Healthcare and Cybersecurity

May 18, 2017

Sarah Ackerman

Clark Schaefer Consulting

Melissa Meeker

Clark Schaefer Hackett

Introductions

clark schaefer consulting

Sarah Ackerman, CISSP, CISA, CICP
Managing Director, Cincinnati Office

- Responsible for overall engagement quality and oversight of projects
- Areas of expertise include information security; risk management; and IT governance, audit, and compliance
- Works with wide variety of clients and industries across Ohio and Kentucky
- In-depth knowledge of IT and security frameworks, regulations, and standards, including ISO, NIST, COBIT, GLBA, FDA, HIPAA, PCI

Introductions

CLARK SCHAEFER HACKETT
CPAS & ADVISORS

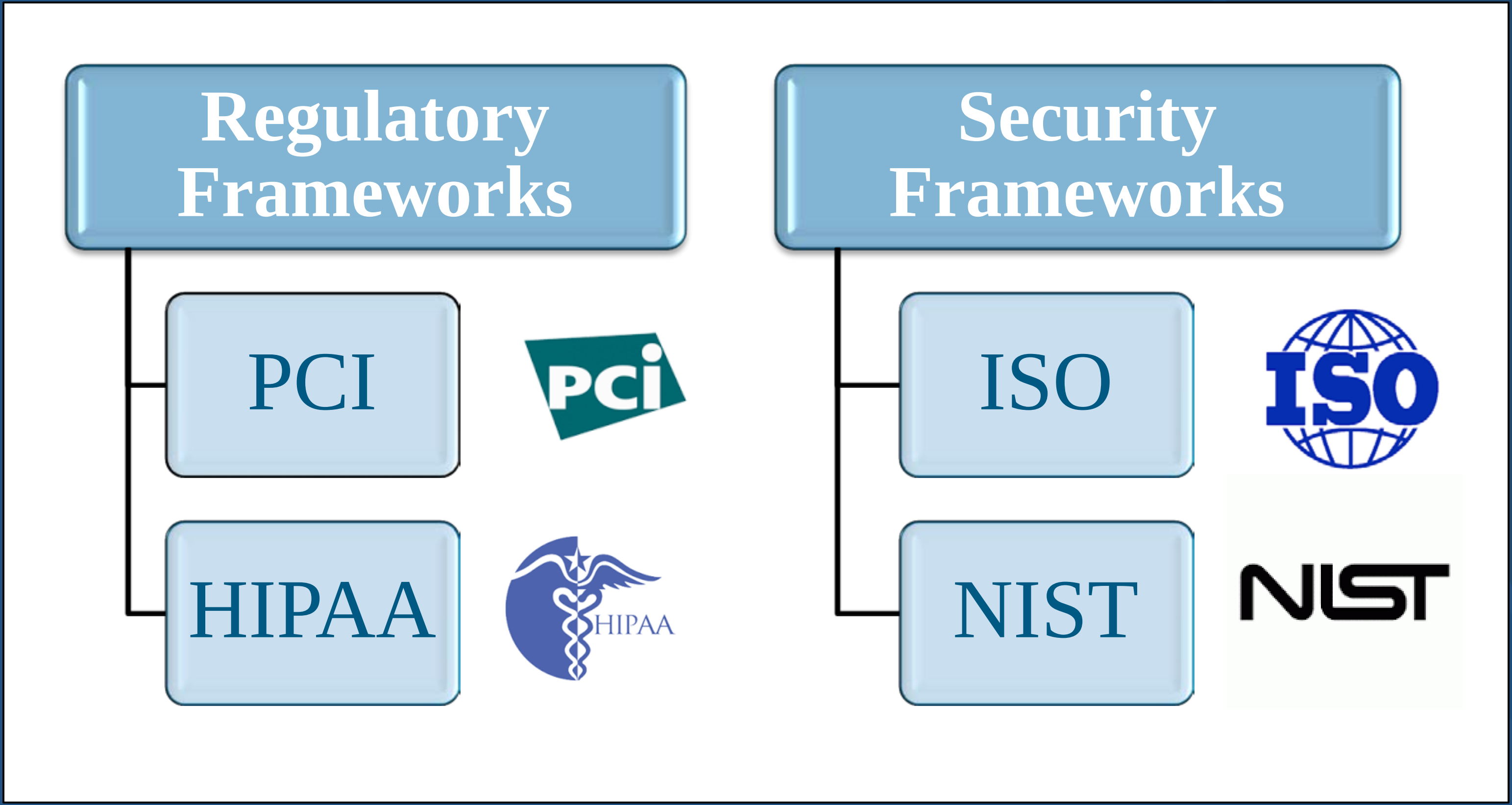
Melissa M. Meeker
Outsource Accounting Specialist

- Melissa Meeker has extensive experience with financial accounting software packages.
- She assists clients through consulting projects that enhance their ability to utilize the more complex functions of the software.
- Melissa specializes in accounting software implementation, training and troubleshooting.

Agenda

- Regulatory versus security frameworks
- HIPAA, HITECH, Meaningful Use
- Case Studies
- Tools for Cybersecurity

Regulatory vs. Security Frameworks



PCI DSS

Payment Card Industry Data Security Standard

What is it? Standards for protecting payment systems from breaches and theft of cardholder data

Who does it apply to? Merchants, financial institutions, point-of-sale vendors

Who enforces it? Individual payment brands or acquiring banks

HIPAA

Health Insurance Portability and Accountability Act of 1996

What is it? Legislation that provides data privacy and security provisions for safeguarding medical information

Who does it apply to? Healthcare providers, health plans, and healthcare clearing houses

Who enforces it? Department of Human and Health Services Office of Civil Rights (OCR)

ISO

International Organization for Standardization

ISO began operations in 1947

Independent, non-governmental international organization with membership of 162 national standards bodies

Published 21,599 international standards and related documents for every industry

NIST

National Institute of Standards and Technology

Founded in 1901, now part of Department of Commerce

Mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology

Standards and guidelines developed by NIST for computer systems are issued as Federal Information Processing Standards (FIPS)

HIPAA

- Security Rule
  - Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting important patient health information that is being housed or transferred in electronic form.
- Privacy Rule
  - The Standards for Privacy of Individually Identifiable Health Information establishes the first national standards to protect patients' personal health information (PHI).
- Breach Notification Rule
  - Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

HITECH

Health Information Technology for Economic and Clinical Health

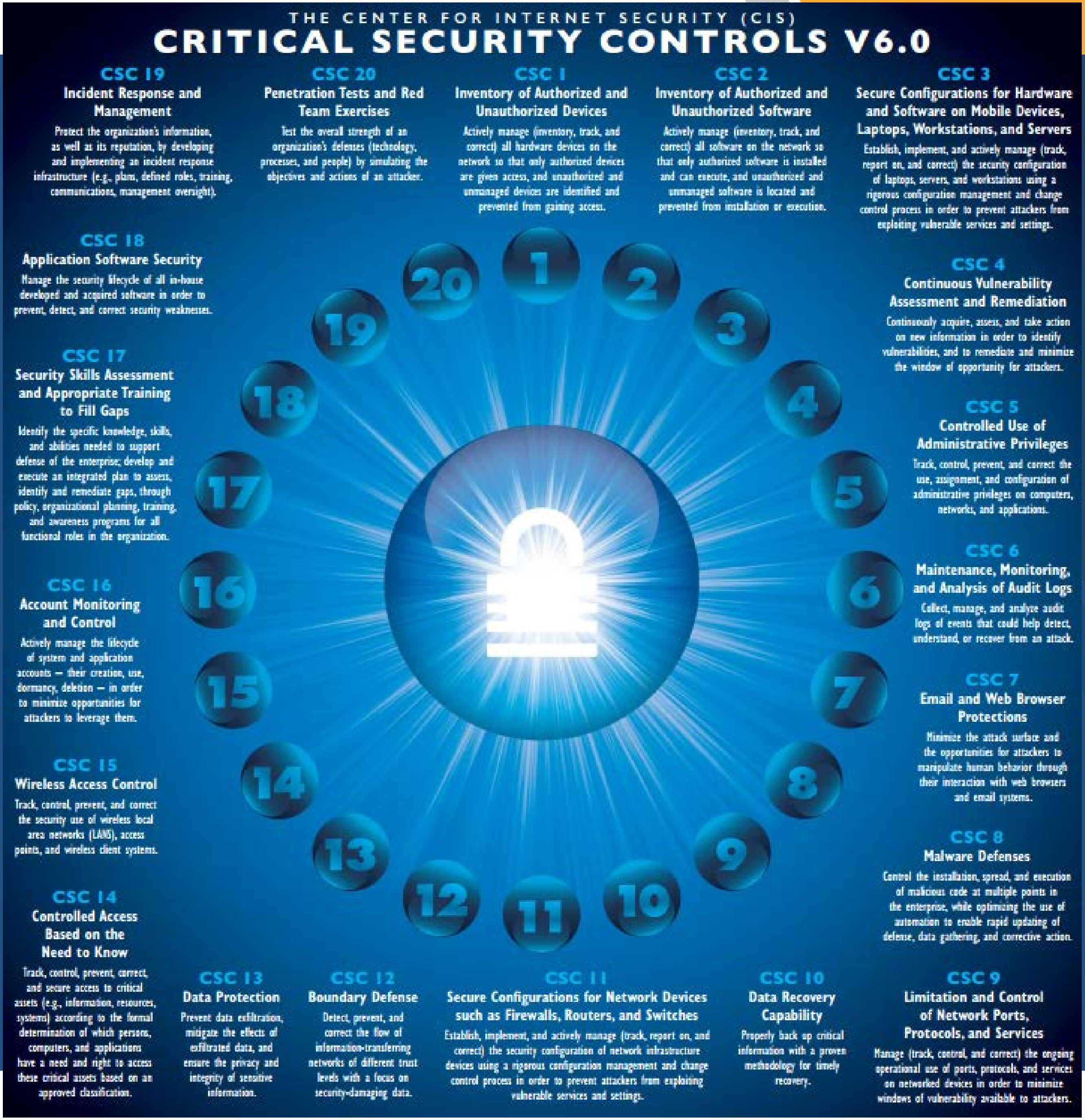
Enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA)

Signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology

HITECH Objectives

1. Extends privacy and security protections of HIPAA
2. Increases penalties for violation
3. Offers financial incentives for use of Electronic Health Records (EHR)
4. Requires notification of a PHI breach

EHR
=
QUALITY OF CARE
PATIENT SAFETY
LOWER COSTS


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

THE CENTER FOR INTERNET SECURITY (CIS)

CRITICAL SECURITY CONTROLS V6.0

CSC 19
Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20
Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

CSC 1
Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are identified and prevented from gaining access.

CSC 2
Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is located and prevented from installation or execution.

CSC 3
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 18
Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 17
Security Skills Assessment and Appropriate Training to Fill Gaps

Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 16
Account Monitoring and Control

Actively manage the lifecycle of system and application accounts — their creation, use, dormancy, deletion — in order to minimize opportunities for attackers to leverage them.

CSC 15
Wireless Access Control

Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 14
Controlled Access Based on the Need to Know

Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 4
Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5
Controlled Use of Administrative Privileges

Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6
Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7
Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

CSC 8
Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 13
Data Protection

Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 12
Boundary Defense

Detect, prevent, and correct the flow of information-transferring networks of different trust levels with a focus on security-damaging data.

CSC 11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 10
Data Recovery Capability

Properly back up critical information with a proven methodology for timely recovery.

CSC 9
Limitation and Control of Network Ports, Protocols, and Services

Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Case Study 1 – Unencrypted Laptop

Advocate Health Care Network, $5.5 million

- Largest HIPAA settlement as of September 2016
- Result of three separate data breaches
- Affected total of 4 million individuals
- One incident involved an unencrypted laptop that was stolen from an employee vehicle
- Another incident involved the theft of four computers
- OCR noted that Advocate Health Care failed to conduct risk analysis of all of its facilities, information systems, applications, and equipment that handle ePHI
  - Risk management plan needs to include not only technical but also physical and administrative measures.

Case Study 2 – Email Phishing

The University of Washington Medicine

- In December 2015, The University of Washington Medicine was first investigated by the OCR
- Facility suffered a significant security breach
- Incident occurred after a staff member **inadvertently opened an email** that contained malicious software
- Over 90,000 digital patient health records were accessed and compromised
- Settlement of $750,000

Case Study 3 – Improper Configured Server

New York and Presbyterian Hospital (NYP) and Columbia University, $4.8 million

- Fined after 6,800 patient records accidently exposed publicly to search engines
- Caused by an improperly configured computer server that was personally owned by a physician
  - Server was connected to network with ePHI
- NYP lacked processes for assessing and monitoring all its systems, equipment, and applications connected with patient data
- NYP also didn’t have appropriate policies and procedures for authorizing access to patient databases
- Both of these violations would have been easy to prevent through administrative processes

Case Study 4 – Malware

Anchorage Community Mental Health Services (ACMHS), $150,000

- Malware infection compromised the records of >2,700 individuals
- ASMHS did not review its systems for unpatched and unsupported software and did not regularly update its IT resources
- Underscores importance of running regular updates and patches
  - Simple yet often ignored practice that could have major implications

Case Study 5 – Cloud Storage

St. Elizabeth’s Medical Center, $218,400

- Stemmed from two incidents, one of which was use of a cloud-based file-sharing application.
  - Specifically, did not evaluate risks of using cloud service, putting ePHI of nearly 500 people at risk
- The cloud provides scalable, cost-effective and flexible solution for storing and sharing patient data
- Conduct risk assessment prior to migrating to cloud environment
  - Risk assessment should also include a comprehensive analysis of the security capabilities of prospective vendors

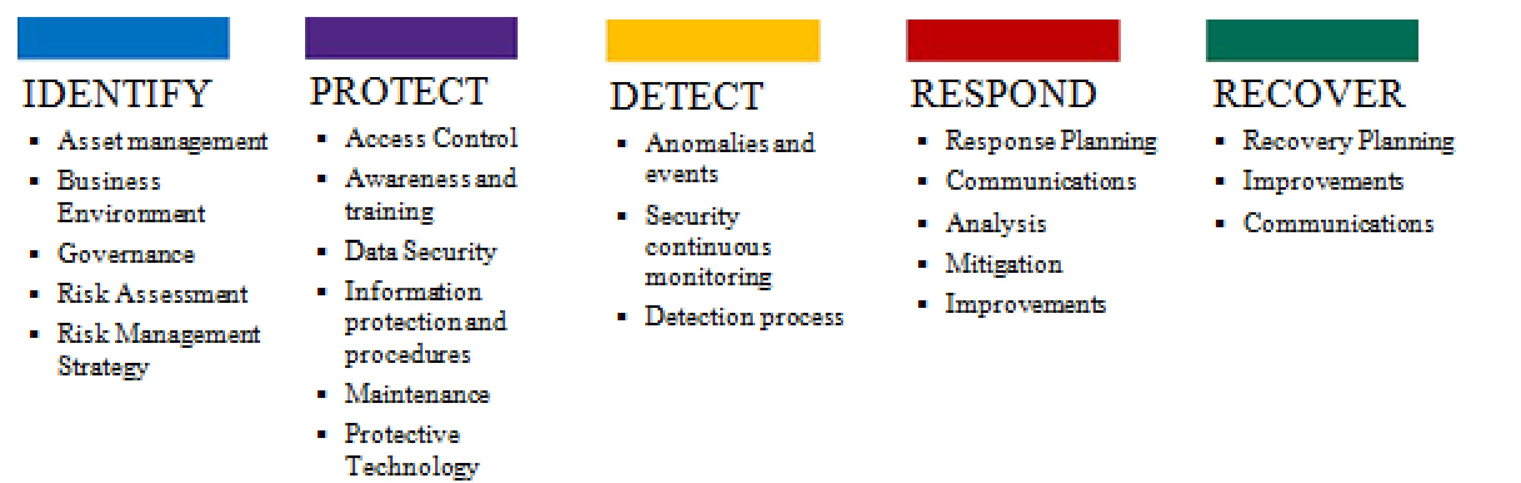
Other Common HIPAA Mistakes

1. Employee Dishonesty
2. Third Party Disclosure
3. Improper Disposal
   - Photocopier can cause HIPAA violation if patient information is saved on the hard drive
4. Unauthorized Release

Cybersecurity Framework (CSF)

- Three parts:
  - – Framework Core
  - – Framework Implementation Tiers
  - – Framework Profiles

Framework Core:



IDENTIFY

- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Access Control
- Awareness and training
- Data Security
- Information protection and procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications

CSF: Tiers/Profiles

- Tiers
  - Tier 1: Partial
  - Tier 2: Risk Informed
  - Tier 3: Repeatable
  - Tier 4: Adaptive
- Profiles
  - *Current* profile (“as is”)
  - *Target* profile (“to be”)

CSF: Benefits, Challenges

- **Benefits:**
  - – Voluntary
  - – Expose new risks
  - – Sharing, collaboration
  - – Layered approach

- **Challenges:**
  - – Not “set it and forget it”
  - – Requires “buy-in”
  - – Communicating risks
  - – Large, complex organizations
  - – Lack of quantifiable metrics

800-53: Security and Privacy Controls for Federal Information Systems and Organizations

- 18 security areas
  - Management/enterprise
  - Operational
  - Technical
- 8 privacy areas

800-53: Security – Technical

- AC: Access Control
- AU: Audit and Accountability
- CM: Configuration Management
- IA: Identification and Authentication
- SC: System and Communications Protection
- SI: System and Information Integrity

800-53: Security – Operational

- CA: Security Assessment and Authorization
- CP: Contingency Planning
- IR: Incident Response
- MA: System Maintenance
- MP: Media Protection
- PE: Physical and Environmental Protection

800-53: Security – Management/ Enterprise

- AT: Security Awareness and Training
- PL: Security Planning
- PM: Program Management
- PS: Personnel Security
- RA: Risk Assessment
- SA: System and Services Acquisition

800-53: Privacy

- AP: Authority and Purpose
- AR: Accountability, Audit, and Risk Management
- DI: Data Quality and Integrity
- DM: Data Minimization and Retention
- IP: Individual Participation and Redress
- SE: Security
- TR: Transparency
- UL: Use Limitation

800-53: Security and Privacy Controls for Federal Information Systems and Organizations

- **Benefits:**
  - Comprehensive
  - Supplemental guidance useful
  - Baselines allow risk-based approach
  - Supported by 53A, allowing for corresponding assessment
  - Cross references throughout and to other NIST SPs

- **Challenges:**
  - Comprehensive! (Complex)
  - Focus on *Federal* systems
    - *Private entities? State/Local government?*
  - Focus on *information* systems
    - *IoT devices, industrial control systems, weapons systems*

800-61: Computer Security Incident Handling Guide

- Organizing a Computer Security Incident Response Capability
  - Understanding Events and Incidents
  - Incident Response Policy, Plan, Procedures
  - Incident Response Team Structure

- Handing an Incident
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activity

800-61: Computer Security Incident Handling Guide (cont.)

- **Benefits:**
  - Easy to understand for detection, analyzing, prioritizing, handling incidents
  - Provides checklists, scenarios, examples, recommendations
- **Challenges:**
  - Less focus on establishing incident response program
  - Doesn’t provide specific template for Incident Response Policy or Plan

800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

- Confidentiality of PII
- Includes the following:
  - Introduction to PII
  - PII Confidentiality Impact Levels
  - PII Confidentiality Safeguards
  - Incident Response for Breaches Involving PII
  - Scenarios for PII Identification and Handling

800-122: Guide to Protecting the Confidentiality of PII (cont.)

- **Benefits:**
  - Categorizing PII by the confidentiality impact level
  - Other terms and definitions used to describe personal information
- **Challenges:**
  - Identifying all PII residing in environment
  - Organizations subject to a different combination of laws, regulations, and other mandates

1800 Series: Cybersecurity Practice Guides

SP 1800-7 (Draft)	February 2017	**Situational Awareness for Electric Utilities** Announcement and Draft Publication
SP 1800-6 (Draft)	November 2016	**Domain Name Systems-Based Electronic Mail Security** Announcement and Draft Publication
SP 1800-5 (Draft)	October 2015	**IT Asset Management: Financial Services** Announcement and Draft Publication
SP 1800-4 (Draft)	November 2015	**Mobile Device Security: Cloud and Hybrid Builds** Announcement and Draft Publication
SP 1800-3 (Draft)	September 2015	**Attribute Based Access Control** Announcement and Draft Publication
SP 1800-2 (Draft)	August 2015	**Identity and Access Management for Electric Utilities** Announcement and Draft Publication
SP 1800-1 (Draft)	July 2015	**Securing Electronic Health Records on Mobile Devices** Announcement and Draft Publication

Questions?

If you wish to discuss any aspect of this presentation in more detail, please feel free to contact us:

Sarah Ackerman

sackerman@clarkschaefer.com

(513) 371-5613

Melissa Meeker

mmeeker@cshco.com
(937) 399-2000