Cyber Security:
Are Your Printers Secure?

This presentation is to be informative and not to promote specific products, services companies, etc. Illinois ASBO Sponsored Programs are permitted to promote products and services in accordance with the Service Associate Ethics Policy and Code of Conduct.

Introductions

Name: Lee Pietrowski. Role: Speaker
- *Partner, IMAGETEC L. P.*

Name: Mark Dodge. Role: Speaker
- *VP of Operations/Managed IT Services, IMAGETEC L.P.*

Name: Tom Kinane. Role: Moderator
- *Director of Technology, Elmwood Park C.U.S.D. 401*

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?

Some Data to Consider

- 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 as a security threat
- Printers are always put on the back burner as IT pros top priority is to secure the end-user devices

Some Data to Consider

- 46% of 2018 K-12 breaches included data about current and former school staff
  - Payroll information
  - Personal records
  - Leads to payroll theft, identify theft, false tax returns
- 60% of 2018 K-12 breaches included student data

Some Data to Consider

- This student information has been found on the dark web for identity thieves
- This will have long-lasting consequences for the students
- Most concerning in 2018 were a number of successful phishing attacks, targeted at school district business officials
- The largest attack was for $2 million in Texas

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?

End-Point Devices

- Printers, multi-functional products and fax units all have a BIOS which are vulnerable to attacks
- To protect against attack use layered security on all endpoint devices which might include
  - Complete end-point security analysis (detects vulnerabilities)
  - Authentication at device
  - Threat detection
  - Notification
  - Self-healing
- Antivirus, anti-malware and OS firewalls will not detect an infected BIOS

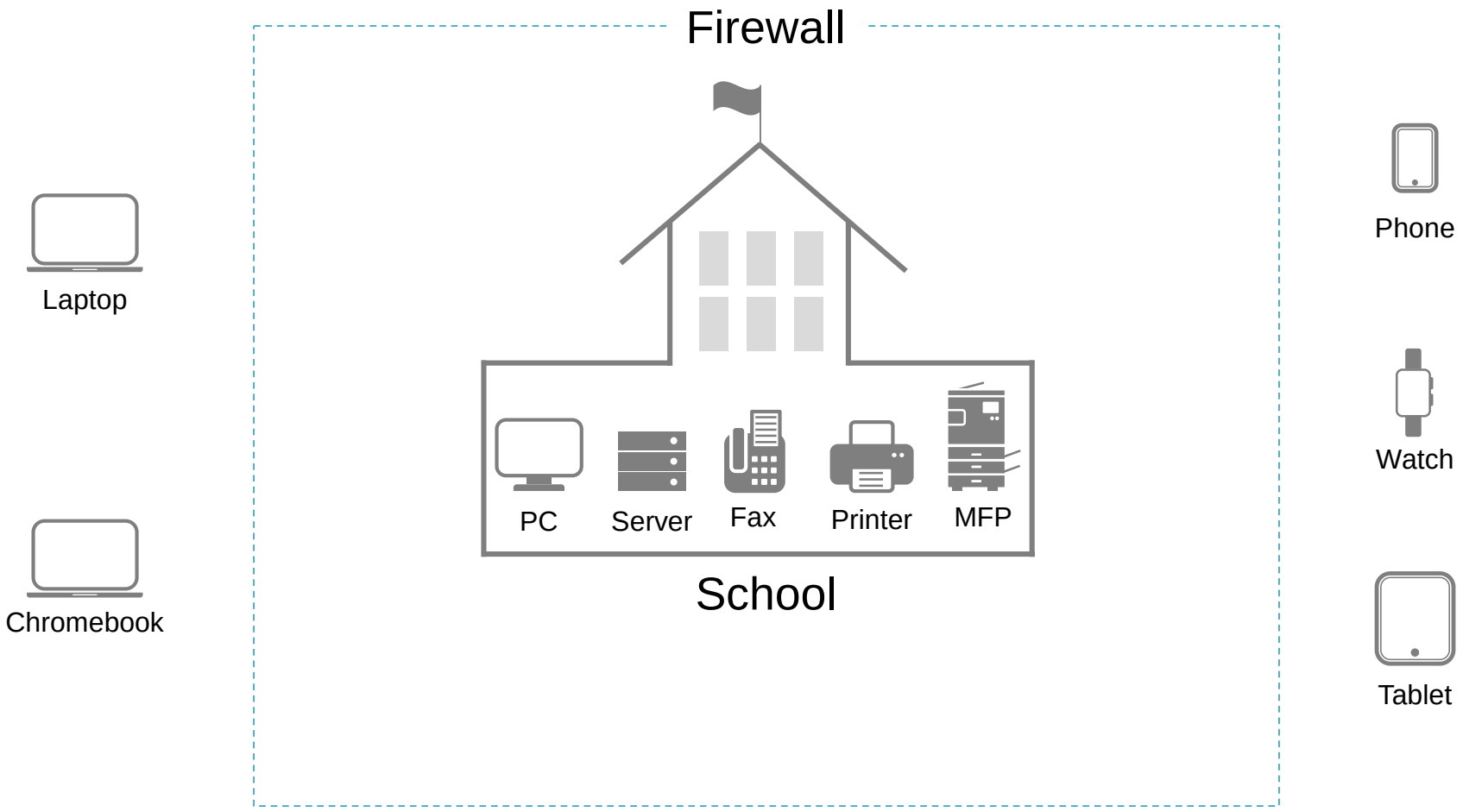
Increasing Risks

- 63% of GDP will be digital in 2020
- Free cloud storage sites are not risk-free
- Cybersecurity is like an arms-race with one fighting the other with AI
- Attacks are increasing; by the end of this presentation there will be 10,000 new malware attacks

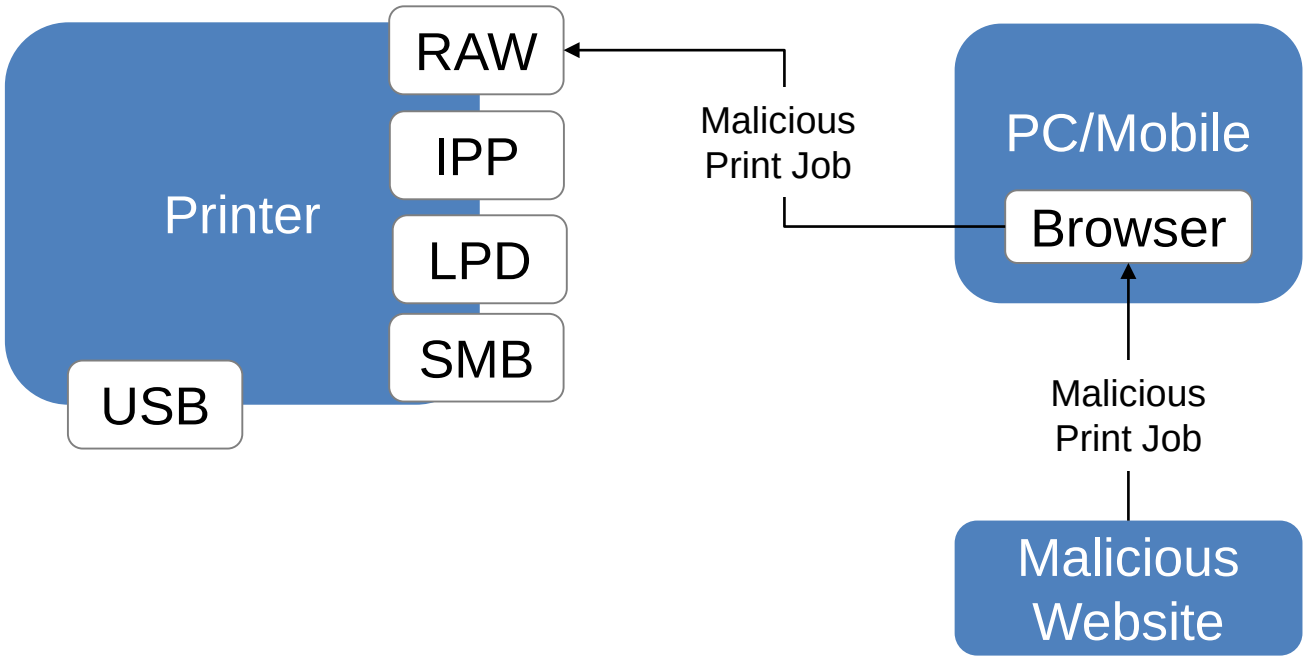
Millennials & How They Work

- Millennials will make up 35% of the workforce in 2020 with GEN 2 digital users entering the workforce
- Millennials use various devices within the work place and for personal use outside the work place and potentially bring compromised applications into the network
- These devices, when outside the work place, are vulnerable

Internet of Things (IoT) Devices



How They're Getting In



Attack Vectors

PS commands	PJL commands	Attack
Disable, hang destroy	offline destroy	Denial of service Physical damage
reset, restart	reset, restart	Factory defaults
overlay, replace	-	Print job manipulation
- hold, capture lock, unlock	nvram hold lock, unlock	Memory access Print job capture Credential disclosure

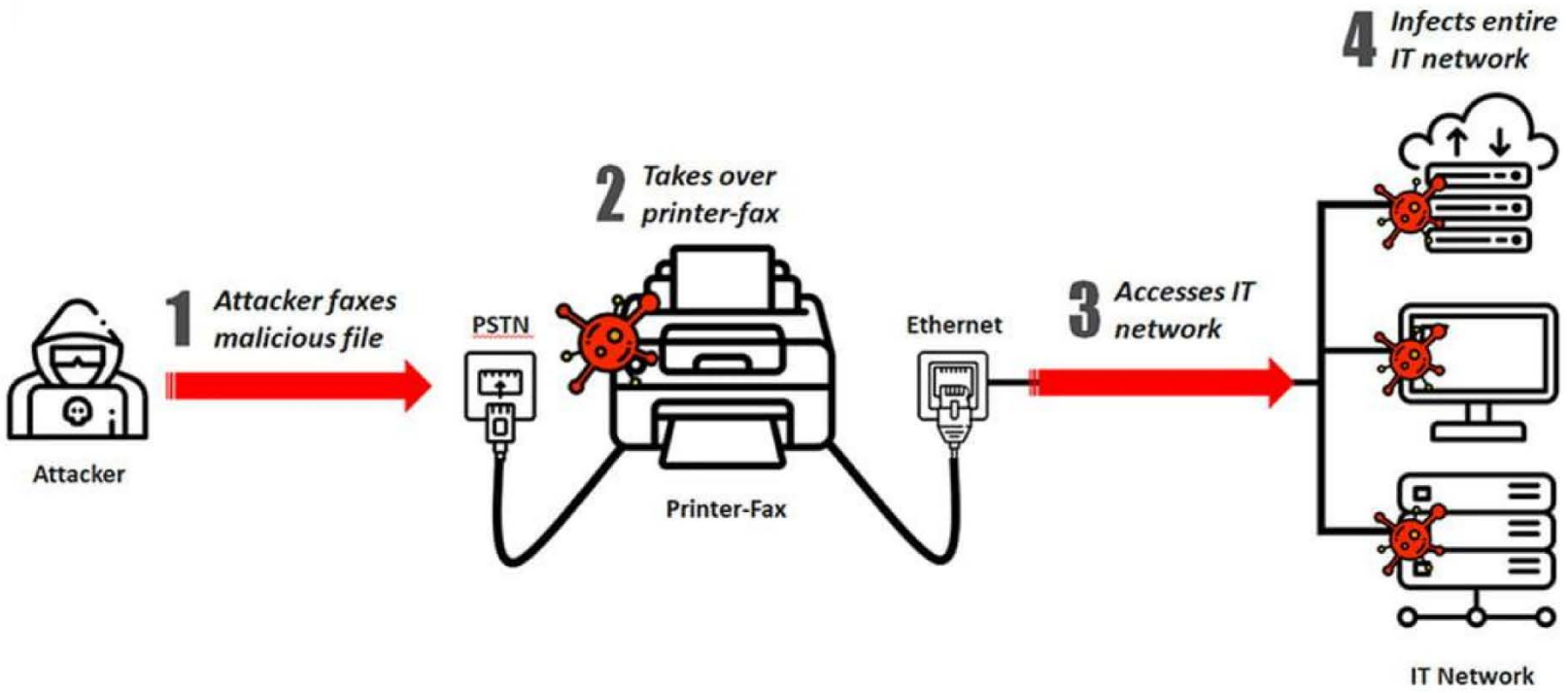
Device Printing Security

- System should have
  - end-to-end security policy
    - from the device, data, to the output document
    - Review security policy regularly
  - device
    - security monitoring
    - firmware updates easily deployed
    - data retention review on the device
    - cyber-resilient BIOS

Added Security Measures

- Change default passwords on all devices
- Close all unnecessary open ports (9120)
- Update firmware
  - Check regularly for updates
  - (MPS) Make sure your vendors are updating firmware during service calls
  - Turn off unused functions such as Airprint, Bluetooth, NFC printing

Fax Vulnerability



Even a stand-alone fax can be hacked, as proven by BlackHat

Additional Resources

- 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

Questions and Answers

We thank you for your time!

Presenters:

MODERATOR INFO:

Tom Kinane, Director of Technology; Elmwood Park CUSD 401
(708) 583-5707; kinanet@epcusd401.org

PANELISTS INFO:

Lee Pietrowski, Partner; IMAGETEC L.P.
(630) 416-7880 Ext. 4272; lpietrowski@imagetec.com

Mark Dodge, VP of Operations/Managed IT Services; IMAGETEC L.P.
(815) 759-3620; mdodge@imagetec.com