BakerHostetler

U.S. SECURITIES AND EXCHANGE COMMISSION

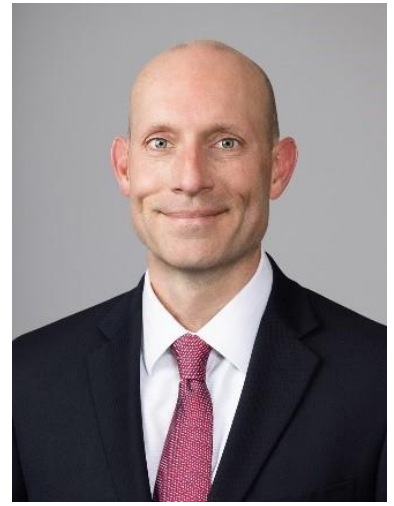
New SEC Cybersecurity Rules

Compliance and Enforcement Risk

beazley

November 16, 2023

Presenters



Eric Gyasi – New York **egyasi@bakerlaw.com** **Digital Risk Advisory & Cybersecurity - Governance**	**John Harrington – Cleveland** **jharrington@bakerlaw.com** **Co-Leader, IPOs and Securities Offerings Team**	**Craig Hoffman – Cincinnati** **cahoffman@bakerlaw.com** **Co-Leader, Digital Risk Advisory & Cybersecurity Team**

Agenda

- Overview of SEC Cybersecurity Rules
- Developing an IRP process to support escalation and impact analysis to support a materiality determination;
- Review a template of a Form 10-K Item 1C disclosure; and
- Review prior and current litigation and SEC enforcement actions to anticipate risk areas.

SEC Cybersecurity Rules Overview

SEC Cybersecurity Rules

- **Disclosure of Material Impact from Cybersecurity Events**
  - file an 8-K within four business days of determining a cybersecurity incident is material that describes (1) the material aspects of the nature, scope, and timing of the incident, and (2) the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.
- **Disclosure of Cybersecurity Risk Management and Strategy**
  - Describe the process of assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand the processes.
  - Describe whether risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to have a material affect, including to business strategy, results of operations, or financial condition and if so, how.
- **Governance - Disclosure of Management and Board Oversight**
  - Describe the Board's oversight of risks from cybersecurity threats
  - Describe management's role in assessing and managing material risks from cybersecurity threats, including three specific areas.

Disclosure of Material Impact

Obligation – file an 8-K within four business days of determining a cybersecurity incident is material that describes (1) the material aspects of the nature, scope, and timing of the incident, and (2) the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.

- The filing may be delayed by up to 30 days if the US Attorney General determines that a disclosure "poses a substantial risk to national security or public safety" and the AG notifies the SEC of the determination.
- The 8-K does not need to include technical details about the incident or the company's resposne plans.
- The materiality determination must be made without unreasonable delay after discovery of the incident.
- If information required to be included in the 8-K is not available at the time of the initial 8-K filing, that must be mentioned in the initial 8-K filing and the 8-K must be amended when that information is determined (within four business days of determining the information that was missing).

Disclosure of Cybersecurity Risk Management Strategy

Obligation – There are two security strategy disclosure obligations that will go in a new Item 1C Cybersecurity section of a 10-K as well as a disclosure about management and board oversight.

- (1) The first is to describe the process of assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand the processes. The stated intent of the SEC is to provide enough detail about cybersecurity practices for an investor to understand the company's cybersecurity risk profile. The non-exhaustive list of disclosure items to address are:
  - (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) The second is to describe whether risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to have a material effect, including to business strategy, results of operations, or financial condition and if so, how.

Disclosure of Management and Board Oversight

Obligation – as a complement to the risk management strategy disclosure, this governance disclosure obligation is focused on how a company's leadership oversees and implements its cybersecurity processes in two parts:

(1) Board of Directors – describe the board's oversight of risks from cybersecurity threats, and, if applicable, identify any committee or subcommittee responsible for this area of oversight and how the board or committee is informed about risks from cybersecurity threats; and

(2) Management – describe management's role in assessing and managing material risks from cybersecurity threats, including addressing the following non-exhaustive list: (i) management positions that are responsible for assessing and managing such risks and the relevant expertise of those individuals (e.g., a CISO or comparable position), (ii) the processes by which responsible managers or management committees are informed about and monitor "prevention, detection, mitigation, and remediation of cybersecurity incidents," and (iii) whether management report information about material cybersecurity risks to the board or a board committee.

IRP ESCALATION & IMPACT ANALYSIS PROCESS

What Companies Should Do

- Develop and implement disclosure controls and procedures
  - Account for stock trading restriction process and stock buyback scenarios
  - Use incident severity classification to establish escalation procedure from IRT to disclosure committee
  - Establish briefing method/cadence for updating executive team and disclosure committee
- Use a “bringdown” process to avoid misleading or inaccurate disclosures
  - Make sure to review Item 1A forward-looking risk factors
  - Starting next year, also review Item 1C cybersecurity risk management strategy disclosure

Incident Severity Classification – Escalation Protocol

Internal Detection
Identify cybersecurity incidents

External Detection
Notices of cybersecurity incidents

Triage IRT
Initial incident classification and core team build
Contact external services (legal, forensics)

INCIDENT RESPONSE TEAM

CORE TEAM
Security
Legal
Communications
Risk Management
IT Operations
EXTENDED TEAM (as needed)
[name]
[name]
[name]
Human Resources
[name]
Others team members as needed

Executive Leadership Team (ELT)

	NOTIFIED IMMEDIATELY		ACTIVELY ENGAGED
Critical	Full Board of Directors **+ Medium Impact Team**		(Controller) (CFO) (Internal Audit) (Inv Relations) (ERM) **+ Medium & High Impact Team**
High	(CEO) (BoD AC) **+ Medium Impact Team**		(CIO) (CCO) (CLO) (Controller) (CTO) **+ Medium Impact Team**
Medium	(CCO) (CLO) (CFO) Controller CTO (Internal Audit) (ERM)		IR Core & Extended Team

INCIDENT SEVERITY CLASSIFICATION LEVELS

LOW	MEDIUM	HIGH	CRITICAL

IRP Example

Privilege/Legal hold/SEC disclosure/insider trading protocol-a potential add to cover these items:

- Legal, in coordination with outside counsel, if any, will advise the IRT regarding the scope of attorney-client or other legal privilege and how to maintain that privilege throughout the investigation.IRT members are advised that, generally, the attorney-client privilege only applies to communications seeking or providing legal advice, and not to every document or communication labeled as “Attorney-Client Privileged” or which includes Legal or outside counsel in the distribution.*If an IRT member has a question regarding whether the attorney-client privilege applies to a particular document or communication, the IRT member should seek the advice of Legal or outside counsel.*
- •If there is an intent to engage the forensic firm to conduct work to support the provision of legal advice to the company regarding the incident, ensure that the forensic firm is engaged by Legal or external legal counsel. If the company has already negotiated an engagement agreement with the forensic firm, request a statement of work specific to the Incident. Ensure that the statement of work contains language to support the application of attorney-client privilege where desired.
- •Legal will also determine if a legal hold is appropriate, and issue a legal hold notice as needed.
- •Legal will notify the company’s [Disclosure Committee] of incidents classified as Critical Risk or Escalated Risk so that the company’s SEC disclosure obligations, if any, may be considered.
- •Legal will maintain a list of the members of the IRT.Depending on the circumstances of the Incident, where applicable, this list will be used to support the issuance of a legal hold [and consideration of the incident in conjunction with the company’s insider trading policy].

Materiality

General Definition of Materiality

- Is there a substantial likelihood that a reasonable investor would consider the information important in deciding whether to buy or sell securities?
- Would disclosure or lack thereof significantly alter the total mix of information available to investors?
- Weigh likelihood of occurrence and magnitude on a sliding scale – something that is a very remote possibility may not be material no matter what, but something that has a reasonably small chance of occurring may be material if it would be of a very large magnitude, should it occur.
- Materiality determinations are inherently judgment calls based on all relevant facts and circumstances. Our role should be to help guide client through the assessment, make sure they are aware of and understand the facts relative to the incident response work we are doing (including what information remains unknown and when it may be determined) and can offer our insights.
- But the decision must be made within the entire context of the client's business, and therefore clients, and in some cases with the assistance their existing securities counsel, are best positioned to make the ultimate determination. Different companies have different tolerances and thresholds for determining materiality, and following past practice is important.
- The assessment must also be made with a full understanding of past public statements by the client regarding cyber practices, risks and incidents, whether in SEC filings or other communications, so that the current incident can be considered in the context of those past statement.

SEC Material Cybersecurity Incident Determination Factors

The following is a list of general quantitative and qualitative factors to consider in assessing the impact of a cybersecurity incident to determine if the impact is material and warrants disclosure using Form 8-K as part of evaluating the unique facts and circumstances of the incident (through the lens of how a reasonable investor would view the impact of the incident on the company). These factors are illustrative.

Quantitative	Qualitative
Direct incident costs (cyber insurance policies may refer to these as first-party costs and these are often costs covered by the policy). Remember to account for any applicable deductible and sublimit. • Incident response legal counsel, forensic investigation, ransom negotiation, IT staff augmentation fees • Costs of mailing notification letters, support call center, and any identity monitoring or credit monitoring services • Ransom payment • Misdirected wire transfer (sometimes only covered by crime-fraud policy) • Costs of containment measures (e.g., new hardware, new software license, etc.) and costs to restore the network (e.g., costs to rebuild systems)(policies vary in how these costs are treated) • Lost net income due to outage	• If data was taken, did it include the company's "crown jewels" (e.g., key customer data, intellectual property)? • Is the identity and motive of the threat actor known (e.g., a nation state where the access or data taken was for a purpose that will not cause direct impact to the company, a competitor/departed employee, or a financially motivated attacker)? • Is security and operational integrity a core part of the company's strategy/value proposition? • Did the incident affect the company's competitiveness, such as through an increase in the cost of sales, accommodations to customers to preserve relationships, changes to products/services to maintain relationships/ability to sell, or impact to profitability? • Were key customer or vendor relationships affected?
Incident related costs (these are not typically covered by cyber policies) • Additional employee expenses (e.g., overtime) • Costs to upgrade/enhance network security measures (e.g., new security tools, new security vendors, additional hiring)	• How, if at all, did they incident affect the company's reputation/brand? o Did the incident reveal that common/baseline security measures were not in place? o Was the company viewed as mishandling the response to the incident? o Did the incident involve access to data people may consider to be highly sensitive or reveal business practices that cause significant scrutiny?
• Third-party demands, claims, and lawsuits (these are typically covered by cyber policies)(contractual liabilities may only be covered by tech errors & omissions policies)	• Has the company had multiple incidents, such that risks of adverse impacts to customer/vendor relationships, reputation/brand and litigation and regulatory risk could be elevated?
• Regulatory investigations, enforcement actions, monetary assessments, and consent orders with injunctive relief requirements (costs of compliance with consent orders may not be covered by cyber policies) (consider whether they have occurred or are reasonably likely to occur) • If the incident is publicly known, a related decline in stock price	
• Are any other impacts, such as from the qualitative factors listed in next column, reasonably estimable and quantifiable?	
If the company uses an established dollar amount threshold for materiality as a starting point in the analysis, there is no need to change that for purposes of this analysis. Such a threshold is only part of the analysis, and any applicable qualitative factors should be considered.	

Example

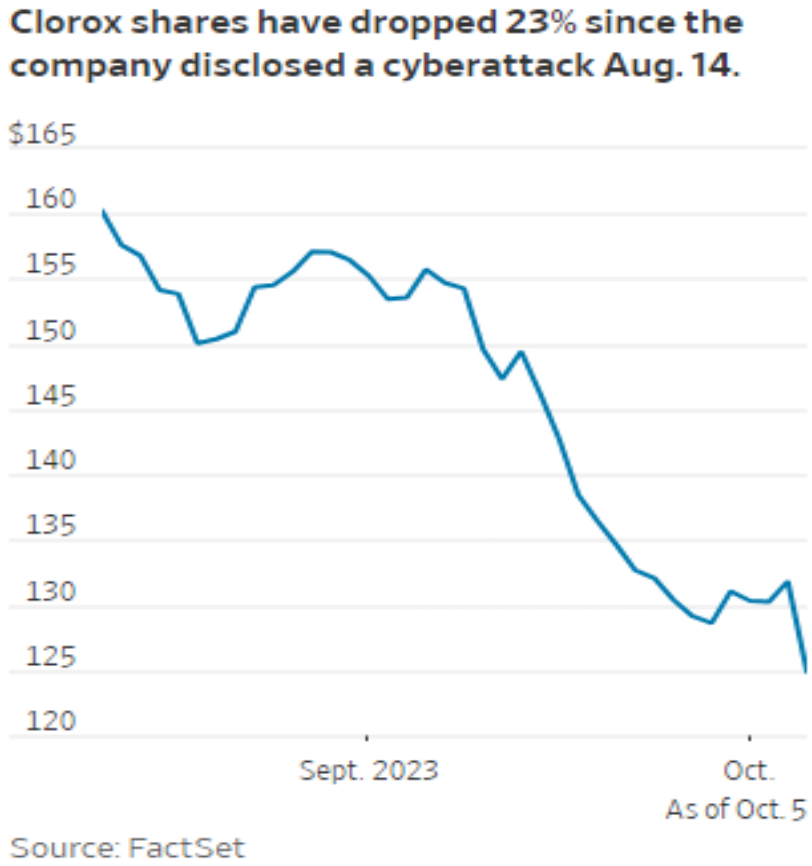
The Clorox Company

WSJ PRO

Clorox Warns of Accruing Costs From Cyberattack

Hack came amid a $500 million digital overhaul at the consumer products maker

- August 14, 2023 | First 8-K filed
- October 4, 2023 | Supplemental 8-K



Clorox Provides Preliminary Q1 Financial Information and Operations Update

OAKLAND, Calif., Oct. 4, 2023 — The Clorox Company (NYSE: CLX) (the "Company" or "Clorox") today announced certain preliminary financial information for the first quarter of fiscal 2024, which ended Sept. 30, 2023, as well as an operations update following the previously announced cybersecurity attack that impacted the Company's business.

- **Net sales** are expected to decrease by 28% to 23% from the year-ago quarter. Organic sales are now expected to decrease by 26% to 21% for the quarter, compared to the Company's prior expectations of mid-single-digits growth as provided in the Q4 earnings remarks. This is due to the impacts of the recent cybersecurity attack that was disclosed in August, which caused wide-scale disruption of Clorox's operations, including order processing delays and significant product outages. Shipment and consumption trends prior to the cybersecurity attack were in line with the Company's prior expectations.
- **Gross margin** is now expected to be down from the year-ago quarter compared to the Company's prior expectations for gross margin to be up, as provided in the Q4 earnings remarks, as the impact of the cybersecurity attack more than offset the benefits of pricing, cost savings and supply chain optimization. The impact of the cybersecurity attack on gross margin also includes lower cost absorption driven by lower volume.
- **Diluted net earnings per share** (diluted EPS) is expected to be between a loss of $0.75 to a loss of $0.35.
- **Adjusted EPS** is expected to be a loss of $0.40 to $0.00, as the impact from the cybersecurity attack more than offset the benefits of pricing, cost savings and supply chain optimization. The impact of the cybersecurity attack also includes lower cost absorption in cost of products sold and operating expenses, which are largely fixed costs in the short term. To provide greater visibility into the underlying operating performance of the business, preliminary adjusted EPS excludes charges related to the Company's long-term strategic investment in digital capabilities and productivity enhancements, costs related to the cybersecurity attack, and the streamlined operating model.

Based on its current assessment of the situation, the Company expects to experience ongoing, but lessening, operational impacts in the second quarter as it makes progress in returning to normalized operations. The Company also expects to begin to benefit from the restocking of retailer inventories as it ramps up fulfillment in the second quarter.

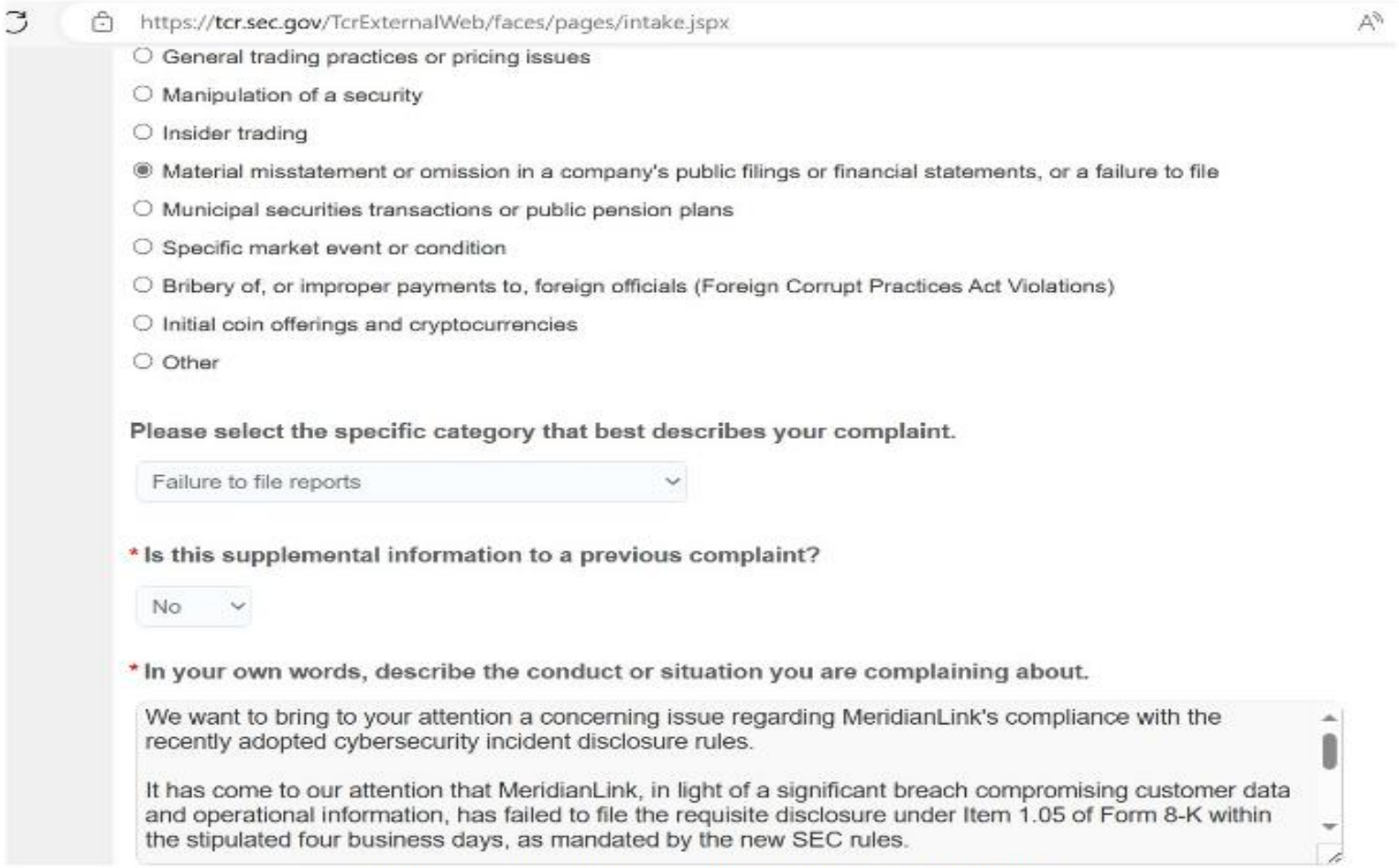
Clorox is in the process of assessing the impact of the cybersecurity attack on fiscal year 2024 and beyond. The Company will provide an updated outlook during its first quarter earnings call in November.

Operational Update

As previously disclosed, the Company believes the cybersecurity attack has been contained and the Company is making progress in restoring its systems and operations. On Sept. 25, Clorox began the process of transitioning back to automated order processing and the vast majority of orders are now taking place in an automated manner, which is enabling the Company to ramp up output and shipments to rebuild retailer inventories. Clorox expects the process of restocking retailer inventories will occur over time as it ships above consumption levels.

Escalation Tactics

In their own words, the attacker told the SEC that MeridianLink suffered a "significant breach" and did not disclose it as required in Form 8-K, under Item 1.05.



ALPHV ransomware SEC complaint against MeridianLink

source: BleepingComputer

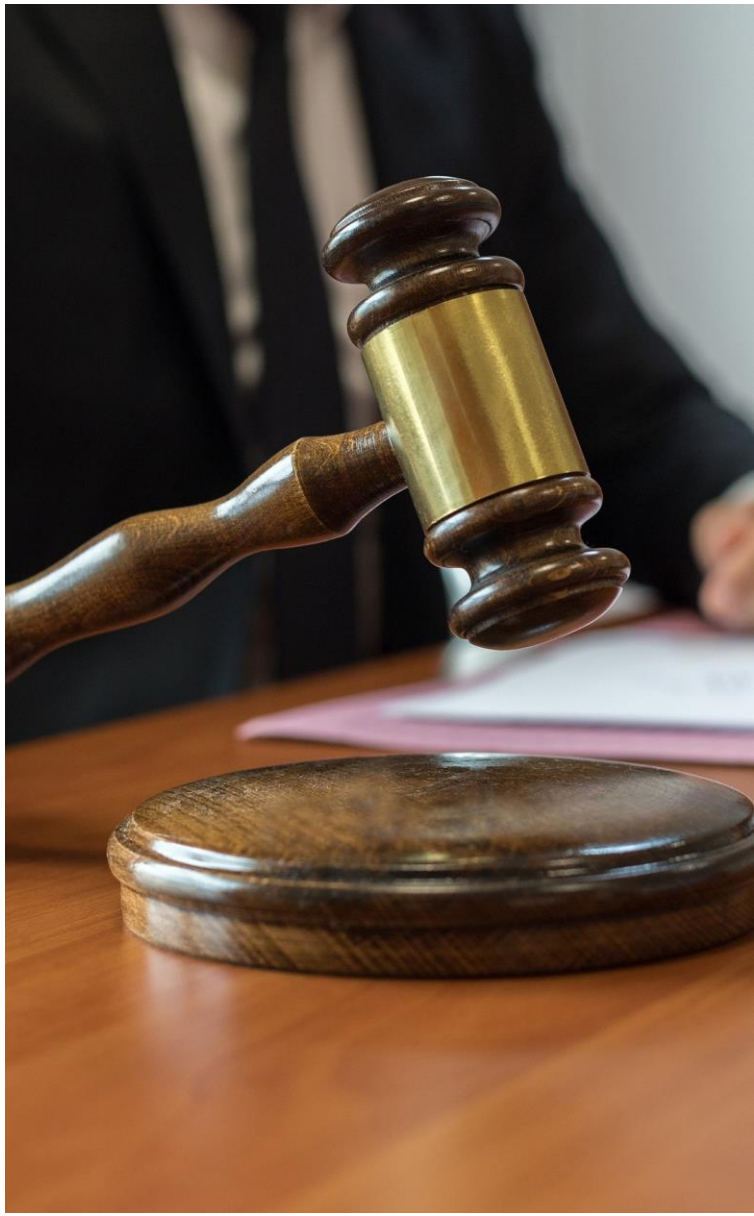
FORM 10-K ITEM 1C CYBERSECURITY DISCLOSURE

Item 1C Cybersecurity Action Items

- Start preparing description of cybersecurity program
- Likely a lot of variation when many companies file in February/March 2023 (subsequent filings will likely become similar)

Regulatory View of “Reasonable Security”

- Risk assessment – conducted annually (+) and done using a recognized method
- Written information security program: (1) based on risk assessment, and (2) security framework (e.g., NIST CSF, Zero Trust)
- Specific technical safeguards
  - Access controls, patch/vulnerability management, logging and monitoring, segmentation, asset management, component hardening, threat intelligence, threat/event detection, DLP, FIM
  - MFA for all remote access, encryption, EDR
- Vendor management: (1) 3-parts (due diligence, contractual requirements, oversight); and (2) enhanced process for “significant” IT vendors
- Secure disposal/data retention
- Employee training and awareness
- Assessments
- Executive reporting regarding security program and incidents



Risk Management and Strategy

BakerHostetler

Item 1C. Cybersecurity.

Risk Management and Strategy. The Company has developed an information security program to address material risks from cybersecurity threats. The program includes policies and procedures that identify how security measures and controls are developed, implemented, and maintained. A risk assessment, based on a method and guidance from a recognized national standards organization, is conducted annually. The risk assessment along with risk-based analysis and judgment are used to select security controls to address risks. During this process, the following factors, among others, are considered: likelihood and severity of risk, impact on the Company and others if a risk materializes, feasibility and cost of controls, and impact of controls on operations and others. Specific controls that are used to some extent include endpoint threat detection and response (EDR), identity and access management (IAM), privileged access management (PAM), logging and monitoring involving the use of security information and event management (SIEM), multi-factor authentication (MFA), firewalls and intrusion detection and prevention, and vulnerability and patch management.

Third-party security firms are used in different capacities to provide or operate some of these controls and technology systems. For example, third parties are used to conduct assessments, such as vulnerability scans and penetration testing. The Company uses a variety of processes to address cybersecurity threats related to the use of third-party technology and services, including pre-acquisition diligence, imposition of contractual obligations, and performance monitoring.

The Company has a written incident response plan and conducts tabletop exercises to enhance incident response preparedness. Business continuity and disaster recovery plans are used to prepare for the potential for a disruption in technology we rely on. The Company is a member of an industry cybersecurity intelligence and risk sharing organization. Employees undergo security awareness training when hired and annually.

The Company has a Governance, Risk, and Compliance (GRC) function to address enterprise risks, and cybersecurity is a risk category addressed by that function. [consider additional detail]. The Company has a privacy and security governance committee.

The Company (or third parties it relies on) may not be able to fully, continuously, and effectively implement security controls as intended. As described above, we utilize a risk-based approach and judgment to determine the security controls to implement and it is possible we may not implement appropriate controls if we do not recognize or underestimate a particular risk. In addition, security controls, no matter how well designed or implemented, may only mitigate and not fully eliminate risks. And events, when detected by security tools or third parties, may not always be immediately understood or acted upon.

(b)(2) Disclosure Uncertainty

BakerHostetler

"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."

ENFORCEMENT & LITIGATION RISK

SEC Enforcement Actions

Pearson - $1 million (educational software 1 million rows of data)

Blackbaud - $3 million

SolarWinds – complaint filed against company and CISO

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.

The SEC's order finds that Pearson made misleading statements and omissions about the 2018 data breach involving the theft of student data and administrator log-in credentials of 13,000 school, district and university customer accounts. In its semi-annual report, filed in July 2019, Pearson referred to a data privacy incident as a hypothetical risk, when, in fact, the 2018 cyber intrusion had already occurred. And in a July 2019 media statement, Pearson stated that the breach may include dates of births and email addresses, when, in fact, it knew that such records were stolen, and that Pearson had "strict protections" in place, when, in fact, it failed to patch the critical vulnerability for six months after it was notified. The media statement also omitted that millions of rows of student data and usernames and hashed passwords were stolen. The order also finds that Pearson's disclosure controls and procedures were not designed to ensure that those responsible for making disclosure determinations were informed of certain information about the circumstances surrounding the breach.

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

FOR IMMEDIATE RELEASE
2023-48

Washington D.C., March 9, 2023 — The Securities and Exchange Commission today announced that Blackbaud Inc., a South Carolina-based public company that provides donor data management software to non-profit organizations, agreed to pay $3 million to settle charges for making misleading disclosures about a 2020 ransomware attack that impacted more than 13,000 customers.

The SEC's order finds that, on July 16, 2020, Blackbaud announced that the ransomware attacker did not access donor bank account information or social security numbers. Within days of these statements, however, the company's technology and customer relations personnel learned that the attacker had in fact accessed and exfiltrated this sensitive information. These employees did not communicate this information to senior management responsible for its public disclosure because the company failed to maintain disclosure controls and procedures. Due to this failure, in August 2020, the company filed a quarterly report with the SEC that omitted this material information about the scope of the attack and misleadingly characterized the risk of an attacker obtaining such sensitive donor information as hypothetical.

"As the order finds, Blackbaud failed to disclose the full impact of a ransomware attack despite its personnel learning that its earlier public statements about the attack were erroneous," said David Hirsch, Chief of the SEC Enforcement Division's Crypto Assets and Cyber Unit. "Public companies have an obligation to provide their investors with accurate and timely material information; Blackbaud failed to do so."

Rel

Press Release

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

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2018 initial public offering through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, dubbed "SUNBURST," SolarWinds and Brown defrauded investors by overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks. In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and Brown knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time.

As the complaint alleges, SolarWinds' public statements about its cybersecurity practices and risks were at odds with its internal assessments, including a 2018 presentation prepared by a company engineer and shared internally, including with Brown, that SolarWinds' remote access set-up was "not very secure" and that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late," which could lead to "major reputation and financial loss" for SolarWinds. Similarly, as alleged in the SEC's complaint, 2018 and 2019 presentations by Brown stated, respectively, that the "current state of security leaves us in a very vulnerable state for our critical assets" and that "[a]ccess and privilege to critical systems/data is inappropriate."

SolarWinds Response

- Denies that they lacked adequate security
- Example – “follow” NIST CST
- Initial attack vector unknown – not a VPN vulnerability
- Lawsuit is wrong approach because it pressures companies to over disclose and CISOs to not evaluate

“We intend to correct the record and push back on their overreach, as the SEC is provably wrong about the facts and lacks the authority or competence to regulate public companies' cybersecurity.”

BakerHostetler

bakerlaw.com

Atlanta | Chicago | Cincinnati | Cleveland | Columbus | Costa Mesa

Dallas | Denver | Houston | Los Angeles | New York | Orlando

Philadelphia | San Francisco | Seattle | Washington, D.C. | Wilmington

BakerHostetler

Disclaimer

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information. BZ_CBR_068_US_11/23