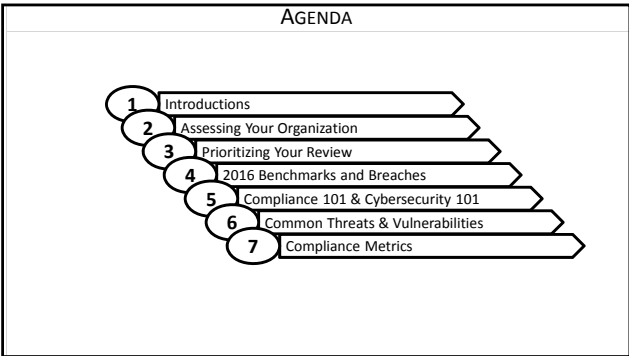


CYBERSECURITY IN THE POST-ACUTE ARENA

Horizontal lines for notes



Horizontal lines for notes

INTRODUCTIONS
Amy Brantley | Chief Compliance Officer, Reliant Post-Acute Care Solutions
Background: Attorney - 25 years experience, Healthcare - 14 years experience, Healthcare Experience, Reliant Post-Acute Care Solutions (current), Golden Living, Arkansas Children's Hospital
Positions: Chief Compliance Officer & EVP IT, Chief Privacy Officer, Assistant GC Healthcare & VP Compliance, Labor & Employment Counsel

Horizontal lines for notes

INTRODUCTIONS

Lisa Spears | Privacy and Information Security Officer, Reliant Post-Acute Care Solutions

- | Background                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Healthcare – Golden Living - 23 years experience</li> <li><a href="#">Links at Golden Living</a></li> <li>Information Systems Security</li> <li>Process Improvement</li> <li>Project Management (PMP)</li> <li>Information Systems Management (CISM)</li> <li>IT Audit (CISA)</li> </ul> |

- | Positions                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Chief Information Security Officer</li> <li>VP Enterprise Project Management &amp; Internal Controls</li> <li>Director Process Improvement</li> <li>Manager IT Systems Audit</li> </ul> |

---

---

---

---

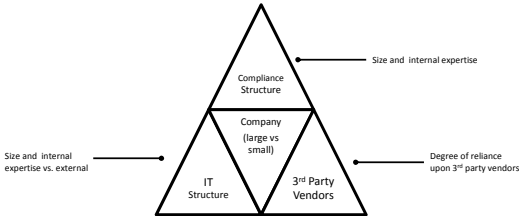
---

---

---

---

ASSESSING YOUR ORGANIZATION




---

---

---

---

---

---

---

---

PRIORITIZING YOUR REVIEW

Small Organizations

- Third Party Vendors
- Information Technology
- Internal Resources

Large Organizations

- Information Technology
- Organization Privacy Program
- Third Party Vendor/BA

---

---

---

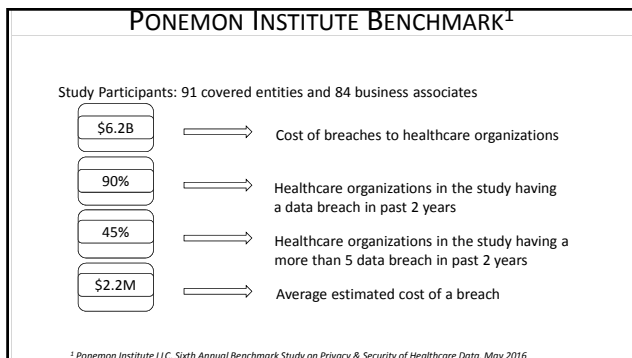
---

---

---

---

---




---

---

---

---

---

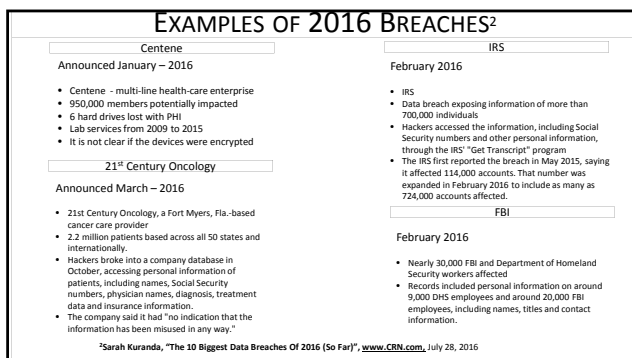
---

---

---

---

---




---

---

---

---

---

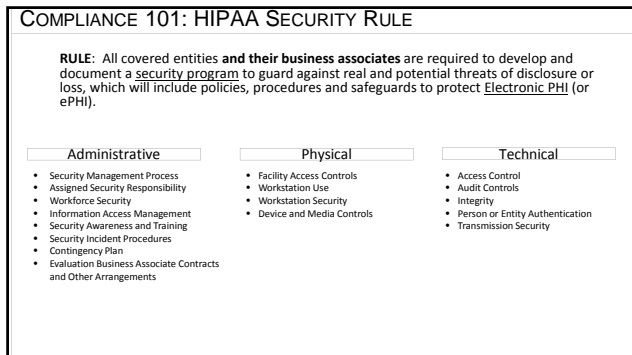
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

**COMPLIANCE 101: HIPAA PRIVACY RULE**

**Rule:**  
Protects all "PHI" (protected health information), which includes just about any piece of information that might possibly identify a person, in any form, including oral information

Grants individuals broader rights in their PHI:

- Access
- Amendment
- Disclosure Accounting
- Restrictions
- Confidential Communications

---

---

---

---

---

---

---

---

**COMPLIANCE 101: BUSINESS ASSOCIATE**

**Business Associate (BA)**

**Definition**  
Any entity that "creates, receives, maintains, or transmits" PHI in performing a function, activity, or service on behalf of a covered entity.  

- Examples: billing companies, accountants, insurance agents/brokers, payroll vendors, consultants, law firms, data processing firms...
- Any entity that has access to PHI to do something for a Covered Entity.

**Requirements**  
Covered Entity (CE) cannot release or disclose PHI to business associates unless both parties have a Business Associates Agreement (BAA) in place. BAA is not a Non Disclosure Agreement (NDA). BAA should minimally include:  

- Confidentiality clause
- Breach disclosure requirements and process
- Disposition requirements and process at BAA termination
- Rights of CE to audit the BA

---

---

---

---


---

---

---

---

**COMPLIANCE 101: BUSINESS ASSOCIATE**

**Best Practices for Business Associates Engagement** 

- Select your vendors carefully as they can be jointly or directly liable for security breaches
- Engage all expertise needed (Legal, Procurement, Operations, Security Officer, Privacy Officer) to create a well rounded and all inclusive agreement
- Ask for and review vendor privacy and security policies to get a sense of controls in place
- Make sure basic technical security controls are in place – encryption, patching, anti-virus, password management, etc.

---

---

---

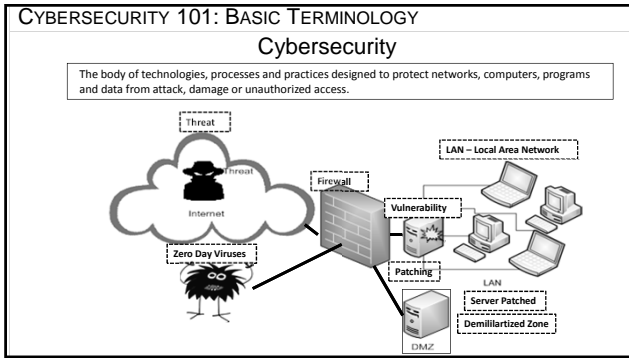
---

---

---

---

---




---

---

---

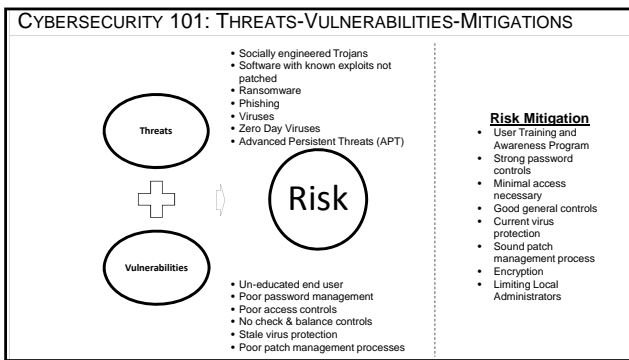
---

---

---

---

---




---

---

---

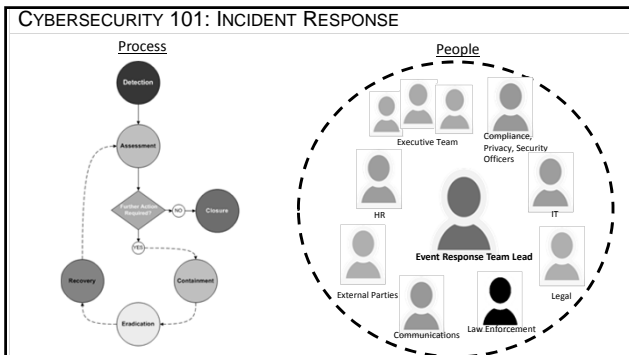
---

---

---

---

---




---

---

---

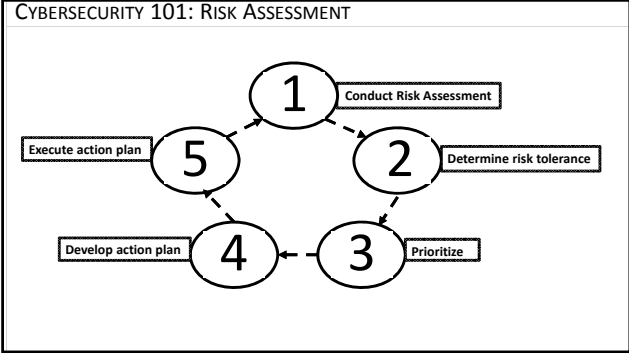
---

---

---

---

---




---



---



---



---



---



---

CYBERSECURITY 101: RISK ASSESSMENT

Risk Tolerance – Business Decision

Example

Risk Tolerance

- Low Tolerance
- Medium Tolerance
- High Tolerance

---



---



---



---



---



---

COMPLIANCE METRICS: EMAIL

Current Month Email Stats

- Initially Blocked Emails
- Quarantined & Blocked (Virus Detected)
- Quarantined & Released
- Allowed Emails

Weekly Heuristics

Total Submissions for analysis week 4: **1,024**

Deemed High Risk: **9**

Submitted to Antivirus software for analysis week: **Zero Day Trend**

Outbreak of IRS Phishing emails increased the number of emails blocked and number of emails quarantined & subsequently blocked. No infections encountered.

---



---



---



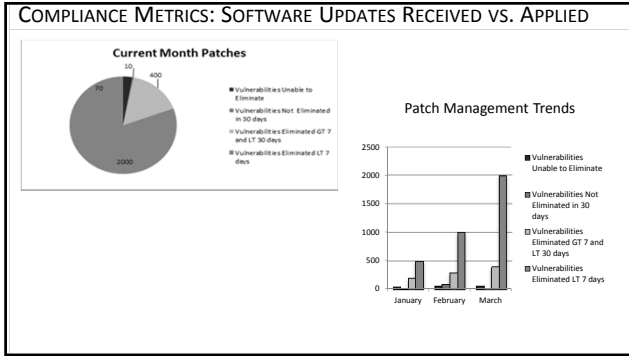
---



---



---




---

---

---

---

---

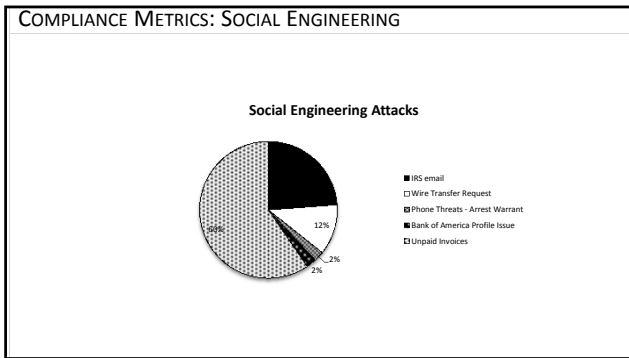
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

### COMPLIANCE METRICS: POLICY REVIEW & ATTESTATIONS

Policy Annual Review Status			Policy Employee Attestation Status		
Information Security Policies	Review Date	Review Status	Information Security Policies	Goal	Policy Attestation Status
Information Security Policy	1/31/2017	🟢	Information Security Policy	1000	1000
Access Control Policy	1/31/2017	🟢	Access Control Policy	1000	1000
Acceptable Use Policy	1/31/2017	🟢	Acceptable Use Policy	1000	900
Business Continuity Policy	1/31/2017	🟢	Business Continuity Policy	250	250
Data Classification Policy	1/31/2017	🟢	Data Classification Policy	1000	900
Encryption Policy	6/30/2017	🟢	Encryption Policy	100	85
Mobile Devices Policy	1/31/2017	🟢	Mobile Devices Policy	250	250
Media Handling Policy	6/30/2017	🟢	Media Handling Policy	1000	1000
Network Security Policy	6/30/2017	🟢	Network Security Policy	250	225
Physical and Environmental Security Policy	6/30/2017	🟢	Physical and Environmental Security Policy	1000	1000
Personnel Security Policy	6/30/2017	🟢	Personnel Security Policy	1000	1000
Risk Assessment & Treatment Policy	12/31/2017	🟢	Risk Assessment & Treatment Policy	100	100
Remote Access Policy	12/31/2017	🟢	Remote Access Policy	250	225
Software Development Policy	12/31/2017	🟢	Software Development Policy	100	100
Security Privacy and Incident Reporting	12/31/2017	🟢	Security Monitoring and System Auditing	1000	1000
Communications & Operations Security	12/31/2017	🟢	Security Privacy and Incident Reporting	100	100
			Communications & Operations Security	100	100

---

---

---

---

---

---

---

---

---

---

2/24/2017



---

---

---

---

---

---

---