RANSOMWARE: Prevention, Detection & the Cyber Insurance Response

Michael McHugh & Lee Pietrowski

Presented November 13, 2020

ILLINOIS ASBO ETHICS STATEMENT

This information is for the presenters only. ***Please remove this slide before your presentation.***

- The Moderator will help ensure the Illinois ASBO Code of Ethics is adhered to throughout the presentation and ensuing audience discussion.
- Moderators are given the authority to ask any attendee to leave if they become combative with presenters.
- This presentation is to be informative and not to promote specific products, services, companies, etc.
- If a Service Associate is a presenter and uses the presentation as a platform to "sell" their product or services, the Moderator has the authority to stop the presentation if the presenter refuses to modify their content.
- Any Service Associate presenter who violates these regulations may be excluded from presenting at future presentations.

Introductions

Name: Michael McHugh (Speaker)
- Area Senior Executive Vice President, Gallagher

Name: Lee Pietrowski (Speaker)
- Partner, IMAGETEC L.P.

Name: Julie-Ann Fuchs (Moderator)
- Associate Superintendent, Kaneland CUSD #302

Agenda

1. What is Malware? What is Ransomware?
2. Latest Ransomware trends
3. Covid-19
4. Case Studies – if infected how does your Cyber Insurance Policy respond?
5. Best steps to avoid falling victim to Ransomware
6. What type of Cyber coverage should you have?
7. How to Protect my Printers/MFP's and Faxes
8. Question & Answer?

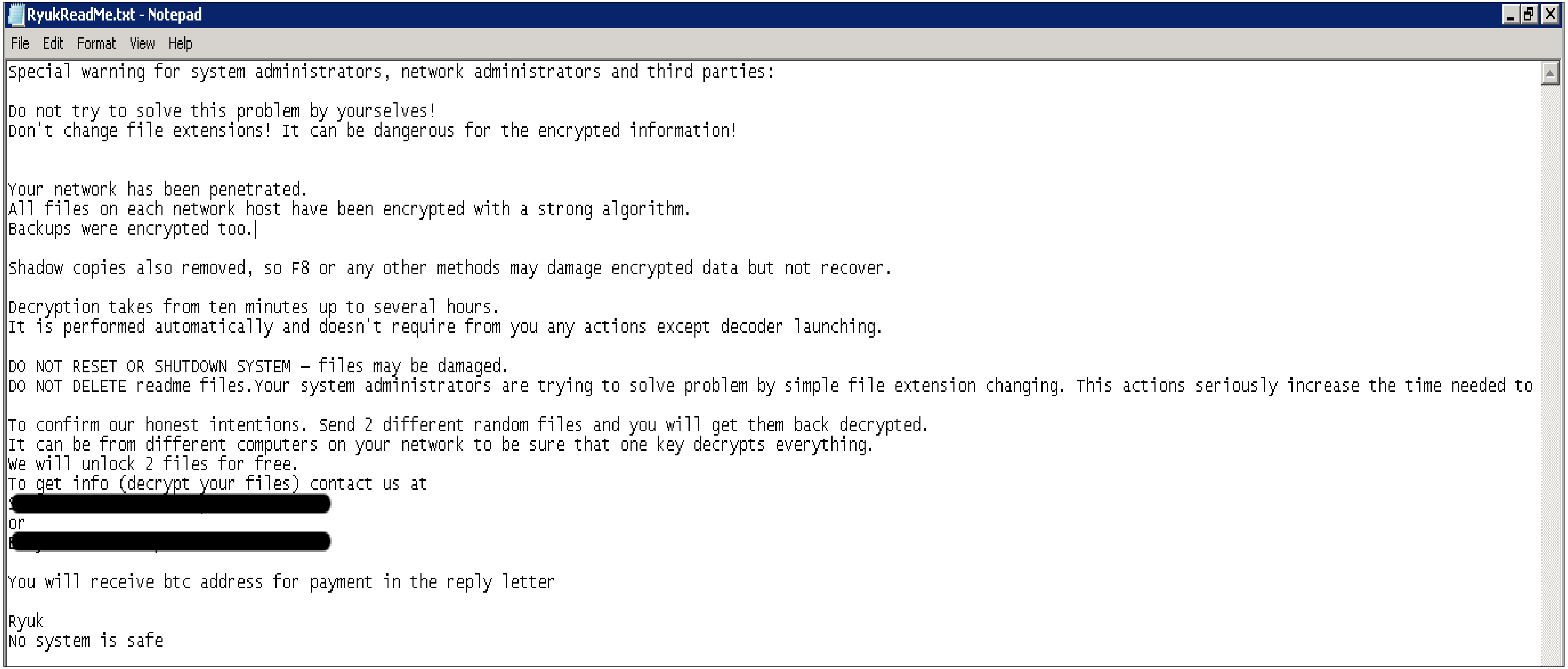
What is Malware?

- Malware is an umbrella term for all software or code which is created with malicious intent
- ***Mal**icious Soft**ware*** = Malware
- Malware includes - viruses, bugs, worms, bots, spyware, adware, Trojans, and… Ransomware

What is Ransomware?

- Ransomware is a sub-set of Malware which is designed to target individuals or organizations
- Ransomware locks access to systems or files by encrypting them
- Attackers then demand a Ransom to provide a decryption key to grant access back to the victim
- Ransoms are typically demanded in cryptocurrencies such as Bitcoin, as they are almost impossible to trace

Ryuk Ransomware Example



```
Special warning for system administrators, network administrators and third parties:

Do not try to solve this problem by yourselves!
Don't change file extensions! It can be dangerous for the encrypted information!


Your network has been penetrated.
All files on each network host have been encrypted with a strong algorithm.
Backups were encrypted too.

Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

Decryption takes from ten minutes up to several hours.
It is performed automatically and doesn't require from you any actions except decoder launching.

DO NOT RESET OR SHUTDOWN SYSTEM – files may be damaged.
DO NOT DELETE readme files.Your system administrators are trying to solve problem by simple file extension changing. This actions seriously increase the time needed to

To confirm our honest intentions. Send 2 different random files and you will get them back decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
We will unlock 2 files for free.
To get info (decrypt your files) contact us at
[redacted]
or
[redacted]

You will receive btc address for payment in the reply letter

Ryuk
No system is safe
```

Latest Ransomware Trends

https://cybermap.kaspersky.com/

Sharp increase in the average Ransoms demanded:

- **2017** – WannaCry & Not Petya – Ransom demanded was $150-300
- **2018** – Baker Hostetler Report – Average Ransom **paid** was $28,920
- **2019** – Baker Hostetler Report – Average Ransom **paid** was $302,539

  – Rise in RYUK Ransomware – Average Ransom **demand** in Q4 of 2019 was $779,856
- **2020** – Average RYUK Ransom **demand** in Q1 2020 was **$1,339,878**

Latest Ransomware Trends

Increased sophistication of Ransomware, enabling it to spread faster and wider

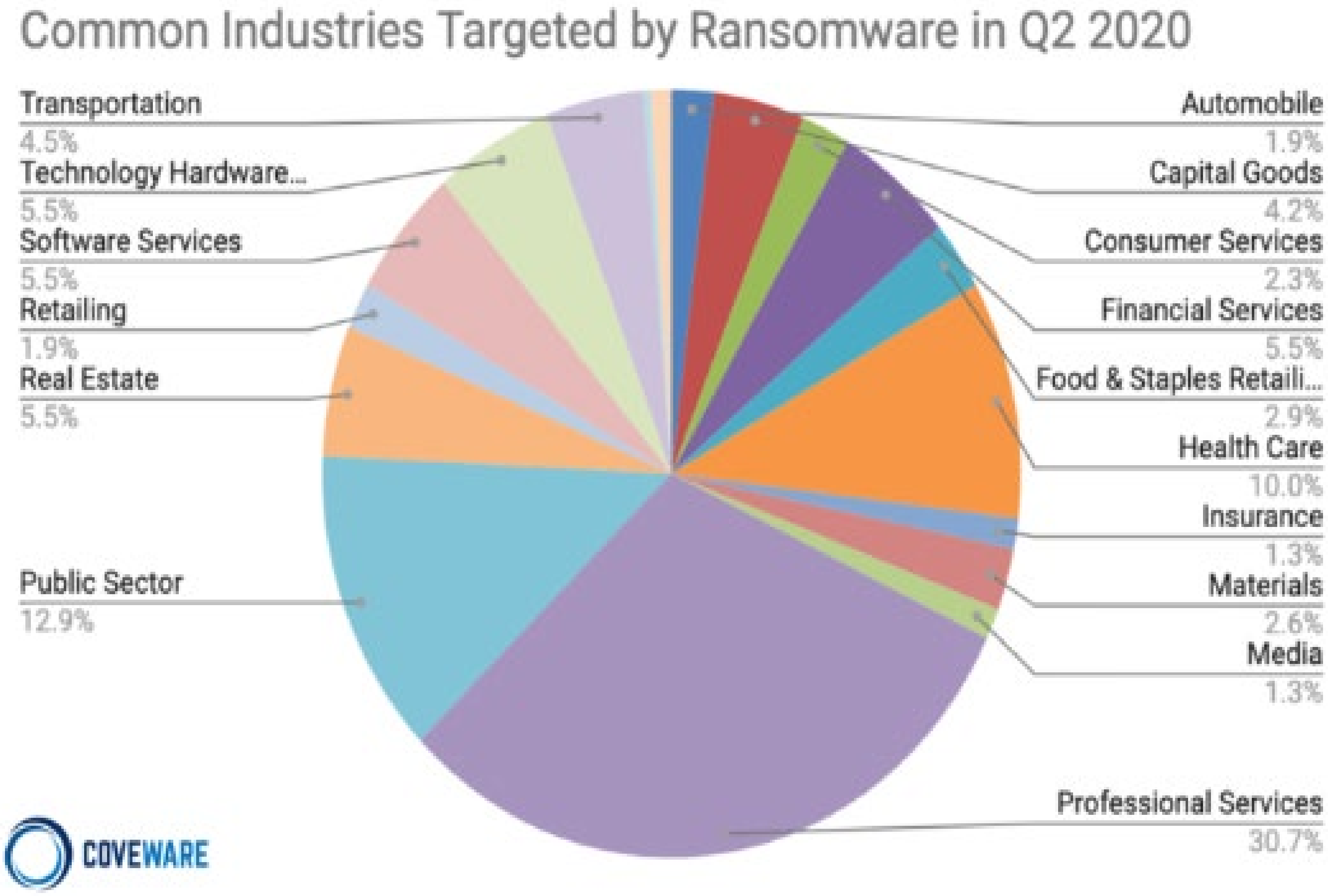
More and more strands of new Ransomware – e.g. Sodinokibi

- As of Q2 2020, Sodinikibi is now most prevalent Ransomware variant, with 15.4% Market share
- It is rumoured that the developers of Sodinokibi are the same developers who created Gandcrab. The developers of Gandcrab 'retired' the Gandcrab strain of ransomware in May 2019, claiming to have earned more than USD 2 billion.

Maze Ransomware – Exfiltrating data before deploying Ransomware

- In late 2019 / early 2020 a new threat actor group (Maze) upped the ante. **They started stealing data before deploying ransomware and leaving a ransom note that pointed the victim to a website where Maze published a sample of the stolen data and threatened to release more unless the ransom was paid.**

Latest Ransomware Trends



From Coveware Q2 2020 blog report:

A good example of this occurred with school districts (Public Sector) during Q2. School districts are typically targeted in July and August. The seasonality is deliberate; the threat actor wants to cripple the school right before school starts. In Q2, schools globally made a rapid, overnight shift to remote learning. The hastiness with which the shift occurred left many remote access vulnerabilities open. The number of vulnerable and cheap school targets increased, and the attacks quickly followed. In fairness to the security administrators of these organizations, the pressure and timing to adopt remote learning was completely unexpected.

Covid-19

- **Ransomware attacks increased 72% in the first half of 2020, amidst the Covid-19 global pandemic**

- Between February and March 2020 (i.e. start of global Covid-19 shutdowns) they increased **148%**

How are hackers getting in?

- Covid-19 related Phishing emails – e.g. Principle's email purporting to contain a Covid-19 update or new set of guidelines

- Data sprawl post Covid-19 – e.g. Teachers/Staff emailing documents to their personal emails, to print on home computers

- Remote login vulnerabilities

- Lower security standards on home/public WiFi networks

Cyber Insurance Coverage Overview

Recommended Cyber Insurance policies generally cover the following:

1. **Breach Response services** – Privacy Attorney, IT Forensics, Notification providers etc.
2. **First Party Business costs** – Extortion payments, Business Interruption, Data Restoration etc.
3. **Third Party Cost**s – Regulatory Fines, Third Party Damages etc.
4. **Limit** – At least $1,000,000 in the form of a standalone policy with a reputable insurer

Policies only responds when a claim/incident is reported – **so notify ASAP without delay!**

- Failure to notify impacts coverage provided – Insurers need to approve work provided by vendors (Breach Attorneys, IT Forensics etc.)

Important Breach Response Features – for K-12 School Districts

- Simple notification process – 1 single call to a 24/7 Breach Response Hotline handled by a reputable Cyber Security firm such as Phelps Dunbar – no need for emailed/written notice and duplicated phone calls
- Access to a Breach Response firm Specialist like Baker Hostetler who is a world leading Privacy Attorney, (handled Marriott and Capital One breaches)
- An IT Forensics panel that includes well known firms like Kroll, Kivu, Mandiant, Coveware (for Ransom negotiations and payments)

Case Studies – If infected how does your Cyber Insurance Policy respond?

Case Study 1:

- District became aware of infection of both RYUK Ransomware and TrickBot trojan malware
  - N.B. TrickBot and Emotet malware are precursors to RYUK, so always take immediate action if these variants of malware are detected

- RYUK Ransomware demand was for over $4m

- District engaged with Crypsis for IT Forensics

- Fortunately the District had adequate backups and was able restore the majority of systems without paying the ransom

- However – incurred over $800k of expenses

Case Studies – if infected how does your Cyber Insurance Policy respond?

Case Study 2:

- District became aware of infection of RYUK Ransomware, demanding 25 Bitcoin = $230k at the time
- Through the policy, District worked with with Phelps Dunbar/Baker Hostetler and was put in touch with Coveware
- Coveware negotiated the ransom down to 18 bitcoin = $165k at the time
- Ransom was paid and the decryption key was successfully deployed on the majority of systems

Best steps to avoid falling victim to Ransomware

1. **BACKUP, BACKUP, BACKUP**
   - Frequency – regularly (weekly minimum)
   - Quality – all critical files and data
   - Location – on and off-site, segmented from production systems
   - Test Backups – establish procedures to regularly test Backups
   - Build restoring from Backups into Incidence Response Planning
   - **Off-site backup required for coverage**

2. **Avoid being Phished**
   - Implement Employee phishing training
   - Use strong passwords – prevent duplication
   - Deploy an email threat filter

3. **Secure Remote Access – Especially in current environment**
   - Implement Multifactor Authentication (MFA) for remote access to systems and emails
     - **This is becoming a mandatory requirement for Cyber insurers to provide coverage**
   - Only implement Remote Desktop Protocol (RDP) where necessary

Best steps to avoid falling victim to Ransomware Cont.

4. **Ensure that you regularly apply all patches (updates)**
   - Attackers exploit software vulnerabilities which can be remedied by patches

5. **Deploy the following security measures:**
   - **Firewalls** – configured properly
   - **Endpoint Monitoring**

A Big Thank You to Will Slater and the Gallagher London Cyber Team!

Their Insight & Expertise was behind much of the vital information we shared with you today.

Cyber References and helpful links

- https://www.coveware.com/blog/q3-ransomware-marketplace-report
- https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report
- https://www.coveware.com/blog/reduce-ransomware-risk-by-90-for-free-in-one-day
- http://e.bakerlaw.com/rv/ff00498db267a11ce4182d53934889997a36f6d4/p%3D8213342
- https://www.fireeye.com/blog/threat-research/2019/09/ransomware-protectionand-containment-strategies.html

Lee Pietrowski

Partner/IMAGETEC L.P.

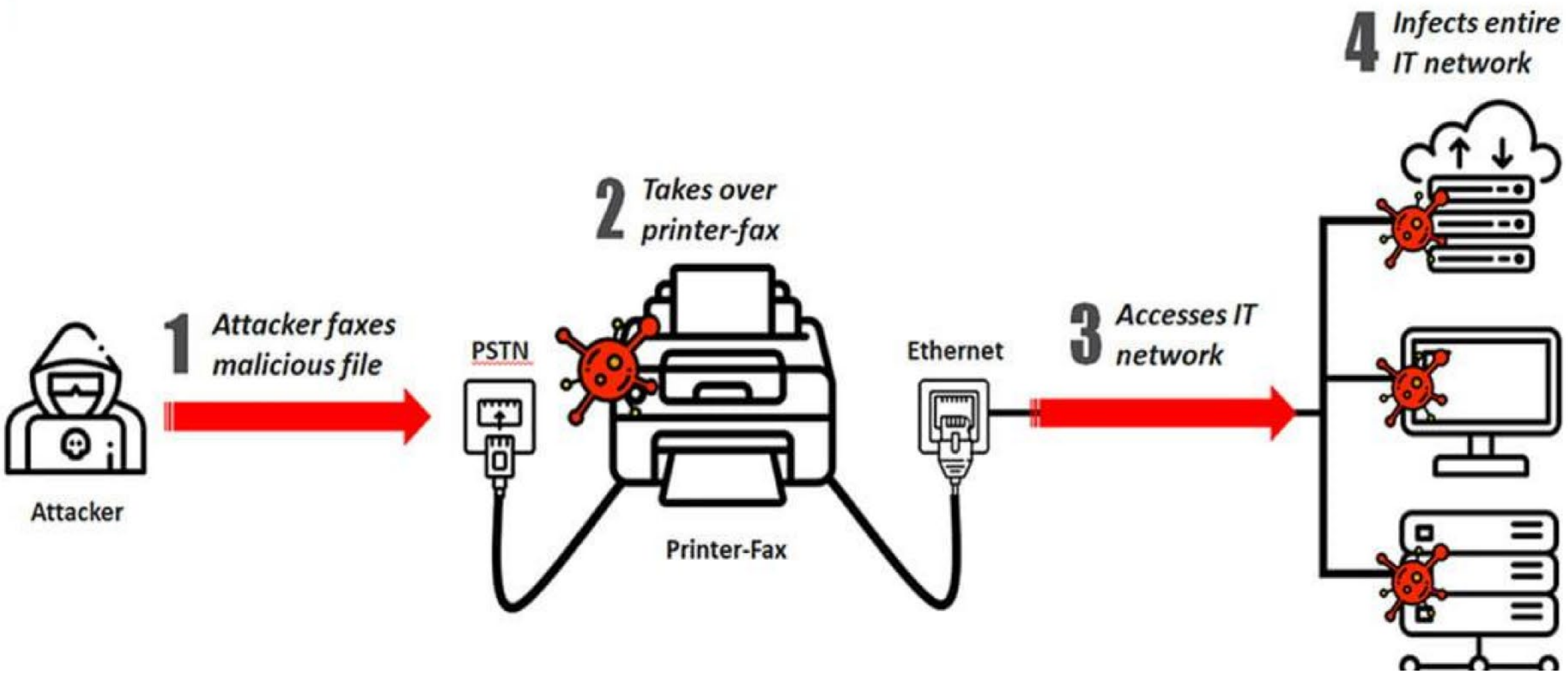
Cybersecurity will be a $6 trillion Problem by 2021

- Attacks are increasing
- AI malware is now being used to attack enterprise/public accounts
- AI will self-adjust the virus to continue attacking, looking for weak points as it learns
- For every 1 attack that is reported there are 50 that do not report.
- The average time from breach to detection is 146 days (*2017 Poneman Institute Cyber Report*)
- Only 38% of companies found their own breaches (*Verizon 2017 DBIR*)
- It is no longer a question of IF or WHEN an attacker will be successful: The question is HOW LONG and HOW MUCH will it take to recover from an attack?

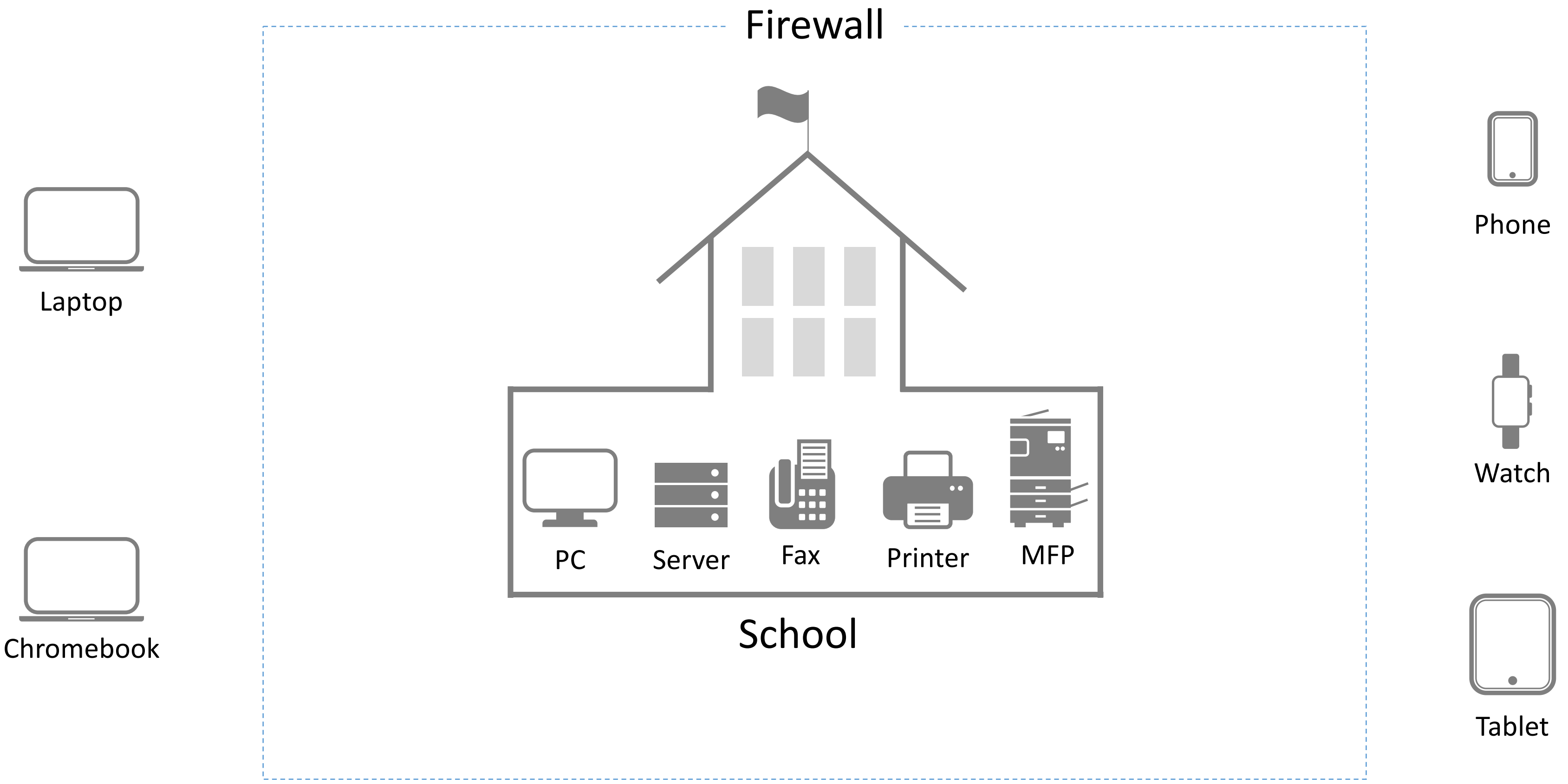
Are Printers, MFP's and Faxes Vulnerable?

- Today a printer is 68% more likely to be the source of an external threat or breach and 118% to be the source of an internal threat or breach
- Only 30% of IT pros recognize the printer/MFP as a security threat
- Printers are always put on the back burner as IT pros top priority is to secure the end-user devices

Fax Vulnerability



Internet of Things (IoT) Devices



Every Organization Should Have a Plan

- Resilience
  1. How long would it take you to recover 1000 of PC's, Printers, MFP's, etc.?
  2. How do you protect against malware you've never seen before?
  3. How do you proactively know when your fleet is under attack?
  4. What will the cost be to the organization, in the event of an attack?

Where Do I Start To Protect My Environment

- Check to make sure all Firmware is up to date on your printers, MFP's and Fax units. (if a model is no longer supported get it out of your environment) This includes 3D printers
- Implement a secure print release software (follow me type). This will act as a dual factor authentication process. (Card Release).
- Close all open ports (9120), Disable Bluetooth, AirPrint and NFC Printing. Devices should be on your network to print.
- Make sure to use a strong administration password on all devices. Do not use manufacture shipped passwords.

@ Home Teaching (Secure It)

- School devices should only be used for school business.
- Make sure that home wireless password is secure and changed from manufacturer’s password
- Make sure that your printer password and administration password are changed. Firmware updated.
- Do not save documents or coupons you found on the web to print back in the office or school for friends
- Disable Air Print

New Devices – What Should We Ask For

- Follow me software with secure release using a key FOB or HID Card. Make sure it works with any manufacture – Investment
- Devices with Cyber-Security Embedded into the units that contain-
  - Sure Start that will Monitor and Maintain the BIOS
  - Whitelisting to help protect the firmware
  - Run-Time Intrusion detection that keeps memory safe
  - Connection Inspector to stop suspicious network connections
  - Encryption to help keep data safe.
  - Card readers that encrypt users card information

Helpful resources

- Security Tips for Remote Workers

https://3bk.b06.myftpupload.com/wp-content/uploads/2020/10/IMAGETEC_NCSA-Remote-Working-Tipsheet.pdf

- Printer Security: The New IT Imperative
  Spiceworks Survey
  - http://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-3699ENW.pdf
- K12 Cybersecurity Resource Center
  - https://k12cybersecure.com

Thank You for a great job

- We would like to thank all the Administrators, Teachers and IT personnel that have done a great job in these times of uncertainty.

Questions and Answers

We thank you for your time!

Presenters:

MODERATOR INFO:

Julie-Ann Fuchs, Associate Superintendent; Kaneland CUSD #302
(630) 365-5111 Ext. 71119; jfuchs@kaneland.org

PANELISTS INFO:

Michael McHugh, Area Senior Executive Vice President; Gallagher
(630) 285-4373; Michael_McHugh@ajg.com

Lee Pietrowski, Partner; IMAGETEC L.P.
Direct: (630) 717-3772; lpietrowski@imagetec.com