Cyber Incident Response Workshop: Lessons Learned from the Trenches

County Reinsurance, Limited

www.eckertseamans.com

Matt Meade and Laura Decker| December 10, 2025

ECKERT SEAMANS ATTORNEYS AT LAW

State Breach Notification Laws

- All 50 states, the District of Columbia, Puerto Rico and the US Virgin Islands have enacted data breach notification laws

Typical Breach Notification Law

An entity that maintains computerized "**personal information**" must disclose a "**security breach**" to any state resident whose unencrypted, unredacted "personal information" was, or is reasonably believed to have been, accessed or accessed and acquired by an unauthorized person.

What is “Personal Information”?

Name information + another **sensitive data element**:

What is a “Security Breach”?

- Unauthorized access and/or access and acquisition of computerized data that materially compromises the security or confidentiality of PII maintained by the business
- Reasonable belief that access has caused or will cause loss

Security Breach

- Excludes good faith acquisition of personal information by an employee or agent if the personal information is not used and is not subject to further “unauthorized disclosure”
- Safe harbor for encrypted data
- Any vendor that maintains data shall provide notice to the entity that manages the data

Key Differences

- Paper
- Notice “triggers” requiring material or significant harm
- Notice to attorney general’s office or other governmental authority
- Varying definitions of “personal information”
  e.g., health and insurance information, DOB, biometric data
- Timing of notice, *e.g.,* 30, 45, 60 days, or “without unreasonable delay”


Mini Cyber Scenarios

Scenario 1
Information Systems Upgrade

- You have a big meeting scheduled with the County Commissioners. In the middle of preparing for the meeting you receive a call from the County's head of IT who insists that he needs to remote into your computer to check on the status of some important upgrades.
- The call could not come at a worse time as you are finalizing your reports for the meeting.
- You ask the head of IT if it can wait and he tells you it is urgent!
- Reluctantly you grant remote access to your computer. You note that the head of IT seems to be searching through County financial records as well as scrolling through accounts receivable files at a high rate.
- The caller sounds like the head of IT, but you have concerns.

Scenario 1
Information Systems Investigation

- While the upgrade is going you call the IT head's cell phone and ask him how much longer the upgrade will take and he asks what you are talking about!
- You explain the situation and he instructs you to turn off your computer immediately.
- He tells you that his team would never affirmatively reach out to you to demand remote access to your computer!

Scenario 1
Information Systems Investigation

- Is this a data breach that requires notice? What else do you need to determine to make this evaluation?
- What do you need to learn about the financial documents and the accounts receivable files to make your decision?
- If your investigation finds that the financial records had SSNs and DLs would that mean it is a breach?
- The next day the County Commissioners all receive cryptic voicemails from a cyber criminal who claims to have exfiltrated County data. The cyber criminal wants 1 million dollars or they will publish the data. What do you do?
- If the County pays does that relieve the County of its obligation to provide breach notification?

Scenario 2 Cyber News Flash

- The County receives a call from a cyber blogger who tells you that a hacker has informed the blogger that it has taken a large amount of data from your network and if you don't pay an extortion demand of $250,000 in 72 hours the hacker will release all of the data to the public.
- The reporter has a sample of data and will go public in 24 hours, and wants a statement from the County.
- How does the County respond?

Scenario 2 Cyber News Flash

- What should the County do to investigate the allegation?
- Would you ask for the sample documents? Why?
- What subject matter experts should be brought in to investigate?
- Should the FBI be notified?
- Should the County pay the extortion demand?
- Should a statement be made to the press?
- What would the statement say?
- Is this a data breach? Why or why not?

Scenario 2 Cyber News Flash

- The County analyzes the sample documents provided by the cyber blogger and determines that they are records maintained by a vendor who was conducting research regarding county payroll and excess.
  - There are SSNs in the data set.
  - There also is significant sensitive information (e.g., County bank accounts and passwords, history of pay raises, and annual salary) included.

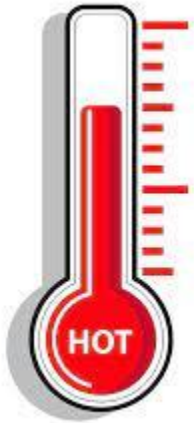
The records were in an unsecured file called MKTRESEARC that appears to be linked to a scanner and has 5000 total records.

Scenario 2 Cyber News Flash

- Should the vendor be fired? Why or why not?
- What should your agreements with vendors say about who is responsible for providing notice of a data breach and paying for costs associated with notice?
- What is the County's role in connection with the breach notification notices?
- Would the County issue a media statement or defer to vendor?
- If yes, would the County identify the vendor in the statement?

Scenario 3
An OT Crisis-HVAC

- In the middle of the summer the County jail reports that temperatures are rising in the common spaces and they can't cool them.
- The County Attorney receives a call from Kela Group, a cyber threat intelligence company, alerting them that access to County computer network environment has been found on the dark web.
- Prisoners and guards are starting to complain about the escalating temperatures.
- What are next steps?
- Who is in the room for these discussions?



Scenario 3
An OT Crisis -HVAC

- On inspection, the jail realizes that they cannot log in to HVAC.
- On reviewing the dark web site, screenshots from camera feeds from the jail's security cameras are posted, along with offers to sell access to the jail's computer environment.
- Your HVAC vendor reports that it was hacked and its access to the jail HVAC and security cameras was compromised
- Is this a data breach requiring notification?
- What are the next steps for:
  - Scoping & Containment
  - Recovery
  - Investigation
- Would this be reported to the FBI?
- Would there be any communications to the community?
- What is the work around?

Email Incident

- An HR employee reports that a large number of spam emails have been sent from her County email without authorization.
- Based upon the County's internal review it appears that the employee clicked on a link in a phishing email.
- What are the next steps?

Email Incident

- After notifying counsel and working with an external IT investigator the County determines that the email account of the HR employee was synched/copied.
- The HR employee had maintained emails with employee's Covid vaccination cards gathered in connection with the return to the office.

Email Incident

- Full review of all contents of email box for PII because there has been acquisition of personal information.
- Depending on size of mailbox review either done by counsel or third-party reviewer
- Covid vaccination cards are medical information which would require notice under some state laws

Email Incident – Common Mistakes

- Assuming that because it was “just” spam emails being sent from employee account there was no possible breach
- Failure to terminate any active sessions
- Failure to search for forwarding rules
- Failure to search to see if other employees clicked on suspicious link
- Failure to change PW
- Email used as a repository for old data like Covid vaccination cards


Ransomware

Ransomware –Vendor

- The vendor that does background searches for new hires notifies the County that it experienced a network interruption and cannot process any new searches.
- A few days later the vendor explains that the network interruption was a ransomware attack but that they do not believe that County data was impacted.

Ransomware – Vendor

- As part of the County's efforts to understand the scope of the incident and to achieve containment the County blocks access to the vendor portal so that no new hire information can be sent electronically.
- What is the operational impact of this decision?
- The vendor assures the County that it has a secure workaround and wants an explanation. Who from the County gives it?

Ransomware –Vendor

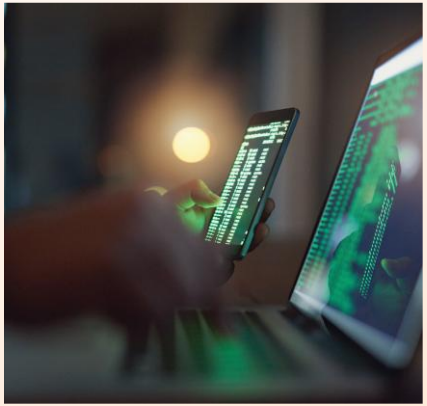
- 2 days later, the vendor updates the County and explains that the TA recently posted County data as well as data from other counties that work with the vendor on the Dark Web.
- What are the contractual notification requirements for vendors in connection with cyber incidents?

Ransomware –Vendor

- The vendor is not being cooperative in providing information to the County about how the breach happened?
- Who would be notified of this incident within the County?
- Would the County hire an external forensic investigator?

Ransomware –Vendor

- The vendor finally reports that the cause of the breach was a known vulnerability that it failed to patch.



Ransomware – Vendor

- How would the County get access to the data on the Dark Web to review it and determine any notification obligations?
- Who would analyze the data?

Unique Challenges/Issues

- What is the role of the incident response team in connection with investigating what happened?
- When should outside counsel get involved?
- Who should send the breach notice?
- If the County sends the notice should the notice identify the vendor?

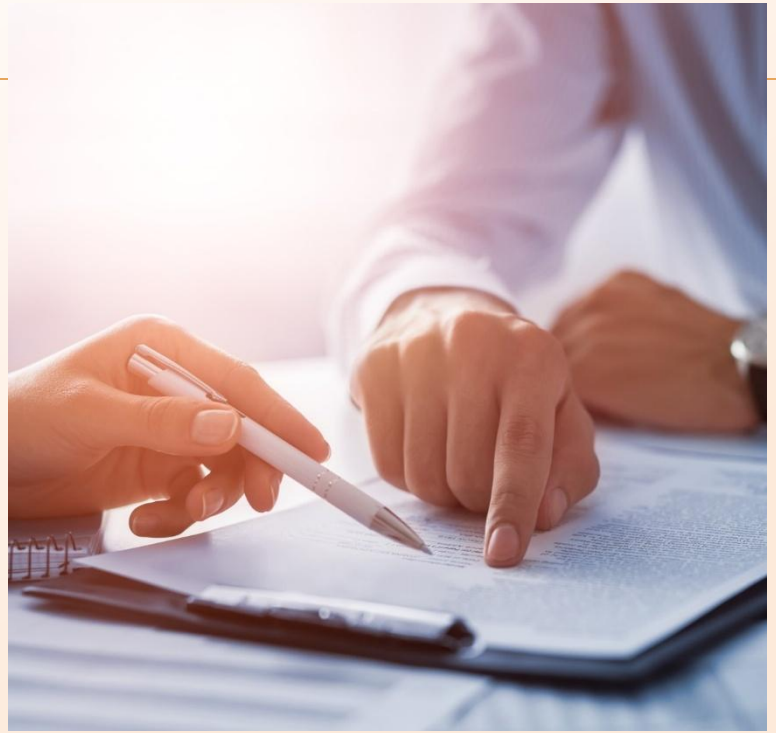
VENDOR RISK

Risk	Consequence	Solution
Agreements with vendors who have access to County personal information	Increased risk of unauthorized access	Require vendors to maintain appropriate security measures

VENDOR REQUIREMENTS

VENDOR DUE DILIGENCE CONSIDERATIONS

- Review and assessment of vendor pre-contract:
- Does vendor have cyber liability insurance?
- Does vendor have any security certifications?
- Risk assessments, penetration testing, employee training?
- Has vendor experienced a data breach?



VENDOR REQUIREMENTS

- Implement reasonable administrative, technical and physical safeguards to protect PII/PHI
- Limit access to those who need PII/PHI in order to perform job
- Provide prompt written notice upon discovery of unauthorized use, access or disclosure
- Responsible for costs and expenses incurred responding to breach including the cost of providing any required notifications
- Cooperation with an investigation of an incident

MANAGED SERVICE PROVIDER ATTACKS

MSP ATTACK

- The third-party company that remotely manages the County's IT and end-user systems has been working with the County for years on a handshake deal. The head of the MSP is good friends with 2 of the commissioners.
- The MSP reaches out to the County to tell you that they have been hit by ransomware. In order for them to do their job they have access to the County's network. You are worried that County data is at risk. The MSP tells you everything is ok. What do you do?
- Notify insurance, get counsel and forensic support to ensure that your network is secure

EMERGING THREAT

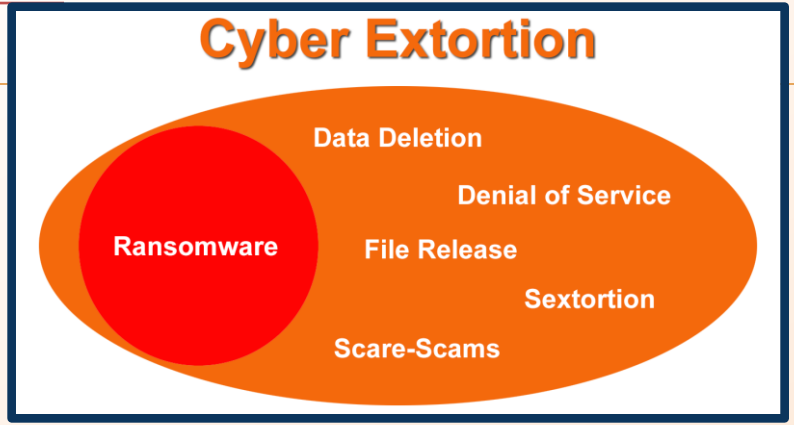
Why are MSPs being attacked?	Single Point of Entry for Multiple Victims
	Highly Privileged Access
	MSP Data Extortion
Threat Tactics	EDR Evasion
	Edge Device Exploits
	Social Engineering

PAYING THE RANSOM?

RANSOM

EXTORTION

- **Cyber Extortion**
  - A demand for payment based on a threat to expose, damage or deny access to data.
    - Release files on dark web
    - Delete backups



- **Ransomware**
  - The malicious encryption of files to deny the owner access and use of the data.

RANSOM

REASONS TO PAY- EVALUATE THE OPERATIONAL IMPACT OF FAILING TO PAY

- Through your investigation the County learns that sensitive County data will be posted on the Dark Web unless the County pays a ransom to suppress the publication of the data on the Dark Web.
- Would the County be willing to pay $350,000 to suppress the publication of data about:
  - Ongoing criminal cases
  - Victims of past criminal cases including sex crimes including child sex abuse cases
  - Information related to undercover officers or informants
  - CYS data related care and treatment of children
  - Home addresses for judges
  - Security plans for transportation or buildings
- What if the amount was $500,000? What is the limit?
- What would the impact on the County be if you did not pay and the data was shared on the Dark Web?

RANSOM

REASONS TO PAY- THE IMPACT OF DATA PUBLICATION

- **Example -- City of Columbus Opposition to Motion to Dismiss:**
- Plaintiff John Doe #1 is a Columbus Police Officer who has dedicated years of service to the community and currently serves in an undercover role. The City obtained and maintained his PII as a condition of his employment, but his PII was exposed in the City's data breach and is now on the Dark Web. He was also locked out of his bank account in mid-August 2024. Id. John Doe #1 fears for his personal financial security. As a law enforcement officer, John Doe #1 has a particularized concern that his information will be identified and targeted by criminals. He has a well-founded fear that, should his identity as a police officer come to light, not only will ongoing criminal investigations be jeopardized, but his life would be in danger. As a result, he fears for his safety more now than ever before. He sleeps with a gun under his pillow, and he has had to install security cameras throughout his home.

RANSOM

REASONS TO PAY- THE OPERATIONAL IMPACT OF NOT BEING ABLE TO RECOVER DATA

- Insufficient Backups
- Back ups encrypted
- Back ups corrupted so some but not all data is available
- Back ups held by 3d party not current

- **Example-Mid Size Midwest County was the victim of a ransomware attack and did not have viable backups which meant that all county data was lost. Left with no choice but to pay in order to restore operations**

Questions?
Thank You!

www.eckertseamans.com

Matt Meade
mmeade@eckertseamans.com
December 10, 2025

ECKERT SEAMANS
ATTORNEYS AT LAW