ECKERT SEAMANS

PREPARING FOR THE INEVITABLE: CYBER SECURITY ISSUES SURROUNDING RESPONDING TO RANSOMWARE ATTACKS

Presented by:

Matthew H. Meade
Member

Eckert Seamans Cherin & Mellott, LLC
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

412.566.6983
mmeade@eckertseamans.com

PITTSBURGH, PENNSYLVANIA
600 Grant St.
44th Floor
Pittsburgh, PA 15219
P: 412.566.6983
F: 412.566.6099
mmeade@eckertseamans.com

Matthew H. Meade

MEMBER
CHAIR, CYBERSECURITY, DATA PROTECTION & PRIVACY

Matt Meade concentrates his practice in the area of data security providing advice to clients regarding data breaches, information and records management, and other areas concerning data security. Matt helps clients identify business risks associated with the use and storage of sensitive information. He regularly guides clients through security incident investigations, analysis, communications, and, if necessary, responding to regulatory inquiries and litigation. He advises clients on security breach notification laws and other U.S. state and federal data security requirements (including laws regarding disposal of records). Matt drafts agreements addressing issues related to data use, privacy, and security. He also prepares document retention and management policies and develops associated training programs.

Matt speaks and writes regularly on data security matters and serves on The Sedona Conference Working Group Series Leadership Council, after previously serving on the Steering Committee for Working Group II on Data Security and Privacy, through which lawyers, judges, policy makers, security experts, technologists, and business leaders work together to identify and develop principles and best practices to constructively resolve issues surrounding data security and privacy liability. Matt has served as a Co-Chair of the ABA's First, Second, and Third Annual National Cybersecurity Institute (2016-2018).

PRACTICE AREAS:

Cybersecurity, Data Protection & Privacy

Business Counseling

Artificial Intelligence, Robotics, and Autonomous Transportation Systems

Infrastructure

STATE ADMISSIONS:

Pennsylvania

New York

New Jersey

EDUCATION:

J.D., Fordham University School of Law, 1992; Editor-in-Chief, Fordham Moot Court Board

B.A., Yale University, 1987; Casner Prize for Outstanding Achievement; Moriarty Prize; Kiphuth Scholar

REPRESENTATIVE MATTERS

- Advised numerous entitles, including healthcare providers, manufacturers, retailers, schools, financial services companies, county governments and collection agency on information security breach notification procedures and development of post breach corrective action plans.
- Coordinated response to multi-state security breaches, ransomware, and hacking incidents with local and federal law enforcement, and United States Attorney.
- Performed comprehensive review and subsequent revisions of all security policies for leading hospitality provider and then provided data security training to managers and executives on subjects covered in policies.
- On behalf of a healthcare automation solutions provider, obtained dismissal of claims arising from the theft of an employee's laptop computer containing protected health

information, on grounds that court lacked subject matter jurisdiction because plaintiff failed to adequately allege injury-in-fact.

- Conducted employee cyber training sessions in hospitality, education, healthcare, manufacturing, insurance, and financial sectors.
- Organized, ran, and oversaw tabletop mock data breach scenarios for multiple organizations including universities, energy companies, banks, insurance companies, and healthcare organizations.
- Developed cyber training for board of directors of community bank and manufacturing company.
- Conducted comprehensive review of security implications of agent agreements for provider of homeowner's insurance.
- Prepared and reviewed company security policies including Written Information Security Programs, document management, and incident response plans.
- Coordinated internal investigations of healthcare data breaches, subsequent patient notice, communication with the Department of Health & Human Services Office of Civil Rights ("OCR") and development of corrective steps. OCR closed the case taking no further action and noting the voluntary compliance efforts of the entity.
- Prepared and reviewed company policies including Written Information Security Programs, document management, social networking and incident response.
- Conducted internal investigation of processes and procedures of professional sports league, including analysis of discipline by league of teams, coaches and players, and of document management policy.
- Conducted an internal investigation of a large-scale data leak of personnel information at a Fortune 100 Corporation; interviewing relevant employees and preparing a report and recommendations for the Executive Board.
- Advised clients on proper security measures in connection with employee and customer personal information.

PROFESSIONAL AFFILIATIONS

- Pennsylvania Bar Association
- New York Bar Association
- American Bar Association National Institute on Cybersecurity, Co-Chair
- The Sedona Conference Working Group Series Leadership Council, Member
- The Sedona Conference Working Group 11 on Data Security and Privacy Liability
    - Leader of Model Data Breach Notification Law Brainstorming Group
    - Former Steering Committee Member
- Carnegie Mellon University CISO-Executive Program, Faculty Member

COMMUNITY INVOLVEMENT

- Children's Museum of Pittsburgh, Board Member
- Chuck Cooper Foundation, Vice President and Board Member
- Yale Day of Service, Co-Chair

AWARDS AND RECOGNITION

- Selected for inclusion in The Best Lawyers in America – Privacy and Data Security Law (2017 – 2024) and Commercial Litigation (2015 – 2021, 2023-2024)

NEWS AND INSIGHTS

PUBLICATIONS

- "State Privacy Bingo," Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, August 2023.
- "New Privacy Civil Litigation Trends in the United States," Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, June 28, 2023.
- "Proposed SEC Cybersecurity Risk Governance Rules for Public Companies," Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, June 27, 2023.
- "The New Colorado and California Privacy Regulations Are Finalized: How Do They Compare?" Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, April 25, 2023.
- "Final NYC Rules on the Use of Automated Employment Decision Tools Published – Enforcement Delayed until July 5, 2023," Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, April 25, 2023.
- "U.S. Department of Treasury Reports Highlights Pitfalls of Using Cloud Platforms: Treasury Sets Up New Interagency Cloud Services Steering Committee," Eckert Seamans' Cybersecurity, Data Protection & Privacy Update, February 2023.
- "Massachusetts Gaming Commission Issues Emergency Privacy and Security Regulations on the Gaming and Sports Betting Industry," Eckert Seamans' Legal Update, February 13, 2023.
- "Joint Cybersecurity Advisory issued by FBI, FDA OCI, and USDA Warns Food & Agriculture Sector About Increase in Business Email Compromise Scams to Divert Shipments of Food Products," co-author, Eckert Seamans Data Privacy & Security Update, December 2022.
- "DHS's Cybersecurity and Infrastructure Security Agency Seeking Guidance on Critical Infrastructure Cyber Reporting," Eckert Seamans' Data Security & Privacy Alert, October 2022, also appeared in the Fall 2022 Construction Law Update.
- "Pennsylvania Amends its Breach of Personal Information Notification Act," Eckert Seamans' Data Privacy & Security Update, November 2022.
- "Incident Response Plan – An Indispensable Tool for Cyber Preparedness," published in The Authority, a publication of the Pennsylvania Municipal Authorities Association, October 2022.

- "FBI Tips to Protect Against Cyber Threats to Medical Devices," co-author, Eckert Seamans' Data Security & Privacy Alert, September 2022.
- "Updated Joint Guidance on the Application of FERPA and HIPAA to Student Health Records," Eckert Seamans' Data Security & Privacy Alert, February 2020.

MEDIA COVERAGE

- "When poor vendor vetting leads to exposed health data," The Parallax View, May 7, 2021.
- Radio interview with Lynn Hayes-Freeland about Cyber Monday: 7 tips for safer online shopping, 1020 KDKA, December 2, 2019.
- "Eckert Seamans Hires Buchanan Ingersoll Cybersecurity Vet," Law360, September 2018.
- "Lessons and Trends from FTC's 2017 Privacy and Data Security Update: Workshops and Guidance (Part Two of Two)," The Cybersecurity Law Report, February 2018.
- "Lessons and Trends from FTC's 2017 Privacy and Data Security Update: Enforcement Actions (Part One of Two)," The Cybersecurity Law Report, January 2018.

SPEAKING ENGAGEMENTS

- "The Sedona Conference Commentary on Proposed Model Data Breach Notification Law," webinar moderator, July 2023.
- "Breach Coach: Working with Outside Counsel," presented at the *Data Breaches: A Primer for County Attorneys* program co-sponsored by Minnesota Counties Intergovernmental Trust and Minnesota County Attorneys Association, March 2023.
- "Preparing for the Inevitable: A Practical Guide to Cyber Incident Response," presented to the Idaho Association of Counties 2022 Annual Conference in Downtown Boise, September 2022.
- "The GDPR in Higher Education," webinar presentation with the National Cyber Forensics & Training Alliance to colleges and universities across the Commonwealth of Pennsylvania, December 2021.
- "Is Cyber Insurance Coverage Holding Local Government Ransom?" panel presenter to the National Association of Counties, October 2021.
- "Legal Issues Associated with Responding to and Remediating a Cyber Attack," also presented "Interactive Cyber Incident Exercises" for the County Commissioners Association of Pennsylvania program, *KEYS: The Anatomy of a Cyber Claim*, May 2021.
- "Practice Makes Perfect: A Proactive Approach to Cybersecurity," presenter, Eckert Seamans' Legal Primer Series (Part 1), April 14, 2021. (recording)
- "Executive Roundtable on Regulations and Privacy," panelist, Converge20, October 2020.
- "Model data breach notification law," panelist, The Sedona Conference Working Group 11 Midyear Meeting 2020, September 2020.
- "Privacy Update," Pennsylvania Bar Institute Cyberlaw Update 2020, September 2020.

- “Anatomy of a Data Breach,” panelist, TextIQ’s The Inevitable 2020 webinar series, September 2020.
- “Data Breach Scenario Panel” Moderator and panel presenter at the 2019 Cyber Law and Privacy Symposium, Hosted by Carnegie Mellon University, May 2019.
- “News You Can Use: A review of recent judicial, legislative, and regulatory developments of significance to employers,” co-presented at Eckert Seamans’ Human Resources Forum, April 2019.
- “The Net without Neutrality: Economic, Regulatory, and Informational Access Impacts,” co-presenter, University of Pittsburgh Law Review 80th Publishing Anniversary Symposium, March 2019.
- “Cybersecurity: An Analysis of the Legal Landscape and Best Practices,” presenter, Eckert Seamans’ Continuing Legal Education Seminar, August 2018.
- “Interactive Breach Scenarios,” presented at the NetDiligence Cyber Risk Summit, June 2018.
- “Practice Makes Perfect: A Proactive Approach to Cybersecurity in an Interconnected Hotel Industry” presented at the Hotel & Lodging Legal Summit at Georgetown University Law Center, October 2017.
- “Cybersecurity: There ARE Things Lawyers Can and Should Do,” CLE presentation, October 2017.
- “You’ve Got Hacked: How to protect yourself against campaign data security dangers and liabilities,” panel presentation at the American Association of Political Consultants’ 2017 Annual Pollie Awards & Conference, March 2017.

Preparing for the Inevitable: Cybersecurity Issues Surrounding Responding to Ransomware Attacks

www.eckertseamans.com

Matt Meade | August 24, 2023

ECKERT SEAMANS ATTORNEYS AT LAW

1

What Keeps Us Up at Night?

CYBERSECURITY!

ECKERT SEAMANS ATTORNEYS AT LAW

www.eckertseamans.com

2

Why are We Up at Night?

Lost productivity

Ransomware

Reputational Damage

Fazio Mechanical

Job Security

FINANCIAL COSTS
(response, remediation)

LEGAL/REGULATORY ACTIONS

3

4

The Ransom Note

```
LockBit 2.0 Ransomware

Your data are stolen and encrypted

The data will be published on TOR website
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and
https://bigblog.at if you do not pay the ransom

You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at



Decryption ID: B2BCDXXXXXXXXXXXX93E181B2F29E710A
```


Ransomware Attack

On Monday, IT discovers that you have been the victim of a ransomware attack. As a result, all employees are locked out of their computers and unable to work. The bad actors are demanding payment of 10 bitcoin to provide the decryption key to restore the network.

There are robust backups from which the team believes it will be able to restore the data. For this reason, a decision is made not to pay the ransom.

Restoring from Backups

- What is the recovery time if restoring from your backups?
  - A. 1 hour
  - B. 1 day
  - C. 1 week
  - D. 2 weeks
  - E. Never
- Who is responsible for coordinating restoration?
- When did you last test recovering from backups?
- What is the most critical system to restore first?
- Should you notify cyber insurance carrier at this time?

Negotiating with the Threat Actor

- The threat actor sends 25 sample files to show that they have been in the network and mean business and threatens to publish all data on the Dark Web unless it is paid
- The files include sensitive information related to customers and employees.
- Some of the files contain employee PII.
- What is your priority at this time?
- Do you have any obligation to provide notice of a data breach at this time?

Action Steps

- Should you use the IT firm you have an ongoing support relationship with to conduct the forensic investigation?
- Why or why not?
- What is the amount that you are willing to pay to get the data back and prevent the release? Who decides?
- If you have cyber insurance what is the amount of ransom payment covered by the policy?

Negotiating with the Threat Actor

- In order to avoid reputational damage, you instruct the negotiator to offers the threat actor 2 bitcoin

Victim: We have seen what you have . . . 2 BITCOIN? Yes or no?

Extortionist: That is not enough. We think that you are not completely aware of the seriousness of the situation. In the event of a further delay, we will be able to use information resource https://continews.best and will start to sell you private data on the black markets.

We will publish the full dump of your data on our news website with 1,000 visitors per day, 50% of them are mass media reporters and regulators, the other part is blackhat hackers. We are not interested in this, and we gain nothing from data publication, that is why we are offer you a deal.

1) your customers data will be used by criminals

2) your ciustomers will fill lawsuit against you

3) government regulators will fine you for data breach, if you have in clients at least one EU resident then you will be also fined by EU government by GDPR law with millions of dollars of fine or permit ban for working with EU citizents. US has the similar laws, but they are not so costly, however the total cost will exceed the asked amount from you, so our offer is the best deal for you to resolve this issue.

Victim: We have no EU concerns. We are very aware of what you have. Most of the info, if not all, is available to the public. $2 Bitcoin?

If You Decide to Pay Ransom (Mechanics)

- Third Party negotiator typically handles all negotiations with threat actor
- Third party verifies that payment is not going to a country or group on US restricted list as required by recent OFAC advisory
- Proof of Life-Third Party negotiator provides threat actor with sample of encrypted files to prove that threat actor can decrypt
  - Encrypted files need to be generic. (Do not send file with PII in it)
- Payment in bitcoin is made by third party after receipt of funds from the client
- Third party makes bitcoin payment (there is typically an additional charge associated with facilitating the payment)

Investigation Continues

- What steps should IT take with respect to the 25 files?
- If you are able to identify the source of the files, what are the next steps?
- Would the source of the files impact the willingness to pay more to the threat actor? Why or why not?

Turning Up the Pressure

- Threat Actor becomes frustrated with pace of negotiations
- They start calling and emailing employees about what will happen if you do not pay ransom
- Employees flood HR with calls and are concerned
- How would you handle this?

Data Released

- The threat actor ultimately rejects the offer and publishes 20 GB of company data on the Dark Web
- The files on the Dark Web include:
  - Data subject to NDAs
  - Information provided in litigation subject to a confidentiality order
  - PII

Notifications

- What are your notification obligations with respect to the NDA, PII, and litigation?
- How would you determine this?
- Who would review records?
- Who would send notice?
- What would the notice to litigation parties say?

Media Contact

- While the ransomware event is happening, a prominent cyber reporter is visiting your offices to do a story on the company. She is unhappy to find out that computers and WIFI are down and overhears employees talking about ransomware.
- As part of her job the reporter also regularly monitors the dark web. She sees your data and wants a statement so she can break the story.
- What would you say to the media?
- What would you say to employees and customers?

Customer and Regulators

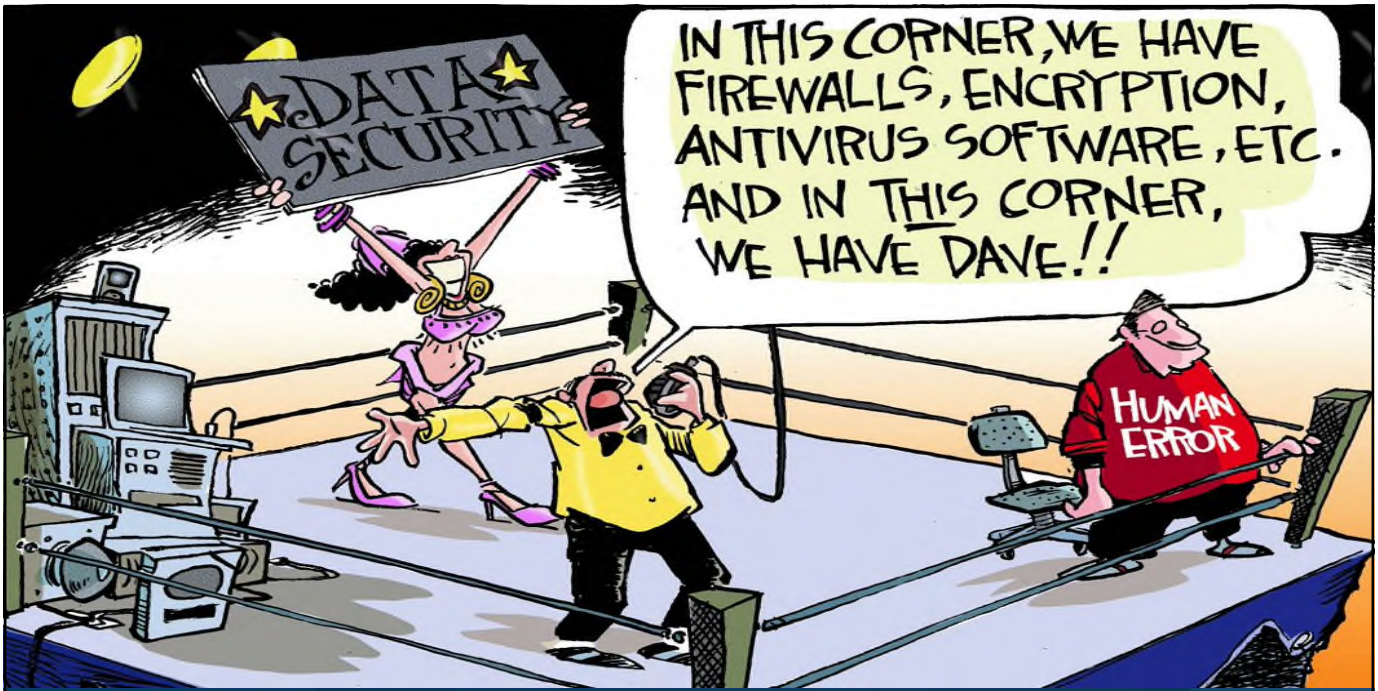
- Customers are starting to call with questions about the incident and the security of their data.
- The AG is calling and wants to know how the attack happened and why they was not told sooner.
- Employees are still unable to work and unsure how to respond to the calls.

More Questions

- Who is responsible for responding to the media inquiry?
- Who is responsible for providing the employees with talking points for handling calls? How will those talking points be distributed?
- Who is responsible for responding to the regulatory inquiry?

Takeaways

- Do you have an incident response plan?
- Do you have an incident response team?
- Have you done a tabletop exercise to test response capabilities?
- Do you have secure backups?
- What do your agreements require vendors with access to PII to do in the event of a cyber incident?



Questions?
Thank You!

www.eckertseamans.com

Matt Meade
mmeade@eckertseamans.com

ECKERT SEAMANS
ATTORNEYS AT LAW

21