FRIDAY – SEPT. 27TH 11:30 A.M. SESSION

CYBERSECURITY BEST PRACTICES FOR AN EAP

---

Learning Objectives:
- Definition of cybersecurity
- Your chances of being hacked
- How IT Forensic Analyst help EAPS
- References to National Standards for Cybersecurity
DEFINITIONS OF CYBERSECURITY:

- **Merriam Webster**
  - Cybersecurity definition is measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

- **Tech Target**
  - Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. Security comprises cybersecurity and physical security — both are used by enterprises to protect against unauthorized access to data centers.
  - [https://searchsecurity.techtarget.com/definition/cybersecurity](https://searchsecurity.techtarget.com/definition/cybersecurity)

What First Sun EAP has in place:

- **People**
  - 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

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

- **Staff Training**
  - Training with all changes
  - Education if new threats arise
  - Support client requests

- **Communication & Authority**
  - All issues overseen by Diana
  - Support/training of affiliates
  - Semi-annual refreshers
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

This is a sampling of graphical data, from 2013 - present, of the world's largest reported data breaches

• 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

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)

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 EAP’s financial viability.
A Brief List of Topics
• DISCLAIMER (super important)
• Something happened
• What to do next, first
• What to do next, after the first next is done

DISCLAIMER
I am not a lawyer and/or certified legal counsel, and I did not stay at a Holiday Inn Express last night. There are laws, statutes, and legal obligations that any business needs to take into account before implementing any recommendations about to be discussed.

The following recommendations are a result of my performing incident response services for over a decade, and are not singularly reflective of any particular case and/or incident.

SOMETHING ISN’T RIGHT…..
Do you have a data breach?
Do you have the internal staff and expertise needed to make that determination?
Do you have someone in mind in the event that something happens?
Something isn’t right ....

This is not the time for “hmm...I wonder if those firefighters are any good at what they do?”

Something isn’t right ........

Call in a Professional

1. Experience in dealing with incidents
   A. Can respond more quickly than most 3rd party IT service provider companies
   B. Can limit timeframe and/or scope of potential exposure
   C. More than likely, have responded to verify similar case(s)
   D. Can draw on experience for best practices.

But, WHY call in a professional?

1. Plenty of companies offer incident response services:
   A. May be covered and/or leveraged by cyber insurance, check with your provider!
   B. Can drastically reduce overall incident cost
   C. Can prove/disprove data access, collection, loss and/or exfiltration
2. Engaging a professional does NOT mean
   A. You are guaranteed to get back or recover data
   B. You will not face fines/penalties for potential exposure
**But, WHY call in a professional?**

1. They can directly engage with 3rd party IT service providers to implement solutions.
2. They can work with legal counsel to review/implement:
   A. Regulatory guidelines
   B. Potential exposure
   C. Informing customers
   D. Informing law enforcement (if needed)

---

**Okay, those are good reasons**

**A Proactive approach can:**
- Identify security gaps
- Much better to find areas needing improvement/BEFORE an incident
- Limits liability
- Limits overall cost
- Proactive security measures are MUCH cheaper than incident response
- Build working relationships BEFORE an incident

---

**Okay, those are good reasons**

- Implement drills to test your security incident response.
  - Response plans and timelines
  - Ensuring right individuals/organizations are contacted
  - Identify security response plan flaws
  - Ensure that data source(s) needed for incident response are available, collected, and accessible

We all practice fire drills, earthquake drills, tornado drills, etc. Why would you not practice security incident response as well?
### Terms to Know

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Modernization Act of 2014</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>SOC</td>
<td>Service and Organization Controls</td>
</tr>
<tr>
<td>HITRUST CSF</td>
<td>Health Information Trust, Certified Security Framework</td>
</tr>
<tr>
<td>C-Suite</td>
<td>Chief Officers</td>
</tr>
</tbody>
</table>

---

**Chief Information Security Officer**

**Responsibilities:** communications, applications and infrastructure, including the policies and procedures which apply

**Who is the HIPAA Privacy & Security officer for your organization?**

It is the person managing your IT security or the liaison to the IT vendor managing your IT security.
Regulations to know

- HIPAA – Subpart C – Security standards for the protection of electronic protected health information
- HITECH – Subpart B – Standards and implementation specifications for health information technology
- Confidentiality of substance use disorder patient records – 42 CFR Part 2

What do you mean there’s more?

- **State Regulations** that are more stringent **supersede** Federal rules

Where do I look?

- National Conference of State Legislatures (NCSL)
  - Cybersecurity Laws
  - Data Security Laws
  - Security Breach Legislation

National standards we utilize

- HIPAA Security Matrix
  - [Website](#)
  - [PDF](#)
- NIST Cybersecurity Framework
  - [Website](#)
  - [PDF](#)
- NIST Risk Management Framework
  - [Website](#)
  - [PDF](#)
Cybersecurity Risk Assessment
– the basis for all your planning

National Compliance Standards
- System Development Life Cycle
- Applications & Data Criticality Analysis
- Risk Assessment Methodology

Audits by External Companies
- Penetration Test (PEN)
- SOC II, Type 2
- HITRUST
- ISO 27000

HIPAA Security Matrix Audit Tool
- Security Risk Assessment Tool V3.0

Cybersecurity with Hacking Healthcare blog

Open Minds
- Telebehavioral Health Institute
- Xtelligent Healthcare Media

Please contact us at 800-968-8143 for further information or questions.

Thanks!
Top 10 recommendations to begin your Cybersecurity Setup

1. The generally accepted FIRST STEP is to conduct a Risk Assessment.
   A. An option to meet this requirement is an external HIPAA Compliance audit. Usually conducted annually.
   B. Many outlines available on the web for the audit.

2. A SECOND STEP is to assure that all of your PHI data is encrypted.
   A. Encrypt data (a) at rest, (b) during transfers (c) on backups
   B. This is your “Safe Harbor” if you are hacked. Very Important.

3. To BE SURE YOU ARE MEETING CYBERSECURITY standards, contract for annual audits by an external group.
   A. Have an external audit using one of the following standards:
      (a) ISO Standards,
      (b) HiTrust standards, or
      (c) SOC II requirements,
      (d) NIST standards.
   Audits organize P&P to meet “Trust Services Criteria” of Security, Confidentiality, Availability, Privacy & Process Integrity.
   B. Complete a PHI Inventory to know where all PHI data resides.
   C. Conduct or contract for Penetration Tests.

4. Something you can do now to strengthen your security are:
   A. Add strong passwords (15 or more characters).
   B. Begin to plan adding 2F Authentication to your sign-ons.

5. Equipment recommendations:
   A. Update your firewall with updates daily if needed.
   B. Updated anti-virus and malware software daily if needed.
   C. Update software and firmware at least weekly
   D. Put a time limit on how long monitors can display data.

6. Appoint a CISO or have one on retainer.

7. Backup your data nightly and keep off-site 1-night p/week.
8. Have Disaster Recovery Plans & conduct tests.

9. Don't have PII on same network (segment networks).

10. If you are from the European Union you need to comply with GDPR.

There are many more standards, but these will go a long way to introducing you to the complex, standards that you need to implement. The external audits provide a detailed list of P&P.

Go to EAPA web site for a list of the facts, data, web-sites, tables and references in our presentation.

OR go to:
https://www.hartingeap.com/EAPA2019