BREACH RESPONSE PREPAREDNESS - PROACTIVE STRATEGIES IN MEETING REQUIREMENTS AND MITIGATING RISK

September 30, 2025

Amy S. Mushahwar

Partner and Chair, Data Privacy, Security, Safety & Risk Management

Lowenstein Sandler

David Meadows

Senior Managing Director

FTI Consulting

Grant Gendron

Senior Corporate Counsel

EchoStar Corporation

SPEAKERS

Amy S. Mushahwar

Partner and Chair, Data Privacy, Security, Safety & Risk Management

Lowenstein Sandler

David Meadows

Senior Managing Director

FTI Consulting

Grant Gendron

Senior Corporate Counsel,

EchoStar Corporation

Structure of Tabletop Scenario

- We will begin by presenting an initial set of hypothetical facts – these will facilitate the panel discussion.
- Time will be artificial in this exercise; an actual event would be longer than the hypothetical days noted here and typically tabletops are 3 to 6 hours, so even this artificial exercise is compressed.
- After working through initial hypothetical facts, we will present hypothetical developments designed to advance the scenario and present further discussion points.
- Participants are encouraged to ask questions if you would like. However, we may not be able to get to all in the tight time frame we have today.
- And sit back, relax and thank goodness this is not a real incident! We're just exercising our IR muscle.

YOUR MISSION

"What would you do differently if you knew you were going to be robbed?"

- Michael Sentonas, *Intel Security*

To fully understand the risks of a cyber incident and communicate with purpose

Things to Consider During the Exercise

Multiple stakeholders

Unintended consequences

Desired results

A ROUGH DAY AT WORK...

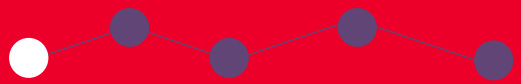
Starting Conditions

US POWER

- US Power Corp. is a publicly-traded, global electricity and gas distribution company based in Atlanta.
- This morning, Sally, a client services representative, was checking her email and opened what she thought was a report from a colleague. However, when Sally downloaded the attachment, nothing saved in her Downloads folder.
- A few minutes later, she attempted to access a document saved in a folder that houses client information, including names, addresses and banking credentials, among other private data. A message quickly appeared on her screen stating that this data was exported and held hostage for ransom.


Your files have been stolen
and encrypted by LOCKBIT 2.0
Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Do not waste your time trying to find your files or telling law enforcement. If you do not pay, we will publish your data on the Dark Web.
We guarantee that you can recover all your files safely and easily if you pay 60 BTC to get the decryption key by 6:00 Tomorrow
Use Buy Decryptor to pay.
Time Left: 23:42:59

SOUNDS EASY, BUT HARD IN PRACTICE



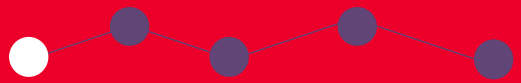
Pivot Point 1

Discussion Questions

Immediate Response

- Who is in charge of the incident response?
- Is there an incident response team, or can we gather key individuals ASAP to organize a response?
- What outside support do we need to engage?
- Which stakeholder audience(s) are most important for us to communicate with at this time?

WAIT! ANYONE WE NEED TO NOTIFY?



Pivot Point 1

Discussion Questions

Initial Notifications

- Do we have reporting obligations?
  - To partners?
  - To clients?
  - To regulators?
- Should we notify law enforcement, and what connections do we already have? If not, why?
- Do we have any insurers we need to put on notice?

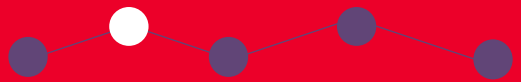
WAIT, PASTEBIN, REALLY?

Pivot Point 2

You find out that some of the stolen data has been leaked. Determine your response.

After six hours, having not yet paid the ransom, you find out that a portion of the stolen data has been leaked. Not only have you confirmed that the hacker has your data, but now some sensitive customer information has been determined to have been compromised. FYI, you are able to see this on your threat intel platform and so can everyone else.

ARE WE REALLY GOING TO PAY THEM?



Pivot Point 2

Discussion Questions

To Pay or Not To Pay

- How will we make the decision whether to pay the threat actor?
- Do we need to tell anyone in advance we are making the payment?
- Any concerns about violating the law if we pay?
- Does it matter what the stolen data is?
- What obligations does US Power have to third parties based on the theft of data?

PRESS, ALREADY, HOW?

Pivot Point 3

Infosecurity Magazine caught wind of the incident. Determine your response.

Cyber-attack at US Power?

TL Thomas Lester
To Media@USPower.com

6:35PM

Hello –

Sources tell me that US Power has suffered a ransomware attack that's impacting many of your systems. Is this LockBit 2.0 behind this? Would you like to comment? I'm writing a story that I plan to publish in about an hour. Let me know ASAP.

Thanks,
Thomas Lester

COMMS MAKE OR BREAK YOUR ORGANIZATION

Pivot Point 3

Discussion Questions

Media Relations

Considerations:

- Has a third-party crisis communications team been retained?
- How do we respond to media inquiries? Who is our spokesperson?
- Which priority stakeholders does the company need to communicate with, now that the incident is becoming public?
- Do we post anything publicly on web properties or social media?
- How much do we need / want to say at this stage?
- Are there any "golden roles" to do or not do?

NOTIFICATIONS

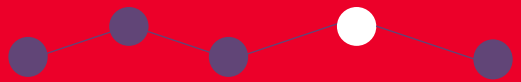
Pivot Point 4

Determine the impacted stakeholders and notification requirements at the state, national and international levels.

Initial findings from the investigation identify data from more than 350,000 customers – including names, addresses, and banking information – may have been impacted.

Consider the applicable regulatory requirements, law enforcement engagement and adjustments needed to the communications approach.

NOTIFICATIONS – CONT'D



Pivot Point 4

Discussion Questions

Notification

- What is the process for disclosing the breach to necessary regulators such as state Attorneys General, CISA, etc.?
- When do we need to notify our Board of Directors, other senior leaders and/or key shareholders?
- Do we know if there will be any fines associated with the breach – and are they material enough to require disclosure in an investor filing?
- Do we need to notify impacted employees or customers? If so, what do we tell them and by when?

CLIENT & PARTNER CONSIDERATIONS

Third-Party Communications

- Network Connectivity Considerations
  - Identify whether third-party clients or vendors have direct connections into your network (e.g., VPN, API integrations, data exchanges).
  - Evaluate whether these connections present propagation risk or require immediate technical containment.
- Prioritization Strategy for Outreach
  - Revenue Impact: Prioritize outreach to clients representing the highest financial exposure.
  - Operational Importance: Focus on critical service providers/vendors essential to business continuity.
  - Regulatory/Contractual Obligations: Identify relationships where contracts or laws mandate notification timelines.

CLIENT & PARTNER CONT'D

Third-Party Communications

- Communication Approach
  - Establish a tiered outreach plan (Tier 1 = key clients/vendors; Tier 2 = medium-impact; Tier 3 = low-impact).
  - Ensure consistent messaging by aligning legal, regulatory, and technical facts of the incident.
  - Use secure communication channels (encrypted email, secure portal) to share sensitive information.
  - Coordinate internally (Legal, Comms, IT/Security) before disseminating external statements to avoid misalignment.

Conclusion

Determine how to continue business operations and discuss what preventative measures could be implemented.

Company leadership decides to NOT pay the ransom.

- The ransomware does not have a public decryption utility.
- Your company did not have an insurance policy.
- Data for 350,000 customers was published, including names, dates of birth, addresses, and billing information.
- US Power may now have to deal with a federal investigation.

Conclusion

Discussion Questions

Prevention

- How do we prevent this type of incident from occurring again?
- Are we going to implement more frequent backups of information?
- Are we certain that the hacker did not keep copies of any sensitive information and, if they did, how can we protect our stakeholders who might be at risk?

Incident Debrief

- What do you need to change to rebuild the company's reputation?
- What do your stakeholders need to hear to trust US Power again?
- What questions should be asked to gather lessons learned?

Partners in the Process

Consider what internal parties and external experts were engaged to effectively respond to the incident.

External Support:

- Insurance Provider
- External Legal Counsel
- E-Discovery / Forensic Investigation Firm
- System Recovery & Restoration Firm
- Threat Actor Negotiations Firm
- Crisis Communications Firm
- FBI and other Government

Internal Parties:

- Information Technology Team
- Chief Information Security Officer (CISO)
- General Counsel & Other Executive Team Members
- Internal Communications Team
- Board of Directors
- Investor Relations Team
- Government Relations Team

KEY TAKEAWAYS

Cyber incident response teams must seamlessly integrate across existing mission-critical functions (C-Suite, Counsel, Public Affairs, Communications etc.).

Audit third party vendors routinely and ensure they have taken steps to secure data.

Preserve necessary forensic artifacts.

Cyber incidents are often designed to compromise all versions of data, including back-up data. Consider how best to protect your most valuable information, how frequently back-ups occur, and how long it takes to restore information.

Being able to combat the full range of cyber threats requires not just risk mitigation processes but also a proper business continuity plan that has been implemented and tested in advance.

How companies react to and communicate about cybersecurity incidents is critical, and there is only once chance to get it right.

RESOURCES

- https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
- https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- https://www.cisa.gov/resources-tools/resources/empowering-small-and-medium-sized-businesses
- https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware
- https://www.cisa.gov/stopransomware
- chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://csrc.nist.gov/CSRC/media/Projects/ransomwareprotectionandresponse/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf

RESOURCES CONT'D

- FTC Privacy and Security Enforcement Page - https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement
- Identity Theft Resource Center (best help pages for individuals as well as a Victim's Help Center) - https://www.idtheftcenter.org/contact-us/?utm_campaign={campaignname}&utm_term=&utm_source=google&utm_medium=cpc&gad_source=1&gad_campaignid=22212099742&gbraid=0AAAAAD_RqEQqOfiiQNk0JPGjlsBC9XiYH&gclid=Cj0KCQjwrc7GBhCfARIsAHGcW5XFQ8O0UUhLBbr2DEadvO1DTIlze_hipyoixqsx2qW-MY05T7pVQqUaAlyWEALw_wcB

RESOURCES – QUICK PRIVILEGE CHECKLIST

- **1. When to Involve Legal?** Early, but work out an escalation protocol by attack vector (i.e., malware, hack, inside attack, physical breach) so legal is not overwhelmed by daily scanning or other routine activity.
- **2. External vs. Internal Legal?** Arguments that documents and communications are privileged are stronger when external legal directs the investigation because it is presumed that external legal is providing legal advice, versus the mixed business advice often provided from in-house counsel.
- **3. Third-Party Experts and the Work Product Doctrine**
  - Retain experts appropriately for privilege to attach: For payment card industry breaches, the PCI forensic investigator is never a privileged party; hire another incident response (IR) firm for a privileged investigation.
  - Clearly identify within the retainer letter that the work the IR firm is doing is for purposes of providing legal advice. Ask experts to mark documents as "Privileged: Prepared at the Direction of Counsel," but even if documents are not so marked, instruct the IR firm to treat them as privileged. Identify a protocol for notifying the legal department/hiring attorney if unauthorized disclosure of privileged information occurs.
  - When possible, an attorney should be the party to engage the IR firm and sign the contract for services. Limit distribution of privileged materials to those involved in the legal investigation; do not distribute to the entire IR team to use for remediation activities.
  - Train IR responders that professional opinions are privileged, facts are not. Train IR responders and retained consultants that all reports must be labeled as "DRAFTS" until legal authorizes a final document.

RESOURCES – QUICK PRIVILEGE CHECKLIST

- **4. Common Third-Party Communications Can Waive Privilege**
  - Sharing information with insurance carriers and brokers, law enforcement, regulators and business partners can result in claims that the privilege has been waived.
  - When having these conversations, limit information shared to known facts and consider joint defense agreements, where feasible.
- **5. Don't Be Afraid to Pick Up the Phone**
  - Fewer documents lead to fewer privilege headaches.
- **6. Don't Prematurely Label Possible Data Event**
  - Don't identify a possible data event as a "breach" until instructed by Legal; don't identify it as an "incident" unless it meets the parameters of such within your organization's incident response plan.
  - Prematurely labeled breaches/incidents may require more privilege analysis. Help your lawyers, help the company.

THANK YOU

NEW YORK PALO ALTO NEW JERSEY UTAH WASHINGTON, D.C.