CYBERSECURITY AND INCIDENT PREPAREDNESS

Presented by:
Melissa Crespo, *Of Counsel,* Morrison & Foerster LLP
Andrew Sczygielski, *Special Agent ,* Federal Bureau of Investigation

Health Care Compliance Association - 2020 Ann Arbor Regional Conference
June 12, 2020

0

Agenda

1

1

CYBER THREATS AND RISKS

2

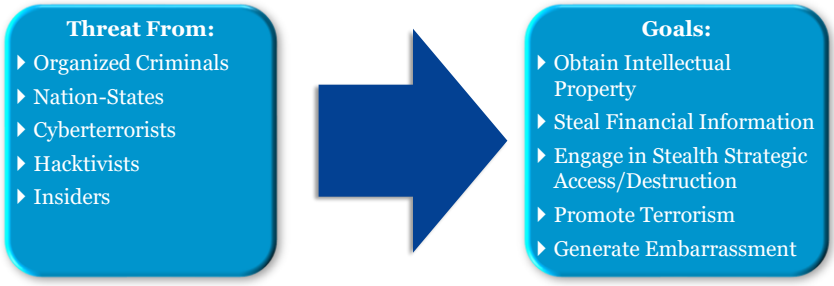
The Operating Environment

- Cyber intrusions and information security incidents are increasing in size and scope
- There is growing international, federal, and state regulatory scrutiny regarding how companies disclose cyber risks and incidents to their customers, shareholders, and the government
- More countries are adopting and enforcing data breach laws
- More countries are adopting laws imposing specific security obligations
- Cybersecurity has become a top-of-mind issue in boardrooms and C-suites in the United States and, increasingly, in other countries

3

3

Understanding Cyber Risks



4

4

Threats Targeting the Health Care Industry

External Cyber Threats

- COVID-19 Frauds/Scams/Intrusions
- Ransomware
- Business Email Compromise (BEC)
- Nation State Actors (Advanced Persistent Threats)

5

5

What Are Regulators Doing?

- Encouraging the reporting of cyber incidents
  - **FTC** – "In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated." ("If the FTC comes to call," May 20, 2015)
  - **SEC** – "Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." ("CF Disclosure Guidance: Topic No. 2, Cybersecurity," October 13, 2011)
    - SEC rule on material false statements (Rule 10b-5, 17 CFR 240.10b-5)
  - **Outside the US**, still making examples of companies following a breach

6

6

What is Law Enforcement Doing?

- FBI Public-Private Partnerships
  - InfraGard (www.infragard.org)
  - PINs & Flashes
- Cyber Task Forces
  - 56 Field Offices
  - Federal, State, Local
- FBI Cywatch
  - cywatch@fbi.gov
- Investigations & Victim Notifications

7

7

Ramifications for US Companies

Regulatory Enforcement

- State AGs
- OCR (HIPAA)
- FTC
- SEC

Litigation and Business Impact

- Consumer class actions
- Shareholder litigation
- Breach of contract
- Indemnifications
- Customer/client loss
- Management time handling internal investigations

Other

- Negative PR
- Consumer/client trust and brand reputation
- Extended oversight regulators
- Cyber insurance
- Costs (internal resources, credit monitoring, call centers, forensic experts, legal counsel)

8

8

9

What Can You Do?

- Governance and oversight
- Cyber risk management
- Incident-response preparedness

What Can You Do?

- Understand what information you have and how you protect it
- Create a governance structure that includes senior stakeholders who are relevant to governing information
- Create a framework that protects your highly valuable information
- Use industry standard technical controls (encryption, network segmentation, strong password management, remote access)
- Make systematic behavioral changes to how information is collected and protected (imbed privacy and data security into the culture)
- Be evaluated by a third-party assessor (under privilege)
- Prepare to respond to a security incident (prepare cross-functional plan, train on it, and practice)

What Can You Do? – FBI Guidance

- **Build a culture of awareness and security**
  - Provide Training for Employees
- **Establish Security Policies….then prioritize**
- **Prepare**
  - Include Law Enforcement notice in your Incident Response Plan
- **Monitor and Analyze Network Traffic**
- **Contact the FBI or file a complaint with www.IC3.gov**

12

12

Incident Response Plan

The cornerstone of any company's cyber preparedness and response

Key components

- Outline process for detecting, responding to, and recovering from cyber security incidents
- Establishes key roles and responsibilities
- Establishes incident priority levels and categories
- Key contacts and contact information
- Overview of legal obligations

13

13

Incident Response Plan *cont.*

- Update regularly based on the current threat environment
- Ensure that it includes a list of key contacts and contact information, and that you have a printed copy in case the breach impacts your company's electronic system

- **Practice it!**
  - Operational leaders should participate in table top exercises to establish clear working relationships and decision-making paths:
    - Who will make the crucial decisions?
    - Who must be consulted?
  - Tabletop serves as a training vehicle and brings together the core members of the response team (IT, HR, compliance, legal, communications) to practice working together

14

15

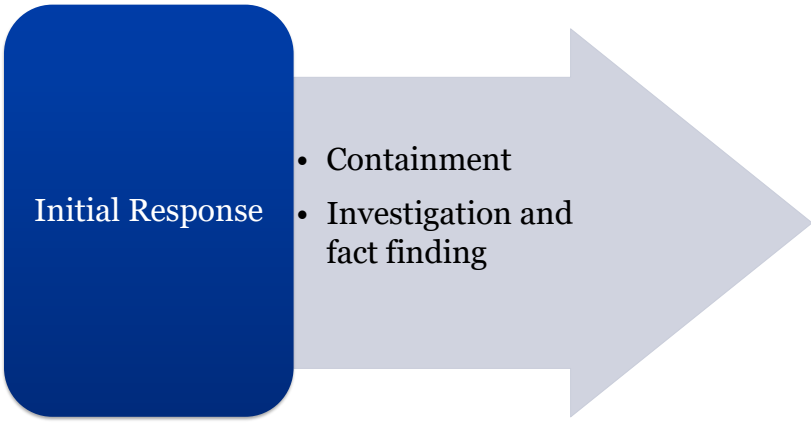
Incident Discovery

- Companies may learn about incidents in various ways
  - Incident response team identifying anomalous activity that involves company information or computer systems that process, handle or store company Information;
  - An employee observing a potential compromise of company information or reporting to the IT Service/Help Desk a lost or stolen device or other type of inadvertent disclosure;
  - An email with an attachment containing personal information is sent to the wrong email recipient;
  - External parties such as law enforcement, customers, suppliers or vendors contacting the company, or potential issues publicly reported in the press; or
  - The discovery of possible employee misconduct relating to company information.

16

16

Initial Response



17

17

Key Questions

- When did the incident start and how was it discovered?
- What systems or devices were involved?
- How did the potential exposure of the data occur? Was it lost, is it missing, or was it stolen? Did the bad actor gain access to the information or remove any of the information (i.e., exfiltrate the data)?
- What type of information was involved?
  - Was personal information involved?
- Is there evidence that information has been misused or likely will be misused?
- What are the principal risks to the business and how can these be mitigated?

18

18

Role of Law Enforcement

- Communicate with victim's Security Team
  - CISO, Director of Technology, Legal, etc.
- Law enforcement will ask for preserved evidence
  - Or, ask for consent to extract digital evidence
  - Or, ask for the incident report
- In some instances, provide indicators of compromise to aid in defending network
- Investigate

19

19

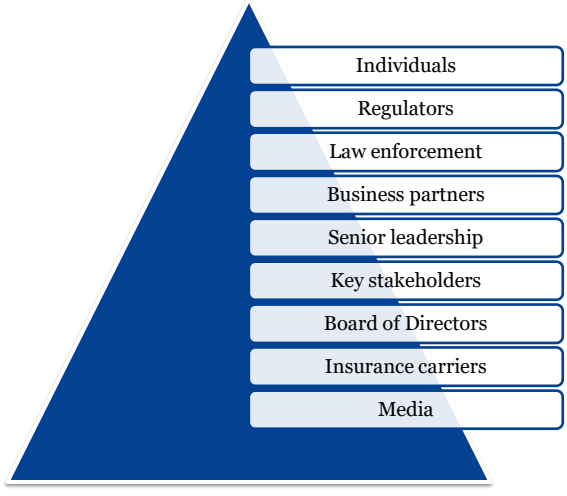
Key Considerations

- Creating a chronology
- Evidence preservation
- Engaging third parties
- Maintaining privilege
- Preliminary notification decisions

20

20

Communication and Notification Considerations



21

21

After an Incident

- Continue to monitor & assess vulnerabilities
- Maintain law enforcement contacts
- Build up resilience
- Train employees & executive teams

22

22

Q&A

23

23