Friday, November 4, 2022

Full Disclosure: C-Suite and Board Perspectives on the SEC's Proposed Cyber Disclosure Rules

Jerry Archer
Chief Security Officer, Sallie Mae Bank

Jess Kosseff
Associate Professor of Cybersecurity Law, U.S. Naval Academy

Tony Kim
Partner, Latham & Watkins LLP

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Jerry Archer

Chief Security Officer
Sallie Mae Bank

Jeff Kosseff

Associate Professor of Cybersecurity Law
United States Naval Academy

Tony Kim

Partner
Latham & Watkins LLP

Escalating Cyber Regulation (the SEC is only one example)

Privacy+ Security Forum

SEC Proposed Rules: Public Companies

Privacy+ Security Forum

- **March 9, 2022:** Commission proposed rules and amendments (public comment period recently re-opened); new rules likely to become effective in early/mid 2023
  - Disclosure of **Policies & Procedures** for identifying and managing cyber risks/threats, such as risk assessments, retained auditors, third-party vendor management, business continuity, etc.
  - Disclosure of **Board's** cyber oversight structure (including cyber "expert"), process, frequency, and how cyber risk is part of "business strategy, risk management and financial oversight"
  - Disclosure of **Management's** cyber roles (including credentials) responsible for cyber (e.g., do you have a CISO) and how the role assesses/monitors cyber risk and implement policies, procedures and strategies, and how/how frequently roles update the Board
  - Disclosure of **incidents** on Form 8-K within four days of **"materiality"** determination (and, in 10-Q/K, any "previously undisclosed individually immaterial incidents that become material in the aggregate")

Key Features of Proposed Rules

Changes to require current reporting about material cybersecurity incidents + updates to previously reported incidents in periodic reports

Changes to periodic disclosures regarding: policies, procedures, management's cyber implementation role, Board's oversight and cyber expertise

Requires cybersecurity disclosures to be made via Inline XBRL

Proposed Ongoing Disclosures

Privacy+ Security Forum

Risk Management and Strategy

Item 106(b)

- Policies and procedures for identifying and managing cyber risks and threats – including operational risk, IP theft, fraud, extortion, harm to employees/customers, violation of privacy laws and other litigation and legal risk, reputational risk, for example, as applicable, "**a discussion of <u>whether</u>**":

1. Co. has a cybersecurity risk assessment program (and provide a description)
2. Co. engages assessors, consultants, auditors or other third parties in connection with assessment program
3. Co. has policies and procedures to identify/manage third-party service provider risks (and describe how cyber affects selection and oversight of third parties, and contractual/other mechanisms to reduce risk)
4. Co. undertakes to prevent, detect, and minimize cyber incidents (and if so, describe types of activities)
5. Co. has business continuity, contingency, recovery plans to respond to cyber incidents
6. Previous cyber incidents "informed changes in . . . governance, policies, procedures or technologies"
7. Cyber-related risks and previous incidents "have affected or are reasonably likely to affect" strategy, business model, results or financial condition (and if so, how)
8. Cyber-related risks are considered in business strategy, financial planning, and capital allocation (and if so, how)

Proposed Ongoing Disclosures

Privacy+ Security Forum

Governance

Item 106(c)

- **Board of Directors** oversight of cybersecurity risk:
  i. Structure of oversight on cyber risks (i.e., entire board, specific members or board committee is responsible)
  ii. Processes by which Board is informed about cyber risk
  iii. Frequency of Board's discussions about cyber risk
  iv. How Board considers cyber risk as part of its "business strategy, risk management and financial oversight"
- **Management's role** in (a) assessing and managing cyber risk and (b) implementing policies, procedures, strategies, e.g.:
  i. Whether certain management positions or committees are responsible for measuring/managing cyber risks (e.g., prevention, mitigation, detection, remediation of incidents) + describe relevant expertise of persons (e.g., previous work experience, degrees, certifications, knowledge, skill, other cyber background)
  ii. Whether there is a designated CISO or someone in comparable position + describe relevant expertise of person + reporting lines in corporate org chart
  iii. Processes by which mgmt. persons or committees are informed about and monitor prevention, mitigation, detection and remediation of cyber incidents; and
  iv. Whether and how frequently mgmt. persons or committees report to the Board on cyber risks

Proposed Ongoing Disclosures

Privacy+ Security Forum

Cybersecurity Expertise

Item 407(j)

- **If** any board member has expertise in cybersecurity:
  i. Disclose name of director
  ii. Provide detail necessary to fully describe nature of expertise, including, among other things:
    - Prior work experience (e.g., CISO, security policy analyst/auditor/architect/engineer/ operations manager, incident response manager, business continuity planner)
    - Cybersecurity certification or degree
    - Knowledge, skills, or other background, for example, in security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, business continuity planning
- Safe harbor applies such that Board member identified or designated as having cyber expertise . . .
  i. will NOT be deemed an expert for any other purpose under securities laws
  ii. will NOT have any duties or liability exposure that are greater than otherwise would be imposed
  iii. does NOT affect any duties or liability exposure of other directors on the board

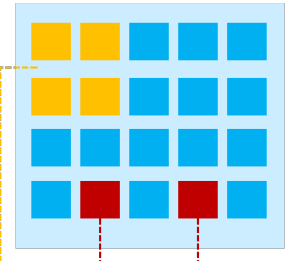
Disclosure of "material" incidents

Privacy+ Security Forum

= Adjust Existing Incident Response (IR) Plan

= Incorporate . . . Based on SEC [Proposed] [Final] Rules

1 Incidents

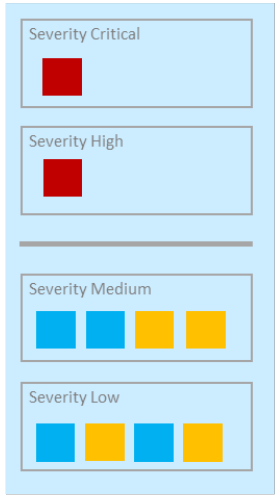


"Cybersecurity Incident": *"unauthorized occurrence on or conducted through" information systems that "jeopardizes confidentiality, integrity or availability" of* ***(a) "information systems"**** *or* ***(b) information therein***

". . . series of previously undisclosed ***individually immaterial*** *cybersecurity incidents . . . "*

* ***Information systems*** = information resources, owned **or used by** registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of registrant's information to maintain or support the registrant's operations

2 Assessment



3 Escalation

Typical escalation points:
- General counsel
- Senior leadership/Board

Add escalation points:
- SEC/Disclosures Counsel
- Disclosure Committee
- Outside Auditor

4 "Materiality" Determination

Standard: *". . . substantial likelihood that a reasonable shareholder would consider it important"* to making an investment decision. SEC's non-exhaustive list of potentially material incidents:

- Unauthorized (accidental or deliberate) incident compromise confidentiality, integrity, or availability of an information asset (data, system, or network); or violates security policies or procedures.
- Unauthorized incident causes degradation, interruption, loss of control, damage to, or loss of operational technology systems;
- Unauthorized party accessed, or party exceeded authorized access, and altered, or stole sensitive business info, personally identifiable info, IP/trade secrets, or info that resulted, or may result, in a loss or liability;
- Malicious actor has offered to sell or has threatened to publicly disclose sensitive company data;
- Malicious actor has demanded payment to restore company data that was stolen or altered

5 Form 8-K

Item 1.05

Disclose the following information *"to the extent known…at the time of filing"*

1. When the incident was discovered and whether it is still ongoing;
2. Brief description of nature and scope of the incident;
3. Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
4. The effect of the incident on operations; and
5. Whether the company has remediated or is currently remediating the incident.

NOTE: SEC filings are in addition to any other statutory, regulatory or contractual notification duties

6 Update Q / K

Item 106(d)

(1) Post-8-K, disclose *"any material changes, additions, or updates regarding such incident"* in 10-Q or 10-K for period in which change, addition, or update occurred. Description should include "but not be limited to":

i. Any material effect on operations/financial conditions
ii. Any potential material future impacts on operations and financial condition
iii. Whether issue remediated or currently remediating
iv. Any changes in policies and procedures, and "how" incident informed changes

7

(2) Disclose ". . . to the extent known to management when *a series of previously undisclosed individually immaterial incidents has become material in the aggregate*" (disclosure content requirements mirror Form 8-K)

TIMELINE

*"**as soon as reasonably practicable after discovery** of the incident"*

*Form 8-K filed "**within four [4] business days** after the registrant determines that it has experienced a **material** cybersecurity incident"*

Our (Unscientific) "Survey Says . . ."

Privacy+ Security Forum

Our (Unscientific) Survey

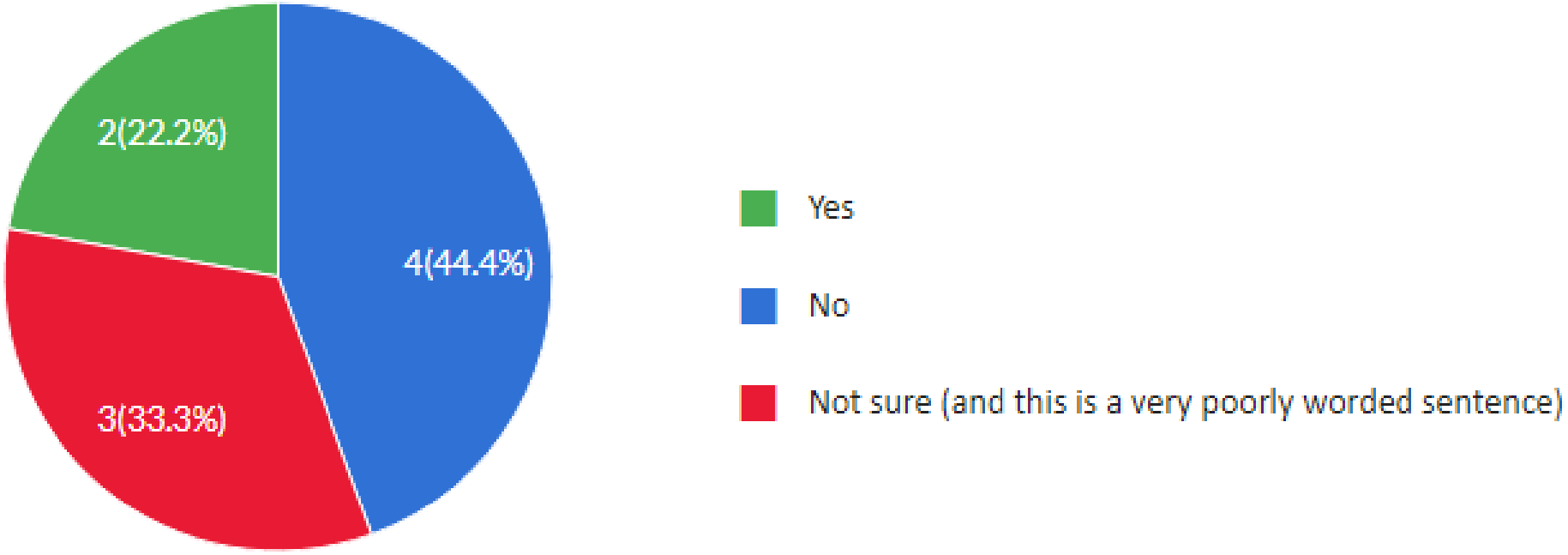
Privacy+ Security Forum

- Nine C-Suite and/or Board members participated in our highly un-scientific (but very anonymous) survey about cybersecurity
- Industries spanned healthcare, defense, insurance, e-commerce, technology and manufacturing
- None of the participants enjoyed the survey, but all were “good sports”

Our (Unscientific) Survey

Privacy+ Security Forum

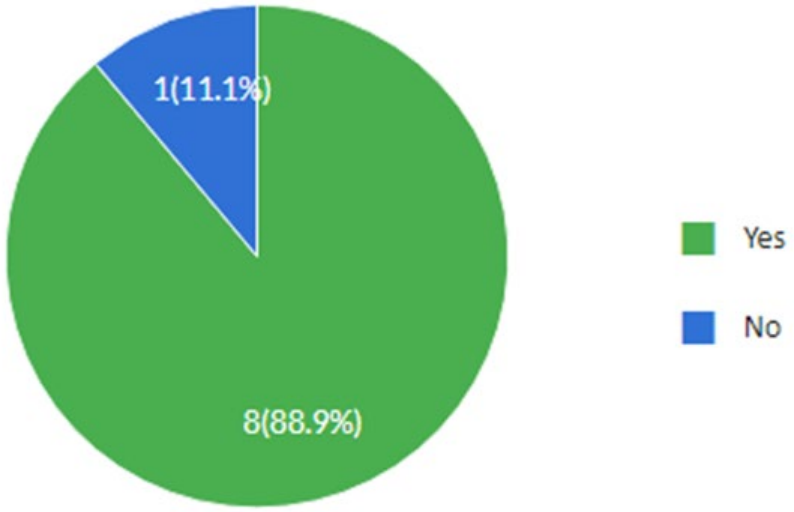
Do you believe that the SEC's proposed cybersecurity rules mark a significant shift in disclosure practice around cybersecurity issues?



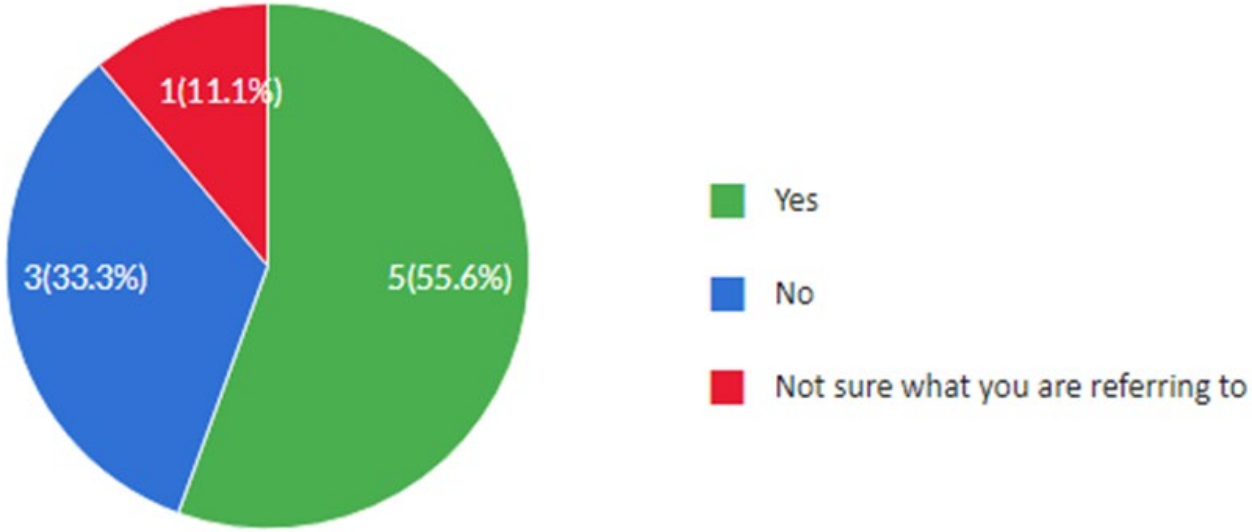
Our (Unscientific) Survey

Privacy+ Security Forum

Have you reviewed your company's cybersecurity incident response plan during the past fiscal year?



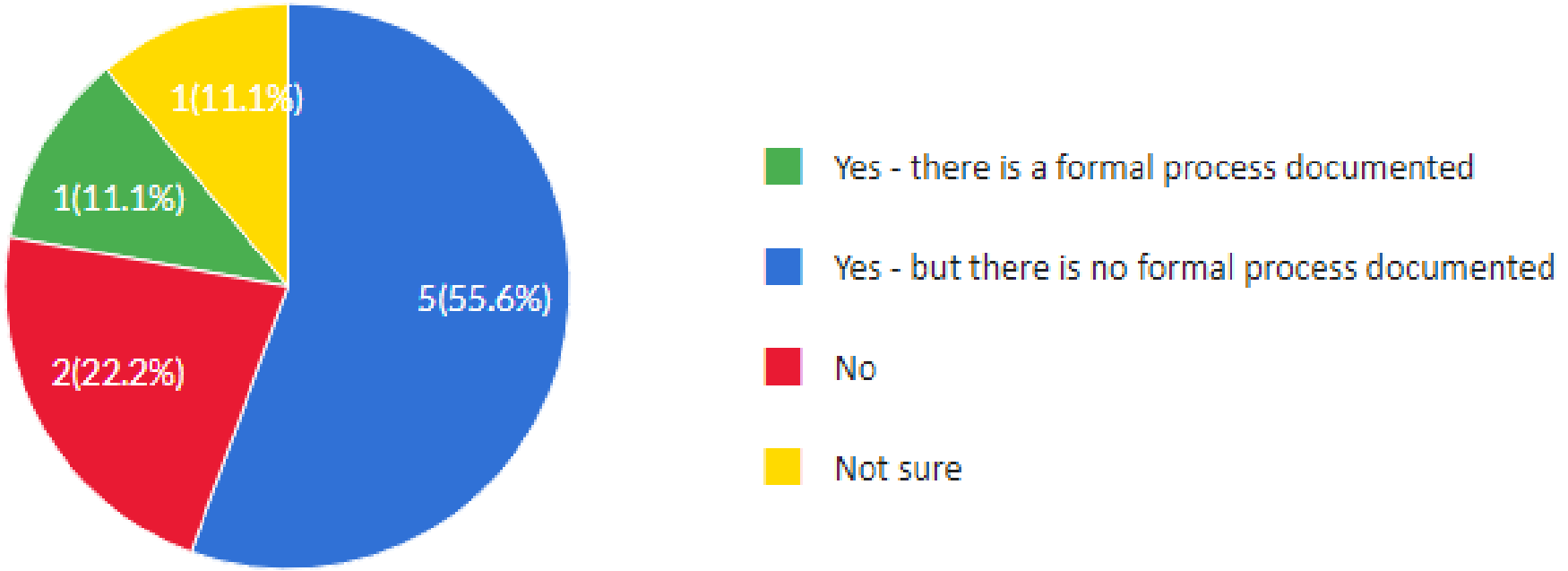
Are you familiar with your cybersecurity incident response plan's "severity" or "escalation" matrix?



Our (Unscientific) Survey

Privacy+ Security Forum

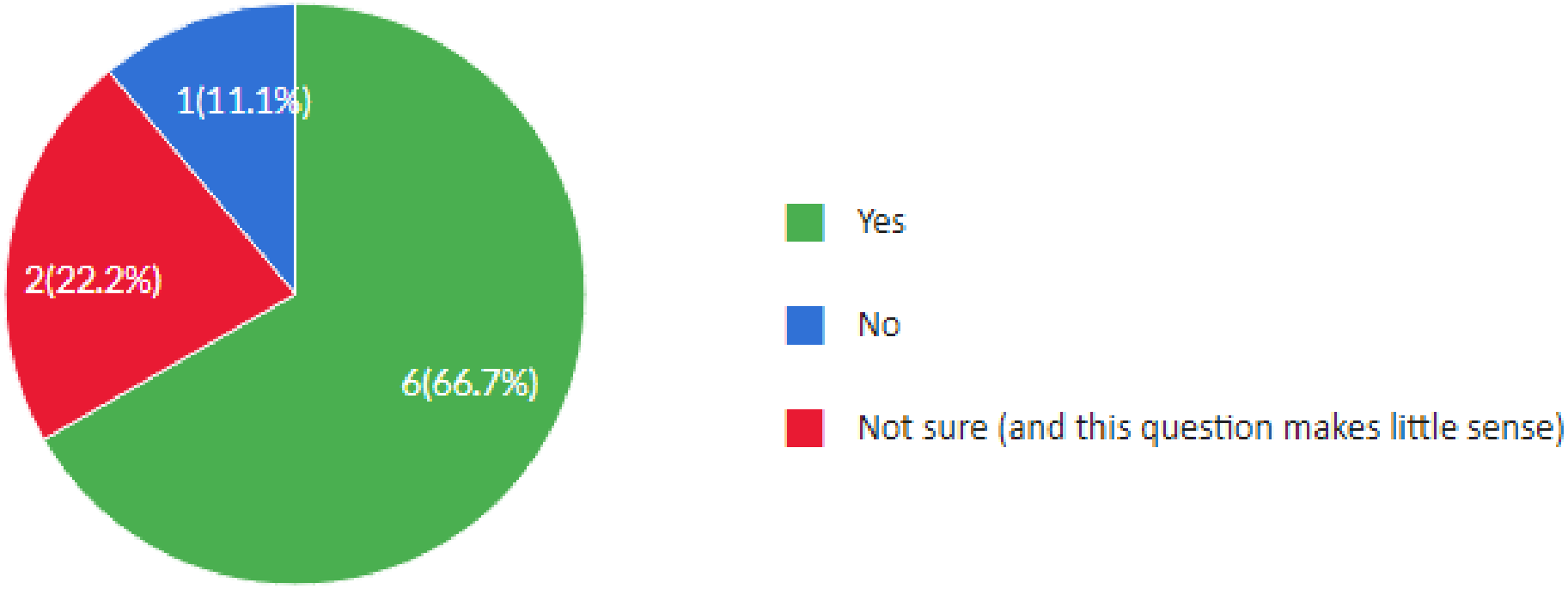
Does your cybersecurity incident response process provide for an analysis of "materiality" for SEC disclosure purposes?



Our (Unscientific) Survey

Privacy+ Security Forum

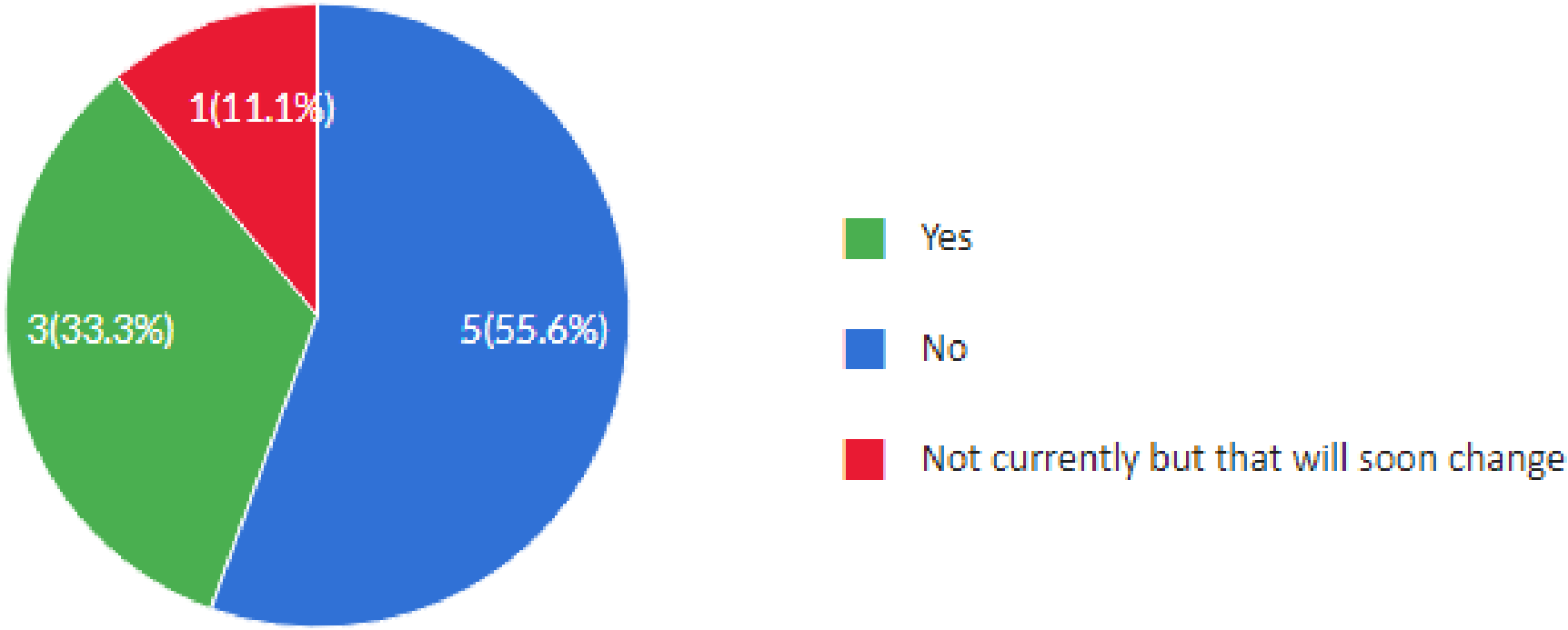
Do you know "how cybersecurity risks are considered as part of your company's business strategy, financial planning and capital allocation"?



Our (Unscientific) Survey

Privacy+ Security Forum

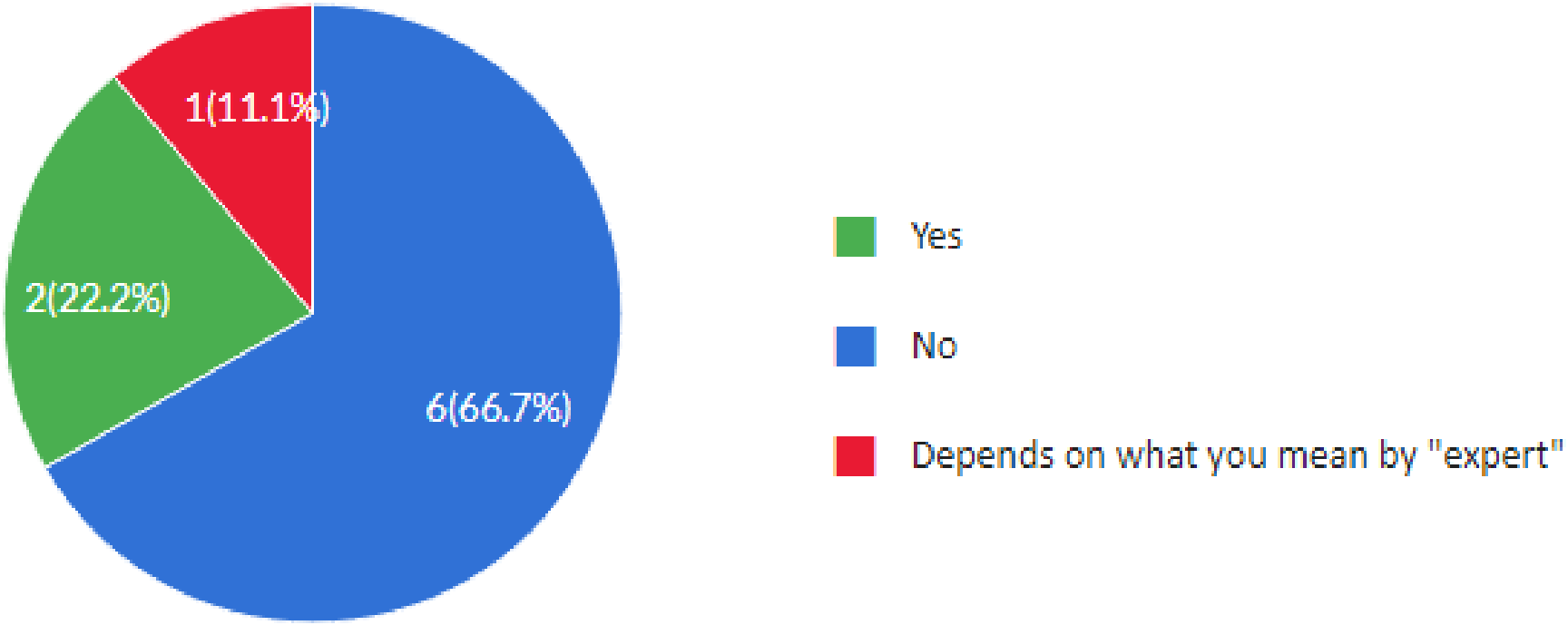
Does your CISO (or equivalent role) report directly to the Board or a Board Committee?



Our (Unscientific) Survey

Privacy+ Security Forum

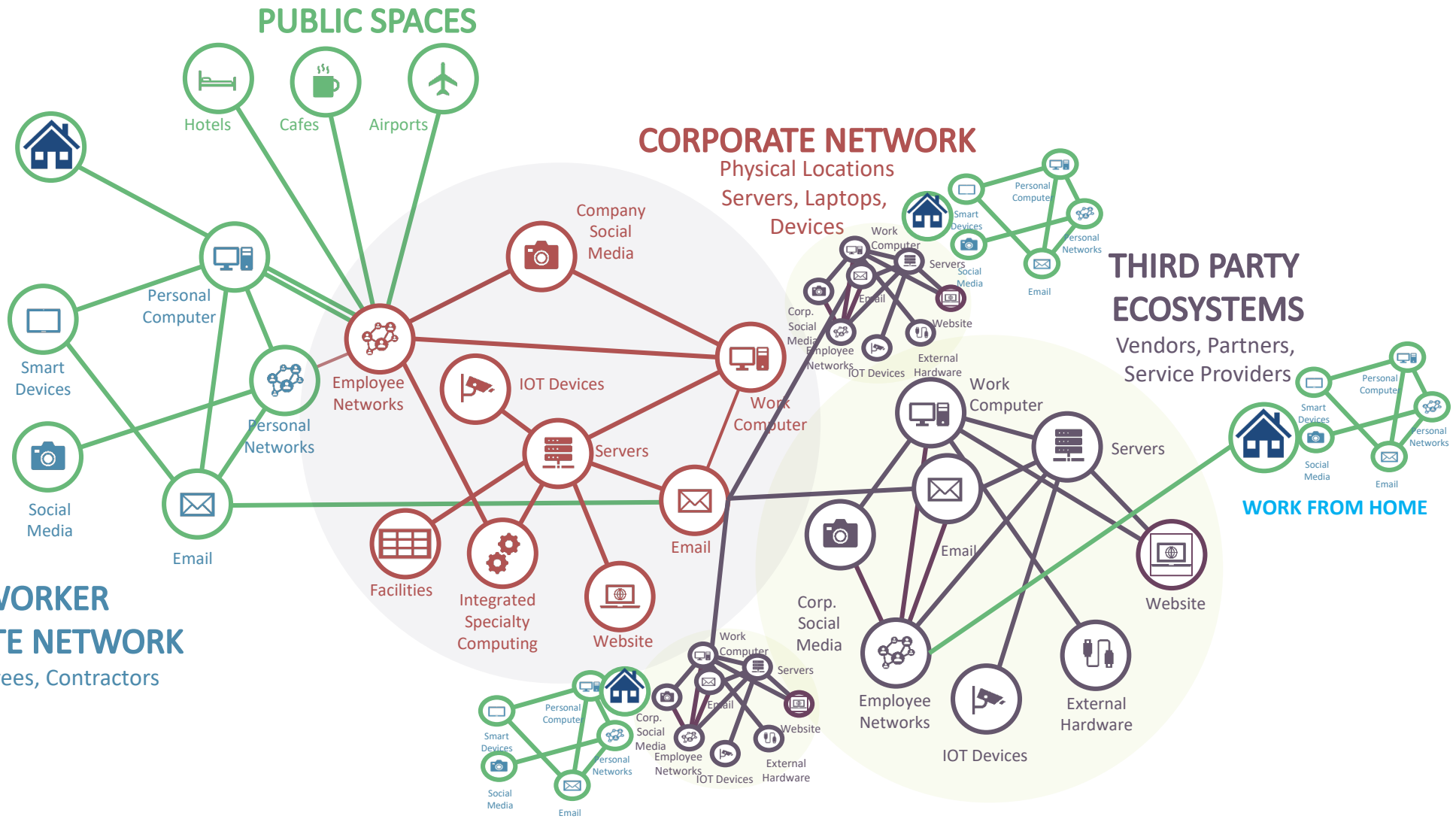
Do you have a cybersecurity expert on your Board?



Scoping the Problem

Modern attack surface

Privacy+ Security Forum



The Covid-19 effect

Privacy+ Security Forum

- FBI reports 400% spike in online crime reports
- COVID-19 blamed for 238% surge in cyberattacks against financial institutions
- Russian cybercriminal group targeting American remote workers at home
- Pharma, research firms warned of cyberattacks linked to COVID-19

Home Wi-Fi network (security?)

3.5x *more likely than corporate networks to have at least one family of malware*

7.5x *more likely than corporate networks to have at least five families of malware*

>25% *home wi-fi routers have one or more services exposed to the internet*

1 in 7 *home IP addresses have exposed web admin interfaces for cable modem, router, camera, storage*

Source: Bitsight

Increased reliance on third parties

63% *of data breaches directly or indirectly caused by third parties*

59% *of respondents reported at least one third party breach*

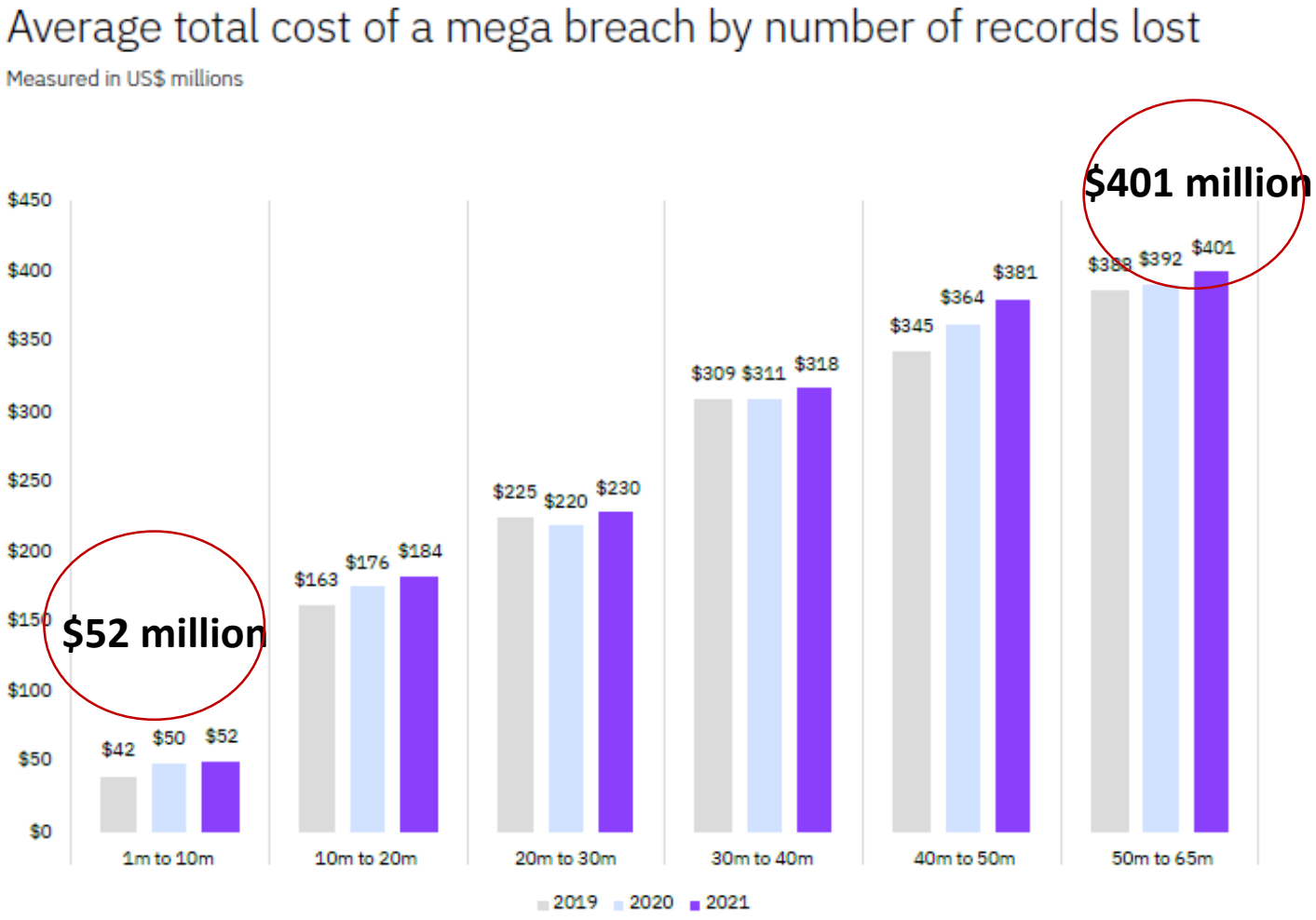
75% *of respondents believe third party breaches are increasing*

65% *of respondents not confident third party vendor would notify them of a breach*

Source: Soha Systems; IBM/Ponemon Cost of Breach Study

Breaches more expensive than ever

Privacy+ Security Forum



Source: Figure 33, 2021 Cost of Data Breach (IBM Security)

For breaches where 50-65 million records were impacted . . . **the average cost to the company was $401 million**

- Share prices of breached companies hit a low point ~14 days post-disclosure
  - Prices fell -7.27% on average
  - *Underperformed* NASDAQ by -4.18%
- After 1 year, shares of breached companies +8.38% on average, but *underperform* NASDAQ by -6.49%
- After 2 years, shares of breach companies +32.53% on average, but *underperform* NASDAQ by -13.27%

Source: S. Bischoff, Comparitech, How data breaches affects stock market share prices *available at* https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis (April 20, 2020)

Escalating Cyber Enforcement (the SEC is only one example)

Privacy+ Security Forum

SEC in 2021 was on fire

Privacy+ Security Forum

First American

mortgage title and settlement company

On June 17, 2021, SEC settled administrative charges, secured a $487,616 penalty, and entered a Cease-and-Desist Order.

On May 24, 2019, a cyber researcher reported a security *vulnerability* (not a data breach) in the Company's document sharing application that was exposing over 800 million images dating back to 2003 that contained sensitive customer PI (e.g., SSNs, tax records, mortgage/tax records, wire transaction receipts, drivers license images). Company issued a press release on May 24, 2019:

> First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information. The company took immediate action to address the situation and shut down external access to the application.

On May 28, 2019, the Company filed a Form 8-K with an additional press release stating "[n]o preliminary indication of large-scale unauthorized access to customer information" and the following:

> First American Financial Corporation advises that it shuts down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data.

SEC charged First American with cybersecurity disclosure controls/procedures failures:

- SEC: The vulnerability had existed since 2014, but it was not discovered by InfoSec personnel until January 2019 – at which time it was documented in an internal report. However, the vulnerability's *severity level was internally miscoded* and thus, not remediated or escalated to the CISO/CIO (both of whom learned of it in May 24-25 after the cyber researcher's outreach).
- SEC: "*First American's* ***senior executives responsible for these public statements were not apprised of certain information*** *that was relevant to their assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk*" including that "*the company's* ***information security personnel had identified the vulnerability several months earlier****, but had* ***failed to remediate it*** *in accordance with the company's policies.*"
- SEC: *"As a result of First American's deficient disclosure controls, senior management was completely unaware of this vulnerability and the company's failure to remediate it . . .* ***Issuers must ensure that information important to investors is reported up the corporate ladder*** *to those responsible for disclosures."*

https://www.sec.gov/litigation/admin/2021/34-92176.pdf

SEC in 2021 was on fire (cont'd)

Privacy+ Security Forum

Pearson
global educational publisher

On August 16, 2021, SEC settled charges, secured a $1 million penalty and entered a Cease-and-Desist Order.

On July 31, 2019, a reporter contacted Pearson, a global educational learning publisher and service company, regarding an impending article describing a ***non-public*** data breach that the Company had *internally* identified four months earlier on March 21, 2019.

A threat actor had hacked AIMSweb 1.0 software used by Pearson to track student academic performance and downloaded (a) 11.5 million rows of student names plus DOBs/emails for a subset of students, and (b) usernames and passwords (hashed with an insecure algorithm) for about 13,000 school administrator accounts. A security patch for AIMSweb 1.0 had been publicized and made available in September 2018, but Pearson failed to implement it until after it learned of the attack.

Senior management met at least twice prior to July 31, 2019 – and both times determined that it was *not* necessary to issue any public statement about the breach. Pearson posted an online Media Statement only *after* being contacted by the reporter on July 31.

SEC charged Pearson with misleading investors about the data breach and inadequate disclosure controls and procedures:

Disclosures in Form 6-K filed on July 26, 2019	SEC Enforcement Findings
Pearson stated that a *"[r]isk of a data privacy incident . . . including a failure to prevent or detect a malicious attack on our systems, could result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss . . ."*	SEC: Pearson "***implied*** that no 'major data privacy or confidentiality breach' had occurred" and portrayed data breaches as a "***hypothetical risk***" but, in fact, by the time the July 26 Form 6-K was filed, Pearson had already known "***months earlier*** about the AIMSweb 1.0 breach."
Statements in Media Statement posted on July 31, 2019	**SEC Enforcement Findings**
Pearson stated that the incident involved "*unauthorized access*" and "*expos[ure] of data*"	SEC: Pearson knew that the threat actor had "***removed***" data "rather than ***just having obtained access*** to view the data"; and ***omitted*** that millions of rows of student data were stolen
Pearson stated that the impacted data was "*isolated to first name, last name, and in some instances may include date of birth and/or email address . . .*"	SEC: Pearson knew that ***impacted data also included*** "usernames and hashed passwords of school personnel were also ex-filtrated"
Pearson stated that the scope of impacted data "*. . . may include date of birth and/or email address . . .*"	SEC: Pearson suggested that the impact to DOBs/emails was "***hypothetical***" by using the word "***may***" but "***[i]n fact, Pearson knew*** that" DOBs and emails were stolen
Pearson stated that it had "*strict data protections in place and have reviewed this incident, found and fixed the vulnerability . . .*"	SEC: Pearson misstated its security protections because it (a) ***failed to patch*** a publicly-known vulnerability for six months and (b) ***used an outdated/insecure hashing algorithm***

https://www.sec.gov/litigation/admin/2021/33-10963.pdf

SEC in 2021 was on fire (cont'd)

Privacy+ Security Forum

U.S. SECURITIES AND EXCHANGE COMMISSION

In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs

The staff of the U.S. Securities and Exchange Commission is conducting an investigation regarding a cyberattack involving the compromise of software made by the SolarWinds Corp., which was widely publicized in December 2020 ("SolarWinds Compromise"). As part of this investigation, the staff issued a letter requesting that certain entities provide information to the staff on a voluntary basis (hereinafter, "Letter"). Below are FAQs the staff expects to be helpful to Letter recipients. The FAQs may be updated periodically, and the most recently updated version will be posted on the Division of Enforcement page of www.sec.gov.

SEC gearing up in 2022 . . .

Privacy+ Security Forum

U.S. SECURITIES AND EXCHANGE COMMISSION

Press Release

SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit

FOR IMMEDIATE RELEASE
2022-78

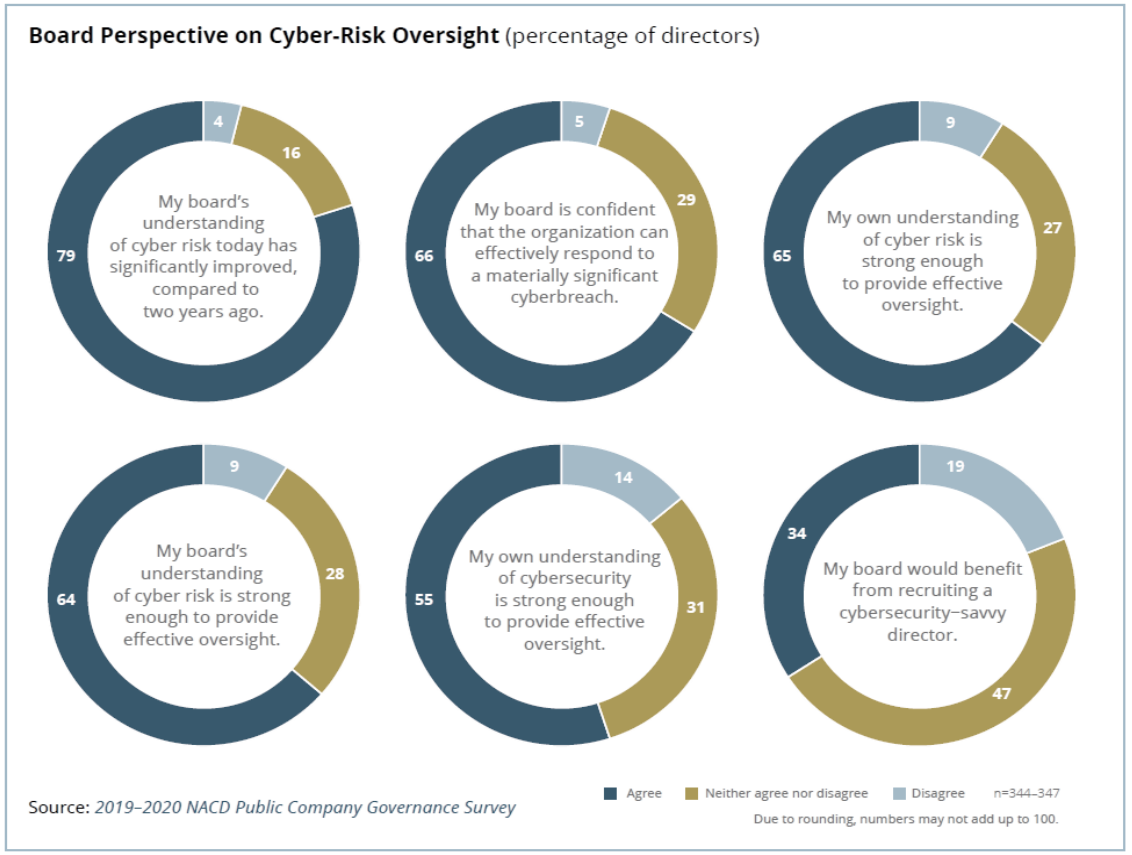
Washington D.C., May 3, 2022 — The Securities and Exchange Commission today announced the allocation of 20 additional positions to the unit responsible for protecting investors in crypto markets and from cyber-related threats. The newly renamed Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) in the Division of Enforcement will grow to 50 dedicated positions.

"The U.S. has the greatest capital markets because investors have faith in them, and as more investors access the crypto markets, it is increasingly important to dedicate more resources to protecting them," said SEC Chair Gary Gensler. "The Division of Enforcement's Crypto Assets and Cyber Unit has successfully brought dozens of cases against those seeking to take advantage of investors in crypto markets. By nearly doubling the size of this key unit, the SEC will be better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."

Directors and Officers are Focused on Governance

Privacy+ Security Forum

Today's Boards are way more active



88% *Reviewed the company's approach to protecting critical data assets*

81% *communicated with management about cyber-risk*

77% *reviewed significant cyber threats and incident response plans*

70% *reviewed data breach response plans*

66% *assessed employee negligence or misconduct risks*

Fiduciary risk oversight

Privacy+ Security Forum

- Cyber or not, the Board's duty is to execute a "**risk oversight**" function
  - Duty of care + Duty of loyalty, including duty of good faith
  - Typical Delaware liability standard is quite high; but *Caremark* and *Stone* case precedent adds depth
- Board protection founded on the **Business Judgment Rule**
  - shields Board from shareholder claims *unless* shareholders can allege

    (i) **failure** to implement a **board-level oversight and reporting system**, or

    (ii) directors **substantially disregarded** cyber reports and **red flags**

The old roadmap

Privacy+ Security Forum

1 Identify cybersecurity governance structure

- Who "owns" cyber risk and cyber resiliency?
- Do we have a CISO role in our company?

2 Understand Company's risk and threat profile

- What is our risk profile?
- What are the core risks and threats to business?

3 Direct management to develop and execute a plan

- What is our framework?
- What are our key People, Processes & Technology?

4 Ask key questions and ask for data from management

- What questions should Board ask and what are the answers?

5 Allocate adequate funds and resources

- Have we committed enough to cyber?

6 Receive and review reports on regular cadence

- Do we have meaningful metrics?
- Do we receive progress updates against roadmap?
- Are we briefed on security incidents?

The new roadmap post-SEC proposal

Privacy+ Security Forum

Risk Management and Strategy

Item 106(b)

- Policies and procedures for identifying and managing cyber risks and threats – including operational risk, IP theft, fraud, extortion, harm to employees/customers, violation of privacy laws and other litigation and legal risk, reputational risk, for example, as applicable, "**a discussion of whether**":
  1. Co. has a cybersecurity risk assessment program (and provide a description)
  2. Co. engages assessors, consultants, auditors or other third parties in connection with assessment program
  3. Co. has policies and procedures to identify/manage third-party service provider risks (and describe how cyber affects selection and oversight of third parties, and contractual/other mechanisms to reduce risk)
  4. Co. undertakes to prevent, detect, and minimize cyber incidents (and if so, describe types of activities)
  5. Co. has business continuity, contingency, recovery plans to respond to cyber incidents
  6. Previous cyber incidents "informed changes in . . . governance, policies, procedures or technologies"
  7. Cyber-related risks and previous incidents "have affected or are reasonably likely to affect" strategy, business model, results or financial condition (and if so, how)
  8. Cyber-related risks are considered in business strategy, financial planning, and capital allocation (and if so, how)

Governance

Item 106(c)

- **Board of Directors** oversight of cybersecurity risk:
  - i. Structure of oversight on cyber risks (i.e., entire board, specific members or board committee is responsible)
  - ii. Processes by which Board is informed about cyber risk
  - iii. Frequency of Board's discussions about cyber risk
  - iv. How Board considers cyber risk as part of its "business strategy, risk management and financial oversight"
- **Management's role** in (a) assessing and managing cyber risk and (b) implementing policies, procedures, strategies, e.g.:
  - i. Whether certain management positions or committees are responsible for measuring/managing cyber risks (e.g., prevention, mitigation, detection, remediation of incidents) + describe relevant expertise of persons (e.g., previous work experience, degrees, certifications, knowledge, skill, other cyber background)
  - ii. Whether there is a designated CISO or someone in comparable position + describe relevant expertise of person + reporting lines in corporate org chart
  - iii. Processes by which mgmt. persons or committees are informed about and monitor prevention, mitigation, detection and remediation of cyber incidents; and
  - iv. Whether and how frequently mgmt. persons or committees report to the Board on cyber risks

Cybersecurity Expertise

Item 407(j)

- **If** any board member has expertise in cybersecurity:
  - i. Disclose name of director
  - ii. Provide detail necessary to fully describe nature of expertise, including, among other things:
    - Prior work experience (e.g., CISO, security policy analyst/auditor/architect/engineer/ operations manager, incident response manager, business continuity planner)
    - Cybersecurity certification or degree
    - Knowledge, skills, or other background, for example, in security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, business continuity planning
- Safe harbor applies such that Board member identified or designated as having cyber expertise . . .
  - i. will NOT be deemed an expert for any other purpose under securities laws
  - ii. will NOT have any duties or liability exposure that are greater than otherwise would be imposed
  - iii. does NOT affect any duties or liability exposure of other directors on the board

Thank You!

Privacy+ Security Forum

Questions & Contacts

Privacy+ Security Forum

Jerry Archer

Chief Security Officer
Sallie Mae Bank
Jerry.Archer@salliemae.com

Jeff Kosseff

Associate Professor of Cybersecurity Law
United States Naval Academy
jkosseff@gmail.com

Tony Kim

Partner
Latham & Watkins LLP
Tony.Kim@lw.com