CONNELL FOLEY

A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Practical and Legal Risk for New Jersey School Districts

Presenters:

Karen P. Randall - *Chair, Cybersecurity and Data Privacy Group - Connell Foley LLP*

"DON'T YOU HAVE ANY HACKING SKILLS?"

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

According to the 2018 Ponemon Institute Study, What Is the Cost of a Data Breach?

A. $2.2 Million
B. $3.9 Million
C. $4.0 Million
D. $5.5 Million

According to the 2018 Ponemon Institute Study, What Is the Cost of a Data Breach? *(cont'd)*

- **ANSWER B - $3.9 Million**
  - The study also reports that the average cost incurred for each lost or stolen record containing sensitive and confidential information is ***$148***.

Cyber-Attacks on School Districts Are on the Rise

- According to report entitled, “The State of K-12 Cybersecurity: 2018 Year in Review” a U.S. school district becomes the victim of a cyber-attack almost as often as every three days.

Cyber-Attacks on School Districts Are on the Rise

- According to the report, this past year, public K-12 education institutions experienced 122 known cybersecurity incidents, ranging from data breaches to phishing scams and ransomware attacks.
- However, this number is believed to be higher because many districts elect not to disclose such incidents to the public.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Cyber-Attacks on School Districts Are on the Rise in New Jersey

- Examples:
  - West Milford School District (May 3, 2017)
  - Wayne School District (April 1, 2017)
  - Bloomfield Public School District (November 6, 2017)
  - Pineland Regional School District (March 7, 2018)
  - Irvington Public School District (April 18, 2018)

Crown Jewel Myth

- **Old Model:** Cybercriminal hacks into a company's network and takes its crown jewels—data that had some measure of value on the cyber black market, *i.e.*, the DarkNet.
  - The bad guy then monetizes this crime by selling the data on the DarkNet to someone who would use it for fraudulent purposes to also make money.
  - The profit was in stealing data and so data has to be worth something to make it profitable for the bad guy.
- **Myth:** If enterprise does not have crown jewels…it will not be a target for hackers.

Crown Jewel Myth

- **<u>The New Model</u>:** Extortion – taking away the availability of your data and your customer's data.
  - Infects a company's computer system with malicious software
  - Encrypts data
  - Demands payment of a ransom to unlock or decrypt the data within a certain timeframe
  - Failure to pay ransom may result in destruction of decryption key and data

Types of Cyber-Attacks

- Although there are many different ways for a data breach to occur, ransomware continues to be the number one method of attack used by threat actors:
  1. **RANSOMWARE**
  2. Unauthorized access
  3. Cryptojacking
  4. Socially Engineered Malware
  5. Hacktivists
  6. Insider Threats

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Consequences of a Ransomware Attack

- Types of Damages Incurred as a Result of a Ransomware Attack:
  - Legal
  - Ethical
  - Regulatory
  - Operational
  - Reputational

Ransomware Damage Costs on the Rise

- The collateral costs of a ransomware attack include:
  - Damage and destruction (or loss) of data
  - Downtime
  - Lost productivity
  - Post-attack disruption to business
  - Forensic investigation
  - Restoration and deletion of hostage data and systems
  - Reputational harm
  - Employee training in direct response to attack
    - Global spending on security awareness training for employees predicted to be $10 billion in 2027

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

What Makes School Districts Attractive Targets for Cyber Criminals?

- School districts are a “virtual buffet” of valuable data, filled with student information, health records, employee payroll data, financial data, and access to security systems, such as cameras, intercoms and security plans (New Jersey Cybersecurity and Communications Integration Cell (NJCCIC).
- School districts tend to have the smallest technology budgets and weakest cybersecurity risk management practices of any state or local government agency, and are least prepared to respond to an attack.

Why Are Threat Actors Using Ransomware?

- High success rate and visibility.
- Simple: Most attacks are executed by doing something as simple as sending a phishing email that tricks somebody in the company into clicking on a link in the email or downloading an infected attachment.
- Ransom is Paid: 70% of businesses hit by ransomware paid on average $20,000 - $40,000 to get their data back.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

What Is Ransomware?

- Form of malware.
- Encrypts victim's data and/or system.
- Demands payment for decryption.
- Numerous iterations.
- One infected user can ***SHUT DOWN*** an entire organization.
- Uses social engineering by sending employees suspicious emails with invoices or business documents most will likely open.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Ransomware Themes

- Ransom Page
  - May have FBI variant, the Internal Revenue Service, or even a “Breaking Bad” TV show called ransomware.
  - Provides information about victim’s computer
  - Cost to decrypt
  - Deadlines
  - Instructions for payment

Are You Infected? Warning Signs

- Cannot open normal files
- Receipt of alarming message on desktop background
- Countdown for ransom payment
- Cannot close window to a ransomware program
- Files are labeled
  - How to decrypt files .TXT, or decrypt instructions HTML


Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/8/2013
5:52 PM
Time left
56 : 16 : 12


PETYA RANSOMWARE
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 13 hours 43 minutes 10 seconds
Start the decryption process


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.
OK
MoneyPak
Where I can buy MoneyPak?
Walmart
Walgreens
RITE AID
CVS pharmacy


Your personal files are encrypted by CTB-Loc
95 59 22


Homeland Security
National Cyber Security Division
THIS COMPUTER HAS BEEN BLOCKED
THE WORK OF YOUR COMPUTER HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.
Article 184. Pornography involving children
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic material)
Article 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)
Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)
To unlock the computer you are obliged to pay a fine of $300.
You must pay the fine through MoneyPak.
You have 48 hours to pay the fine. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer and take You to Court.
MoneyPak
Code:
Pay MoneyPak
How to pay the fine using MoneyPak?
Walmart
Walgreens
CVS/pharmacy

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Dangerous Strains of Ransomware

- Ransomware attacks are on the rise with more than 4,000 occurring each day, across all industries, according to the U.S. Justice Department.
- 400,000 new strains of ransomware are detected daily making the attacks more sophisticated and harder to respond to.
- The following are some of the worst types of ransomware:
  - WannaCry
  - Locky
  - Petya/NotPetya
  - Cryptolocker
  - zCrypt
  - BitPaymer
  - Crysis
  - Cerber
  - CryptoWall
  - Emotet/Trickbot
  - Sodinokibi
  - Ryuk

Unique Strains of Ransomware

- Unique Strains of Ransomware:
  - **Popcorn Time**
    - Offers free decryption if you infect two others and they pay
    - Still proof of concept.
  - **Koolava (a.k.a. Nice Jigsaw)**
    - Offers free decryption if you learn how not to be infected
    - Once the victim reads two articles, the Decrypt My Files button becomes available.
    - It will delete all files if the articles are not read.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Responding to a Ransomware Attack

- Your organization has suffered a Ransomware Attack…**WHAT DO YOU DO?**

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

The First 72 Hours May Be the Most Crucial!

- Limit the economic/reputational harm to municipality.
- Limit legal liability.
- Containing an intrusion before it reaches systems holding staff/students' PII or PHI may stop a data breach from ever occurring.
- Help to promote confidence.
- Maintain employee morale.
- Forestall regulatory scrutiny.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Step 1: Don't Panic, Assemble the Incident Response Team

- FIRST AND FOREMOST…

- Locate the school's incident response plan and assemble the members of the incident response team.

Assembling the Team

- Incident Lead
- Executive Leaders
- IT Department
- Legal and Privacy Team
- Forensics

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Assembling the Team

- Public Relations
- Customer Care and Human Resources
- Law Enforcement
- Data Breach Resolution Provider
- Insurance Broker/Carrier

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Best Incident Response Practices

- Have an experienced Incident Response law firm and security vendor on retainer in advance
  - Enterprise should have a Bitcoin wallet and access to Bitcoin
- Ensure your Incident Response Team and Plan has a ransomware playbook
  - Ransomware requires accelerated response!
- Include ransomware scenarios in your incident response Tabletop exercises
- Ensure that your cyber liability insurance policy covers losses related to ransomware attacks

Step 2: Containment

- Once you determine you have been infected with ransomware, you must act immediately.

Step 2: Containment

Limit damage with containment:

- Unplug the computer and disconnect from the network, including all devices and on-line back-ups.
- Drop all connectivity between sites (VPNs, etc.).
- Check status of all on/off-site back-ups.
- Initiate alternate communications (personal email and cell phones).
- Do not erase or clean-up any files.
- Determine which computer is “Patient Zero”.

Step 3: Determine Scope of Compromise/Encryption

- Did infected machine have access to:
  - Cloud-based storage
  - Network storage
  - Shared or unsecured drives/folders
  - USB memory sticks

Step 4: Determine Strain of Ransomware

- Knowing strain will help you make the informed decision on next step
- Some strains already have decryption keys
- Some strains may not exfiltrate data
- May need security experts
  - See www.bleepingcomputer.com

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Step 5: Response Options

- After identifying scope and strain, the following are four basic responses to a ransomware attack
  - First Response: Restore Files from a Backup
  - Second Response: Try to Decrypt
  - Third Response: Do Nothing and Lose Data
  - Fourth Response: Negotiate and/or Pay the Ransom

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

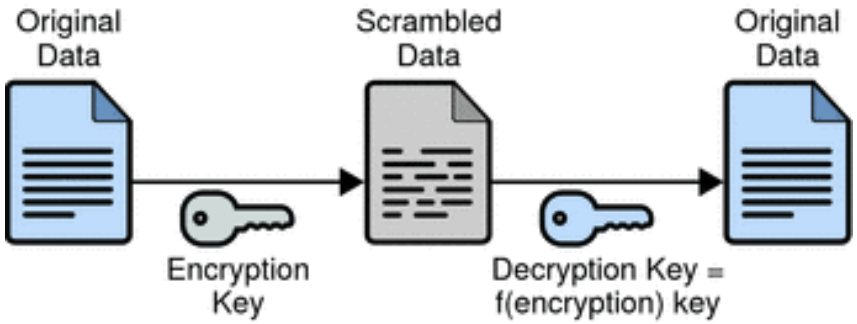
Response Option #1: Restore from Back-Ups

- First Option: Restore from Back-Ups
  - Do you have back-ups? How current are the back-ups? Where are they located? Is there a cloud service provider and vendor agreement involved?
- Back-ups are critical
  - If infected, back-ups may be the only way to recover lost data
- Ensure robust backup and restore procedures
- Secure back-ups offline

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Response Option #2
Try to Decrypt

- Second Option: Depending upon the particular ransomware variant that encrypted your system, you may be able to decrypt it.
  - Many of the decryption keys are available online free of charge.
- DOWNSIDE: In some cases, the files are so corrupt that even if you are able to decrypt and restore them, you may still lose data.



CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Response Option #3
Do Nothing and Lose Data

- Third Option: In some cases depending upon the type of data that is encrypted and the amount of the ransom demanded, it may be best to do nothing and accept that the data is lost.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Response Option #4
Negotiate and/or Pay the Ransom

- Fourth Option: In some scenarios you may determine that the data is too crucial to lose and you have no other means of restoring same.
- Thus, an organization may choose to negotiate with the threat actor and pay the ransom through an experienced incident response team.
- The FBI does not advocate payment.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

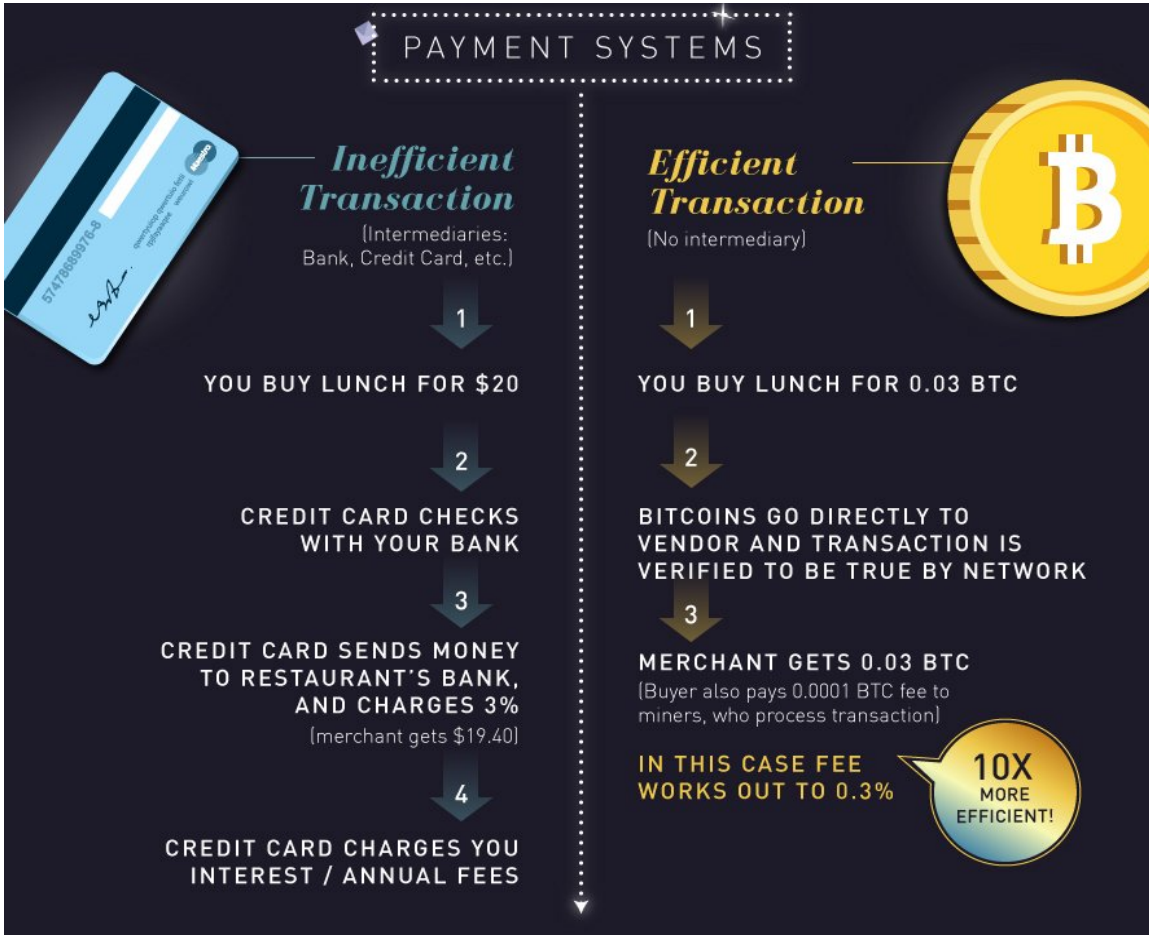
"Ideal" Payment Process

- IR firm contacts ransomer and indicates willingness to pay upon confirmation that keys will work (proof of life)
- IR firm and victim provide several encrypted files
- Ransomer returns decrypted files and provides account for bitcoin payment
- Insurance firm or victim authorize IR firm to execute payment
- Ransomer provides decryption key/tool and IR firm tests it in a sandbox
- IR firm and victim agree on process to decrypt systems
  - Generally off-line
  - Install endpoint security tools to prevent reinfection before reconnecting to the network

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Why Bitcoin and Not a Credit Card?

- Quicker
- Untraceable
- Virtual currency
- Price fluctuates



CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Step 6: Notification

Notification/Alert

Step 6: Notification

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.
- Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Step 6: Notification

- No consistency among state laws – impossible to craft single notification letter to all affected:
  - Varying definitions of personally identifiable information and what triggers reporting.
  - Many require notification of State AG (some in advance of notice to consumers).
  - Timelines for response vary widely; many "without unreasonable delay;" some as short as 5 days.
  - Prescribed content varies from state to state.

Step 6: Regulatory Requirements

- Similar to legal requirements, depending upon the industry in which you do business, certain regulations have notification requirements
- The Family Educational Rights and Privacy Act, or FERPA (20 U.S.C. § 1232g; 34 CFR Part 99)
  - The term "education record" is defined as those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. 20 U.S.C. § 1232g(a)(4)(i) and (ii).
  - Under the FERPA regulations, "disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.
  - The regulations further define "personally identifiable information" to include, but not limited to: the student's name; the name of the student's parent or other family member; the address of the student or student's family; a personal identifier, such as the student's social security number or student number; a list of personal characteristics that would make the student's identity easily traceable; or other information that would make the student's identity easily traceable. 34 CFR § 99.3.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Step 7: Defensive Measures to Avoid Ransomware Attacks

- Conduct a post-breach assessment to improve cybersecurity practices and remedial action is the final step.
- Engage a data security consultant to review existing practices under the guise of the attorney-client privilege.
- Promptly identify gaps and remedy security flaws.
- Use layered defense approach.
- Software based protections (antivirus, antispam/firewalls) and updates.
- Backup everything and Tested Restore.
- Implement security awareness training, simulate phishing attacks, and pen test personnel.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Step 7: Remedial Measures for Preventing a Ransomware Attack

- Have strong access controls. Student accounts should not have administrative privileges. Use internal restrictions on access.
- Vet and manage third-party vendors to transfer risk and ensure they follow appropriate data security laws and regulations.
- Review all policies of insurance and procure a standalone cyber liability policy that best fits coverage needs, including ransomware.
- Have an incident response team and plan ready.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

2019 Ransomware Trends

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Top 5 Ransomware Trends for 2019

1. Global ransomware damage costs are predicted to exceed $11.5 billion in 2019.
2. Ransomware generates over $25 million in revenue for hackers each year.
3. A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021.
4. 34% of businesses hit with malware took a week or more to regain access to their data.
5. A total of 850 million ransomware infections were detected by the Ponemon Institute in 2018.

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Final Thoughts on Cybersecurity

- "If you're not doing scans and penetration tests, then just know that someone else is. And they don't work for you."
  - George Grachis, Senior Consultant, Maxis360 - 2016

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938