New York Department of Financial Services Cybersecurity Regulation

pillsbury

Incident Response and Notification Checklist

In responding to a Cybersecurity Incident and determining security and notification issues, consider the following steps:

1. Did a "Cybersecurity Incident" occur?

- Have you notified another government or regulatory agency (such as a state attorney general or the SEC, FTC, HHS Office for Civil Rights)?
- Does the incident have "a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity"?
- Was ransomware deployed "within a material part of the" information systems?
- Factors
  - Forensic assessment
  - Scope
  - What information systems were accessed?
  - What information was accessed or acquired or impacted?
  - Assess harm.
  - Was incident contained?
  - When was determination made triggering the notification clock?

2. Implement Written Incident Response and 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 and Restore Security

- Depending on the incident, consider appropriate steps such as:
  - Disabling user accounts, installing patches, changing passwords among other tailored steps to contain and mitigate the incident.
- Analyze root cause.

4. Attorney Client Privilege

As soon as a potential cybersecurity incident is anticipated, confirm legal protections are in place to receive legal guidance on cyber investigation, notification, regulatory inquires and potential litigation.

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. Did the Cybersecurity Incident Impact the Covered Entity, Affiliate and/or Third-Party Service Provider?

- Since the November 2023 amendment, notification extends to "cybersecurity Incidents" at Affiliates and Third Party Service Providers.
  - An "Affiliate" is "any person that controls, is controlled by or is under common control with another person."
  - A "Third-Party Service Provider "maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity."

7. Notification Timing

- Cybersecurity Incident
  - Notification of a cybersecurity incident is required "as promptly as possible but in no event later than **72 hours** after determining that a cybersecurity incident has occurred."
  - The "determination" typically involves legal guidance based on forensic facts.

— Examples:

- Whether an incident has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity," normally requires a forensic understanding of what happened with a legal assessment on whether the Cybersecurity Incident meets the double "materiality" standard.
- Whether the incident results "in the deployment of ransomware within a material part of the covered entity's information systems."

- Ransomware and Extortion Payments
  - — Determine whether the incident resulted "in the deployment of ransomware within a material part of the covered entity's information systems"?
  - — Was an "extortion payment" made?
    - Notice is required "within **24 hours** of the extortion payment."
    - Provide "a written description of the reasons payment was necessary" within "**30 days** of the extortion payment."
    - Consider other "applicable rules and regulations" such as the Office of Foreign Assets Control.

8. Online Notification

- If notification is required, use the DFS Portal and website form.
- Save a copy of the DFS confirmation email and receipt number, for your records.

9. Other Notifications

- Determine whether other notifications may be required based on other statutory, regulatory or contractual requirements.
  - — Consider other applicable statutes such as the SHIELD ACT, General Business Law Section 899-aa.
  - — Consider other statutes and regulators (such as state attorneys general if there was breach of PII)
  - — Consider individual notifications.
  - — Review contractual obligations.

10. Customer and Public Relations and External Messaging

- Consider customer notifications and updates.
- Consider employee notifications and updates.
- Address public relation issues, as needed.

11. Consider Potential Regulatory and Litigation Issues to be Mitigated and Avoided

- Can you anticipate potential areas of regulatory inquiry?
- What issues can be remediated?
- Do indemnification terms apply?
- Consult with litigation counsel on potential claims.

12. Criminal Law Enforcement Referral

- In appropriate cases, consider whether there is sufficient evidence for criminal enforcement.
- Consider what jurisdictions may apply based on unauthorized access and transmissions.
- Do you have forensically sound images of the relevant data?

Mark Krotoski
Cyber Disputes Leader
+1.650.233.4021
mark.krotoski@pillsburylaw.com
Former National Coordinator for the Computer Hacking and Intellectual Property Program in the Department of Justice

Brian Montgomery
Consumer Finance Leader
+1.212.858.1238
brian.montgomery@pillsburylaw.com
Former NYDFS Deputy Superintendent