Cyber Threats to Healthcare: Mitigating the Risk

Sean B. Hoar
Partner & Chair, Data Privacy & Cybersecurity
Lewis Brisbois Bisgaard & Smith LLP

EXPLORE
HEALTHCARE SUMMIT

Overview of Discussion

The discussion will involve an overview of the following:

The most dangerous online threats
Dark web marketplace
HIPAA Breach Notification Rule
State and federal regulatory environment
Ransom payment considerations
Ransom payment regulatory environment
Measures for mitigating risk
Resources

Along the way, please feel free to ask questions as they arise!

Extortionate Threats: Theft, Destruction & Disclosure of Data

Full-scale extortionate criminal business models:

- Business development: investors, franchising, Ransomware as a Service;
- Research and development: continuous evolution of exploits;
- Marketing and communications: press releases, shaming sites, outreach to leverage payment; and
- Accounts receivable/collections: aggressive communication, threats, and secondary attacks.

Effective execution of attacks:

- Thorough, persistent, patient **reconnaissance**;
- **High value targets**: managed service providers and critical supply chain providers;
- **Expertise** with multiple attack vectors: phishing, RDP, perimeter devices, and unpatched vulnerabilities; and
- Customized malware and **legitimate applications** used for malicious purposes.

Sophisticated attacks:

- **Extortionate encryption/exfiltration attacks**: Deletion of backup data, theft of sensitive data before encryption of core apps and networks, or "invisible" attack with subsequent extortion;
- **Extortionate email compromises**: theft of sensitive data from OneDrive and SharePoint; and
- **Email compromises** to gain secondary access to funds through fraudulent wire and ACH transfers, direct deposit redirects, and theft of W-2 images.

Continuously evolving threats require continuously evolving defenses

The Dark Web … A Complex Cyber Underground Where Criminals, Working in Syndicates or Individually, Buy and Sell Services

Online Forums: Criminals operate through a variety of online forums used to buy and/or sell products and services.

Bullet Proof Hosting: Criminals provide a vital infrastructure (including by operating dedicated servers and domains) to host malicious websites, malware, botnet command and control stations, VPNs and proxies.

Data Monetization: Criminals utilize the dark web for sensitive data sales.

Coding Services: Criminals customize malware, tailoring it to impact specific targets and improve its ability to bypass anti-fraud mechanisms.

Anti-Virus Checking Services: Criminals run malware through numerous anti-virus products to maximize infection rates.

Exploit Kits: Criminals utilize a variety of tools to identify and exploit vulnerabilities on victim systems.

Anonymization: Criminals employ means to communicate securely and to receive payment through untraceable systems (i.e. digital currencies).

The Regulatory Environment – HIPAA Breach Notification Rule

HIPAA Breach Notification Rule

Consumer notification:

- Covered entities must notify affected individuals following discovery of a breach of unsecured PHI.
- Notice must be provided:
  - in written form by first-class mail or
  - by e-mail if the affected individual has agreed to receive such notices electronically.
- If the covered entity has insufficient contact information for 10 or more individuals, substitute individual notice must be provided by:
  - posting the notice on the home page of its web site for at least 90 days or
  - providing the notice in major print or broadcast media where affected individuals likely reside.
- The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
- If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, by telephone, or other means.

The Regulatory Environment – HIPAA Breach Notification Rule

HIPAA Breach Notification Rule

Consumer notification:

- must be provided without unreasonable delay and no later than 60 days following discovery of a breach;

Notification must include, to the extent possible:

- a brief description of the breach,
- a description of the types of information involved in the breach,
- steps affected individuals should take to protect themselves from potential harm,
- a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, and
- contact information for the covered entity (or business associate, as applicable).

The Regulatory Environment – HIPAA Breach Notification Rule

HIPAA Breach Notification Rule

Media notification:

- When more than 500 residents of a State or jurisdiction are affected:
  - Notice must also be provided to prominent media outlets serving the State or jurisdiction;
  - The media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach; and
  - media notice must include the same information required for the individual notice.

HHS/OCR notification:

- In addition to notifying affected individuals and media, the Secretary of HHS/OCR must be notified
  - Via the HHS web site by submission of a breach report form.
- If a breach affects 500 or more individuals, the Secretary of HHS/OCR must be notified without unreasonable delay and no later than 60 days following a breach.
- If a breach affects fewer than 500 individuals, the Secretary of HHS/OCR must be notified of such breaches on an annual basis.
  - Reports of breaches affecting fewer than 500 individuals are due no later than 60 days after the end of the calendar year in which the breaches are discovered.

The Regulatory Environment – HIPAA Breach Notification Rule

HIPAA Breach Notification Rule

Definition of Breach:

- An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- Presumed to be a breach unless it is demonstrated that there is a low probability that PHI has been compromised based on a risk assessment of at least the following four (4) factors:
  1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  2. The unauthorized person who used the protected health information or to whom the disclosure was made;
  3. Whether the protected health information was actually acquired or viewed; and
  4. The extent to which the risk to the protected health information has been mitigated.
- There are three (3) exceptions to the definition of “breach:”
  1. Unintentional acquisition, access, or use of PHI by authorized person if such acquisition, access, or use was made in good faith and within the scope of authority.
  2. Inadvertent disclosure of PHI by authorized person to another authorized person, and PHI is not further used or disclosed impermissibly.
  3. The unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the PHI.

The Regulatory Environment – Increasingly Monitored Consumer and Regulatory Notification

State Regulations

- **Operations budgets - funded by assessments**
  - Increasing number of state attorneys general involved in process
- **50 state data breach notification statutes** – All cover electronic, 10 also cover paper
  - Notification of consumers
  - Expanding definition of personal information
  - Required timing and content of notification
  - Notification of regulators
- **State Data Privacy Legislation**
  - CCPA and many similar enactments
- **State Information security standards**
- **State Insurance Information Security Standards (NAIC laws)**

Federal Regulations and "Guidance"

- **GLBA; SEC; FinCEN, OFAC, etc.**

Industry Regulations

- **PCI DSS**

Ransomware - To Pay or Not To Pay

Ransom payment considerations - typically two primary reasons:

- Decryption tool necessary to decrypt mission critical data; and/or
- Preventing disclosure of highly sensitive information necessary to prevent substantial reputational harm.

If ransom payment is being considered:

- Who must be involved in decision making?
- What is likelihood malicious actors will keep their word?
- Can terms be negotiated?
  - Amount;
  - Data to be deleted;
  - Proof of data deletion;
  - Receipt of stolen data;
  - Promise to not post data.
- What is likelihood that decryption key will decrypt all the data?
- How long will it take to decrypt the data?
- What is the risk that entity will become a bigger target for extortion?
- What regulatory issues are to be considered?

The Regulatory Environment – Increasingly Aggressive Ransomware Payment Regulatory Notification

Regulation of digital currency used in ransom payments

- **Federal regulatory agencies**
  - **Office of Foreign Asset Control (OFAC)**
    - Increasingly aggressive guidance
  - **Financial Crimes Enforcement Network (FinCEN)**
    - Increasingly aggressive enforcement
- **Increasing federal law enforcement presence**
  - Federal Bureau of Investigation (FBI)
  - United States Secret Service (USSS)
  - Department of Homeland Security (DHS)
    - Cybersecurity and Infrastructure Security Agency (CISA)
  - Securities and Exchange Commission (SEC)

The Constant Battle - Mitigating the Risk

Measures for Mitigating Cyber Risk

- Develop **preventive cybersecurity measures**
  - Layered defense for email platform, network, major applications and hosted data
  - Key components
    - Multi-factor authentication for email platform, network and major applications
    - Heuristic-based endpoint detection and response tool for all endpoints
- Identify **risk transfer options** in contracts
- Develop **comprehensive data backup and restoration system**
  - Identify essential data to backup
  - Identify type, location, frequency and process of backups
  - Identify retention timeframe for backup data
  - Air gap one copy of backup data
- Develop or revise **incident response plan**
- Test incident response plan through **tabletop exercises**
- Establish a **culture of security** – develop a human firewall
- Know the **resources available through cyber insurance policy**

Lewis Brisbois Free Resources For Risk Managers

- Resources for information technology and security personnel, risk management personnel, brokers, and cyber insurance claims counsel and underwriters:
  - **Digital Insights Blog** (subscribe online)
  - **Digital Insights Quarterly Newsletter** (subscribe online)
  - **Quarterly Cybersecurity Webinars**
  - **Interactive Maps**:
    - Data breach notification statute maps
    - Information security standards
    - Data privacy statute summaries
  - **Data Privacy & Cybersecurity Handbook** (subscribe online)
- **24/7 Telephonic Hotline: 844.312.3961**
- **24/7 Email Hotline:** breachresponse@lewisbrisbois.com

Questions?

Sean Hoar, CISSP, GISP, CIPP/US, is a Partner and Chair of Lewis Brisbois' national Data Privacy & Cybersecurity Practice. Sean has extensive experience managing responses to digital crises, and the Lewis Brisbois Rapid Response Team has managed thousands of data security incidents. While managing the national Data Privacy & Cybersecurity Team, Sean manages responses to complex data breaches and facilitates executive briefings and tabletop exercises.

Sean served as the lead cyber attorney for the U.S. Attorney's Office in Oregon, and worked closely with the Computer Crime & Intellectual Property Section in Washington D.C. He holds the Certified Information Systems Security Professional (CISSP), the Global Information Security Professional (GISP), and the Certified Information Privacy Professional/United States (CIPP/US) credentials. He taught courses in cybercrime at the University of Oregon School of Law and the Lewis & Clark Law School, and he serves as the Executive Director of the Financial Crimes & Digital Evidence Foundation.

Sean B. Hoar
Partner, CISSP, CIPP/US
Lewis Brisbois Bisgaard & Smith LLP
Sean.Hoar@lewisbrisbois.com
503.459.7707