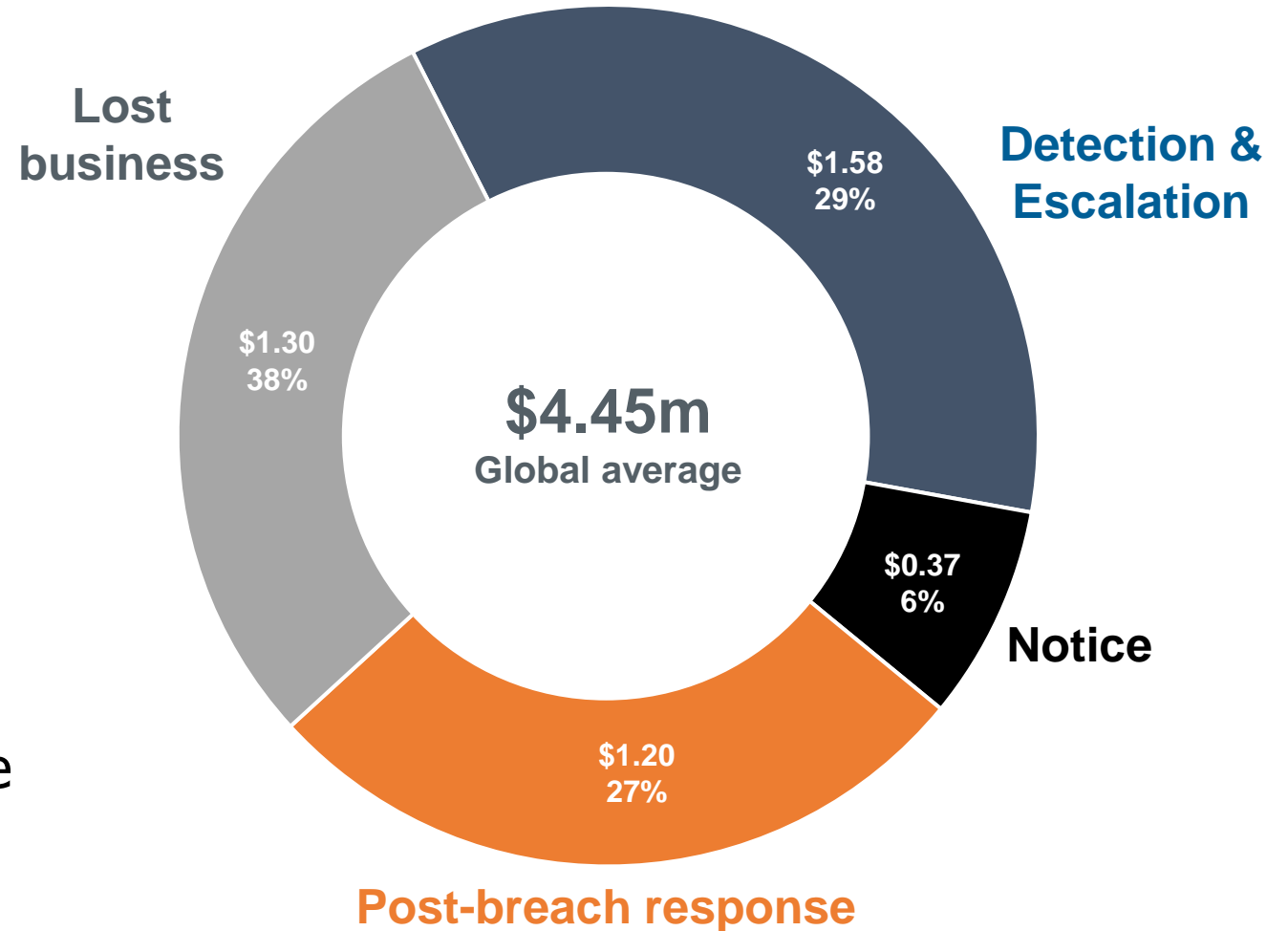


Implications of a data breach



Cost of a data breach is growing

- Between Mar. 2022 and Mar. 2023, the **average** data breach cost to the entity experiencing the breach reached an all-time high: **\$4.45 million**
- This is a 15.3% increase since 2020 when the average cost was \$3.86 million
- Significant potential harms from loss of client trust and confidence / damage to market reputation



Duties of Corporate Boards

State Statutory Standards for Directors

*Act in **good faith**, with the care an **ordinarily prudent person** would exercise in similar circumstances, and in what they **reasonably believe** to be in the **best interests of the corporation**.*

Fiduciary Duties

Duty of Care

- Stay educated and make informed decisions

Duty of Loyalty

- Act in the corporation's best interests
- Avoid conflicts of interest

New SEC Cybersecurity Requirements

- New regulations adopted July 26, 2023, effective Dec. 2023 for most issuers
- 8-K disclosure within **four business days** after the registrant determines that it has experienced a material cybersecurity incident
- 10-K periodic disclosures regarding material cybersecurity risks including:
 - Disclosures of previously undisclosed individually immaterial cybersecurity incidents that become material in the aggregate
- 10-K periodic disclosures of policies and procedures to identify and manage cybersecurity risks
 - Management's role in implementing cybersecurity policies and procedures
 - Board of directors' oversight of cybersecurity risk; and
 - Updates about previously reported material cybersecurity incidents

Content of 8-K Incident Reporting

- Under the new rules, Form 8-K requires a registrant to disclose the following information about a material cybersecurity incident, to the extent the information is known at the time of the Form 8-K filing:
 - When the incident was discovered
 - Whether it is ongoing;
 - A brief description of the nature and scope of the incident;
 - Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
 - The effect of the incident on the registrant's operations; and
 - Whether the registrant has remediated or is currently remediating the incident.
- No expectation of disclosure of specific, technical information.

Timing of 8-K Incident Reporting

- Four business day clock starts upon determination of materiality
 - Date of discovery of incident does not start clock
 - “a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.”
- Existence of ongoing internal investigation not a basis for delay
- No law enforcement investigation delay, unless the US Attorney General determines disclosure poses substantial risk to national security or public safety
 - “Form 8-K would require disclosure in a situation in which a state law delay provision would excuse notification,”
 - “a registrant would be required to disclose the incident on Form 8-K even though it could delay incident reporting under a particular state law”

Assessing materiality of an incident

- Information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision, or if it would have “significantly altered the ‘total mix’ of information made available.”
- Guidance to resolve doubts “in favor of those the statute is designed to protect,” investors.
- Registrants will need to “thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material. Even if the probability of an adverse consequence is relatively low, if the magnitude of the loss or liability is high, the incident may still be material; materiality ‘depends on the significance the reasonable investor would place on’ the information.”

Shareholder Derivative Litigation

- If data breach causes significant harm to a company, shareholders may attempt to bring **shareholder derivative litigation** against officers or directors whom they allege breached their “duty” to the company by allowing harm to occur.
- Shareholders must meet a **high hurdle before being permitted to sue** on behalf of the company, as courts typically presume that directors and officers make decisions that they believe, in good faith, to be in the companies’ best interests.
- **Business Judgment Rule:** [P]laintiffs must demonstrate that the board’s refusal to sue was made in “**bad faith**” or “**based on an unreasonable investigation.**”

Shareholder Derivative Litigation Standard

- Defeating this presumption of good faith requires plaintiffs to show that the board acted in **bad faith**.
 - Directors intentionally acted with a purpose that was not intended to advance the company's best interests
 - Directors intentionally violated the law, or
 - Directors intentionally "fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities." (*Stone v. Ritter*, 911 A.2d 362 (Del. 2006))

Significant Cases for Board Liability

Boards are increasingly expected to exercise significant oversight over cybersecurity functions. Alleged failures to exercise appropriate oversight lead to shareholder derivative suits, securities fraud actions, and regulatory civil and criminal enforcement.

- In January 2019, **Yahoo** settled a shareholder derivative lawsuit for \$29 million following high-profile data breaches in 2013 and 2015, which resulted in a \$350 million reduction in the company's sale price. *Prior breach-related derivative suits had been largely unsuccessful.*
- In October 2021, the Delaware Chancery Court *dismissed a cybersecurity-related derivative lawsuit* against **Marriot**, in part because board-level monitoring and reporting systems were in place and proved that the board educated itself on the evolving cyber threat environment.
- **SolarWinds** obtained *dismissal of several derivative actions by shareholders* claiming company leadership should have foreseen and protected against the data breach that took place in 2020 – despite the fact that SolarWinds was attacked by a top-tier Russian espionage team. Securities fraud claims, now settled, were premised on company comments on its cybersecurity readiness. In April 2022, a federal district court rejected the motion to dismiss of two private equity shareholders (each holding roughly 40% of the stock) premised on the allegation that they together had sufficient control for potential § 20(a) securities fraud liability.

Insurance coverages to consider*

- Cyber insurance
 - SEC exclusions
 - Other coverage issues
- Tech E&O
- Directors and officers
 - Definition of insureds
 - Does the policy apply only to individuals in specified roles?
 - Cyber or privacy-related exclusions
- Management liability
- Holistic approach to insurance portfolio
- Evaluated insurance policy limits in light of increasing exposures

***Consider personal indemnity agreements in addition to insurance coverage**

Typical breach notifications v. Form 8-K filing

- **Notifications that may be covered under cyber policies**

- Impacted individuals under breach notification laws
- Pre-approved service providers
- Impacted business partners pursuant to contractual obligations
- State AGs and certain other regulators (i.e., OCR)

- **Form 8-K**

- “Current report”
- ***Filed*** with the SEC
- Announce major events that ***shareholders*** should know about
- Non-compliance could lead to SEC investigation, fraud allegations, litigation regarding board’s cyber expertise, etc.



yahoo!

Ex-Yahoo Directors Settle Data-Breach Claims for \$29 Million

Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack



U.S. SECURITIES AND
EXCHANGE COMMISSION

The New York Times

Verizon Will Pay \$350 Million Less for Yahoo

Altaba, Formerly Known as Yahoo!,
Charged With Failing to Disclose
Massive Cybersecurity Breach; Agrees
To Pay \$35 Million

SEC Settlement

blackbaud®

**Software firm Blackbaud to pay \$3 mln
for misleading disclosures on
ransomware attack -SEC**



SEC Charges Software Company
Blackbaud Inc. for Misleading
Disclosures About Ransomware Attack
That Impacted Charitable Donors

FOR IMMEDIATE RELEASE
2023-48



Recent SEC Litigation



**US SEC sues SolarWinds for concealing
cyber risks before massive hacking**



SEC Charges SolarWinds and Chief
Information Security Officer with Fraud,
Internal Control Failures

Complaint alleges software company misled investors about
its cybersecurity practices and known risks

FOR IMMEDIATE RELEASE
2023-227



Organizational Responses to Cyber Risk

- Create, maintain, and exercise a **cyber incident response plan** and integrated legal and communications plan that includes response, notification, and escalation procedures.
- **Awareness and training programs** are key to address the human factor. The vast majority of significant information security incidents include a material element of human error.
- Create **relationships with cybersecurity response specialists** including forensic firms, attorneys, public relations, investor relations, cybersecurity insurance, and relevant law enforcement
- Emphasize appropriate **cybersecurity hygiene practices. Tone from the top is a key element of cybersecurity risk management leadership.**
- Elevate **third party risk management.** Even “internal” data often flows across the networks of several third parties, managed service providers, and cloud computing companies. Contractual assurances alone are not adequate to insure effective management of cyber risk and real-time coordination in responding to cyber attacks.

Questions and Answers

Panelists



Corey M. Dennis
Senior Director, Counsel,
Info. Sec & Privacy
Eli Lilly and Company



Ed McNicholas
Partner
Ropes & Gray



Caitlin Sarian
CEO
Cybersecurity Girl LLC



Judy Selby
Partner
Kennedys LLP

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: **IAPP TO ADD SURVEY LINK HERE**

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org