Cybersecurity Audits - Top 5 Findings

June 28, 2018

Carly Devlin
Mark Stoudemire
Clark Schaefer Consulting

clark schaefer consulting

Interested in CPE for today's event?

CPE Option 1 (Digital method)

- Be logged into the webinar for at least 50 min.
- Complete three of our interactive polls
- Complete the webinar survey

CPE Option 2 (Paper method)

- Be logged into the webinar for at least 50 min.
- Record the three CPE codes on the CPE form (located in the Handout List)
- Complete the webinar survey
- Send completed CPE form to nboudreau@clarkschaefer.com

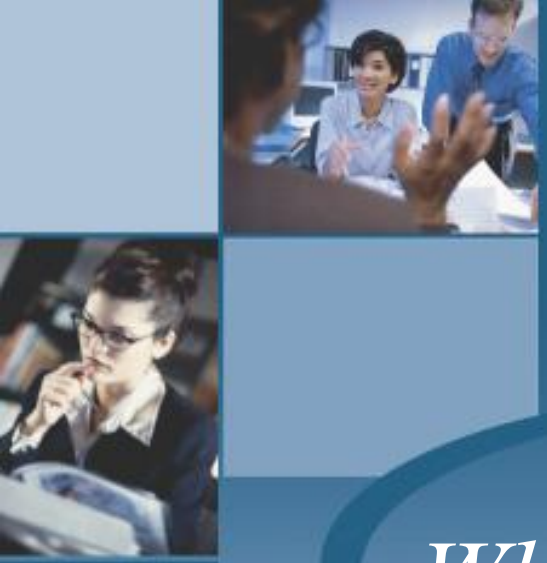
Today's Presenters

Carly Devlin, CISA, CISSP
Managing Director, Columbus Office
Connect on LinkedIn

Mark Stoudemire, CEH, CHFI, CCNA
Consultant, Columbus Office
Connect on LinkedIn

Agenda

- Importance of Cybersecurity Audit
- Cybersecurity Audit Approaches
- Top 5 Findings
- Cybersecurity Control Frameworks



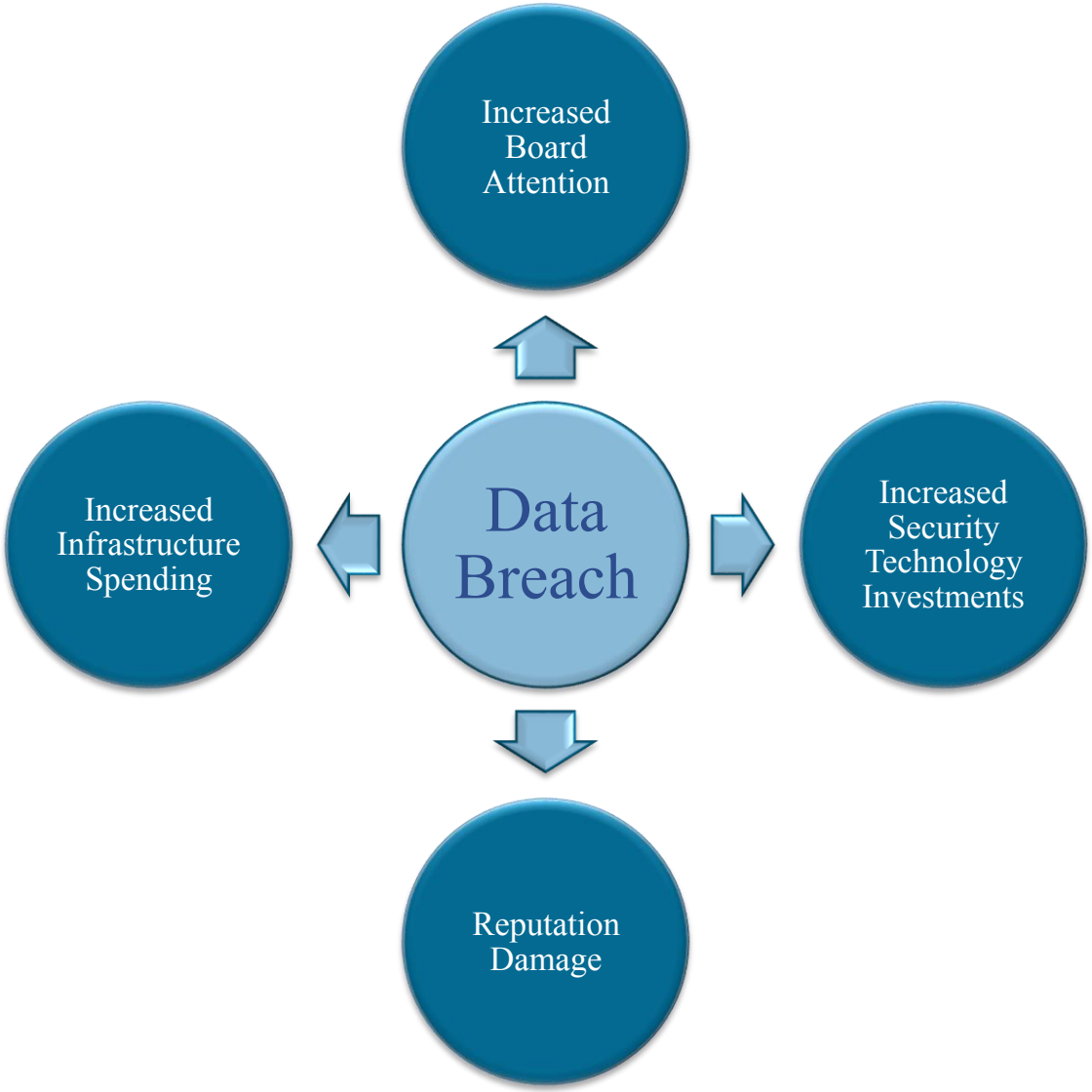
Why Audit Cybersecurity?

clark schaefer consulting

Three Lines of Defense

- **First Line: Operational Management**
  - Owns the risk decisions made for the organization - vested interest in ensuring cyber security controls exist and are operating effectively.
- **Second Line: Risk Management**
  - Facilitates and monitors the implementation of effective cyber risk management practices by operational management and assists risk owners in defining the target risk exposure.
- **Third Line: Internal Audit**
  - Independent and objective view of cybersecurity communicated to the board level of the enterprise.

Increased Awareness



Increased Risk

- Failure to mitigate cyber risk may cause:
  - Disruption of systems/business processes
  - Loss of confidential data
  - Financial loss
  - Fraudulent reporting & metrics
  - Damage to reputation

Cybersecurity Audit Approaches

clark schaefer consulting

Governance

Governance Audit

- Cybersecurity policy and related technical key operating procedures
- Point in time
- Address the business function/local design and implementation of key operating procedures supporting the security policy.

Risk

Cyber Risk Management Audit

- Risk register update, treatment, and risk reporting in cyber security
- Point in time (year-end)
- Address risk register accuracy, completeness and proper updating. Also address risk reporting (timeliness, completeness, accuracy).

Management

Cyber Incident Review Audit

- Cybersecurity incident reviews
- Continuous, based on actual attacks, breaches and incidents
- Semiformal review of any attach or breach (including near misses) as part of standard third-line-of-defense involvement

Assurance

Assurance Audit

- Cyber security controls review
- Point in time and transformational
- Independently review the efficiency and effectiveness of cybersecurity controls in place

Cybersecurity Goals vs. Audit Objectives

Cybersecurity Goal	Audit Objective(s)
Cybersecurity policies, standards, and procedures are adequate and effective	▪ Documentation is complete and up to date ▪ Formal approval, release, and enforcement are in place ▪ Documentation covers all cyber security requirements ▪ Subsidiary controls cover all provisions made in P&P
Emerging risk is reliably identified, appropriately evaluated and adequately treated	▪ Risk identification process is reliable ▪ Risk evaluation process (including tools, methods, and techniques used) is adequate ▪ All risk is treated in line with the evaluation of results ▪ Risk treatment is adequate or formal risk acceptances exist for untreated risk
Cyber security transformation processes are defined, deployed and measured	▪ Transformation process and related guidance exists and is complete ▪ The transformation process is implemented and followed by all parts of the enterprise ▪ Controls, metrics, and measurements relating to transformation goals, risk and performance exist
Attacks and breaches are identified and treated in a timely and appropriate manner	▪ Monitoring and specific technical attack recognition solutions exist ▪ Interfaces to security incident management and crisis management processes and plans exist ▪ On the basis of past attacks, attack response is timely and adequate.

Source: ISACA

Top 5 Audit Findings

clark schaefer consulting

1. Cyber Risk Management

- Lack of a cyber risk management framework
- Cyber risk management is not incorporated into ERM process
- Lack of executive management/board buy in
- Lack of governance structure
- Lack of information sharing
- Inadequate risk identification

2. Policies and Procedures

- Lack of information security policies and procedures
- Policies and procedures are not comprehensive
- Lack of defined roles and responsibilities
- Lack of policy and procedure enforcement/auditing
- Lack of alignment to a framework

3. Vulnerability/Patch Management

- Vulnerability scanning/assessment is not performed on a periodic basis
- Identified vulnerabilities are not prioritized and addressed adequately
- Vulnerabilities are not tied to specific assets
- Lack of formal patch management processes
- Patches are not applied timely

4. User Access Management

- Default account passwords are not changed
- Multifactor authentication is not in place
- Segregation of duties concerns are not identified
- Lack of user access review process (from a user *and* role/permissions perspective)
- Lack of break glass process for shared accounts

5. Security Awareness Training

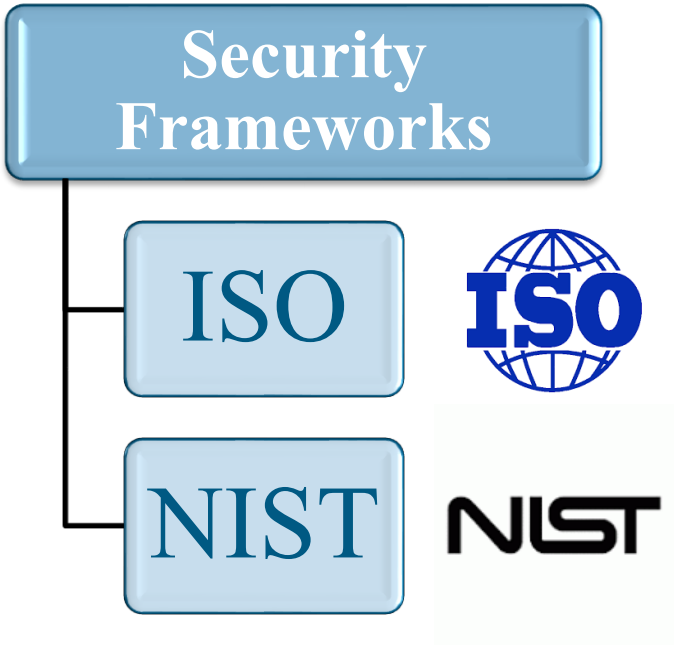
- Security awareness training is not performed on a periodic basis
- Training is “one size fits all”
- Training is not interactive
- Lack of awareness training metrics
- Metrics are not used to measure success

Cybersecurity Control Frameworks

clark schaefer consulting

Use of a Security Framework

- A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.



ISO/IEC 27001: 2013

- **Established by:**

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

- **Designed to:**

Provide requirements for an information security management system (ISMS)

- **Overview:**

Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements are intended to be applicable to all organizations, regardless of type, size, or nature.

NIST Cybersecurity Framework

- **Established by:**

The National Institute of Standards and Technology (NIST)

- **Designed to:**

Be a US government-ordered, cybersecurity framework

- **Overview:**

A structure for the nation's financial, energy, healthcare, and other critical systems to better protect their information and physical assets from cyber attack. NIST provides a common language with which to address and manage cyber risk in a cost-effective way based on business needs, without additional regulatory requirements.

NIST Cybersecurity Framework (CSF)

- **Three Parts:**
  - Framework Core
  - Framework Implementation Tiers
  - Framework Profiles

Allows organizations to:

- Describe current cybersecurity posture
- Describe target state for cybersecurity
- Identify and prioritize opportunities for improvement
- Assess progress towards target state
- Communicate using common language among internal and external stakeholders about cybersecurity risk

CSF 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 Core

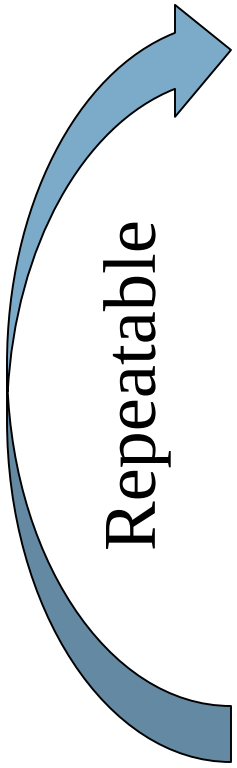
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

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 – Applying the Framework



1. Prioritize & scope
2. Orient
3. Create a current profile
4. Conduct a risk assessment
5. Create a target profile
6. Determine, analyze & prioritize gaps
7. Implement action plans

CSF – Benefits and 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

Questions?

Carly Devlin, CISA, CISSP
Managing Director, Columbus Office
cdevlin@clarkschaefer.com
Connect on LinkedIn

Mark Stoudemire, CEH, CHFI, CCNA
Consultant, Columbus Office
mstoudemire@clarkschaefer.com
Connect on LinkedIn

CPE Overview

CPE Option 1 (Digital method)

- Be logged into the webinar for at least 50 min.
- Complete three of our interactive polls
- Complete the webinar survey

CPE Option 2 (Paper method)

- Be logged into the webinar for at least 50 min.
- Record the three CPE codes on the CPE form (located in the Handout List)
- Complete the webinar survey
- Send completed CPE form to nboudreau@clarkschaefer.com

Thank You!

Carly Devlin, CISA, CISSP
Managing Director, Columbus Office
cdevlin@clarkschaefer.com
Connect on LinkedIn

Mark Stoudemire, CEH, CHFI, CCNA
Consultant, Columbus Office
mstoudemire@clarkschaefer.com
Connect on LinkedIn