JANUARY 22, 2025

Public Readiness – Are Your Cybersecurity Controls Ready?

MIKE BLANKENSHIP
CO-CHAIR – CAPITAL MARKETS GROUP, HOUSTON MANAGING PARTNER
Houston
(713) 651-2678
mblankenship@winston.com

ERIC SHINABARGER
PARTNER, GLOBAL PRIVACY & DATA SECURITY PRACTICE
Chicago
(312) 558-8823
eshinabarger@winston.com

BRIAN TOGLIA
RISK & INSURANCE ADVISOR
WTW
(713) 625-1033
brian.toglia@wtwco.com

Agenda

1	Going Public: Cybersecurity Disclosures • Form 8-K • Form 10-K
2	Ransomware and Cyber Statistics
3	Real World Cyber Incidents and Impacts on Executive Liability
4	Controls & Insurance Coverage to Defend Against Derivative Suits

WINSTON & STRAWN LLP

Going Public: Cybersecurity Disclosures

Form 8-K Disclosures

- Form 8-K is used to file a "current report" with the SEC whenever a "material" event occurs that stockholders should be aware of.
- Under recently enacted SEC cybersecurity rules, public companies **must** disclose a "**material**" cybersecurity incident within **4 business days** of determining the incident is material.

"CYBERSECURITY INCIDENT"	"MATERIAL"	DETERMINING "MATERIALITY"
• Unauthorized occurrence on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the company's information systems or any information residing therein.	• Substantial likelihood a reasonable shareholder would consider it important to investment decision-making, such as short/long term impacts on operations; financial conditions; reputational harm; competitiveness; relationships; and intellectual property.	• Must make materiality determination "without unreasonable delay" after discovering incident. Unreasonable bases for delays include being unable to determine the full extent of the incident due to its nature or needing to continue the investigation.

- The disclosure must include:
  - Material aspects of the nature, scope, and timing of incident
  - Reasonably likely impact of incident on the company, including its finances and operations
- The disclosure does *not* have to provide details about the incident itself, or steps being taken to remediate.

Form 10-K Disclosures

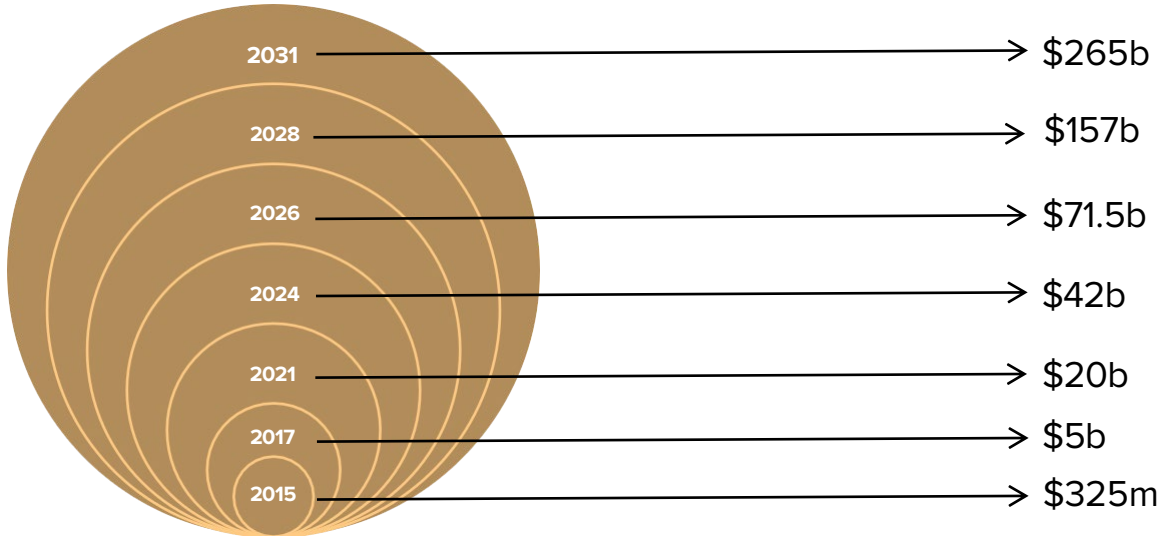
- Form 10-K is a comprehensive annual report filed by publicly traded companies with the SEC that provides a detailed summary of the company's financial performance.
- Under Item 106, public companies must include disclosures in their annual reports regarding cybersecurity issues. Specifically, companies must disclose:
  - **Cybersecurity risk management measures:** Description of process, if any, to assess, identify, manage material risks arising from threat of cybersecurity incidents.
  - **The impact of cybersecurity threats and incidents:** Description of whether any risks from cybersecurity threats/incidents have or are reasonably likely to materially affect the company.
  - **The board's role in oversight of cybersecurity risk:** Description of the board's oversight, identifying process for informing board or any relevant committees / subcommittees of cybersecurity risks.
  - **Management's role in cybersecurity risk management:** Description of management's role in assessing and managing the company's material risks from cybersecurity threats.

WINSTON & STRAWN LLP

Ransomware and Cyber Statistics

The Ransomware Crisis

ESTIMATED AND PROJECTED GLOBAL COSTS



LATEST TRENDS

Q2 23: +126% +20%	• Increase in average ransom payments from 1st quarter of 2023* • Increase in median ransom payments from 1st quarter of 2023*
Q3 23: +15% +5%	• Increase in average ransom payments from 2nd quarter of 2023* • Increase in median ransom payments from 2nd quarter of 2023 *
Q4 23: -33% +0%	• Decrease in average ransom payment from 3rd quarter of 2023* • Increase in median ransom payment from 3rd quarter of 2023*
Q1 24: -32% +25%	• Decrease in average ransom payment from 4th quarter of 2023* • Increase in median ransom payment from 4th quarter of 2023*

OTHER KEY STATISTICS

In 2023, ransomware incidents were once again on the rise with over **2,825 complaints**, which represents an increase of 18% from 2022. *FBI Internet Crime Report 2023*

The number of known ransomware attacks increased **68%** in 2023. *2024 State of Malware by Malwarebytes*

In 2018, ransom payments averaged $5,000, but by 2023 that had **increased by 29,900% to about $1.5m.** *Coveware Global Ransomware Marketplace Report.*

Ransomware affected **66%** of organizations in 2023. *Sophos The State of Ransomware 2023*

$5.13m average cost of a ransomware attack in 2023, an increase of 13% from 2022. *IBM Cost of a Data Breach Report 2023*

Average ransomware payments almost doubled from $812,380 in 2022 to $1,542,333 in 2023 according to independent, survey of 3,000 IT/cybersecurity leaders across 14 countries. *Sophos The State of Ransomware 2023*

Ransomware continues to be a major threat for organizations of all sizes and industries and is present in **24% of breaches** and in more than **62% of all incidents** committed by organized crime actors. *Verizon Data Breach Investigations Report*

March 2023 was the most prolific month recorded for ransomware attacks, measuring **459 attacks**, an increase of **91% from the previous month** and 62% compared to March 2022. *NCC Group*

Current Cyber Risk Threat Landscape: The Statistics

Worldwide cybercrime costs are estimated to grow **15%** per year over the next two years, hitting **$10.5t** annually by 2025

Cybersecurity Ventures

45% of experts say cyber incidents are the most feared cause of business interruption, surpassing natural disasters or energy concerns.

Allianz Risk Barometer 2023

74% of all breaches can be attributed to the human element with people involved via error, privilege misuse, use of stolen credentials or social engineering.

2023 Verizon Data Breach Investigations Report

Malware jumped **11%** from 2022, as SonicWall threat researchers recorded **6.06b** malware attacks. This marks the highest global attack volume for any year since 2019.

Sonic Wall Cyber Threat Report 2024

28,902 Common Vulnerabilities and Exposures (CVEs) published in 2023, up from 25,081 in 2022, which marks the 7th year in a row that a record number of vulnerabilities have been discovered.

Cisco Threat Detection & Response

86% of business leaders and **93%** of cyber leaders believe global geopolitical instability is moderately or very likely to lead to a catastrophic cyber event in the next two years.

World Economic Forum Global Risks Report 2024

Data breach costs reached an all-time high in 2023, with an average cost of **$4.45m**, a 2.3% increase from 2022.

IBM Cost of a Data Breach Report 2023

SonicWall threat researchers observed 15.7m encrypted attacks, the most since this threat metric has been reported.

Sonic Wall Cyber Threat Report 2024

7.6T intrusion attempts in 2023, up 20% from 2022.

Sonic Wall Cyber Threat Report 2024

2024 End-of-Year Report

REVIEW OF CONFIRMED RANSOMWARE ATTACKS

- 1,204 confirmed ransomware attacks.
- Average ransom demand was over $3.5M
- Average ransom paid was $9,532,263
- Total ransom paid was $133.5M
- 195,414,994 records compromised by attacks
- Top 5 biggest data breaches of 2024:
  - US Healthcare Payment & Claim Management Company: 100 million patients affected, $22M ransom paid.
  - US Mortgage Lender: 16.9 million people affected, $27 million in expenses related to attack.
  - Australian Healthcare Technology Company: 12.9 million people affected.
  - Japanese Company: 7.8 million people affected.
  - US Bank: 7.6 million people affected. Hackers stole social security numbers.

CompariTech Ransomware Roundup

Data Breach Litigation

- Breach costs may not stop at the end of the incident
- Class action litigation and enforcement settlements are on the rise
  - Partially thanks to the CCPA's private right of action and statutory damages
- A few examples:
  - $65 million class settlement by a health network for a breach affecting 600 patients and employees
  - $52 million settlement by a hospitality company with 50+ state and federal regulators
  - $30 million class settlement by an ancestry company

WINSTON & STRAWN LLP

Real World Cyber Incidents and Impacts on Executive Liability

How Does a Cyber Event Become a D&O Claim?

- Several high-profile cyber incidents have resulted in shareholder class actions. The following is a real-world example of how a cyber event can lead to a filing of D&O claims:
  - American company became aware of security failing in March 2017.
  - Company did not adequately and promptly remedy the security failure.
  - Company confirmed a breach in July 2017.
  - Company revealed the breach publicly in September 2017.
  - Company's stock dropped over 15% upon announcement.
  - A shareholder complaint was subsequently filed, alleging:
    - The company failed to maintain adequate protective measures and monitoring systems/controls.
    - The company's financial statements, which stated it had such systems in place, were materially false and misleading.

Cyber Losses and Ensuing D&O Impacts

SOME KEY EXAMPLES TO DATE:

Industry	Event	Cyber Impact	D&O Impact
Technology	**Supply chain cyber attack**	**4Q20**: The company was the victim of a cyber-attack on their software platform. Malicious code transmitted to an estimated 18,000 corporate and government customers via firm's proprietary platform, used by a total of 33,000 customers. This attack affected versions of the platform released during a 4 month period.	**4Q22:** The company entered into a binding settlement term sheet for $26 million to resolve a securities class action lawsuit. There are numerous open investigations and inquiries by domestic and foreign law enforcement and other governmental entities including the DOJ and SEC. Subsequently, the company received a "Wells Notice" from the SEC indicating a preliminary determination to proceed with an SEC enforcement action in connection with cybersecurity disclosures and public statements. The company expects to incur significant expenses in responding to the SEC investigation.
Financial Institution	**Data breach**	**2Q19:** Breach occurred in June/July 2019. Impact of over 100 million credit card customer records stored on company servers. Biggest category of information was from credit card applications gathered over a 15-year span. The perpetrator was arrested in connection with the incident – she previously (2015-2016) worked at the Company.	**1Q20**: Firm named in 73 putative consumer class actions, one securities class action, and under investigation by a variety of governmental authorities in US and Canada.
Hospitality	**Data breach**	**4Q19:** 500 million consumer records impacted over a 4-year period. First publicly disclosed by firm late in **November 2018.**	**4Q18**: Securities class action filed against company alleging that the organization failed to protect personal data, resulting in a breach of 500M records. As a result, the company's public statements about their cyber security were alleged to be materially false or misleading.
Transportation / Logistics	**Ransomware**	**2Q17:** Worldwide operations of a subsidiary were significantly affected by NotPetya- Company focused on finalizing the restoration of key customer-specific specialized solutions and systems in time for the peak shipping season	**2Q19:** Securities class action filed, alleging the company continually assured investors about its recovery from the Cyberattack and that any negative impact from the attack was minimal. Specifically, the Complaint alleges Defendants made false and misleading statements and/or failed to disclose the full extent of business disruption and financial damages.

Executive Liability

- Executive liability for cyber attacks is not limited to shareholder lawsuits.
  - In 2022, the Federal Trade Commission held a CEO of an LLC personally liable for presiding over the company's failure to implement and apply appropriate information security practices, which led to a data breach exposing the personal information of 2.5 million customers.
- Executive liability can potentially stem from external data breaches where oversight by executives is insufficient.
  - A 2020 derivative suit filed against the directors and officers of a laboratory services company alleged the executives were personally liable for the effects of third-party vendors' data breaches.
  - A third-party vendor's website portal was breached, leading to the disclosure of credit cards and personally identifiable information belonging to clients of the laboratory services company.
  - The suit alleges the data breach was caused in large part by insufficient cybersecurity procedures and lax oversight over the third-party vendor by board members of the laboratory service company.
  - The suit is ongoing but currently stayed pending resolution of multidistrict litigation.

WINSTON & STRAWN LLP

Controls & Insurance Coverage to Defend Against Derivative Suits

Cybersecurity Requirements

GENERAL REQUIREMENTS

- "Reasonableness" standard
- State cybersecurity laws (e.g., 201 CMR 17.00)
- CCPA Regulations

INDUSTRY SPECIFIC

- HIPAA Security Rule
- Financial services requirements (e.g., 23 NYCRR Part 500, GLBA)
- Government contractors (e.g., CMMC)

INDUSTRY STANDARDS

- PCI-DSS
- NIST CSF
- ISO 27001
- SOC

Alleged Damages in a Typical Derivative Lawsuit

Further, as a direct and proximate result of the Individual Defendants' actions, Company has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

a) Costs incurred from defending and paying any settlement in the numerous consumer class actions filed against the Company;

b) Costs incurred from the Secret Service and DOJ investigations into the data breach, including, but not limited to, liability for any potential fines;

c) Costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense

d) for legal, investigative, and consulting fees;

e) Costs incurred from expenses and capital investments for remediation activities;

f) Costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges;

g) Costs incurred from Company fulfilling its promise to provide free credit monitoring to victims of the data breach;

h) Loss of revenue and profit resulting from Company’s offer of a l0%; discount to U.S. shoppers during the last

i) weekend before Christmas in an effort to lure customers back into its stores, and

j) Costs incurred from compensation and benefits paid to the defendants who have breached their duties to Company.

Insurance Coverage

- Most of these damages can be mitigated by cyber insurance coverage.
- Cyber Insurance (or “Cyber Liability Insurance”) can help cover costs associated with data breaches and cyberattacks, such as:
  - Forensic investigations
  - Crisis management expenses
  - Business interruption losses
  - Regulatory defense expenses and fines
  - Legal fees in lawsuits related to cyber attacks
  - Data recovery expenses
  - Consumer notification expenses
  - Cyber extortion payments
- Cyber insurance also mitigates risk by incentivizing stronger security.
  - Agencies often encourage (through lower premiums) or require the adoption of best practices for cybersecurity before insuring a company.
  - Some policies also provide companies with compliance support.

Controls to Implement to Mitigate Cybersecurity-Based Derivative Suits

DEVELOP AND TEST AN INCIDENT RESPONSE PLAN

Create a business-wide incident response plan that includes legal considerations and means for assessing severity.

REGULAR RISK AND THREAT ASSESSMENTS

Conduct frequent cybersecurity risk assessments to identify vulnerabilities. Scrutinize third-party vendor practices.

UTILIZE DETAILED RECORD-KEEPING PROTOCOL

Develop and implement a detailed record-retention protocol related to cybersecurity management.

CREATE A CYBER-SAFETY CULTURE

Foster a culture where cybersecurity is everyone's responsibility, not just IT. Offer top-down cybersecurity trainings.

ESTABLISH CLEAR REPORTING LINES

Create protocols outlining how cybersecurity threats should be reported up the company and to the board.

INCLUDE CYBERSECURITY EXPERTS ON THE BOARD

Bring in board members with expertise who can provide valuable insights into emerging threats and best practices.

PROVIDE SUFFICIENT RESOURCES TO CISO

Make appropriate resources available to the Chief Information Security Officer, including continued education.

PROMOTE A STRONG CISO + LEGAL COUNSEL CULTURE

Build a framework for counsel and the Chief Information Security Officer to work together to make informed decisions.

KEEP UP WITH LEGAL & REGULATORY OBLIGATIONS

Stay apprised of evolving cybersecurity laws and regulations and establish procedures and policies for compliance.

Controls to Implement to Mitigate Cybersecurity-Based Derivative Suits

- Delegate cybersecurity and data privacy oversight to a board committee.
  - Review the committee's charter to consider specific cybersecurity language.
- Establish reporting systems to ensure directors receive reports from management about internal and external cybersecurity events.
  - The reports should occur at whatever intervals make sense for the particular company.
- Coordinate with management and advisers regarding compliance with new cybersecurity disclosures and regulations.
- Document the Board's efforts and processes in sufficient detail to demonstrate the Board's:
  - Oversight and understanding of risk and compliance systems
  - Active response to cybersecurity issues once they arise

First Steps in Responding to an Incident

PRACTICE, PRACTICE, PRACTICE	Responding to an attack should not be the first time that your various teams (technical, legal, communications, executive, BOD, etc.) use your incident response plan and procedures.
MOBILIZE SUPPORT	Talk to your cyber insurance broker to begin the process of retaining external vendors (legal, forensic, crisis communication)
DETERMINE THE SCOPE AND MITIGATE DAMAGE	Understand the extent of the damage and potential compromise and determine what workarounds are required (e.g., alternative secured communication channels, severing data flows to specific customers or vendors, taking systems offline to prevent spread)
IDENTIFY REPORTING OBLIGATIONS	While most notification will occur only after an investigation, identify any immediate reporting requirements (e.g., to cyber carrier, regulatory requirements, contractual obligations)


wtw
WINSTON
& STRAWN
LLP