November 10, 2023

New SEC Cyber Disclosure Rules: *Tell it Early, Tell it All, and Tell it Yourself?*

Amy Yeung
Sallie Mae

Evan Roberts
FTI Consulting

Paul Dudek
Latham & Watkins LLP

Tony Kim
Latham & Watkins LLP

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Amy Yeung

VP and Deputy GC
Sallie Mae

(former General Counsel and Chief Privacy Officer at Lotame)

Paul Dudek

Partner
Latham & Watkins LLP

(former SEC - Chief of the Office of International Corporate Finance)

Evan Roberts

Senior Managing Director
FTI Consulting

Tony Kim

Partner
Latham & Watkins LLP

The New Rules

In a Nutshell

Privacy+ Security Forum

New SEC Cyber Disclosure Rules

Privacy+ Security Forum

Form 8-K | Item 1.05

- ✓ **Disclose** any "cybersecurity incident" determined "without unreasonable delay" to be **material** and describe material aspects of incident's:
  - nature, scope and timing; and
  - impact or reasonably likely impact (e.g., financial/operational results)
- ✓ **File** Item 1.05 Form 8-K **within four (4) business days** of determining an incident is material, absent national security/safety/FCC exception
- ✓ **Amend** prior Item 1.05 Form 8-K to disclose information that was not determined or unavailable at time of initial Form 8-K filing

Form 10-K

Item 106(b) | *Risk management and strategy*

- ✓ **Describe** (i) **processes**, if any, for the assessment, identification, and management of material cyber risks and (ii) whether any cyber risks have materially affected or are reasonably likely to **affect business strategy, result of operation, or financial condition**

Item 106(c) | *Governance*

- ✓ **Describe** (i) **board's oversight** (e.g., committees, processes) of cyber risks and (ii) **management's role** in assessing and managing material cyber risks (e.g., positions/committees; expertise; processes for preventing, monitoring, detecting, mitigating incidents; reporting to the board)

Compliance Deadlines

December 18, 2023 (June 15, 2024 for smaller companies)

Upcoming Annual Reports for all Fiscal Years ending on or after December 15, 2023

New SEC Cyber Disclosure Rules

Privacy+ Security Forum

Form 8-K | Item 1.05

01
Is it a "Cybersecurity Incident"?

- ✓ Definition covers "availability" incidents regardless of data impact; accidental (non-malicious) incidents; third-party and supply chain incidents; electronic but not hardcopy resources; and "a series of related" occurrences counts

02
Is the incident "material" ?

- ✓ Traditional "materiality" concepts and caselaw apply but with an increasing emphasis on **qualitative** factors such as reputation, customer relationships, and competitiveness

03
Is our determination timely?

- ✓ Per Instructions to Item 1.05, the materiality determination must be made "without unreasonable delay" post-discovery; internal processes cannot be modified to support delay

04
File Form 8-K within 4 biz days

- ✓ Note that "specific or technical information" about the registrant's "planned response" or "systems, related networks and devices, or potential system vulnerabilities" need NOT be disclosed if it would "impede" the response or remediation efforts

05
Unless (narrow) exceptions

- ✓ 30 / 30 / 60 day delays (and potentially more) available if U.S. Attorney General notifies SEC, in writing, that the disclosure poses a "substantial risk to national security or public safety"
- ✓ 7-day delay if FCC's CPNI breach rule applies

06
Amend Form 8-K (as needed)

- ✓ Per Instructions to Item 1.05, if required info is "not determined" or "unavailable" at time of initial 8-K, then note that fact in the initial filing; and file amended 8-K within 4 biz days after registrant "without unreasonable delay" determines such info or such info becomes available

New SEC Cyber Disclosure Rules

Privacy+ Security Forum

Form 10-K

Item 106(b) | *Risk management and strategy*

1) Describe the registrant's **processes***, if any, for **assessing, identifying, and managing material risks** from cybersecurity threats in sufficient detail for a reasonable investor to understand those **processes**. In providing such disclosure, a registrant should address, as applicable, the following **non-exclusive list** of disclosure items:

    i. Whether and how any such processes have been **integrated** into the registrant's overall risk management system or processes;

    ii. Whether the registrant engages assessors, consultants, auditors, or other **third parties** in connection with any such processes; and

    iii. Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of **any third-party service provider**.

2) Describe whether any **risks** from cybersecurity threats, including as a result of any **previous cybersecurity incidents**, have **materially** affected or are reasonably likely to **materially** affect the registrant, including its **business strategy, results of operations, or financial condition** and if so, **how**.

Item 106(c) | *Governance*

1) Describe the board of directors' **oversight of risks** from cybersecurity threats. If applicable, identify any **board committee or subcommittee** responsible for the oversight of risks from cybersecurity threats and describe the **processes*** by which the board or such committee is **informed about such risks**.

2) Describe management's **role in assessing and managing** the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

    i. Whether and which **management positions or committees are responsible** for assessing and managing such risks, and the relevant **expertise** of such persons or members in such detail as necessary to fully describe the nature of the expertise;

    ii. The **processes** by which such persons or committees are informed about and monitor the **prevention, detection, mitigation, and remediation** of cybersecurity incidents; and

    iii. Whether such persons or committees **report** information about such risks to the **board** of directors or a **committee or subcommittee** of the board of directors.

** In the Final Rule, the term "processes" replaced "policies and procedures" – and refers to practices, even if not codified in writing.*

The New Rules

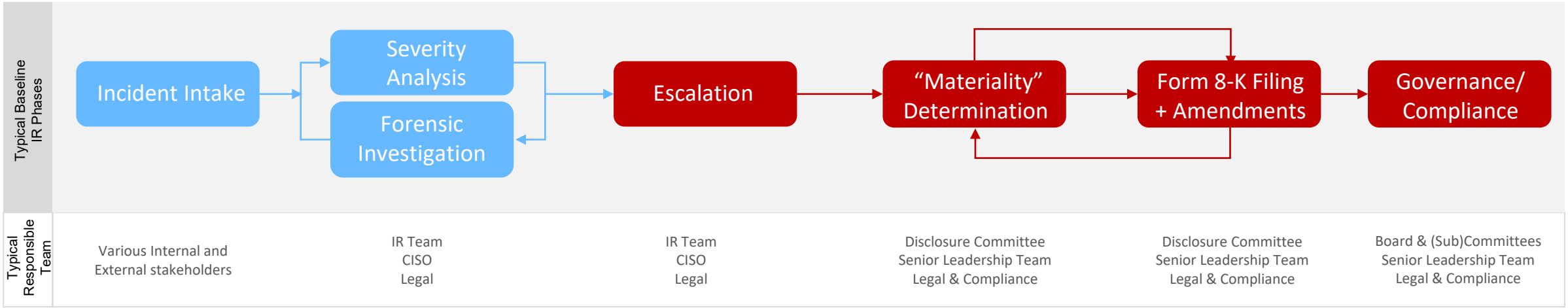
In Practice

Privacy+ Security Forum

Implementing the New Rules

Privacy+ Security Forum

Aligning Processes Across Multiple Stakeholders



Implementing the New Rules

Privacy+ Security Forum

Process Uplifts

- Escalation points and paths from the IR Team/CISO to a broader internal audience –
  - *What types of incidents require escalation (e.g., SEC's emphasis on **qualitative** materiality factors)?*
  - *How do we get on the same page as the CISO?*
- Materiality analysis –
  - *Who are the Co's "disclosure decision makers"?*
  - *What info do they need, when and how?*
  - *What goes into the materiality analysis for cyber?*
- Documentation – *How do we document these processes? Can we maintain privilege (and over what)?*
- Training, training, training

Some Pain Points

- Timing pressure is real given duty to conduct materiality analysis "without unreasonable delay" and market practice of accelerated Form 8-K filings being observed – *What can we really know in such a short amount of time?*
- Exceptions to the four business day timing are extremely narrow (e.g., CPNI or "national security or public safety" process through U.S. Attorney General) – *Who qualifies and what's the process?*
- Potential for a required public disclosure of an incident prior to completion of containment or remediation – *How do we protect our companies while complying with the rules?*
- Overlapping notification and disclosure requirements (and timing) across regulators and jurisdictions – *How should we prioritize competing interests?*

SEC v. Pearson

A Case Study in Comms

Privacy+ Security Forum

Background on the Pearson case

Privacy+ Security Forum

- On July 31, 2019, a reporter allegedly 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.
- Threat actor had allegedly 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.
- Alleged that the security patch for AIMSweb 1.0 had been publicized and made available in September 2018, but Pearson allegedly failed to implement it until after it learned of the attack.
- SEC alleged that Senior Management at Pearson 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 allegedly posted an online Media Statement *after* being contacted by the reporter on July 31.

Core Allegations in the Order

Privacy+ Security Forum

Disclosures in **Form 6-K** filed on July 26, 2019	SEC Enforcement Findings
Pearson stated that a *"**risk** 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 argued that 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 allegedly 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 argued that Pearson knew that data was "***removed***" from the system, not just "accessed"; and Pearson ***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 argued that Pearson knew that ***the 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 argued that Pearson suggested the impact to DOBs/emails was "***hypothetical***" by using the word "***may***" but "***[i]n fact, Pearson knew***" DOBs/emails were stolen
Pearson stated that it had "***strict data protections*** *in place and have reviewed this incident, found and fixed the vulnerability . . .*"	SEC argued that Pearson misstated its "strict" security protections because it had (a) ***failed to patch*** a publicly-known vulnerability for six months and (b) ***used an outdated/insecure hashing algorithm***

Lessons Learned

Privacy+ Security Forum

Interplay with the New Rules

- *Every* public statement counts (e.g., media statements)
- Time pressures are intensified under the new four business day trigger to file 8K/6K from materiality determination
- The balancing act for companies:
  - transparency vs. confidentiality
  - speed vs. accuracy
  - legal obligations vs. brand / reputation
- SEC's enforcement of "disclosure controls and procedures"
- Risk of litigation and enforcement – uptick in sophistication (e.g., questions being asked in aftermath of incidents)

Some Pro Tips

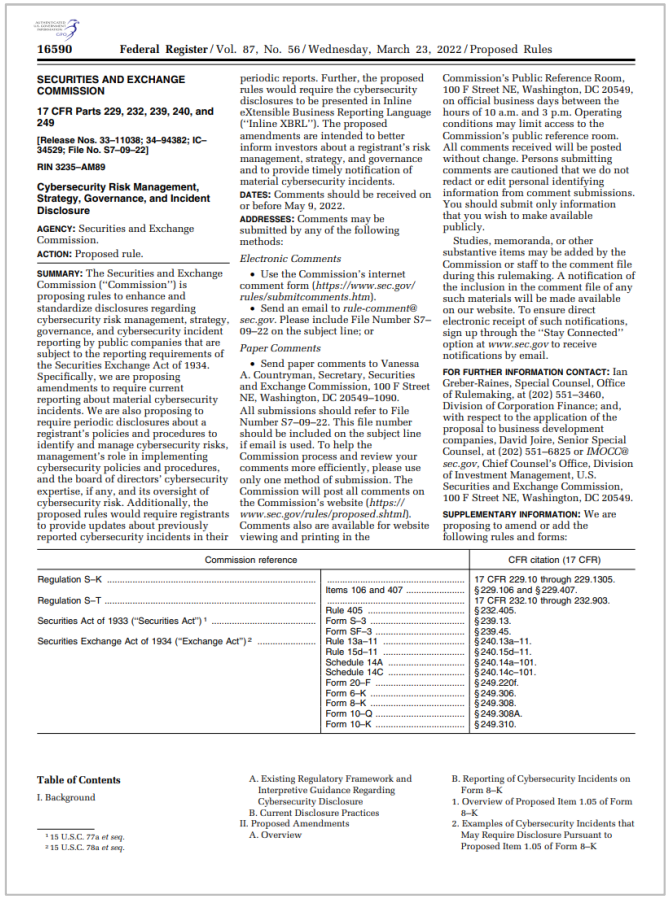
- Plans in place that contemplate different scenarios (e.g., data impact versus operational impact or both; employee impact versus customer impact or both)
- "Next gen" tabletops and simulation exercises (e.g., practicing escalation and materiality workflows)
- Investor Relations function embedded into incident response frameworks
- Nested teams of 3rd party advisors (e.g., legal, forensics, ransom negotiation, restoration, communications)

Appendix Materials

Privacy+ Security Forum

SEC Proposing Release commentary re: characteristics and consequences of potentially material cyber incidents

Privacy+ Security Forum



16590 Federal Register / Vol. 87, No. 56 / Wednesday, March 23, 2022 / Proposed Rules

SECURITIES AND EXCHANGE COMMISSION

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

[Release Nos. 33–11038; 34–94382; IC–34529; File No. S7–09–22]

RIN 3235–AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is proposing rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents. We are also proposing to require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk. Additionally, the proposed rules would require registrants to provide updates about previously reported cybersecurity incidents in their periodic reports. Further, the proposed rules would require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL"). The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.

DATES: Comments should be received on or before May 9, 2022.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (*https://www.sec.gov/rules/submitcomments.htm*).
- Send an email to *rule-comment@sec.gov*. Please include File Number S7–09–22 on the subject line; or

Paper Comments

- Send paper comments to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to File Number S7–09–22. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (*https://www.sec.gov/rules/proposed.shtml*). Comments also are available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission's public reference room. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on our website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at *www.sec.gov* to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Ian Greber-Raines, Special Counsel, Office of Rulemaking, at (202) 551–3460, Division of Corporation Finance; and, with respect to the application of the proposal to business development companies, David Joire, Senior Special Counsel, at (202) 551–6825 or *IMOCO@sec.gov*, Chief Counsel's Office, Division of Investment Management, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION: We are proposing to amend or add the following rules and forms:

Commission reference		CFR citation (17 CFR)
Regulation S–K	Items 106 and 407	17 CFR 229.10 through 229.1305. §229.106 and §229.407.
Regulation S–T	Rule 405	17 CFR 232.10 through 232.903. §232.405.
Securities Act of 1933 ("Securities Act")[1]	Form S–3	§239.13.
	Form SF–3	§239.45.
Securities Exchange Act of 1934 ("Exchange Act")[2]	Rule 13a–11	§240.13a–11.
	Rule 15d–11	§240.15d–11.
	Schedule 14A	§240.14a–101.
	Schedule 14C	§240.14c–101.
	Form 20–F	§249.220f.
	Form 6–K	§249.306.
	Form 8–K	§249.308.
	Form 10–Q	§249.308A.
	Form 10–K	§249.310.

Table of Contents

[1] 15 U.S.C. 77a *et seq.*
[2] 15 U.S.C. 78a *et seq.*

*SEC commentary: The following is a non-exclusive list of **examples of cybersecurity incidents** that may, if determined by the registrant to be material, trigger the proposed Item 1.05 disclosure requirement:*

1. An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
2. An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;
3. An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
4. An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
5. An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

*SEC commentary: The **types of costs and adverse consequences** that companies may incur or experience as a result of a cybersecurity incident include the following non-exhaustive list:*

1. Costs due to business interruption, decreases in production, and delays in product launches;
2. Payments to meet ransom and other extortion demands;
3. Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
4. Increased cybersecurity protection costs, which may include increased insurance premiums and the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants;
5. Lost revenues resulting from intellectual property theft and the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
6. Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
7. Harm to employees and customers, violation of privacy laws, and reputational damage that adversely affects customer or investor confidence; and
8. Damage to the company's competitiveness, stock price, and long-term shareholder value.

SEC Cyber Enforcement – Recent Cases

Privacy+ Security Forum

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 alleged: The vulnerability had existed since 2014, but it was not discovered by InfoSec personnel until Jan 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 alleged: "*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 alleged: *"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."*

SEC Cyber Enforcement – Recent Cases

Privacy+ Security Forum

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.

Pearson
global educational publisher

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***

SEC Cyber Enforcement – Recent Cases

Privacy+ Security Forum

On March 9, 2023, SEC settled administrative charges, secured a $3,000,000 penalty, and entered a Cease-and-Desist Order.

On July 16, 2020, Blackbaud (a donor data management software provider to non-profit organizations), announced a ransomware attack. The website notification and notification letters sent to customer stated as follows – in relevant part:

blackbaud
global software company

> "The cybercriminal did not access . . . bank account information, or social security numbers."

However, by the end of July 2020, Company personnel learned that ***the attacker had, in fact, accessed donor bank account information and social security numbers in an un-encrypted form*** for a number of the impacted customers.

SEC charged Blackbaud with cybersecurity-related disclosure controls/procedures failures:

- SEC alleged: In the Form 10-Q filed on August 4, 2020, Blackbaud "omitted the material fact that a number of customers had unencrypted bank account and social security numbers exfiltrated, in contrast to the company's unequivocal, and ultimately erroneous claims in the July 16, 2020 website post and customer notices."
- SEC alleged: In the Form 10-Q, Blackbaud stated that "[a] compromise of our data security that results in ***customer or donor personal*** or payment card data being obtained by unauthorized persons ***could*** adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties." "This statement omitted the material fact that such customer or donor personal data was exfiltrated by the attacker, which entailed that the risks of such an attack . . . ***were no longer hypothetical***."
- SEC alleged: In a Form 8-K filed on September 29, 2020, Blackbaud acknowledged publicly for the first time that "the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords."
- SEC alleged: "[T]he company's senior management responsible for the company's disclosures were ***not made aware of these facts prior to the company filing its Form 10-Q*** on August 4, 2020, or indeed until several weeks later, nor were there controls or procedures designed to ensure that such information was communicated to senior management. . . . ***As a result, relevant information related to the incident was never assessed from a disclosure perspective***."

Thank You!

Privacy+ Security Forum