SEC Cybersecurity Governance Expectations For Public Companies

ROPES & GRAY

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.

AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- Cybersecurity Duties of Directors
- Existing SEC Expectations
- New SEC Rules
- Significant Litigation
- Cybersecurity Governance Best Practices

AGENDA

- Executive Summary
- **Cybersecurity Risk Landscape**
- Cybersecurity Duties of Directors
- Existing SEC Expectations
- New SEC Rules
- Significant Litigation
- Cybersecurity Governance Best Practices

Understanding cyber attackers

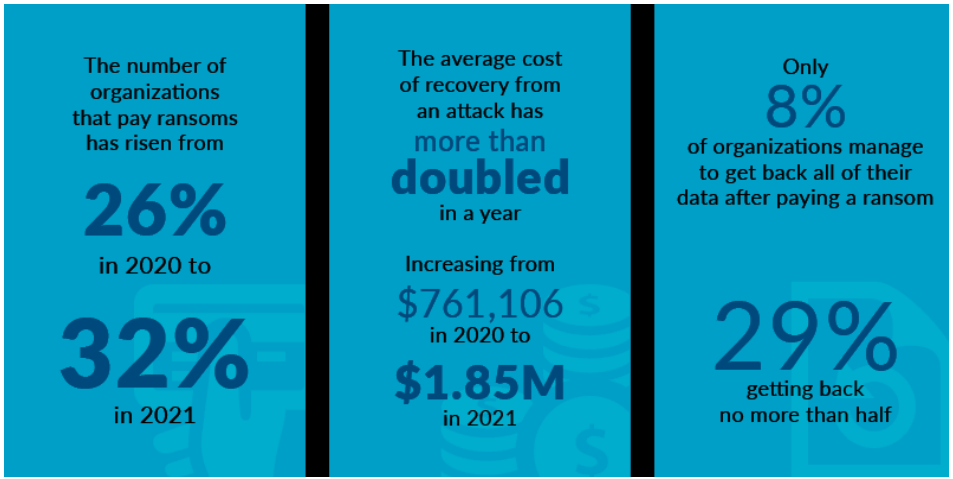
	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders 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.

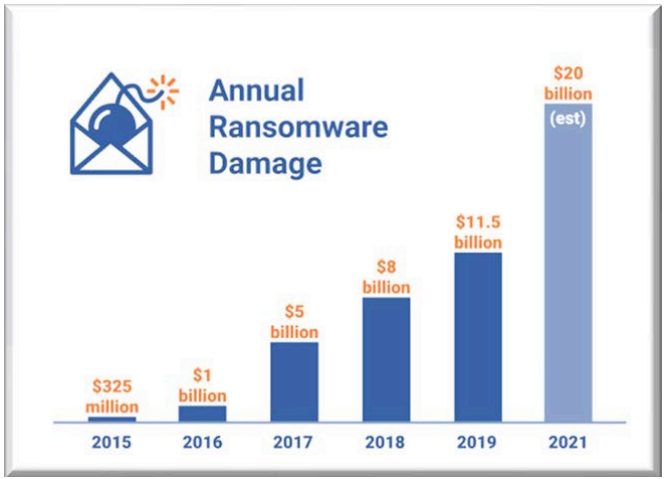
Drivers of Ransomware's Growth

- Unregulated cryptocurrency exchanges: Allow large international transfers that are exceptionally difficult to trace
  - Colonial Pipeline is a rare exception
- Ransomware-as-a-Service: Decreases entry costs and supports growth of specialized threat actor groups with particular skill sets, e.g., obtaining passwords, hacking systems, searching stolen data, compiling stolen identity dossiers, filing false tax returns, obtaining credit fraudulently
- Safe-harbor nations: Rogue nations offer attack groups security and effective immunity from international criminal proceedings and allow them to develop specializations. Some hacking groups have HR departments.
- Nation-state involvement: Rogue nations encourage attackers to explore effects of critical infrastructure and supply chain attacks.
- Increased sophistication of attacks: increased rewards drive innovative hacking techniques

Cyber Threats Dramatically Increasing

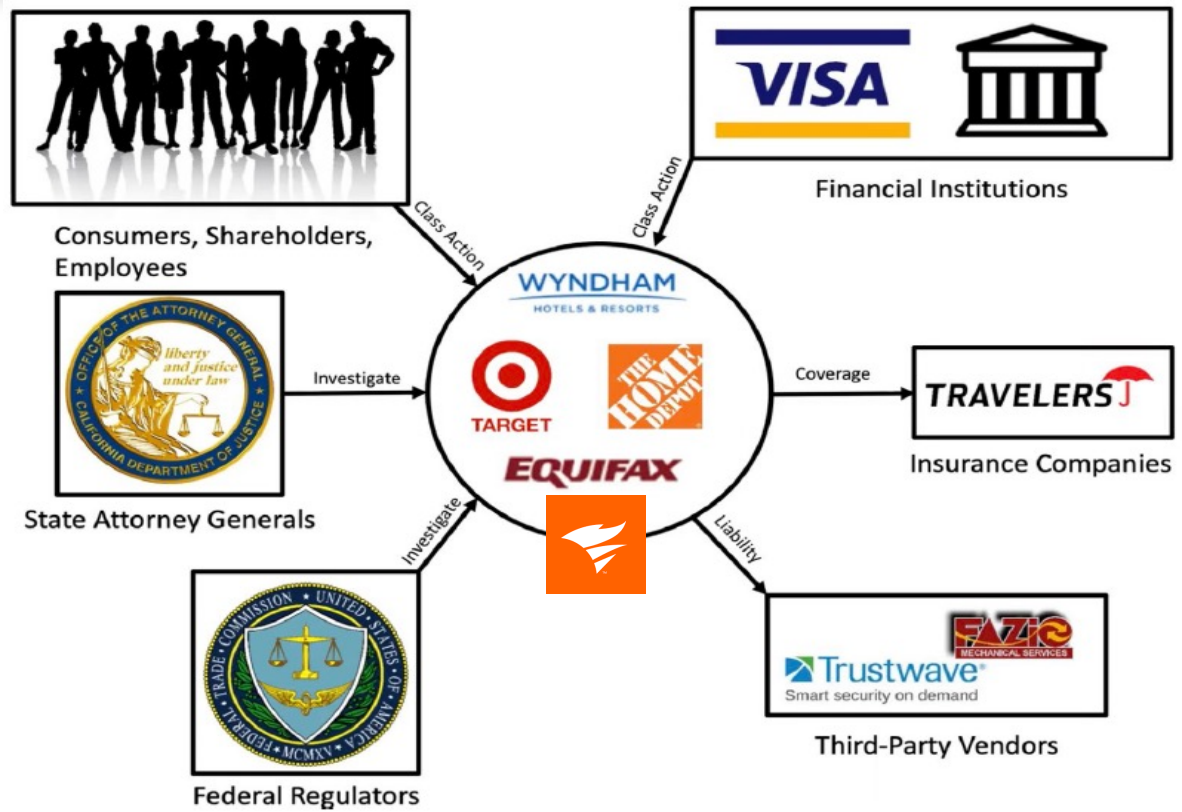
- In 2022, the FBI received 800,944 cyber-incident complaints
- $26 billion in losses reported to the FBI between 2016 and 2019 from business email compromise, a/k/a “Phishing.”





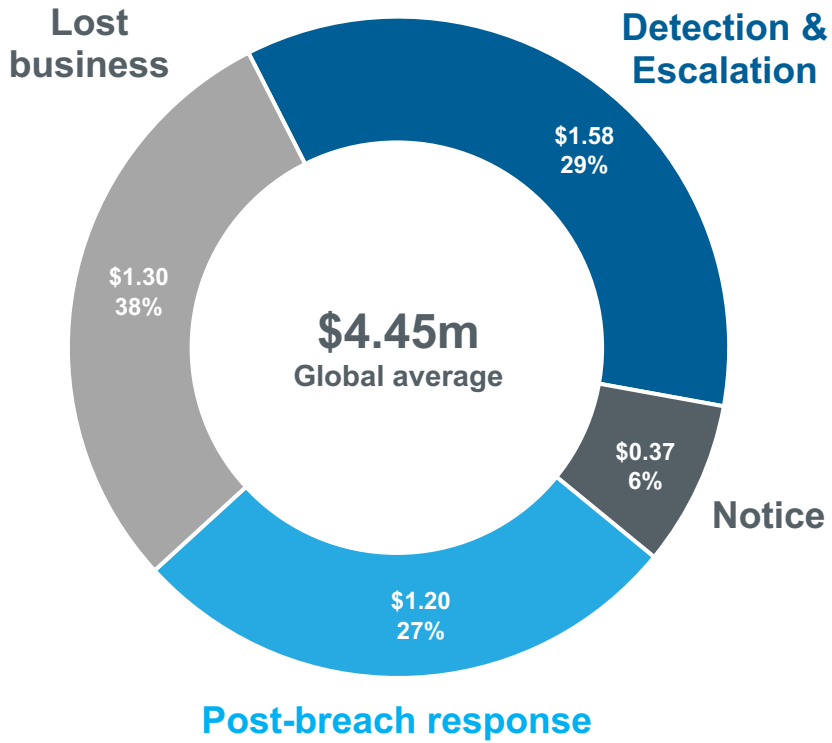
Sometimes Complex and Slow: Anatomy of APT

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



AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- **Cybersecurity Duties of Directors**
- Existing SEC Expectations
- New SEC Rules
- Significant Litigation
- Cybersecurity Governance Best Practices

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

In re Caremark International Inc., 698 A.2d 959 (Del. Ch. 1996)

- Shareholder derivative suit, alleging directors breached their duty of care by failing to adequately oversee employee conduct.
- Employees were allegedly making payments to doctors that exposed Caremark to penalties.
- The Court said boards should: exercise a **good faith judgment** that the corporation's information and reporting system is adequate to assure the board that appropriate information will come to its attention in a timely manner, so the board may satisfy its responsibility.
- This case set the standard for board **liability for inaction** as well as action (referred to as the *Caremark* standard).
- The court ultimately found that the Caremark board properly executed their duties because they had some system for monitoring compliance.

CAREMARK

*"[O]nly a **sustained or systemic failure** of the board to exercise oversight such as an **utter failure to attempt to assure a reasonable information and reporting system** exists will establish the lack of good faith that is a necessary condition to liability."*

Marchand v. Barnhill, No. 533, 2018 (Del. Sup. Ct. 2019)

- Shareholder derivative suit alleged board oversight led to listeria outbreak that sickened consumers, caused three deaths, and resulted in recall of Blue Bell ice cream.
- The Delaware Supreme Court held that the board failed to provide adequate oversight of a key risk area
and thus breached its duty of loyalty.
- The oversight occurred because the board "failed to implement any system to monitor Blue Bell's food safety performance or compliance."

Execution of Corporate Director Duties

Directors need not be omniscient; they may rely on information, opinions, reports, or statements prepared or presented by:

- **Officers or employees** whom the director reasonably believes to be reliable and competent
- **Lawyers, accountants, or other experts** as to matters the director reasonably believes are within the person's professional or expert competence, and
- **Committees of directors**
  - Boards may create one or more standing or ad hoc committees and appoint members to serve on them
  - Committees exercise powers of the board
  - Common committees include audit, compensation, nominating, and increasingly cybersecurity

AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- Cybersecurity Duties of Directors
- **Existing SEC Expectations**
- New SEC Rules
- Significant Litigation
- Cybersecurity Governance Best Practices

Historic SEC Cybersecurity Requirements

SEC expects companies to disclose all material risks, including cybersecurity

- Neither the SEC Act of 1934 nor Regulation S-K currently have an explicit requirement to disclose cybersecurity risks in their 10-Ks or other SEC filings.
- **Initial Guidance:** In October 2011, the SEC's Division of Corporation Finance issued *CF Disclosure Guidance: Topic No. 2, Cybersecurity*. This nonbinding guidance encourages companies to disclose "material information regarding cybersecurity risks and cyber incidents … when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."
- **Further Guidance:** In February 2018, the SEC adopted interpretive guidance that reinforced and expanded upon the 2011 Guidance ("2018 Guidance"), shortly before issuing its first enforcement action related to cybersecurity disclosures.
- Increasingly standard for companies to file an 8-K to notify investors soon after a data breach occurs.
- Directors are liable for violations of anti-fraud and disclosure requirements of federal securities law

"SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information"
SEC Commissioner Luis Aguilar, March 2014

SEC 2018 Guidance on Disclosures

Requirements:

- All public companies must consider the materiality of cybersecurity risks and incidents when preparing the disclosures, including:
- Concise list of most significant factors that make the offering speculative or risky.
- How the risk affects the issuer.
- Disclosure of past or current incidents.
- Disclosure without revealing vulnerability
- "[i]f cybersecurity incidents or risks materially affect a company's products, services, relationships with customers and suppliers, or competitive conditions, the company must provide appropriate disclosure"

  "unusual or infrequent events or transactions or significant economic changes that materially affected the amount of reported income from continuous operations" 17 CFR 229.303

- The occurrence of prior cybersecurity incidents, including their severity and frequency;
- The probability of the occurrence and potential magnitude of cybersecurity incidents;
- The adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- The aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;
- The costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- The potential for reputational harm;
- Existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.[10]

SEC Disclosure Example

- Filed 8-K promptly after suffering a breach from April-Sept. 2014
- Balanced need to provide information with not over-disclosing

Home Depot
Form 8-K
September 8, 2014

THE HOME DEPOT

On September 8, 2014, The Home Depot®, the world's largest home improvement retailer, confirmed that its payment data systems have been breached, which could potentially impact customers using payment cards at its U.S. and Canadian stores. There is no evidence that the breach has impacted stores in Mexico or customers who shopped online at HomeDepot.com.

While the Company continues to determine the full scope, scale and impact of the breach, there is no evidence that debit PIN numbers were compromised.

Home Depot's investigation is focused on April forward, and the Company has taken aggressive steps to address the malware and protect customer data. The Home Depot is offering free identity protection services, including credit monitoring, to any customer who used a payment card at a Home Depot store in 2014, from April on.

AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- Cybersecurity Duties of Directors
- Existing SEC Expectations
- **New SEC Rules**
- Significant Litigation
- Cybersecurity Governance Best Practices

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

New SEC Cybersecurity Requirements

- Form 20-F for private issuers (“FPIs”) will require cybersecurity disclosures in their annual reports filed on that form consistent with the disclosures in the domestic forms
- Form 6-K will add “cybersecurity incidents” as a reporting topic; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL)
  - Will facilitate trend analysis and enforcement

Content of Cybersecurity Incident 8-K 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 Cybersecurity Incident 8-K 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 a cyber 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.”

Strategic Cybersecurity Disclosures

- [E]xposure to cybersecurity risks and previous cybersecurity incidents may affect . . . critical components, informing changes in . . . business model, financial condition, financial planning, and allocation of capital.
  - For example, a company with a business model that relies highly on collecting and safeguarding sensitive and personally identifiable information from its customers may consider raising additional capital to invest in enhanced cybersecurity protection, improvements in its information security infrastructure, or employee cybersecurity training.
  - Another company may examine the risks and decide that its business model should be adapted to minimize its collection of sensitive and personally identifiable information in order to reduce its risk exposure."

Cyber Risk Management Disclosures

- In providing disclosures about the process for assessing and managing material cyber risks, a registrant should address, as applicable, the following non-exclusive list of items:
  - Whether and how any such processes have been integrated into the registrant's overall risk management system or processes
  - Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes
  - Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider
- Requirement is pared back from what was featured in the proposing release, which would have also required disclosure about whether the registrant undertook activities to prevent, detect, and minimize the effects of cybersecurity incidents and had established business continuity and recovery plans
- Registrants will still need to consider how they describe their processes to avoid giving bad actors a "road map" to potential vulnerabilities in them or in associated information systems

Management Governance Disclosures

- Disclosures would describe management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies, including:
- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and
  - The expertise of the relevant persons or members;
- Whether the registrant has a designated chief information security officer, or someone in a comparable position,
  - to whom that individual reports within the registrant's organizational chart, and
  - the relevant expertise of any such persons;
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
- Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Board Governance Disclosures

- Disclosures of board's oversight of cyber risk should include:
  - Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
  - Processes by which the board is informed about cybersecurity risks;
  - Frequency of board discussions;
  - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- Cybersecurity Duties of Directors
- Existing SEC Expectations
- New SEC Rules
- **Significant Litigation**
- Cybersecurity Governance Best Practices

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.
- **Pearson plc,** the UK public company education giant, paid $1 million to settle SEC charges that it misled investors about a 2018 cyber intrusion involving the theft of millions of student records. The action was premised on statements in the securities offering documents and reassuring language in the data breach notification letter and related public statements.

THE HOME DEPOT

Officers and Directors Spared Home Depot Data Breach Derivative Lawsuit

Home Depot to Pay Banks $25 Million in Data Breach Settlement

Home Depot settles consumer lawsuit over big 2014 data breach

(Reuters) - Home Depot Inc HD.N agreed to pay at least $19.5 million to compensate U.S. consumers harmed by a 2014 data breach affecting more than 50 million cardholders.

TARGET®

Judge tosses Target shareholder lawsuit on cyber breach

CNN BUSINESS Markets Tech Media Success Video

Target will pay hack victims $10 million

The New York Times

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

Target in $39.4 million settlement with banks over data breach

(Reuters) - Target Corp has agreed to pay $39.4 million to resolve claims by banks and credit unions that said they lost money because of the retailer's late 2013 data breach.

DISMISSED

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

The New York Times

Verizon Will Pay $350 Million Less for Yahoo

U.S. SECURITIES AND EXCHANGE COMMISSION

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

SEC SETTLEMENT

Pearson

SEC Charges Pearson plc for Misleading Investors About Cyber Breach

FOR IMMEDIATE RELEASE
2021-154

Washington D.C., Aug. 16, 2021 — The Securities and Exchange Commission today announced that Pearson plc, a London-based public company that provides educational publishing and other services to schools and universities, agreed to pay $1 million to settle charges that it misled investors about a 2018 cyber intrusion involving the theft of millions of student records, including dates of births and email addresses, and had inadequate disclosure controls and procedures.

SEC SETTLED ORDERS

Cetera™ ADVISOR NETWORKS

CAMBRIDGE

KMS FINANCIAL GROUP
Strategies for business. Strategies for life.

SEC Announces Three Actions Charging Deficient Cybersecurity Procedures

FOR IMMEDIATE RELEASE
2021-169

Washington D.C., Aug. 30, 2021 — The Securities and Exchange Commission today sanctioned eight firms in three actions for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm. The eight firms, which have agreed to settle the charges, are: Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (collectively, the Cetera Entities); Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. (collectively, Cambridge); and KMS Financial Services Inc. (KMS). All were Commission-registered as broker dealers, investment advisory firms, or both.

SEC SETTLEMENT

blackbaud

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

REUTERS®

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

REUTERS®

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

AGENDA

- Executive Summary
- Cybersecurity Risk Landscape
- Cybersecurity Duties of Directors
- Existing SEC Expectations
- New SEC Rules
- Significant Litigation
- **Cybersecurity Governance Best Practices**

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 insurance effective management of cyber risk and real-time coordination in responding to cyber attacks.

Board Actions: Understand cyber risks

- **Revise 10-K**
- **Create system to decide who decides on an 8-K, when and how.**
  - Boards need the technical expertise, support, and resources necessary to evaluate cybersecurity management
  - Consider a separate cybersecurity or enterprise risk committee
- **Hold substantive training sessions on cyber and privacy risks**
  - Consider engaging outside experts to advise
- **Discuss cybersecurity issues at the board meetings**
  - Regular reports from the CISO or other representatives
  - Use standardized metrics to measure progress
  - Document briefings

Board Actions: Cyber security risk assessment

- **Key is to have a cyber risk assessment that will**
  - Identify the company's "crown jewels" and material personal data and operational data
  - Anticipate key threats
  - Map risks to controls
  - Be updated annually
  - Employ security frameworks like NIST or ISO
  - Ideally be tested externally and audited independently
  - Set targets for potential improvement with accountable timelines
  - Budget for realistic personnel, technology, and process oversight