Are you ahead of the Hackers? This session will help you decide

Jim Harting, LCSW, CEAP
Maria Lund, LPC, CEAP, LEAP
Brian Moran

Learning Objectives:
- Definition - cybersecurity
- Likelihood of being hacked
- Steps to take to stop hackers
- Examples of ‘hacking’
- Steps to cybersecurity remediation
DEFINITIONS OF CYBERSECURITY:

- **Merriam Webster**
  - Cybersecurity definition - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.
  - [https://www.merriam-webster.com/dictionary/cybersecurity](https://www.merriam-webster.com/dictionary/cybersecurity)

- **Tech Target**
  - Cybersecurity is the protection of internet-connected systems, i.e. hardware, software & data, from cyberattacks. Security involves protection of cyber & physical unauthorized access of data centers & other systems.
  - [https://searchsecurity.techtarget.com/definition/cybersecurity](https://searchsecurity.techtarget.com/definition/cybersecurity)

---

**Cybersecurity Facts – August 2019**

1. 91% of cyberattacks begin with a spear phishing email, which is commonly used to infect organizations with ransomware. (KnowBe4)
2. It takes most companies over 6 months to detect a data breach. (ZD Net)
3. There were >3 million crypto jacking hits between Jan. and May 2018. (Quick Heal)
4. The total cost of a successful cyber-attack is over $5 million. (Ponemon)
5. More than 4,000 ransomware attacks occur every day. (FBI) 1.5 million p/yr
6. 43% of cyber-attacks aimed at small businesses. (Small Business Trends)
7. 76% of businesses reported being a victim of a phishing attack in the last year. (Wombat Security)
Ginni Rometty, IBM’s chairman, president and CEO:
“Cybercrime is the greatest threat to every company in the world.” We are behind in security.

Maria Lund, LPC, CEAP LEAP
President / COO

What First Sun EAP has in place
- People
  - In House Expertise:
    - FTE for policies and procedures
    - Executive and VP involvement
  - Vendor Expertise:
    - EAP database vendor
    - Tech vendor
    - Specialist attorney
  - Other Expertise:
    - EAPA and EAP colleagues
    - Auditors
What First Sun EAP has in place – Paper and Practice

Policies and Procedures:
• HIPAA and HITECH
• Fed/State confidentiality / security
• Home office and BYOD specific
• Annual forms review

Staff Training:
• Semi-annual refreshers
• Training with all changes
• Education if new threats arise

Communication & Authority:
• All issues overseen by Diana
• Support/training of affiliates

What First Sun EAP has in place – Hardware and Software

1. PIN secured VPN
2. Password/PIN secured VOIP
3. Password/firewall for modem/wifi
4. External ports closed on copier
5. 2 step login for workstations
6. Virus/malware with firewall
7. Password/encryption for email
8. Spam blocking service for email
9. Secure/encrypted online fax

Please contact us at 900-966-8143 for further information or questions.
Brian Moran
FOUNDER OF BRIMOR LABS

9/5/2019

What can happen?
Examples

WiFi Hacked – Phone or connecting to a device through WiFi

Hack your User-Name/Password
steal your data
- encrypt your data so you cannot use it

Put a file on your server
using a Phising email and hack into other computers from your server.
We’ve got some problems

Rough estimate of a breach cost is ~$158 per record lost ---
- Healthcare record lost is over double at ~$355 per record

A very small business, holding 5,000 records, estimated breach cost is roughly $1.75 million
- Is your business in a position to handle an unexpected $2 million cost?

---

We’ve got some problems

• Data breach/loss of data can happen in many ways
  • Ransomware
  • Servers/inadvertently exposed to internet
  • Database hacking/exploits
  • Phishing (usually employee credentials)
  • Spear phishing (usually “executive” credentials)

---

We’ve got some problems

Ransomware attack

Your files have been encrypted

Do not attempt to remove the lock on your files—this may make things worse.

To recover your files, you must pay the ransom or the lock will remain.

You can use the computer to perform tasks other than file recovery.

Contact us for assistance, and we will be happy to help.

---

Contact us at 033-123-4567 for assistance, and we will be happy to help.

---

We strongly recommend you contact us immediately, and disable any email receipt you may have received.

---
We've got some problems

- Data breach/loss of data can happen in many ways
  - Ransomware
  - Servers/systems inadvertently exposed to internet
  - Database hacking/exploits
  - Phishing (usually employee credentials)
  - Spear phishing (usually - "executive" credentials)

Data breach will cost more than just $$$

- Loss of trust
- Loss of trust of confidentiality
- Loss of reputation
- Loss of utilization

Losing any one of these items will negatively impact revenue. Losing them all, combined with the cost of a breach, can jeopardize your EAPs financial viability.

The Good News ............

- Proactive response is paramount
  - Don't have to be 100% perfect. Just have to be better than some/most
  - Can leverage third party resources to determine cost vs risk valuation.
    Just like any business decision
  - There is truth to:
    "An ounce of prevention is worth a pound of cure"
QUESTIONS

Brian Moran
brian@brimorlabs.com
Twitter: @brianjmoran

To view this session again along with the PowerPoint, go to the EAPA Web Site in 2 – 3 weeks.

OR – go to www.hartingeap.com/eapa2019