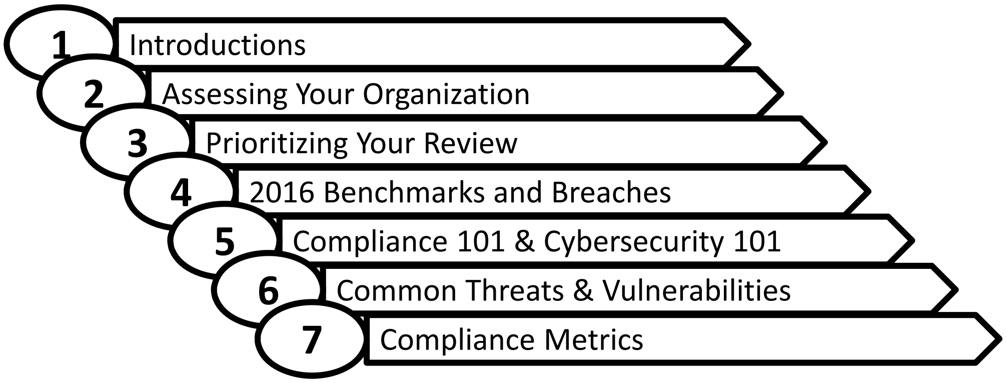
CYBERSECURITY IN THE POST-ACUTE ARENA

AGENDA



1 Introductions

2 Assessing Your Organization

3 Prioritizing Your Review

4 2016 Benchmarks and Breaches

5 Compliance 101 & Cybersecurity 101

6 Common Threats & Vulnerabilities

7 Compliance Metrics

INTRODUCTIONS

Amy Brantley| Chief Compliance Officer, Reliant Post-Acute Care Solutions

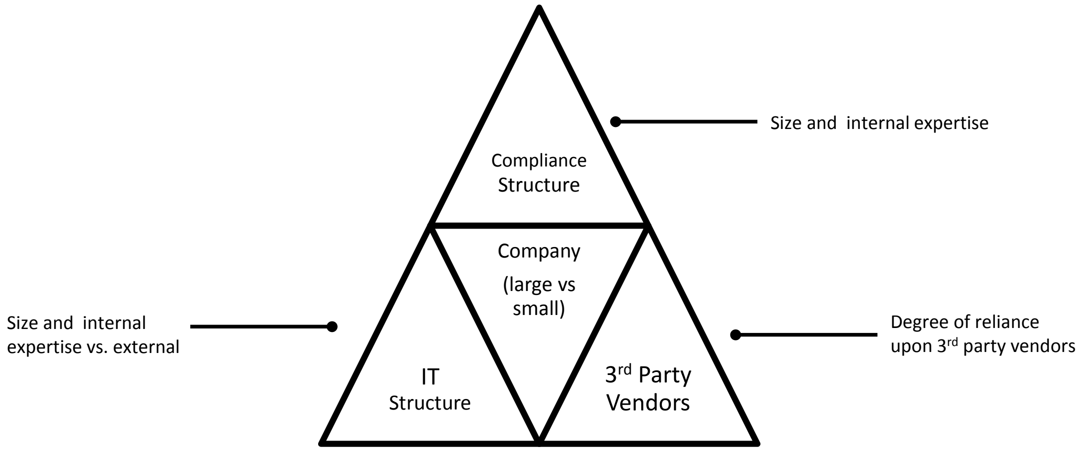
Background	Positions
• Attorney – 25 years experience • Healthcare – 14 years experience Healthcare Experience • Reliant Post-Acute Care Solutions (current) • Golden Living • Arkansas Children's Hospital	• Chief Compliance Officer & EVP IT • Chief Privacy Officer • Assistant GC Healthcare & VP Compliance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

INTRODUCTIONS

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

Background	Positions
• Healthcare – Golden Living - 23 years experience Roles at Golden Living • Information Systems Security • Process Improvement • Project Management (PMP) • Information Systems Management (CISM) • IT Audit (CISA)	• Chief Information Security Officer • VP Enterprise Project Management & Internal Controls • Director Process Improvement • Manager IT Systems Audit

Assessing Your Organization



Compliance Structure

Company (large vs small)

IT Structure

3rd Party Vendors

Size and internal expertise

Size and internal expertise vs. external

Degree of reliance upon 3rd party vendors

Prioritizing Your Review

Small Organizations

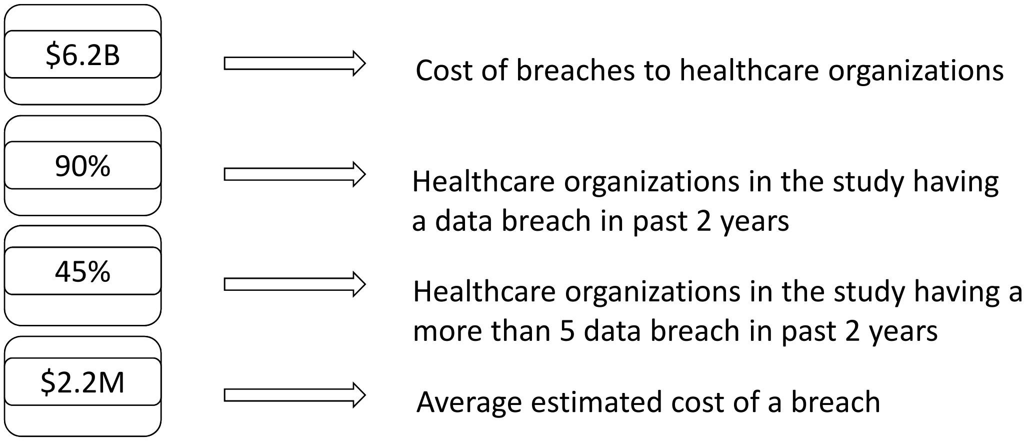
- Third Party Vendors
- Information Technology
- Internal Resources

Large Organizations

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

PONEMON INSTITUTE BENCHMARK[1]

Study Participants: 91 covered entities and 84 business associates



$6.2B → Cost of breaches to healthcare organizations

90% → Healthcare organizations in the study having a data breach in past 2 years

45% → Healthcare organizations in the study having a more than 5 data breach in past 2 years

$2.2M → Average estimated cost of a breach

[1] *Ponemon Institute LLC, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016*

EXAMPLES OF 2016 BREACHES[2]

Centene

Announced January – 2016

- Centene - multi-line health-care enterprise
- 950,000 members potentially impacted
- 6 hard drives lost with PHI
- Lab services from 2009 to 2015
- It is not clear if the devices were encrypted

21st Century Oncology

Announced March – 2016

- 21st Century Oncology, a Fort Myers, Fla.-based cancer care provider
- 2.2 million patients based across all 50 states and internationally.
- Hackers broke into a company database in October, accessing personal information of patients, including names, Social Security numbers, physician names, diagnosis, treatment data and insurance information.
- The company said it had "no indication that the information has been misused in any way."

IRS

February 2016

- IRS
- Data breach exposing information of more than 700,000 individuals
- Hackers accessed the information, including Social Security numbers and other personal information, through the IRS' "Get Transcript" program
- The IRS first reported the breach in May 2015, saying it affected 114,000 accounts. That number was expanded in February 2016 to include as many as 724,000 accounts affected.

FBI

February 2016

- Nearly 30,000 FBI and Department of Homeland Security workers affected
- Records included personal information on around 9,000 DHS employees and around 20,000 FBI employees, including names, titles and contact information.

[2] **Sarah Kuranda, "The 10 Biggest Data Breaches Of 2016 (So Far)", www.CRN.com,** July 28, 2016

COMPLIANCE 101: HIPAA SECURITY RULE

RULE: All covered entities **and their business associates** are required to develop and document a security program to guard against real and potential threats of disclosure or loss, which will include policies, procedures and safeguards to protect Electronic PHI (or ePHI).

Administrative

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation Business Associate Contracts and Other Arrangements

Physical

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

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 <u>on behalf of</u> a covered entity.

- Examples: billing companies, accountants, insurance agents/brokers, payroll vendors, consultants, law firms, data processing firms…
- <u>Any entity</u> 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

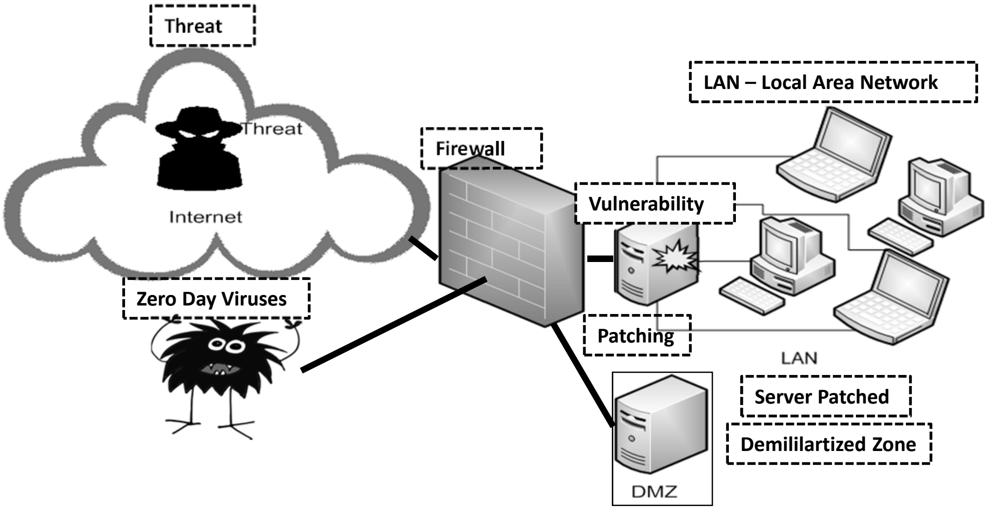
☑ Ask for and review vendor privacy and security policies to get a sense of controls in place

☑ Make sure basic technical security controls are in place – encryption, patching, anti-virus, password management, etc.

CYBERSECURITY 101: BASIC TERMINOLOGY

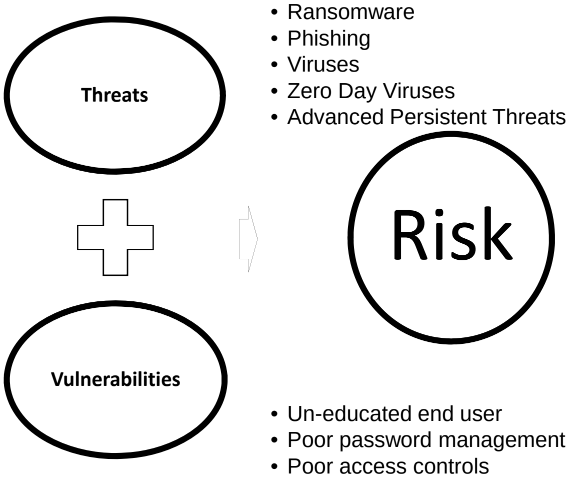
Cybersecurity

The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.



CYBERSECURITY 101: THREATS-VULNERABILITIES-MITIGATIONS

- Socially engineered Trojans
- Software with known exploits not patched
- Ransomware
- Phishing
- Viruses
- Zero Day Viruses
- Advanced Persistent Threats (APT)



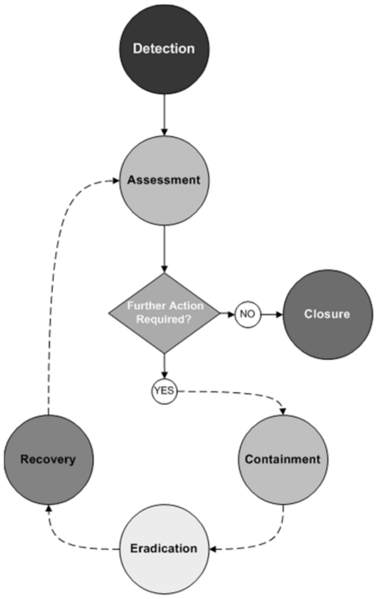
- Un-educated end user
- Poor password management
- Poor access controls
- No check & balance controls
- Stale virus protection
- Poor patch management processes

Risk Mitigation

- User Training and Awareness Program
- Strong password controls
- Minimal access necessary
- Good general controls
- Current virus protection
- Sound patch management process
- Encryption
- Limiting Local Administrators

CYBERSECURITY 101: INCIDENT RESPONSE

Process



Detection

Assessment

Further Action Required?

NO

Closure

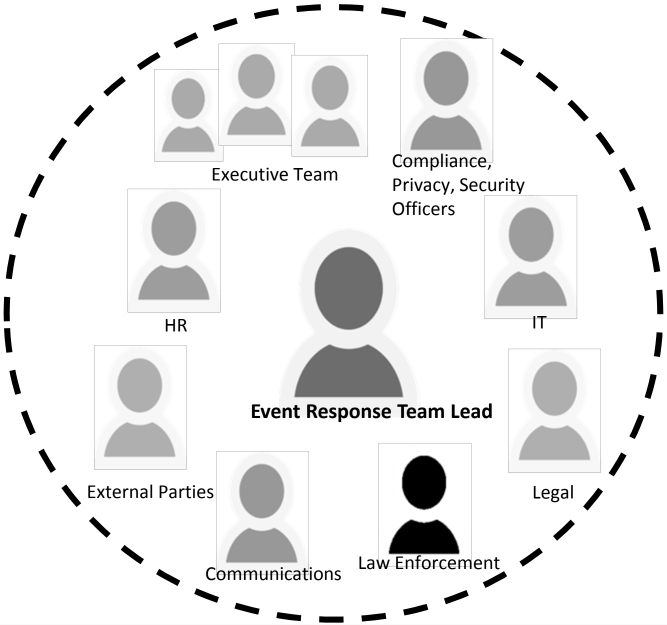
YES

Containment

Eradication

Recovery

People



Executive Team

Compliance, Privacy, Security Officers

HR

IT

Event Response Team Lead

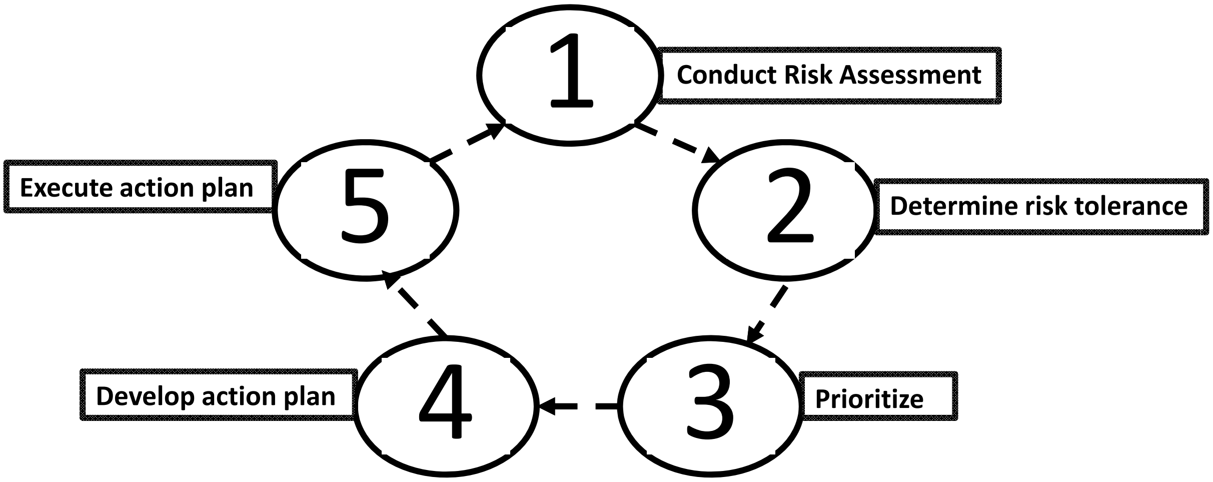
External Parties

Legal

Communications

Law Enforcement

CYBERSECURITY 101: RISK ASSESSMENT



1 Conduct Risk Assessment

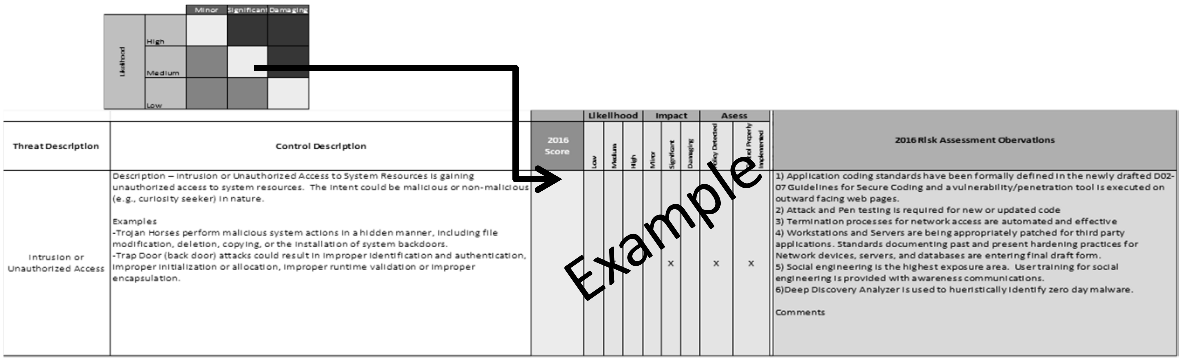
2 Determine risk tolerance

3 Prioritize

4 Develop action plan

5 Execute action plan

CYBERSECURITY 101: RISK ASSESSMENT

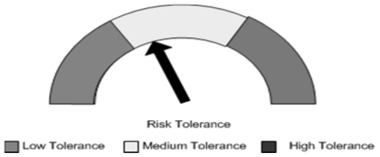


Likelihood		Minor	Significant	Damaging
	High	□	■	■
	Medium	▨	□	■
	Low	▨	▨	□

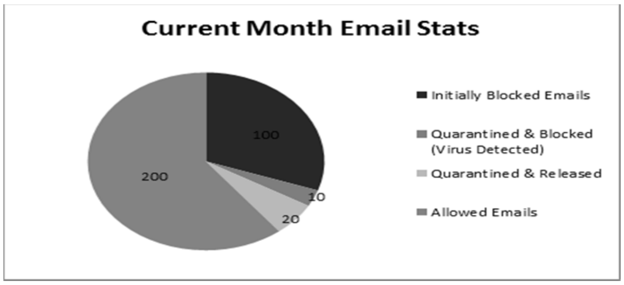
			Likelihood			Impact			Asess		
Threat Description	Control Description	2016 Score	Low	Medium	High	Minor	Significant	Damaging	Policy Detected	Control Properly Implemented	2016 Risk Assessment Obervations
Intrusion or Unauthorized Access	Description – Intrusion or Unauthorized Access to System Resources is gaining unauthorized access to system resources. The intent could be malicious or non-malicious (e.g., curiosity seeker) in nature. Examples -Trojan Horses perform malicious system actions in a hidden manner, including file modification, deletion, copying, or the installation of system backdoors. -Trap Door (back door) attacks could result in improper identification and authentication, improper initialization or allocation, improper runtime validation or improper encapsulation.						x		x	x	1) Application coding standards have been formally defined in the newly drafted D02-07 Guidelines for Secure Coding and a vulnerability/penetration tool is executed on outward facing web pages. 2) Attack and Pen testing is required for new or updated code 3) Termination processes for network access are automated and effective 4) Workstations and Servers are being appropriately patched for third party applications. Standards documenting past and present hardening practices for Network devices, servers, and databases are entering final draft form. 5) Social engineering is the highest exposure area. User training for social engineering is provided with awareness communications. 6)Deep Discovery Analyzer is used to hueristically identify zero day malware. Comments

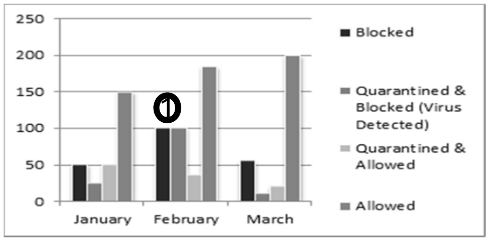
Example

Risk Tolerance – Business Decision



COMPLIANCE METRICS: EMAIL





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

Weekly Heuristics

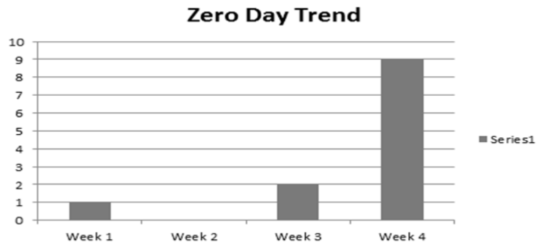
Total Submissions for analysis week 4

1,024

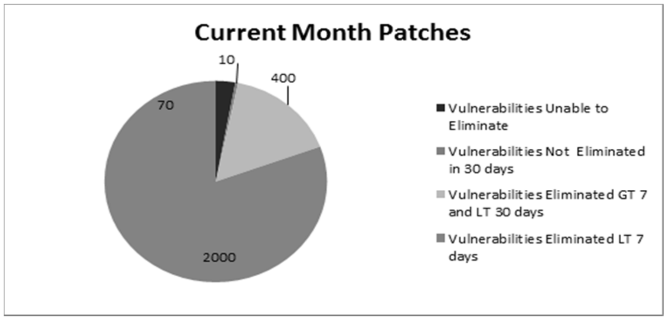
Deemed **High Risk**

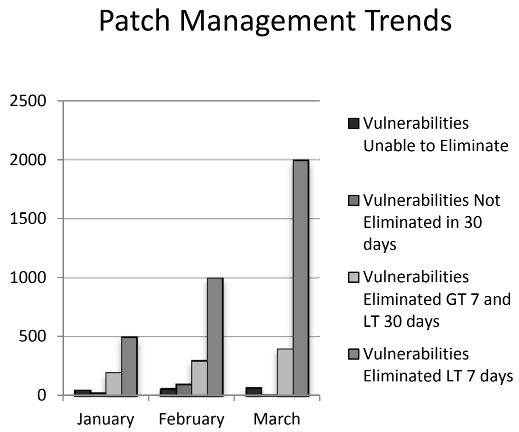
9

Submitted to Antivirus vendor for analysis and

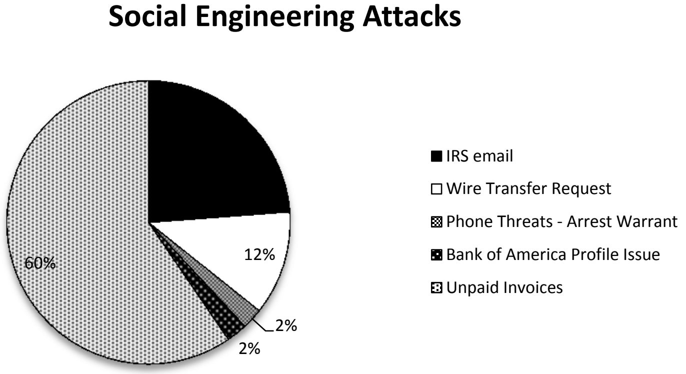


COMPLIANCE METRICS: SOFTWARE UPDATES RECEIVED VS. APPLIED



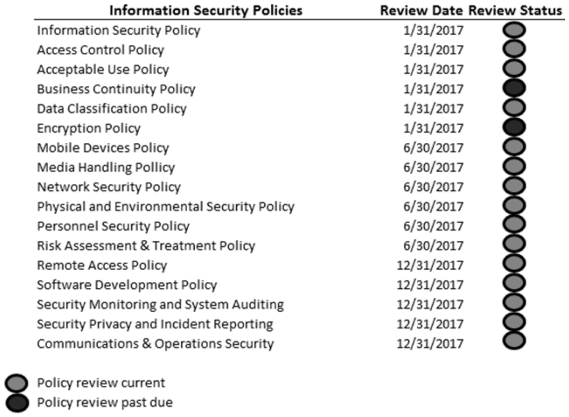


COMPLIANCE METRICS: SOCIAL ENGINEERING



Compliance Metrics: Policy Review & Attestations

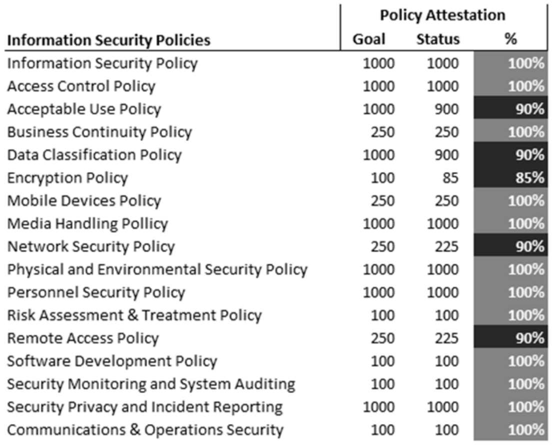
Policy Annual Review Status



Information Security Policies	Review Date	Review Status
Information Security Policy	1/31/2017	○
Access Control Policy	1/31/2017	○
Acceptable Use Policy	1/31/2017	○
Business Continuity Policy	1/31/2017	●
Data Classification Policy	1/31/2017	○
Encryption Policy	1/31/2017	●
Mobile Devices Policy	6/30/2017	○
Media Handling Pollicy	6/30/2017	○
Network Security Policy	6/30/2017	○
Physical and Environmental Security Policy	6/30/2017	○
Personnel Security Policy	6/30/2017	○
Risk Assessment & Treatment Policy	6/30/2017	○
Remote Access Policy	12/31/2017	○
Software Development Policy	12/31/2017	○
Security Monitoring and System Auditing	12/31/2017	○
Security Privacy and Incident Reporting	12/31/2017	○
Communications & Operations Security	12/31/2017	○

○ Policy review current
● Policy review past due

Policy Employee Attestation Status



	Policy Attestation		
Information Security Policies	Goal	Status	%
Information Security Policy	1000	1000	100%
Access Control Policy	1000	1000	100%
Acceptable Use Policy	1000	900	90%
Business Continuity Policy	250	250	100%
Data Classification Policy	1000	900	90%
Encryption Policy	100	85	85%
Mobile Devices Policy	250	250	100%
Media Handling Pollicy	1000	1000	100%
Network Security Policy	250	225	90%
Physical and Environmental Security Policy	1000	1000	100%
Personnel Security Policy	1000	1000	100%
Risk Assessment & Treatment Policy	100	100	100%
Remote Access Policy	250	225	90%
Software Development Policy	100	100	100%
Security Monitoring and System Auditing	100	100	100%
Security Privacy and Incident Reporting	1000	1000	100%
Communications & Operations Security	100	100	100%

Questions?