Cyber Incident Response

Common Mistakes Counties Make

MATT MEADE & LAURA DECKER
OCTOBER 15, 2026

ECKERT SEAMANS
ATTORNEYS AT LAW



Cyber Incidents Top 13 Mistakes

1. Creating Dumpster Fires
2. Ignoring Warnings
3. Not Confirming a Change in Wiring Instructions Properly & Once Money is Lost, Not Taking Steps to Recover the Lost Funds
4. Not Reporting to Insurance and Resisting Help
5. HIPAA - Not Knowing/Meeting Requirements
6. Not Investigating a Business Email Compromise



Cyber Incidents Top 13 Mistakes

7. Not Being Aware of Deadlines
8. Discussing/Reporting the Incident too Early
9. Failing to Recognize that your Network is a Crime Scene
10. Failing to Row the Boat in the Same Direction
11. Failure to Slow Down
12. Failure to Delete or Archive Data
13. Not Having an Incident Response Plan

1. Creating a Dumpster Fire when Responding to a Cyber Incident

- What can create a dumpster fire?
  - Working with vendors who have inadequate cyber procedures
  - Failing to have written contracts with vendors that have been entrusted with County data
  - Entrusting an MSP with unlimited access to your network
  - Issuing factually inaccurate and inflammatory statements to the media
  - Not reviewing media statements with forensic investigator and counsel



2. Ignoring Warnings

- What do you do when Federal Law Enforcement warns the County of an imminent cyber attack?
- Is an Endpoint Detection and Response (EDR) tool in place and being monitored?
  - Advanced AI driven security tools
- What do you do when the EDR alerts the County of suspicious activity.





3. Not Confirming a Change in Wiring Instructions Properly & Once Money is Lost, Not Taking Steps to Recover the Lost Funds

- The County just wired $777,000 to a contractor who claims not to have received it. What do you do?
  - Changes in wiring instructions must be confirmed via a phone call to a known phone number. Never use the phone number included with the change.
  - Always double check for spoofed emails. However, threat actors will also utilize legitimate email accounts to further wire fraud.
  - Once the money is sent and the fraud is discovered, it is important to report the incident to insurance.
  - 72 Hours – the first 72 hours are key to getting a wire stopped. If the wire is international, the report must be within the 72 hours for the USSS to activate the Financial Fraud Kill Chain.
  - Always report incident to your bank and complete hold harmless letter.

4. Not Reporting the Incident to Insurance and/or Resisting Help

- The County just had a cyber incident. IT says it is under control. What do you do?
  - Prompt reporting to insurance is key to a timely response.
  - Insurance will get ball rolling on legal counsel and third-party support.
  - Required by law to conduct a reasonable investigation.
    - Do not delete data or erase endpoints.
  - Do not do your own investigation – checking your own homework, rely on the experts.
  - Regulators and law enforcement want to see a third party conducting the investigation.
  - Using counsel and third-party investigators allows for protection of the investigation and findings of the investigation to fall under attorney-client privilege.
  - A reported incident may not be a breach.

5. HIPAA – Lack of Awareness of Requirements

- Knowing what departments, if any, are Covered Entities.
  - Covered Entities are regulated by HIPAA
  - Provide medical/psychological services.
- HIPAA has its own deadlines and penalties.
  - Notification to individuals within 60 days of discovery of breach.
  - Notification to HHS:
    - For breaches impacting 500 or more individuals – within 60 days of discovery of breach.
    - For breaches impacting less than 500 individuals – within 60 days from the end of the calendar year in which the breach is discovered.
- HIPAA requires certain policies be in place including technical risk assessments, training, physical safeguards, etc.
  - Office of Civil Rights investigates all breaches impacting over 500 individuals and will ask for proof of compliance.
- Business Associate Agreements
- OCR will fine government entities.





6. Not Investigating a Business Email Compromise

- A county employee reports that he is getting calls about strange emails being sent from his county email box. IT changes his password and it stops. Is that enough?

- Business Email Compromise (BEC) – threat actor gains access to an email account. Can seem like low risk and innocuous.
- Usually occurs due to phishing email.



6. Not Investigating a Business Email Compromise

- Can lead to further phishing incidents. Stealing of credentials which can lead to identity theft or ransomware. Wire fraud to County and vendors.
- Data theft is common. Threat actors will sync the impacted email account or add a third-party application which will copy the contents of the email account. This can occur quickly.
- Email policies – receiving and keeping PII in email accounts should be prohibited. Users should not be able to add third-party applications without IT approval.
- Failure to have adequate email retention policies

7. Not Being Aware of Deadlines

- HIPAA deadlines
- Legal requirements are determined by the state of residence of the impacted individual at the time of mailing.
  - An employee can work in PA and move to Indiana, IN law would be applicable.
  - Other states have other requirements – different definition of "breach," different protected PII, other deadlines – 10 days, 14 business days, 30 days, 45 days, 60 days.
- Notification to the Attorney General's Office.



8. Discussing/Reporting the Incident too Early

- A day before hiring counsel to handle the investigation a county commissioner appears on TV and says the Chinese were responsible for the breach. What problems do you see?
  - Do not refer to an incident as a breach – specific legal term.
  - Transparency is good but incorrect information is hard to walk back.
  - Releasing information too early can lead to questions that the County cannot answer.
  - We will assist in writing public statements. Have experience and can prepare the County for the usual pitfalls.
  - Consistency is key. Designate one person to address the media and answer questions.
  - Always get questions from the media in writing and respond in wiring.

9. Failure to Recognize that Your Network is a Crime Scene

- The day after a cyber attack County IT starts erasing data files and logs and telling the community that it was the only option it had. What issues do you see?

- Treat IT environment like a crime scene. It is when you have a cyber incident!
- Preserve forensic evidence
- Critical to determining what has happened and the County's obligations
- Minimize communications - Threat Actors monitor the news







10. FAILING TO ROW THE BOAT IN THE SAME DIRECTION

What happens when IT, elected officials, HR and communications don’t work together when responding to an incident?

STRIVE TO HAVE THE IR TEAM AND COUNTY OFFICIALS ROW THE BOAT IN THE SAME DIRECTION



11. Failure to SLOW DOWN

- A county employee sent a spreadsheet with sensitive employee data to Joseph A. Smith instead of Josephine Smith. Joseph Smith is blogger who always writes negative posts about “corrupt” County. What should the county do?

- Sending things to the incorrect recipient is common. Use encrypted email and/or file sharing sites as appropriate to help mitigate this issue.
- Always double check work. This is extremely important when redacting personal information.



12. Failure to Delete or Archive Data



- The County network maintains a data base with every concealed carry permit submitted to the County for the last 25 years. What issues do you see?

- Today's ransomware attacks are double extortion – data encryption and data theft.
- Data on the network can be and will be stolen and ransomed by the threat actor.
- Retaining large amounts of data on network or in email increases notifications.
  - Still must notify whether a ransom is paid or not.
- Data does not age out of notification – you must notify an individual of an incident even if that data is 30 years old.
- Data deletion and archival policies and procedures are important.

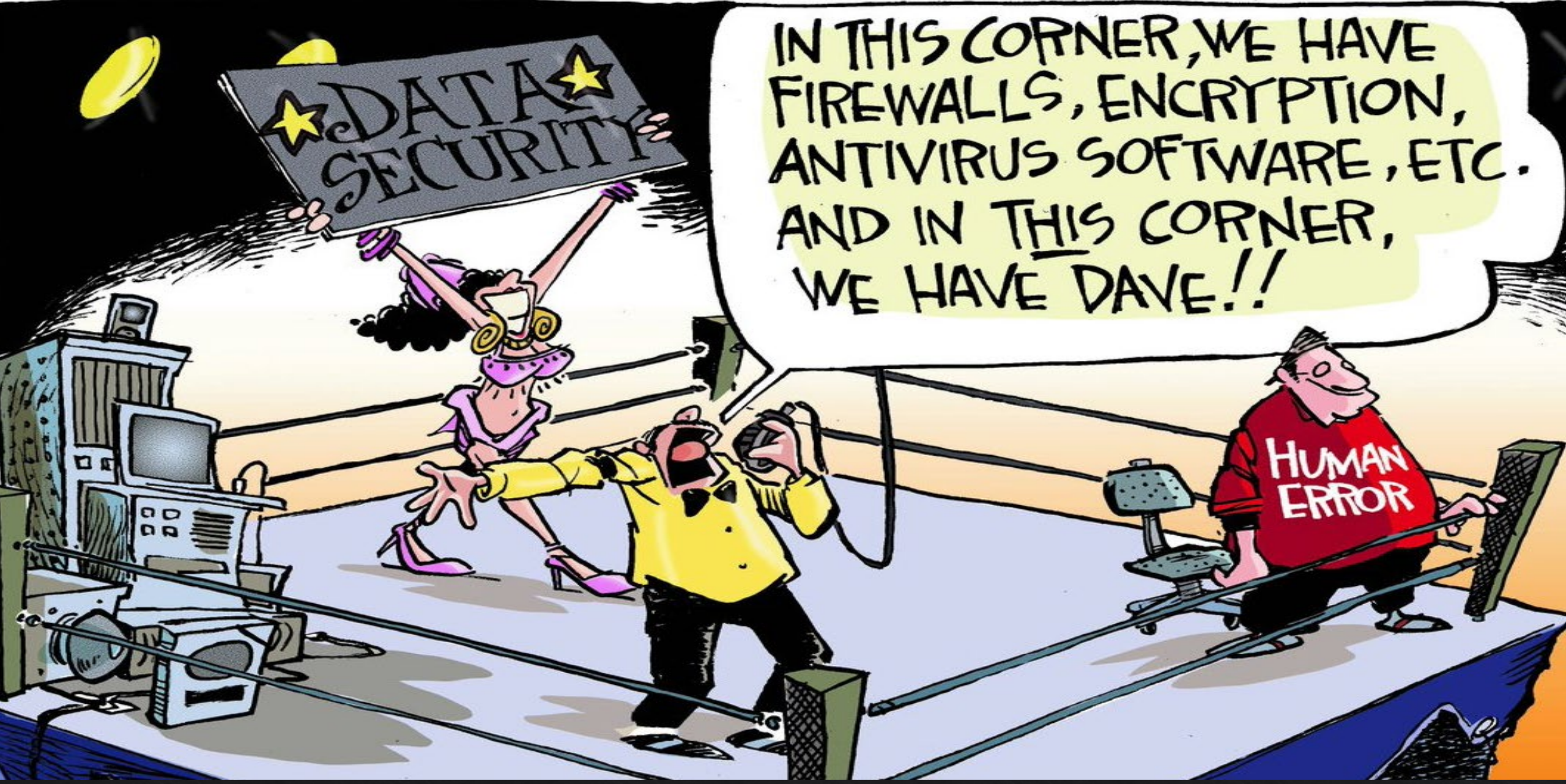
13. Not Having An Incident Response Plan

- The County is the victim of a ransomware attack. Nobody seems to know what to do?
- Develop and test an Incident Response Plan.
  - Step by step plan for what to do in the event of a cyber security attack.
  - Test it using tabletop exercises.
- Create a playbook that identifies members of the incident response team and strategies for notification, communication and reporting.



Final Takeaways

- Have strong clear written policies and procedures
  - Incident Response Plans | Trainings
- Data Retention prevents small incidents becoming large incidents
  - Only keep what is required
  - Use other storage methods to keep required data that is not needed not day-to-day
  - Auto-deletion or archiving of emails after a certain period of time
- If you have an incident – always report it quickly. Even if you are on the fence, we will help you determine if any further steps are necessary
- Slow Down – Human error incidents can usually be prevented if a person double checks their work
- Never ignore warning signs. Better to be overly cautious than have a ransomware attack.
- Always confirm changes in wiring instructions over the phone to a known phone number. This also applies to suspicious emails with attachments/links. Call before clicking on anything.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Contact Us

Matthew Meade
W: 412.566.6983
C: 412.596.5245
mmeade@eckertseamans.com

- The information contained in this presentation is for educational purposes only and should not be construed as an endorsement of any kind for any vendor, service, or technology.
- Do you own due diligence. You are encouraged to conduct your own research and due diligence before making any decisions based on the information presented.
- No Legal Advice. The information presented is not a substitute for legal advice. Please consult with a qualified legal professional for advice specific to your situation.
- Intended Purpose of Use. The information provided is furnished solely for the internal business purpose for which it was transmitted and may not be redistributed or used for any other purpose without prior written consent.