AGENDA

• Introduction:
  • William Miaoulis, Chief Information Security Officer (CISO)
    • Bill.Miaoulis@auburn.edu

• Define Cybersecurity

• Fortran

• HIPAA

• NIST

• Have controls changed
Definitions: Security (NIST 800-53)

• **Security:** A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

• **Security Control:** A safeguard or countermeasure prescribed for an information system or an organization designed to **protect the confidentiality, integrity, and availability** of its information and to meet a set of defined security requirements.
HIPAA: The General Rule

- **Covered entities must do the following:**
  - Ensure the **confidentiality, integrity, and availability** of all Electronic Protected Health Information (E PHI) the covered entity creates, receives, maintains, or transmits; and
  - Protect against any **reasonably anticipated threats or hazards** to the security or integrity of such information.
  - **Protect** against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy rule; and
  - **Ensure** compliance by its workforce.
  - Covered entities **may use any security measures** that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications.
I will NEVER work with Computers!!!! - 1977
EDP AUDIT: Banking (1982)
ENERGY (1987)

• My First Hack
• Social Engineering (My second hack)
• From Mainframe to Distributed Processing
• 1988 (The first computer worm was created, 99-line program, Robert Morris)
• HIPAA – 1996
• What is Compliance?
• Why Protect Healthcare Information?
• Passwords, who needs passwords?
National Institute of Standards and Technology: (NIST)

- NIST publishes many other special publications that are important to security, this is just one of them.
Identifying Security Risks

• Security **risks** are *potential events* that threaten the **availability, integrity and confidentiality** of our information.

• Security **incidents** are *actual events* that have or are currently impacting the **availability, integrity and confidentiality** of our information.
§ 164.308 Administrative safeguards

- **Security management process (R)** - Policies and procedures to prevent, detect, contain, and correct security violations. The following are required:
  - **Risk analysis (R)** - An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI;
  - **Risk management (R)** - Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
  - **Sanction policy (R)** - Sanctions against workforce members who fail to comply with security policies and procedures; and
  - **Information system activity review (R)** - Procedures to regularly review records of information system activity, such as:
    - audit logs;
    - access reports; and
    - security incident tracking reports.

Note:

- The security management process is the **foundation of the security rule** and the foundation of all effective information security programs;
- Risk Analysis/Management ensures that the organization identifies risks, conducts a risk analysis, determines existing and potential controls, and **creates a plan** to mitigate risks;
- Any employee that is in violation policies will be subject to disciplinary action
- Information System Activity Review: reviews of who is accessing records (audit logs), who has access to information), and a review of security incidents.
§ 164.316 Policies and procedures and documentation requirements

- **Policies and procedures (R)** - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the security rule.
  - A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the rule.

- **Documentation (R)** - Maintain policies, procedures, and records of actions, activities, or assessments required by the rule in **written** (which may be electronic) form. Three **required** implementation specifications:
  - **Time limit** - retain the documentation for 6 years from the later of the date of its creation or the last effective date;
  - **Availability** - make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and
  - **Updates** - Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

**Note:**
- It is important that every HIPAA standard is addressed in a written (can be electronic) policy.
- Build a cross-reference from the Standard to YOUR policies, missing one, create it.
Is your organization, HIPAA Compliant?

• HIPAA Compliance
  • You have a **WRITTEN** policy
  • You follow **YOUR** policy
  • You can **PROVE** you are following your policies
  • **DOCUMENT, DOCUMENT, DOCUMENT AND THEN DOCUMENT MORE**
Keep Your Head in Sand
Breach Notification Laws

• HIPAA
• States
• European Union (GDPR)
• Other Countries?
Criminal Justice & HIPAA (2015)
Attack Vectors
Back to the Future or The Wild Wild West (CISO-2016)
Standards, Standards, Everywhere

- Standards, Standards, Everywhere

- HIPAA
- Security
- Information
- NIST
- PCI
- DSS
- Data
- Procedures
- Access
- Implement
- Policies
- Information
- Protection
- Plan
- Controlled
- Compliance
- Requirements
- Audit
- Information Security Management System
- Certified
Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.DS-1: Data-at-rest is protected</td>
<td>CCS CSC 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 3.4, SR 4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013 A.8.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 SC-28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.DS-2: Data-in-transit is protected</td>
<td>CCS CSC 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>COBIT 5 APO01.06, DSS06.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 SC-8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition</td>
<td>COBIT 5 BAI09.03</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.DS-4: Adequate capacity to ensure availability is maintained</td>
<td>COBIT 5 APO13.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 7.1, SR 7.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013 A.12.3.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.DS-5: Protections against data leaks are</td>
<td>CCS CSC 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>COBIT 5 APO01.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 5.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Is your organization, ??????? Compliant?

• Compliance (GLBA, NIST 800-171, HIPAA)
  • You have a **WRITTEN** policy
  • You follow **YOUR** policy and procedures (Security Plans)
  • You can **PROVE** you are following your policies and procedures
  • **DOCUMENT, DOCUMENT, DOCUMENT AND THEN DOCUMENT MORE**
Have controls changed?
THE FUTURE: 2017-2057

• Driverless Cars – Drones
• IOT
• CYBORGS
• Artificial Intelligence (Will they take over)
• Digital Immortality (Virtual Immortality)
  • Storing a person's personality (Brains) uploaded to machines
• The Circle?
• 1984? All Remote Workers? No Human Workers?
• Look at the last 40 years, what can we imagine in the next 40 years?