Checklist for Cybersecurity Issues in Securities Enforcement and Litigation

pillsbury

This checklist identifies issues and risks that may arise on cybersecurity matters and data breaches in securities enforcement and litigation. For these cases, determining the "materiality" of the cybersecurity incident can be dynamic and time-sensitive. Early focus on the initial forensics, remediation and security will help guide the regulatory and litigation strategy. The cybersecurity incident may also test the company controls and governance of cybersecurity risk.

1. Cybersecurity Incident.

☐ Confirm whether a "cybersecurity incident" occurred as defined by the SEC.

"Cybersecurity incident" refers to "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."

☐ Confirm if a cybersecurity incident or data breach occurred as defined under other applicable federal or state law standards. Consult with counsel if you have questions.

☐ Determine the type of cybersecurity incident, scope and timing, which will guide forensic review, remediation and other key steps as part of the incident response. Examples may include:

- ✓ Cyber Intrusion
- ✓ Phishing
- ✓ Ransomware
- ✓ Business Email Compromise
- ✓ Denial of Service Attacks
- ✓ Supply Chain Issues
- ✓ Cyber Fraud
- ✓ Nation State Attacks
- ✓ Manipulation
- ✓ Misuse by Insiders
- ✓ Targeted or Malicious Attacks
- ✓ Attacks by Former Employees
- ✓ Insider Threats
- ✓ AI-Enabled Attacks
- ✓ Third Party Vendors
- ✓ Employee Inadvertence

For more information, contact the team:

Mark L. Krotoski
Partner, Cyber Disputes Leader
Silicon Valley & Washington, DC
mark.krotoski@pillsburylaw.com
+1.650.233.4021

David Oliwenstein
Partner, Securities Enforcement Leader
New York
david.oliwenstein@pillsburylaw.com
+1.212.858.1031

Bruce A. Ericson
Partner, Securities Litigation Leader
San Francisco
bruce.ericson@pillsburylaw.com
+1.415.983.1560

2. Implement Written Incident Response, Business Continuity and Disaster Recovery Plans.

- ☐ Assign responsible personnel to coordinate response and manage needed recovery and/or communications tailored to the incident.

3. Contain Incident, Restore Security and Business Operations.

- ☐ Isolate systems used in the intrusion or incident.
- ☐ Disable accounts, patch, change passwords and address vulnerabilities, among other measures tailored to the incident.
- ☐ Address initial customer questions including about the Indicators of Compromise.

4. Implement Attorney Client Privilege and Work Product Legal Protections.

- ☐ As soon as a potential cybersecurity incident is anticipated, confirm legal protections are in place to receive legal guidance on the confidential and privileged cyber investigation, notification obligations, regulatory inquiries, potential litigation and related issues.
- ☐ Ensure legal protections are properly memorialized, to defend if necessary.
- ☐ Ensure forensic providers and any other vendors assisting on the matter are acting at the direction of counsel to preserve the attorney-client privilege and work product doctrine.
- ☐ Place legal hold under attorney-client privilege and work product doctrine to maintain confidentiality and materials are protected as legal strategy is developed.
- ☐ Use *Upjohn* interviews for privileged, confidential employee interviews conducted during a corporate internal investigation for the purpose of obtaining information needed by counsel to provide legal advice to the company.[1]
- ☐ Reconstruct an accurate incident timeline for legal guidance and forensic review.

5. Insurance Coverage.

- ☐ Is the cybersecurity incident covered by insurance?
- ☐ Consider cybersecurity, crime or other applicable insurance policies.
- ☐ If needed, obtain legal guidance on the scope of coverage and insurance notification.

6. Consider SEC Notification Issues.

- ☐ Confirm whether a "cybersecurity incident" occurred as defined by the SEC (see definition in Q1).
- ☐ Determine whether the cybersecurity incident is "material."
  - ☐ Consider SEC areas of focus including the "material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."
- ☐ File Form 8-K, Item 1.05 within four business days after a "materiality" decision.
- ☐ Does delayed notification apply?

  Note: If the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing, notification may be delayed.

[1] *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

7. Consider Other Notification Standards and Requirements.

- ☐ Confirm whether the cybersecurity incident may trigger other federal or state notification laws and requirements.

  Examples may include notification to: State Attorney Generals, individuals, the Federal Trade Commission, the Health and Human Services for the Office for Civil Rights (for Health Insurance Portability and Accountability Act (HIPAA) data), the New York Department of Financial Services, among others.

- ☐ Consider whether any contractual notification obligations apply (based on contract terms).

8. Address Customer and Public Relations and External Messaging.

- ☐ Coordinate customer notifications and updates.
- ☐ Develop public relation strategy.
- ☐ Consider employee notifications and updates, if applicable.
- ☐ Implement legal protections for guidance and strategy for customer and public relations.

9. Implement Disclosure Controls and Procedures.

- ☐ Implement governance and legal review of any notifications.
- ☐ Review **timeliness** for each notification.

  Note: Different deadlines may apply depending on the jurisdiction and applicable standards.

- ☐ Determine who is notified.
  - ☐ Federal regulators.
  - ☐ State regulators.
  - ☐ Individuals.

    Note: Some jurisdictions require regulator and individual notice at the same time, while others require regulator notice after individual notice.

- ☐ Review the **adequacy** and **accuracy** of the notification.
- ☐ Consider whether update notifications may be required based on the circumstances or new developments.

10. Anticipate and Prepare for Regulatory Review and Scrutiny.

- ☐ Demonstrate governance structure and process to manage cybersecurity risks.
- ☐ Show cybersecurity controls and policies are based on risk assessment to establish reasonable cybersecurity measures and system.
- ☐ Highlight remediation efforts have address root cause and vulnerabilities.

11. Anticipate and Prepare for Derivative & Shareholder Litigation.

- ☐ Review and collect board oversight documentation.
  - ☐ Board and senior management regular review of risks and security.
  - ☐ Cybersecurity briefings to the board.
  - ☐ Audit/risk committee reports.
  - ☐ Responses to prior audit findings.
  - ☐ Opinions given to directors.
  - ☐ Disclose risks and update risk factors as risks and security processes change.
- ☐ Assess governance posture at time of incident.

- ☐ Were there known weaknesses in cyber controls?
- ☐ Did the company follow its own written cybersecurity policies?
- ☐ Are statements about cybersecurity posture accurate?
- ☐ Assess the company's monitoring of cyber risk.

☐ Prepare a chronology of governance actions.

- ☐ Board minutes.
- ☐ Risk reports.
- ☐ Cybersecurity tabletop exercises.
- ☐ Results of internal audits.

12. Anticipate and Develop Litigation Strategy.

☐ Develop forensic and case narrative based on facts and incident.

☐ Assess exposure and anticipate claims and defenses based on forensics, vulnerabilities, remediation and privileged internal investigation including for:

- ☐ Consumer class actions.
- ☐ Shareholder derivative suits.
- ☐ Securities class actions.
- ☐ Contractual indemnity claims.
- ☐ Cyber insurance disputes.

☐ Assess litigation focus and defense on the "reasonableness" of the company's cybersecurity practices **before** the incident.

☐ Assess damages, harm and lack of standing (no concrete injury).

☐ Protect privileged communications and work products, including forensic analyses and reports.

☐ Consider arbitration and class waivers, if applicable.

☐ Consider jurisdictional issues.

13. Constructive Lessons and View to the Future.

☐ Following the incident, consider under attorney-client privilege key areas to address and enhance security and preventative measures.

☐ Consider how the company and employees can constructively learn from the incident and reinforce cybersecurity.

Note: *This checklist is a general tool for issue-spotting and considering key issues. The checklist does not constitute legal advice, and users should obtain legal guidance based on the particular facts and circumstances to assess the potential impact of using specific tools in specific situations.*