FOLEY
FOLEY & LARDNER LLP

Are You Prepared for a Ransomware or Business Email Compromise Attack?

May 2017 Midwest Cyber Security Alliance Meeting

Thursday,
May 18, 2017

4:30 p.m. –
6:30 p.m. CT

Thank You to Our Co-Hosts

4Discovery

HALOCK
Purpose Driven Security

Disclaimer

- The information presented in this seminar is not legal advice or a legal opinion, and should not be construed as a recommendation regarding any particular course of action.
- The views of the presenters are their own personal views and should not be attributed to their respective employers or to any of their employer's clients.

FOLEY
FOLEY & LARDNER LLP

3

Presenters

MODERATOR:

Jennifer Rathburn
Partner, Foley & Lardner LLP

Chad Gough
Co-Founder and Partner, 4Discovery

Terry Kurzynski
Founder and Senior Partner, HALOCK Security Labs

FOLEY
FOLEY & LARDNER LLP

4

FOLEY
FOLEY & LARDNER LLP

Cybersecurity Governance Issues

Director's and C-Level Executive's View of Cybersecurity

- More than 90% of corporate executives at the most vulnerable organizations say they cannot read a cybersecurity report and are not prepared to handle a major cybersecurity attack.
- 98% of the most vulnerable have little confidence in their company's ability to monitor devices/users on their systems.
- 40% said they don't feel responsible for the repercussions of hacking and are not personally responsible for cybersecurity or for protecting customer data.
  - It's the IT department's problem

- Source: "The Accountability Gap: Cybersecurity & Building a Culture of Responsibility" Tanium Inc. and Nasdaq, Inc. (2016)

FOLEY
FOLEY & LARDNER LLP

Core Duties for Board Privacy and Security Governance

- **Oversee** the cybersecurity program and **ensure staff** are taking measures to secure data to ensure **fiduciary duties** are met.
- Decisions should be made with the duties of **care** and **loyalty** in mind.
- Organizations using the **NIST Framework** will have the ability to demonstrate that they used **prudent practices and due care** in line with nationally recognized industry standards.

FOLEY
FOLEY & LARDNER LLP

7

Five Cybersecurity Principles Every Board Director Needs to Know

1. Understand and Approach Cybersecurity as an Enterprisewide Risk Management Issue, Not Just an IT Issue
2. Understand the Legal Implications of Cyber Risks as They Relate to the Company's Specific Circumstances
3. Have Adequate Access to Cybersecurity Expertise and Give Cyber Risk Management Regular and Adequate Time on Board Meeting Agendas
4. Set the Expectation That Management Will Establish an Enterprisewide Risk Management Framework With Adequate Staffing and Budget
5. Management Discussions Should Include Identification of Which Risks to Avoid, Which to Accept and Which to Mitigate or Transfer Through Insurance

- Source: "NACD Director's Handbook on Cyber-Risk Oversight" National Association of Corporate Directors (2017)

FOLEY
FOLEY & LARDNER LLP

8

FOLEY
FOLEY & LARDNER LLP

Intro to Ransomware

Ransomware

- Malware that disrupts and asks for payment to restore access to digital assets
- Every type and strain of ransomware has a different solution
  - Dynamic malware that is constantly updated
- Varies in level of sophistication, intrusiveness, and persistence
  - Can spread like wildfire
  - Can be timed
  - Can be fake
- Attacks typically center on:
  - Blocking system access; or
  - Encrypting data
- Victims are told the only way to access files is to pay a ransom
- Most ransomware spreads by a phishing scam or malicious link

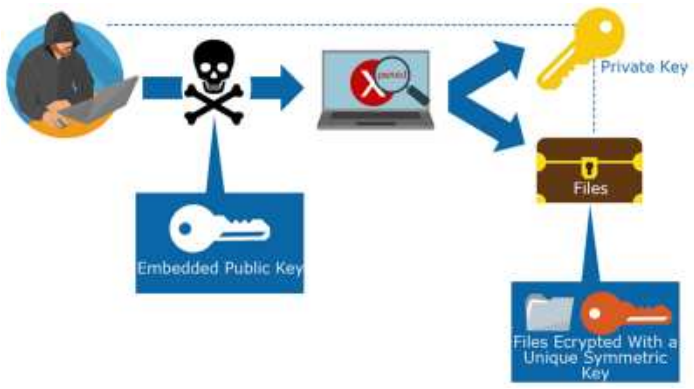
FOLEY
FOLEY & LARDNER LLP

Ransomware Facts

- First type of ransomware was written in 1989 and asked for $189
  - The "AIDS Trojan" encrypted file names, hid files, and asked for a ransom
  - Ransom did not have to be paid to get data back
- Today's ransomware varies in sophistication, but is far more lucrative
  - 2016 - Number of variants expanded by somewhere between 11x and 30x
  - 2016 - Average ransom amount was $679
  - 2016 - For corporations, can be as high as $60K
- There were approximately 638 million ransomware attacks in 2016
  - Every 10 seconds, a consumer is hit with ransomware
  - Every 40 seconds, a business is hit with ransomware
- Ransom payouts likely topped $1 billion in 2016

FOLEY
FOLEY & LARDNER LLP

How Ransomware Works



FOLEY
FOLEY & LARDNER LLP

Popular Ransomware

- Locky
  - Spread via email containing malicious MS Office docs
- Crysis / Dharma
  - Weak passwords via MS Remote Desktop
- WannaCry
  - Used a patched vulnerability in MS File Sharing (SMB) to spread

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Triaging Ransomware

Quarantining and Triaging Devices

- As close to immediate response as possible
- First 48 hours are most important in response
  - Blocked access costs clients time and money
  - Insurance claims can be impacted based upon the speed of solutions
  - Many ransomware variants are timed
- Must identify and quarantine infected devices
  - Many ransomware variants spread amongst devices and can hit entire networks
  - Remove from network to stop potential spread
- Create a log of infected devices and prioritize them
  - Some machines and data sources are more valuable than others
  - This will help inform your workflow

You Have Backups Right?

- If you still have a copy of your data, nothing is held for ransom
- Once devices are identified, attempt to identify backup solutions for each infected device
- If backups are available, solutions are simpler
  - If backups are new, there may be very little data loss
  - If backups are old, client may face data loss
- If backups are encrypted, solutions are more limited
  - Some ransomware cases have ended in almost total data loss
- Be careful with near time snapshots and replication as “backups”, your backups will soon become encrypted

No Backups? Encrypted? Data Important?

- You're probably going to have to pay
- There are a few things you need to do first?

FOLEY
FOLEY & LARDNER LLP

17

FOLEY
FOLEY & LARDNER LLP

Identifying & Eradicating Ransomware

Ransomware?

- In order to identify the severity of the problem, you have to ensure it is actually ransomware
- Some "variants" appear to be legit but are just annoying malware
- Is it an annoying lockscreen?
  - Some lockscreen variants disappear with a simple Alt+F4 or Ctrl+Alt+Del
  - Once you close the screen, you can examine files
- Is anything actually encrypted?
  - Especially with simple lockscreens, files are not encrypted
  - For unsophisticated malware, file extensions may be changed, but no encryption occurred
    - Sometimes changing it back to the original filetype is all that is required
- If it is just malware, remove it like you would any other malicious item

FOLEY
FOLEY & LARDNER LLP
19

Tips for Identifying Malware

- Use the original lockscreen to look for clues
  - Does it tell you its name?
  - Is there an email address listed?
  - Is there a BTC wallet address or other payment method specified?
  - Is there anything else unique about this page that you can use as a search term?
- Use these clues to conduct your research
  - With ransomware, online research is king
- Resource ideas
  - Comb through your own personal knowledge base
  - Look at databases maintained by security experts
  - Search for posts on forums
  - Read news articles and blog posts
- Most importantly: ensure it is actually ransomware . . .

FOLEY
FOLEY & LARDNER LLP
20

Initial Triage

- Are your files really encrypted?
  - Some ransomware only encrypts the first few bytes of a file
- What strain of ransomware do you have?
  - Is decryption available?
- How many machines, how much data?
  - Make a list, most important machines first
- Many antivirus and spyware vendors advertise solutions that will screen out certain strains of ransomware

FOLEY
FOLEY & LARDNER LLP
21

Data Recovery

- Volume Shadows are not securely deleted
- Can be recovered and parsed using forensics
- Data can be carved
- Not all file types get encrypted

FOLEY
FOLEY & LARDNER LLP
22

Ransomware Removal

- Quarantine devices
- **DO NOT** start running AV and removing malware on ransom's computers

Finding Ransomware Solutions

- Information regarding ransomware is often disparate and difficult to find
  - There is no comprehensive database, solution, or tool set
- Once the ransomware has been identified, look for solutions
  - Comb through your own personal knowledge base
  - Look at databases and tools maintained by security experts
  - Search for posts on forums
  - Read news articles and blog posts
- If decryption is possible, there are more solutions available
  - Try known keys and available to attempt decryption
- If decryption is not possible, have to rely on backups and/or pay up

If No Solution Can Be Found . . .

- . . . and the data isn't critical
  - Install a new hard drive
  - Do a fresh install
  - Load backup if available
- . . . and the data is critical
  - Might have to pay
  - Don't get your hopes up

If You Get a Key . . .

- Use it to decrypt your device(s)
  - Make sure to save this key
- Remove files associated with the ransomware
  - Many security researchers have identified specific files associated with each strain
- Make backups of all of the available data and store for later use
- Nuke the systems and do a fresh install from known good media

FOLEY
FOLEY & LARDNER LLP

Paying Ransoms

Before You Pay . . . NO MORE RANSOM!

- Double check to make sure there is no known solution!
- https://www.nomoreransom.org/index.html

Before We Talk About Payment . . .

- Understand that it should be an absolute last resort
- It is not recommended as a best practice
- It should only be used in cases where data is a necessity and cannot be replicated by any other means
- Paying ransoms will:
  - Perpetuate the scheme
  - Make you more likely to be struck again
  - Possibly not result in getting your data back

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Cooperating With Law Enforcement

Help Them Help You

- Information sharing allows LEAs to track individuals dispensing ransomware
  - Incidents are underreported, which makes their investigations more difficult
- It is best to conduct your own investigation and share information with the FBI
  - Because time is of the essence, you have to be the first responder
  - This way, you are able to give them information and move on your merry way
- If the actors are caught, it is possible the assets can be seized and payments can be returned
  - Because most people do not report their breaches, they are unable to get back the money that was taken from them

What to Submit

- The FBI asks victims to reach out to local FBI office and/or file a complaint
- Complaints should be filed at Internet Crime Complaint Center (www.IC3.gov) with the following ransomware infection details:
  - Date of Infection
  - Ransomware Variant (identified on the ransom page or by the encrypted file extension)
  - Victim Company Information (industry type, business size, etc.)
  - How the Infection Occurred (link in email, browsing the Internet, etc.)
  - Requested Ransom Amount
  - Actor's Bitcoin Wallet Address (may be listed on the ransom page)
  - Ransom Amount Paid (if any)
  - Overall Losses Associated with a Ransomware Infection
  - Victim Impact Statement

Security Community Information Sharing

- In addition to handing over data to law enforcement, you can also opt to share with security researchers
- Providing decryption keys and other important data to members of the security community can help them develop new solutions and tools
- They often use this research to also brief law enforcement on new developments and new approaches
- Without information sharing, little can be done to tackle ransomware

FOLEY
FOLEY & LARDNER LLP

FOLEY
FOLEY & LARDNER LLP

Preventing Infections & Data Loss

Education is Key

- The vast majority of ransomware cases include error on the part of the user
- Typically, the user:
  - Clicks on a shady link
  - Opens an email attachment from a phishing email
  - Visits a website drowning in malicious code
- By training people to have better security habits, you can help prevent it
  - Training should be done on a routine basis with staff to update them
- You should also send security updates via newsletter
  - As long as it's interesting to read, it keeps people alert and aware of their surroundings

FOLEY
FOLEY & LARDNER LLP
35

Backing Up Like a Boss

- Make sure backups are conducted regularly
  - This ensures the loss of data is minimal if you have to restore from backup
- Make sure that backups can't be easily accessed during a ransomware attack
  - Make physical tape backups and disconnect them
  - Keep backups in a separate network environment
- If backups are easily accessible during an attack, they often get encrypted
  - Pro tip: If they are hit, they are typically unusable
- This way, even if you do get hit, it won't matter

FOLEY
FOLEY & LARDNER LLP
36

Have a Plan

- Make sure you have a plan and that it's updated regularly
  - This environment changes rapidly
  - You will not go far with a stale playbook
- Maintain a KB of solutions, especially ones you have troubleshot
  - Share this info with the community
  - We can all learn through info sharing

Forensics for Root Cause

- APT - advanced persistent threat
  - Use the persistence to help you identify infection point
- AutoRuns
- Timelines
- Log Analysis
- Event Correlation
- Anything else in your forensic bag of tricks . . .
- You want to know how it got in, so future events can be avoided

FOLEY
FOLEY & LARDNER LLP

Business Email Compromise

Business Email Compromise (BEC)

- Also known as email account compromise (EAC)
- Is a form of phishing attack where a cyber criminal impersonates an executive (often the CEO), and attempts to get an employee, customer, or vendor to transfer funds or sensitive information to the phisher
- Common compromises:
  - Wire Fraud
  - W2 Scam
- Targets individuals of companies that handle wire transfers and W2 records
- BEC scams have increased 2,370% from last year

FOLEY
FOLEY & LARDNER LLP

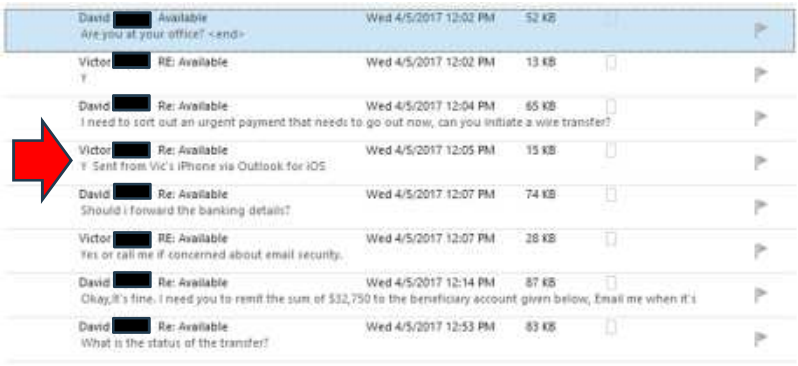
(BEC) – Scam Types

- Version 1
  - A long standing supplier asks for wire funds for payment to be sent to new fraudulent account, "The Supplier Swindle."
- Version 2
  - C-suite email is compromised or spoofed by hacker requesting a wire transfer to employee responsible for wire transfers. Request is usually made at 3:30PM on a Friday and the C-suite is not available to verify, "CEO Fraud or Whaling."
- Version 3
  - Company Controller's email is hacked and criminals identify known vendors that pay by wire. Email is sent out from hacked email account to suppliers requesting wire be sent to new fraudulent account.

(BEC) – Scam Types (cont'd.)

- Version 4
  - Target is contacted by fraudster posing as attorney of law firm who needs funds immediately to handle time sensitive matter, "The Attorney Swindle."
- Version 5
  - Fraudsters use compromised or spoofed Executive email account to request W2 records for all employees. This is usually around tax season and may or may not be accompanied by a wire fraud request.
- Version 6
  - Real estate transactions are monitored by fraudsters and they perpetrate one of the transaction parties to change the payment to a wire transfer with the correct timing of the transaction.

(BEC) – Wire Fraud Actual Example



David [redacted]	Available Are you at your office? <end>	Wed 4/5/2017 12:02 PM	52 KB
Victor [redacted]	RE: Available Y	Wed 4/5/2017 12:02 PM	13 KB
David [redacted]	Re: Available I need to sort out an urgent payment that needs to go out now, can you initiate a wire transfer?	Wed 4/5/2017 12:04 PM	65 KB
Victor [redacted]	Re: Available Y Sent from Vic's iPhone via Outlook for iOS	Wed 4/5/2017 12:05 PM	15 KB
David [redacted]	Re: Available Should I forward the banking details?	Wed 4/5/2017 12:07 PM	74 KB
Victor [redacted]	RE: Available Yes or call me if concerned about email security.	Wed 4/5/2017 12:07 PM	28 KB
David [redacted]	Re: Available Okay,It's fine. I need you to remit the sum of $32,750 to the beneficiary account given below, Email me when it's	Wed 4/5/2017 12:14 PM	87 KB
David [redacted]	Re: Available What is the status of the transfer?	Wed 4/5/2017 12:53 PM	83 KB

Bank Name: Wells Fargo

Account Name: [redacted]

Account Number: 3133238539

Routing Number: 121000248

Bank address: 4454 Roswell Rd NE Atlanta GA 30342

The email with the arrow is where Vic was texting with David – and emailing the Bad Actor so they would reveal themselves. He answered with a "Y" from his phone while texting David. At this point, he knew this was bogus – he could also tell the email address was fraudulent.

(BEC) – Statistics

- FBI reports that between 2013 and December 2016:
  - 40,203 cases of BEC (22,292 US)
  - 5.3B in earnings from BEC (1.6B US) wire fraud
  - Second half of 2016: 3,044 attacks and $346M in losses for US
- Ubiquiti (San Jose technology provider) hit with $39M BEC scam in 2015
- In 2016, Fischer Advanced Composite (Austrian Company) fired its CEO of 17 years because the company fell victim to a $47M BEC scam.

(BEC) – W2 Scam

- According to IRS Commissioner, John Koskinen:

"This is one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme."

W2 Scam Statistics

- 145 reports in which cybercriminals successfully obtained the information they were after in 2016.
- According to the IRS, more than 29,000 employees were impacted by these fraudulent schemes in 2016.
- In January 2017 alone there were 23 of these attacks that were successfully implemented.
- Industries most impacted: chain restaurants, temporary staffing agencies, healthcare organizations, shipping and freight companies, tribal casinos, and school districts.

W2 Scam Example Subject Lines

- Request for Employee W2 2016
- 2016 W2's
- John's W2
- Accounting firm lost the W-2s
- The company is preparing for an audit
- The manager wants to send the form to central storage

W2 Scam Example Text

- "Kindly send me the individual 2016 W-2 (pdf) and earnings of all W-2s of our company for a quick review."
- "Can you send me the updated list of employees with full details (name, Social Security number, date of birth, home address, and salary)?"
- "I want you to send me the list of W-2 copy of employees wage and tax statements for 2016. I need them in pdf file type, you can send it as an attachment. Kindly prepare the list and email to me asap."

(BEC) – Recommendations

- Establish “out-of-band” communication to verify new wire transfers and changes to account for wire transfers.
- Perform regular Security Awareness Training and have specialized training for those who have privileged access.
- Perform social engineering testing to evaluate the effectiveness of your security awareness training.
- Review your Incident Response Plan and IR Readiness.
- Evaluate email security solutions that are able to block some of the fraudster emails (especially the Ransomware, which is a precursor to BEC).

(BEC) – Personal Recommendations

- File your taxes early.
- Freeze your credit file:
  - Equifax
  - Experian
  - Innovis
  - TransUnion
- Notify ChexSystems.
- Opt out of pre-approved credit offers and postal mailings.

Thank You

CONTACT US

Jennifer Rathburn
JRathburn@foley.com

Chad Gough
Chad@4discovery.com

Terry Kurzynski
TerryK@halock.com

FOLEY
FOLEY & LARDNER LLP