Advising County Departments & Addressing Insurance Issues When Facing Cyberattacks

Meghan S. Ferally, Esq.

This page intentionally left blank

Advising County Departments and Addressing Insurance Issues When Facing a Cyberattack

May 20, 2025

1

Panelist:

- **Meghan S. Farally, Esq.**: Partner, Cipriani & Werner P.C.

2

Objective Understandings

- An overview of the various ways that a cybersecurity incident can impact an organization, their operations, and their business reputation.
- Identify measures that can be taken pre-incident to minimize the impact of a cybersecurity incident.
- Understanding the role that cybersecurity insurance can play in mitigating the financial impact on an organization arising from a cybersecurity incident.
- Highlighting regulatory and litigation costs associated with data breaches.

3

Why Should Cybersecurity Preparedness Be an Important Focus for your Organization?

- The costs associated with cybersecurity are growing every year.
  - It is not a matter of *if* your organization will be affected by a cyber attack, it is a matter of *when*.
  - In 2018 companies spent approximately $188B on cybersecurity, that number was estimated to grow to $215B in 2024.[1]
  - The total average cost to a company due to a data breach rose from $4.45M in 2023 to $4.88M in 2024 and is expected to continue to grow.[2]

[1] Stuart Madnick, *What's Behind the Increase in Data Breaches?,* WALL ST. J. (Mar. 14, 2024), https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c
[2] IBM Cost of a Data Breach Report 2024, https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

4

Why Should Cybersecurity Preparedness Be an Important Focus for your Organization?

- Organizations could be better prepared to respond to cybersecurity incidents.
  - 94% of business leaders are not confident in their ability to identify root causes of an attack.[4]
  - 46% of corporations are unable to contain a threat in less than 1 hour of initial compromise.[5]
    - Local government agencies are particularly vulnerable due to limited (or reduced) funding and resources.
    - Across all industry sectors, external Remote Access is the most prevalent attack vector for ransomware attacks; phishing is the most prevalent attack vector for email compromises.

[4] Red Canary State of Incident Response Report 2021, https://redcanary.com/resources/guides/the-state-of-incident-response-2021/
[5] Red Canary State of Incident Response Report 2021, https://redcanary.com/resources/guides/the-state-of-incident-response-2021/

5

Why Should Cybersecurity Preparedness be an Important Focus for your Organization?

- There was a 42% increase in reported Business Email Compromises (BEC) in 2024 compared to 2023.[6]
- Vendor Email Compromises (VEC) impacting supply chain communications to defraud business increased 66% in 2024.[7]
- The FBI reported that between October 2013 and December 2023 Business Email Compromises were attributable to $55.5 Billion in stolen funds.[8]

[5] H1 2024 Report Cybersecurity Trends & Insights, Perception Point https://info.perception-point.io/pdf-h1-report-2024?submissionGuid=d834959e-44e3-4832-b5d2-d45c16c378b8
[6] H1 2024 Report Cybersecurity Trends & Insights, Perception Point https://info.perception-point.io/pdf-h1-report-2024?submissionGuid=d834959e-44e3-4832-b5d2-d45c16c378b8
[7] FBI Alert Number: I-091124-PSA, FBI Internet Crime Complaint Center (IC3) | Business Email Compromise: The $55 Billion Scam

6

Mitigating Risk BEFORE an Incident: Insurance

- What type of insurance is available to organizations?
  - Cyber forensics
  - Breach Coach Coverage
  - Extortion Coverage
  - Funds Transfer Fraud Coverage
  - Litigation Coverage
  - Restoration and Recovery Services
  - Business interruption
  - Table Tops and pre-breach services

7

Mitigating Risk BEFORE an Incident: Have a Plan

- Put in place an Incident Response Plan & Incident Response Team.
- Have contracts and relationships in place with potential vendors before an incident occurs.
  - Legal Counsel
  - Cyber forensics Firms
  - Digital Restoration Services
  - Public Relations Firms

8

Mitigating Risk BEFORE an Incident: Minimizing Potential Risk

- How well do you know yourself?
  - Do you know your existing contractual obligations?
  - Do you know your regulator(s) and regulatory obligations?
- Conduct regular internal audits and reviews
  - What is your data retention policy? Is it being followed?
  - Are your systems up to date and patched?
  - Run through a tabletop with key team members to simulate your incident response preparedness.

9

You Think Something Happened: What Do You Do?

Contact your three biggest partners in a cybersecurity incident:

- Insurance
  - To assist in financial coverage for the incident response.
  - To connect the Company with appropriate counsel and cyber forensics.
- Counsel
  - To maintain privilege.
  - To ensure regulatory compliance.
  - To mitigate litigation and regulatory exposure.
- Cyberforensics
  - To secure the digital environment.
  - To identify the root cause of the incident.
  - To identify the extent of any unauthorized access or exfiltration of data.

10

Role of Counsel: Attorney-Client Privilege

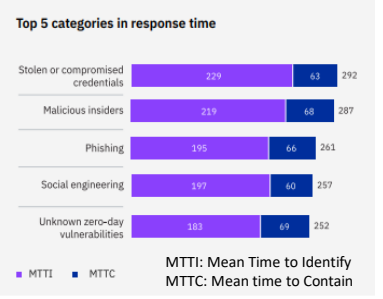
- What does privilege protect?
  - Attorney-client privilege.
  - Attorney work product privilege.
- When should legal counsel get involved? *Why?*
- What are limitations to attorney-client privilege during incident response?
  - Tri-party agreements and relationships with third parties.
  - Distinguishing post-incident activities for business purposes or for legal purposes.

11

You're the Victim of a Cybersecurity Incident: What Should You expect?

Responding to a cybersecurity incident is a marathon, not a sprint.

- 59% of impacted companies reported that it took over 4 months to fully recover from an incident.[9]



[9] IBM Cost of a Data Breach Report 2024, https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

12

What are your primary concerns after discovering a cybersecurity incident?

- Identifying and containing the threat
  - Are systems encrypted? If so, do you have valid backups?
  - Is there persistent access?
- Immediate business impact
  - What is the cost to the business if systems are encrypted?
  - What is the reputational damage if services are disrupted?
  - How long can your company afford to be offline or impacted by an incident?

13

What are your primary concerns after discovering a cybersecurity incident?

- Communication strategy
  - Transparency vs. Sensitivity
  - Pre-Approved internal and external communications
    - Role of Counsel in developing communications
    - Use in litigation
  - Identifying points of contact
    - Regulatory inquiries
    - Media Inquiries
    - Employee Inquiries

14

What are your primary concerns after discovering a cybersecurity incident?

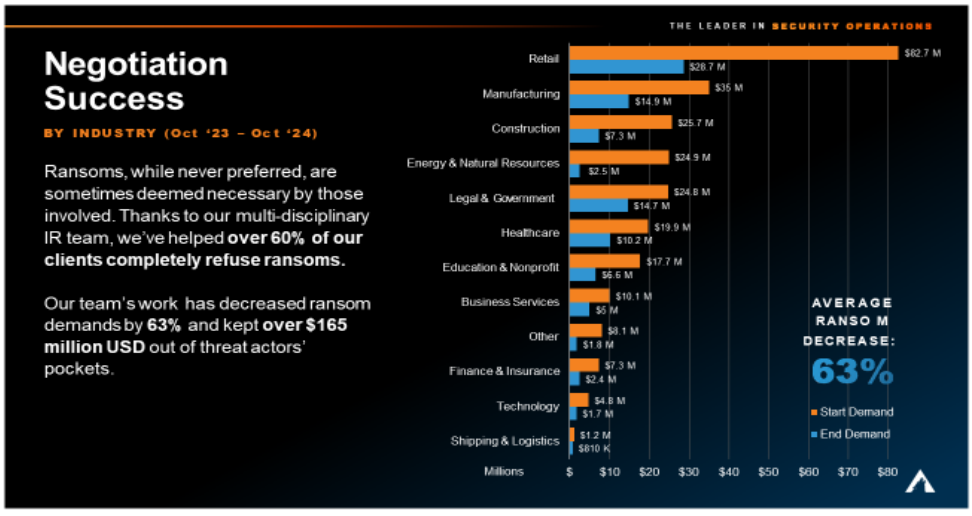
- Communication Strategy Cont.
  - Who are the stakeholders and what do they need to know?
    - Higher-Ups / Other Agencies
    - Employees
    - Clients
    - High Level Information
  - How do you want to communicate?
    - Use of out of band communication methods
    - Phone calls to key parties/stakeholders
    - Written communications may become evidence in a future litigation

15

Threat Actor Communications

- How can you communicate with a threat actor?
- Why would you communicate with a threat actor?
- Is it legal to pay a ransom? What are the considerations that should be made beforehand?
  - “Honor among thieves”
  - Some states (Florida and North Carolina) prohibit state agencies from paying ransom (or even communicating with the bad actors)>
- How are ransoms paid and what can you expect to get in return?

16



17

The Forensic Investigation

- Why is the forensic investigation important?
  - Identifying the root cause of the incident
  - Ensuring no ongoing persistent unauthorized activity
  - Identifying any data which was subject to unauthorized access or exfiltration
- How will a forensic investigation be referenced in a litigation down the line?
  - What should and should *not* be in a forensic report?

18

Sensitive Data has been impacted: Now What?

- You have a legal obligation to identify and notify individuals whose personal information has been impacted by an incident
- Internal review of impacted data to identify these individuals
- Engaging a data review vendor do manually review each potentially impacted document
  - Takes Time

19

Considerations to Assess Legal Obligations

- What are the potential jurisdictions impacted?
- State breach notification obligations
  - Timing and content considerations
  - Regulator vs individual
  - State sector specific
- Preservation of evidence as a mitigation tool
- Sector specific obligations
  - SEC
  - Payment Card Industry Standards
  - ABA Standard for Law Firms
  - State Departments of Insurance
  - Department of Finance
  - FERPA
  - HHS OCR

20

Data Breach Litigation Trends

- There is a significant increase in recent years in the quantity of lawsuits relating to data breaches.
  - The number of lawsuits mentioning 'data breach' increased from 296 in 2020 to 1,278 in 2023.[11]
  - Less than 5% of Data Breach Class actions go to trial. [12]

[10] Ransomware Attacks: Litigating a Growing Threat, Bloomberg Law https://assets.bbhub.io/bna/sites/18/2024/07/FINAL-1099107-BLAW-2024-Litigation-Data-Breach-Report.pdf

[11] What Boards Need to Know about Data breach Class Actions, Mark Henriques, Directors & Boards, https://www.directorsandboards.com/legal-and-regulatory/what-boards-need-to-know-about-data-breach-class-actions/#:~:text=Less%20than%205%25%20of%20class,a%20total%20loss%20is%20appealing.

21

Regulatory Fines & Consent Orders

- Attorney Generals individually and in coalition with other states can levy fines in relation to data breaches impacting residents of their states
  - 50 state coalition of Attorneys General agreed to a $52 Million settlement with a prominent hotel company over a data breach.[12]
  - NY AG and DFS Superintendent obtained an $11.3M in penalties from Auto Insurance Companies over Data Breaches.[13]
- Since Data Breach Laws are based on the current residency of the impacted individual, a company may be subject to regulatory investigations in many states at the same time resulting from one breach.

[12] Attorney General Platkin, Multistate Coalition Announce $52 Million Settlement for Marriott, Starwood Data Breaches https://www.njoag.gov/attorney-general-platkin-multistate-coalition-announce-52-million-settlement-for-marriott-starwood-data-breaches/

[13] Attorney General James and DFS Superintendent Harris Secure $11.3 Million from Auto Insurance Companies over Data Breaches https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20241125

22

Additional Considerations for Law Firms Experiencing a Data Breach

- 29% of law firms reported experiencing a form of security breach.[14]
- ABA Formal Opinion 483 addresses how law firms have an ethical obligation to notify current and or former client of a data breach due to a data breaches ability to impact:[15]

- Model Rule 1.1: Requires lawyers to "provide competent representation to a client,"
- Model Rule 1.4: Requires, that lawyers "keep the client reasonably informed about the status of the matter"
- Model Rule 1.6: Requires that lawyers "not reveal information relating to the representation of a client unless the client gives informed consent" and "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
- Model Rule 1.15: Requires lawyers to "appropriately safeguard" clients' documents and property.
- Model Rule 5.1: Requires that lawyers with "managerial authority in a law firm . . . make reasonable efforts to ensure that … all lawyers in the firm conform to the Rules of Professional Conduct."
- Model Rule 5.3: Requires that lawyers in supervisory capacities "make reasonable efforts to ensure that [any non-lawyer's] conduct is compatible with the professional obligations of the lawyer."

[14] 2023 ABA Cybersecurity TechReport https://www.americanbar.org/content/aba-cms-dotorg/en/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/

[15] ABA Formal Opinion 483, October 17, 2028, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf

23

Final Thoughts: Recommendations & Practical Tips

- Cybersecurity incidents impact companies in many different ways over a prolonged period of time
  - Understanding how your company may be impacted by an incident can allow you to better prepare and better mitigate the impact that a breach may have on your organization.

24

THANK YOU