What Leaders Need To Know To Improve Cyber Security

www.eckertseamans.com

Matt Meade - Eckert Seamans | **Jeff Birnbach** - Sylint
December 13, 2023

ECKERT SEAMANS ATTORNEYS AT LAW

Cyber Extortion & Ransomware

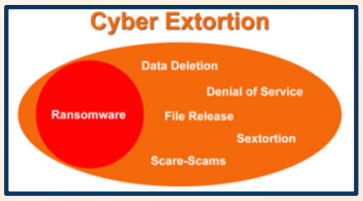
ECKERT SEAMANS ATTORNEYS AT LAW

Sylint.

www.eckertseamans.com

Growing Threats

- **Cyber Extortion**
  - A demand for payment based on a threat to expose, damage or deny access to data.
    - Release files on the dark web
    - Delete backups
    - Launch DDOS attacks
- **Ransomware**
  - The malicious encryption of files to deny the owner access and use of the data.



Scenario #1
County Ransomware Attack

On Monday, IT discovers that the County has been the victim of a ransomware attack. As a result, all employees are locked out of their computers and unable to work.

The IT team finds copies of a ransom note on workstations and servers.

The Ransom Note

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought
by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we
want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly
make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being
properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over
it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us
on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know
about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you.
```


Action Steps

- Should the County use the IT firm it has an ongoing support relationship with to conduct the forensic investigation?
- Why or why not?
- How much is this going to cost the County. Who approves?
- What, if anything, is the amount that the County is willing to pay to get its data back and prevent the release? Who decides?
- How involved is MCIT?

ECKERT SEAMANS ATTORNEYS AT LAW
Sylint
www.eckertseamans.com

Notify MCIT

Who does the county notify?
Who does the county NOT notify?

County notified MCIT, immediately begins working with Counsel & Sylint to assess the scope of the incident and identify options to recovery.

ECKERT SEAMANS ATTORNEYS AT LAW

Sylint.

www.eckertseamans.com

Sylint initiates contact with TA

- Sylint reaches out to the Threat Actors (TA) who are demanding payment of 30 bitcoin ($1.25 million) to provide a decryption key to restore the network.
- TA sends 15 sample files to “prove” they have been in the network and mean business and threatens to publish all data unless it is paid
- The files include sensitive information related to residents.
- Some of the files contain employee PII.
- What is the County’s priority at this time?
- Does the County have any obligation to provide notice at this time?

ECKERT SEAMANS ATTORNEYS AT LAW

Sylint.

www.eckertseamans.com

Impact Becomes Clearer

The County working in conjunction with Counsel & Sylint, determines that the backups they were depending on for recovery were impacted by the TA and are not viable. Unless a deal can be reached to acquire a decryption key, the County will likely be missing vital files from several departments including county clerk, courts, sheriff, human resources and social services

Sylint negotiates to (1) gather additional intelligence; and (2) attempt to reduce the extortion demand to a more acceptable amount.

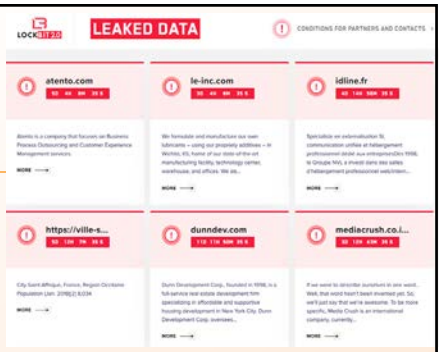
TA Applies Leverage

- The TA becomes frustrated with the pace of negotiations and does the following:
  - ✓ Start calling employees and leave messages about what will happen if payment is not made.
  - ✓ Launch DDOS attacks to shut down County website
  - ✓ Email employees
- Employees flood HR with calls and are very concerned.
- What do you tell employees?
- What do you tell member residents about the website?
- What if anything can be done?

TA Leaks Sensitive County Data on the Dark Web

- In order to incentivize payment, 15 County files are posted on the Dark Web by the TA.
- TA demand reduced to $430,000.
- Does County pay? Who makes this decision?
- Open Meeting rules? County Attorney?

Data Released



- TA publishes 15 files on their Dark Net site.
- The files include:
  - information provided in litigation subject to a confidentiality order
  - PII of employees
  - Contracts related to a new water treatment facility
  - Voter registration information

It's a Criminal Investigation

- Treat IT environment like the crime scene it is!
- Preserve evidence
- Critical to determining what has happened and the County's obligations

Media

- Local television and newspapers are demanding statements about the ransomware attack. The lead story on the 12:00 news is "County Shut Down – Ransomware Attack Stops them in their Tracks"
- Numerous other media sources including Krebs on Security begin publishing articles that your data was subject to unauthorized access.

An employee who started last month is trying to handle communications.

County Residents

- Residents are starting to call with questions about the incident and the security of their data.
- The AG is calling and wants to know how the attack happened and why they was not told sooner.

Employees are still unable to work and unsure how to respond to the calls.

Logistics

- The County decides to pay because it believes it can not recover the information from damaged backups. Who makes this decision?
- What is the recovery time if decrypting?
  - A. 1 hour
  - B. 1 day
  - C. 1 week
  - D. 2 weeks
  - E. Never
- Who is responsible for coordinating restoration?
- When did you last test recovering from backups?
- What is the most critical system to restore first?

If You Decide to Pay Ransom (Mechanics)

- Sylint typically handles all negotiations with TA
- 3rd party verifies that payment is not going to a country or group on US restricted list as required by recent OFAC advisory
- Sylint provides TA with sample of encrypted files to prove that TA can decrypt
  - Encrypted files need to be generic. (Do not send file with PII in it)
- Payment in bitcoin is made by 3rd party after receipt of funds from the County
- 3rd party makes bitcoin payment (there is typically an additional charge associated with facilitating the payment)

Notifications

- What notification obligations with respect to PII and litigation?
- How would you determine this?
- Who would review records?
- Who would send notice?
- What would the notice to litigation parties say?

More Questions

- Who is responsible for responding to the media inquiry?
- Who is responsible for providing the employees with talking points for handling resident calls? How will those talking points be distributed?
- Who is responsible for responding to the regulatory inquiry?
- Do you have enough information to determine there is a reportable data breach?

7 Stages of Incident Response

1. Containment – Prevent subsequent spread/damage
2. Assessment* (Scope) – Identify impacted assets
3. Preservation – Secure evidentiary material
4. Eradication – Remove and confirm clean environment
5. Restoration – Decrypt/restore data to resume functionality
6. Investigation – Determine cause, scope and impact
7. Modification – Adjust P&P, rules, training, settings as needed

CAPE RIM

* May include Threat Actor negotiations

Scenario #2
Business Email Compromise (BEC)

On Monday morning Acme Builders, a construction contractor that the County has been working with on jail improvement, asks about the status of a $250,000 payment that was due 17 NOV 2023.

The County has a record of wiring the money to Acme 13 NOV 2023.

BEC - Questions

- Would IT have any role in connection with this incident at this time?
- How would the County's legal team find out about this?
- What would the investigation be focused on at this time?

Review

Upon further review of the email account of the employee who made the wire transfer, it appears that Acme sent an email on 13 NOV 2023 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 13 NOV 2023 email came from accounts@acmebuilderz.com rather than accounts@acmebuilders.com.

More Questions

- Should MCIT be alerted to this situation?
- Is this incident a data breach?
- Should outside counsel be contacted?
- Who is responsible for the lost payment?

Investigation

The forensic investigation determines that the employee responded to a phishing email and provided his credentials. 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.

Considerations

- 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?

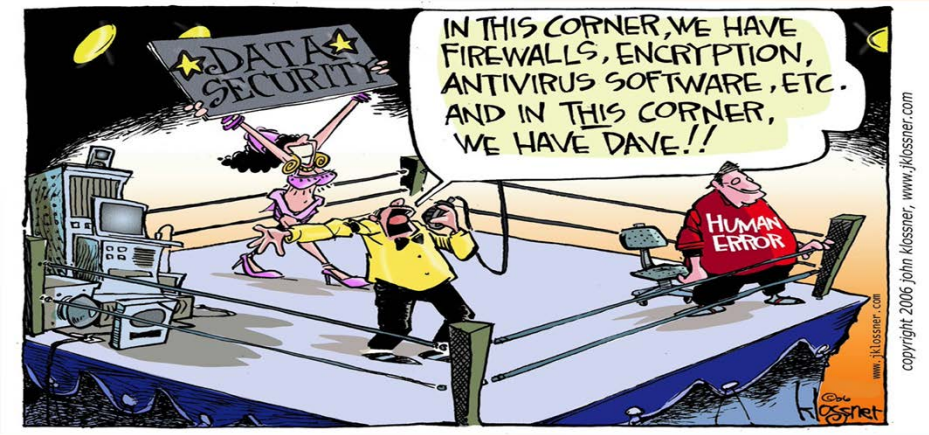
Financial Fraud Kill Chain (FFKC)

- FBI Initiative
  - < 72 Hours
  - > $50,000
  - International
  - SWIFT recall notice initiated

Take Aways

- Does the County have an incident response plan?
- Does the County have an incident response team?
- Has the County done a tabletop exercise to test response?
- Does the County have multi-factor authentication in place?
- Does the County have end point monitoring?
- Does the County outsource IT?
- Does the County have secure backups? Tested?
- What do the County's agreements require vendors with access to PII to do in the event of a cyber incident?

A Reminder!



ECKERT SEAMANS ATTORNEYS AT LAW

Sylint.

www.eckertseamans.com

Questions?

Thank You!

Matt Meade
Eckert Seamans
mmeade@eckertseamans.com

Jeff Birnbach
Sylint
jbirnbach@sylint.com

www.eckertseamans.com

Sylint.

ECKERT SEAMANS ATTORNEYS AT LAW