BEHIND THE BREACH

WHAT COUNTIES MUST KNOW ABOUT TODAY'S CYBER THREATS

ECKERT SEAMANS
ATTORNEYS AT LAW

Sylint
now part of Crowe

SEPTEMBER 15, 2025

AGENDA

TODAY'S TOPICS

1. Threat Intelligence Update
2. Business Email Compromise (BEC) Examples
3. Vendor Risks – Who is The Weakest Link
4. Managed Service Provider Attacks
5. Pay the Ransom?
6. Mitigating the Risk

TODAY'S SPEAKERS

MATTHEW MEADE, ESQ.

JOSEPH BEAULIEU

WHAT KEEPS US UP AT NIGHT?

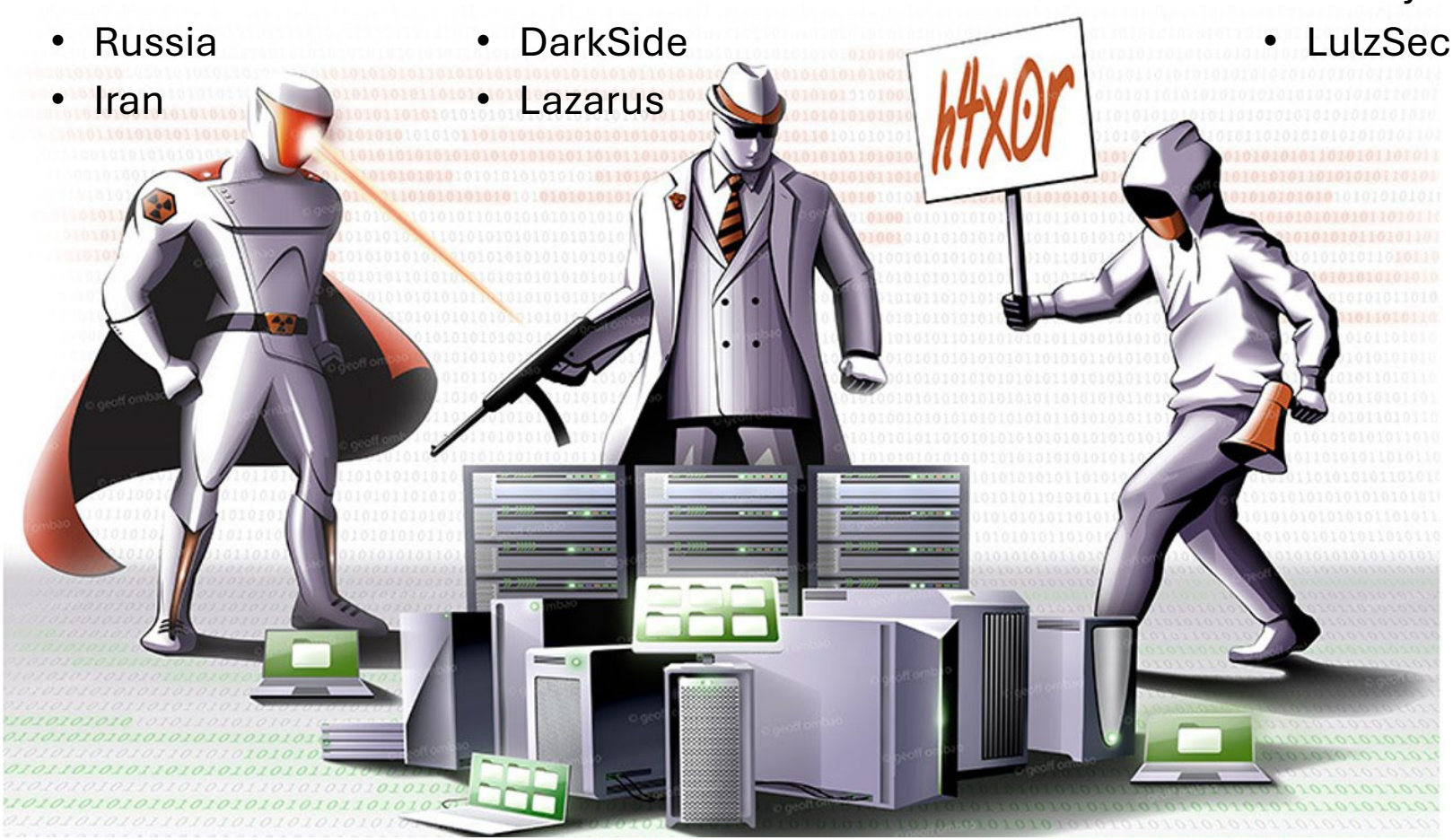
Cybersecurity!

01

THREAT INTELLIGENCE UPDATE

THREAT ACTORS

- Nation States
  - China
  - Russia
  - Iran
- Organized Crime
  - LockBit
  - DarkSide
  - Lazarus
- Hacktivists
  - Anonymous
  - LulzSec



ATTACK OBJECTIVES

Nation State

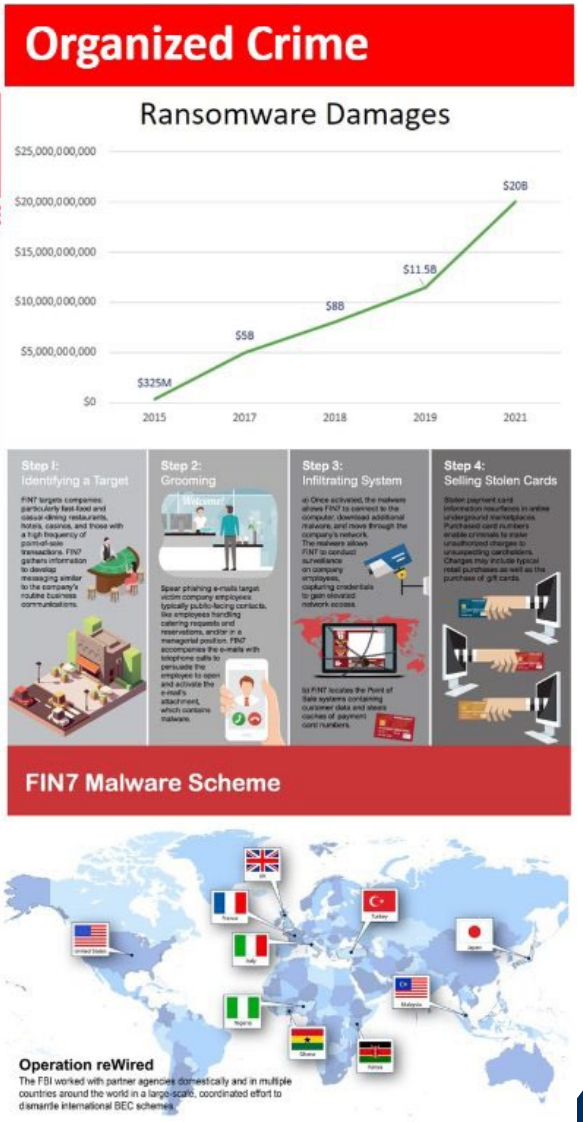
- Intelligence Collection
- Political Objectives
- Economic/Industrial Espionage
- Hybrid Warfare

Organized Crime

- Monetization
  - Data Theft
  - Ransomware
  - Extortion
- Hybrid Warfare

Hacktivist

- Defacement
- DDoS
- Hybrid Warfare



CURRENT THREAT LANDSCAPE

Smarter Adversaries

- Cybercriminals and nation-state actors are more organized, patient, and well-funded.
- Social engineering (like BEC) is the #1 tactic—not technical exploits.

Evolving Tactics, Techniques & Procedures (TTPs)

- Shift from ransomware-only to **multifaceted extortion**, **BEC**, and **supply chain attacks**.
- Cybercriminals use AI and automation to scale attacks faster than defenders can respond.

Government & Public Sector = Prime Targets

- Local governments are attractive: high trust, lower budgets, and lots of sensitive data.
- BEC, ransomware, and data exfiltration are top threats in this sector.

Resource Gaps = Risk

- IT and security teams are often under-resourced.
- Legacy systems, limited MFA, and lack of user training widen the attack surface.

The Cost of Inaction

- Average cost of a data breach (U.S.): **$9.48 million**
- Beyond money: loss of public trust, operational downtime, legal consequences

02

BUSINESS EMAIL COMPROMISE

BUSINESS EMAIL COMPROMISE

Definition

- Business Email Compromise (BEC) is a type of cybercrime where attackers use social engineering and email spoofing or gain unauthorized access to a legitimate email account to deceive individuals into transferring funds or sensitive data to the attacker.

Key Characteristics

- Impersonation of executives, vendors, or trusted partners
- Use of legitimate-looking but fraudulent emails
- Often no malware involved—relies on human trust
- Financially motivated and highly targeted

WHAT IS THE INTENT OF A BEC?

Financial – Fraudster supply chain interruption

Distraction – Creating *noise* to distract from other goals.

Information theft – Access to personally/organizationally sensitive information

Reputation – Attempt to negatively impact organization/partner relationships

BUSINESS EMAIL COMPROMISE SCENARIO

- Monday morning Acme Builders, a construction contractor that the County has been working with on city hall improvements, asks about the status of a $250,000 payment that was due on August 29, 2025.

The County has a record of wiring the money to Acme on August 15, 2025.

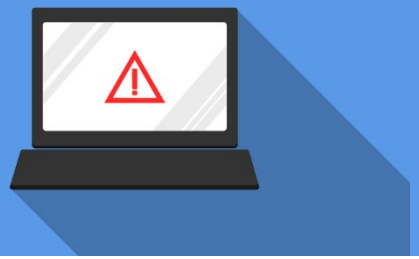
BUSINESS EMAIL COMPROMISE SCENARIO

1. Would IT have any role in connection with this incident at this time?
2. How would the County's Prosecuting Attorney find out about this?
3. What would the investigation be focused on at this time?

BUSINESS EMAIL COMPROMISE SCENARIO

- Upon further review of the email account of the employee who made the wire transfer it appears that Acme sent an email on August 1, 2025 changing payment instructions from prior transactions.

- The employee called the number on the email and verified the new instructions.



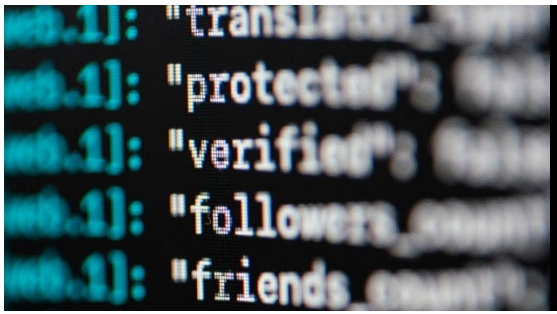
IT investigates the incident and determines that the 8/1 email came from accounts@acmebuilderz.com rather than accounts@acmebuilders.com.

BUSINESS EMAIL COMPROMISE SCENARIO

- Should ICRMP be alerted to this situation?
- Is this incident a data breach?
- Should outside counsel be contacted?
- Who is responsible for the lost payment?
- What steps can you take to try to recover the funds?

BUSINESS EMAIL COMPROMISE SCENARIO

1. Your forensic investigation determines that the employee responded to a phishing email and provided his credentials.
2. Shortly after giving up the credentials, the bad actor accessed the employee's email account and set up forwarding rules so that all legitimate emails from Acme Builders were sent to the user's deleted email folder.



The employee had 6 GB of data in his email account including tax information related to the payment of vendors.

BUSINESS EMAIL COMPROMISE SCENARIO

- How would you determine whether this is a breach?
- Who would conduct the investigation of the nature of the access by the bad actor?
- If the forensic investigator finds evidence of copying or synching of the employee's email box what are the next steps?
- If there is no evidence of synching what are the next steps?

BEC - MITIGATE THE RISK

Identifying Threat Actors

- **Verify the Sender**: Check email addresses for discrepancies or unusual domains.
- **Unexpected Requests**: Treat unsolicited payroll change requests with suspicion.
- **Red Flags**: Look for poor grammar, spelling mistakes, and a sense of urgency.

Steps to Verify Requests

- **Secondary Confirmation**: Always verify requests through a known, trusted method (e.g., phone call).
- **Employee Education**: Regularly train employees to recognize phishing attempts.

Process for Handling Requests

- **Implement Verification Procedures**: Require multi-step authentication for payroll changes.
- **Secure Submission Channels**: Use secure internal portals for submitting payroll update requests.
- **Regular Monitoring**: Continuously monitor for unauthorized changes to payroll information.

03

VENDOR RISKS AND STRATEGY

RANSOMWARE - VENDOR

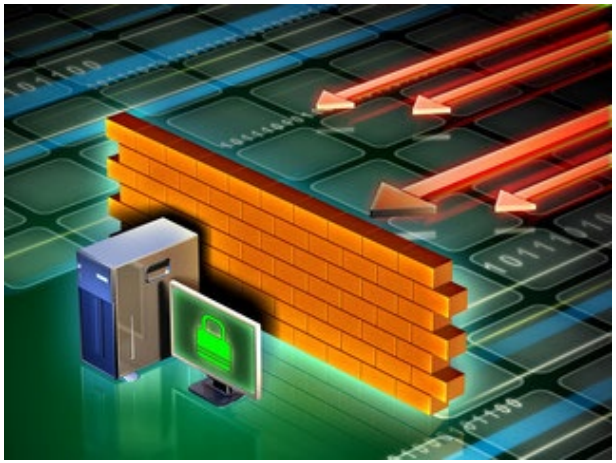
RANSOMWARE - VENDOR

- 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

- Two (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?

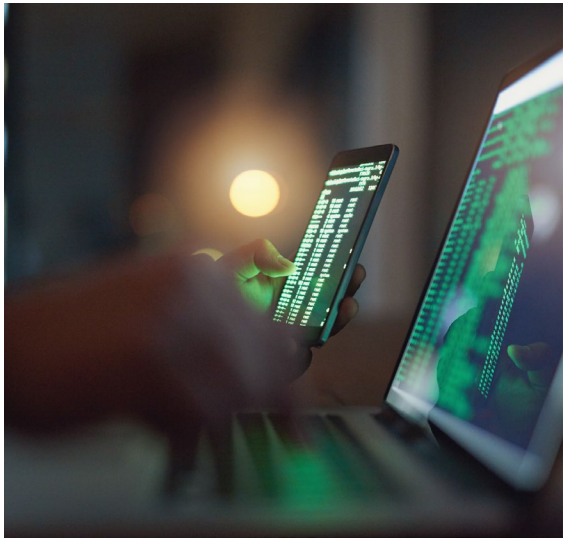
RANSOMWARE - VENDOR

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?
- ❑ What would the role of the IRT be?
- ❑ What would the role of the external forensic investigator be?

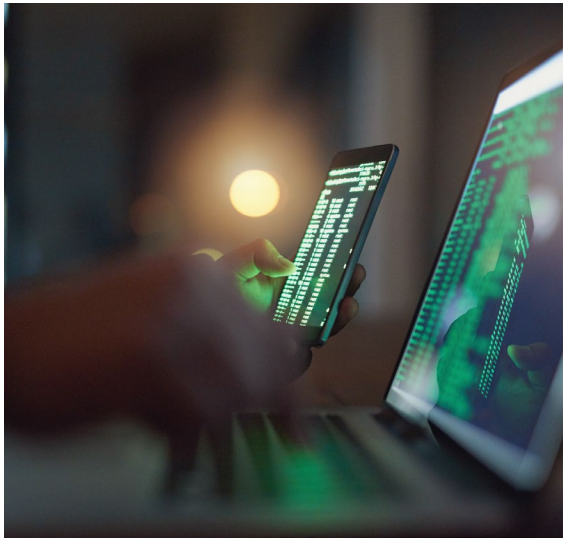
RANSOMWARE - VENDOR

- 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?



RANSOMWARE - VENDOR

Unique Challenges

- 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

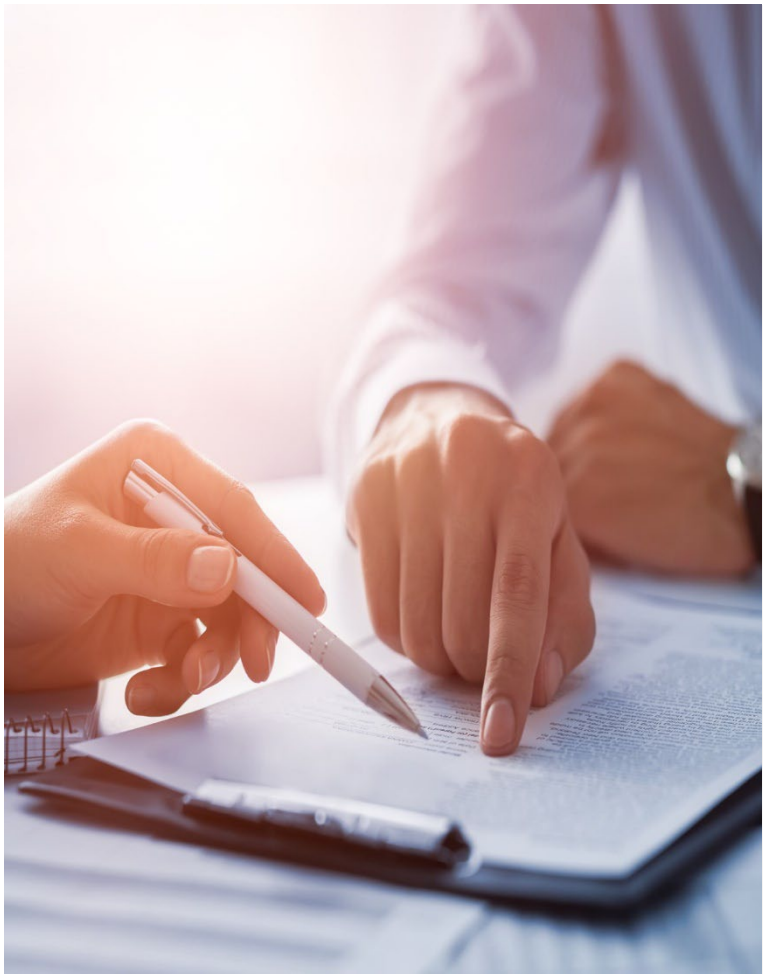
Risk	Consequence	Solution
Agreements with vendors who have access to personal information	Increased risk of unauthorized access	Require vendors to maintain appropriate security measures

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?



PROCUREMENT

VENDOR DUE DILIGENCE CONSIDERATIONS

Adopt standard cybersecurity contract language

- Confidential data and duty of care including notification to County of compromise
- Require background screening and training of personnel accessing County data

Build procurement Process

- Request vendor response to security due diligence questions
- Review and grade responses as part of the procurement process

Update existing contracts at renewal

- Add the cybersecurity language to renewal agreements with long standing vendors
- Request responses to due diligence questions

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

VENDOR ENDPOINTS

VENDOR MACHINES

Require vendor equipment to meet minimum standards

- Appropriate operating system
- Require system to be patched frequently

Deploy County security tools on vendor-provided equipment

- Enterprise Detection and Response deployment
- Remote access only via approved means (VPN, MFA, etc)

Monitor vendor maintenance activity

- Create accounts within Active Directory for vendor use
- Log access by vendors to systems and *monitor activity*

VENDOR ACCOUNTS

VENDOR CONSIDERATIONS

Use primary identity provider solution to authenticate vendors

- County security policies are applicable
- Access by vendor granted via least privilege

Audit vendor accounts at least quarterly

- Remove access when no longer needed as soon as possible

Maintain good vendor account hygiene

- Ensure vendor accounts must use MFA
- Change or disable accounts with long standing passwords
- Change passwords on vendor account according to policy

04

MANAGED SERVICE PROVIDER ATTACKS

EMERGING THREAT

- 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 and are good friends with 2 of the commissioners.

- They reach 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?

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

➢ Notify ICRMP, get counsel and forensic support, shut down access, make sure you have a contract going forward, etc.

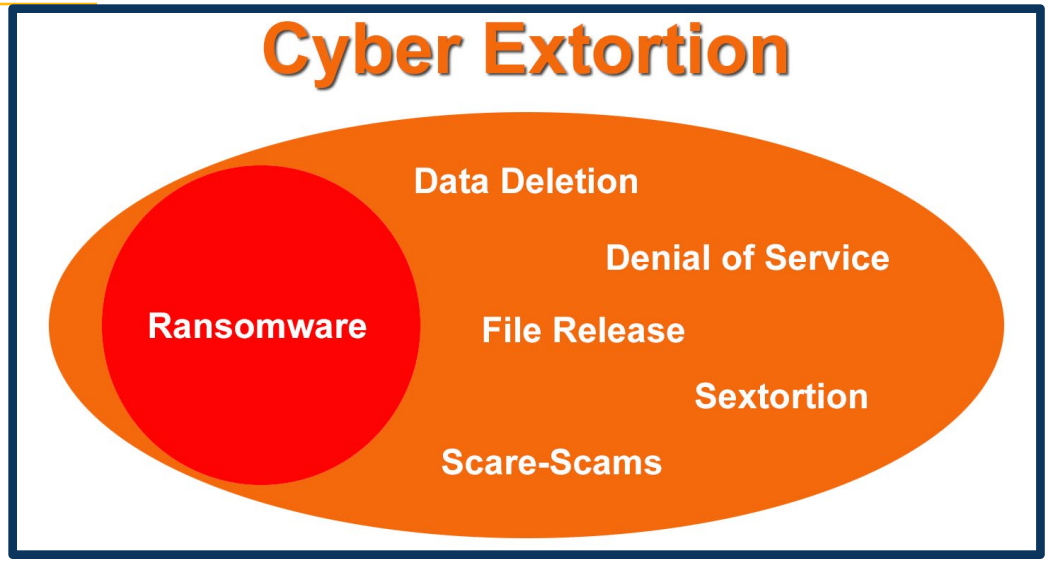
05

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

1) Sensitive Data Will Be Posted on the Dark Web

- Ongoing criminal cases
- Victims of past criminal cases including sex crimes including child sex abuse cases
- Information related to undercover officers or informants
- Data related care and treatment of children
- Home addresses for judges
- Security plans for transportation or buildings

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. 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.**

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

2) No recoverable backups

- Insufficient Backups
- Backups encrypted
- Backups corrupted so some, but not all data is available
- Backups held by 3rd 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

06

SO WHAT CAN WE DO?

DEFENSE IN DEPTH

Purpose

- Protect valued assets
- Keep assets operational

Core Principles

- Layered security approach
- Strength is in the sum of the individual parts
- Resiliency and continuous operations are key to success

PROTECTING OUR DATA

Common Issues

- Limited or missing logging & retention configuration
- No endpoint detection or misconfigured
- Flat network
- Did not adhere to least privilege
- No immutable backup solution
- Improper MFA configuration

Mitigation Strategy

- ✓ Defense in Depth strategy
- ✓ Advanced EDR
- ✓ EDR & MDR logging – minimum 60 days
- ✓ Segmented Network
- ✓ MFA – VPN, administrator accounts
- ✓ Immutable backup solution
- ✓ Incident Response Plan
- ✓ Document and Record Management
- ✓ Training- “If you see something say something”

Crowe

Sylint
now part of
Crowe

ECKERT
SEAMANS
ATTORNEYS AT LAW

THANK YOU

Matthew Meade, Esq.

Chair, Cybersecurity, Data Protection & Privacy

MMeade@eckertseamans.com

Joe Beaulieu

Cyber Managing Director

Joseph.Beaulieu@crowe.com