University of Dar es Salaam

Lecture 7 – Auditing Cybersecurity Programs

Aron Kondoro

Introduction

- Increased security incidents
  - Credit card info breaches
  - Theft of personal data
- Data and systems protection
  - Payment Card Industry (PCI) standards
  - European Union General Data Protection Regulation (GDPR)
  - Health Insurance Portability and Accountability Act (HIPAA)
- Therefore, necessary to defend organizations against cyberattacks and ensure compliance
- Auditor ensures efforts and investments into security programs meet organization’s needs

Introduction

- Understand **size**, **scope**, and **purpose** of organization's cybersecurity program
- Organizations have security programs with different purposes:
  - Compliance requirements e.g. retailers must comply with PCI rules, banks must comply with different government rules
  - Protecting intellectual property e.g. technology companies, companies in defence/aerospace industries
  - Protecting production lines e.g. manufacturing firms
  - Protection of personal information e.g. credit agencies, NGOs, healthcare providers

Introduction

- No “one size fits all”
- Must consider **business needs** & **risk posture**

Steps for Auditing Cybersecurity Programs

1. Assess placement of cybersecurity program

- Identify responsibility for information security in organization
  - E.g. CISO, IT Security manager, CIO
- How
  - Review organization charts to identify the information security team
  - Ensure existence of clear reporting structure
  - Interview CISO to understand level of oversight
    - i.e. regular reporting to CIO, executive steering committee, board of directors

2. Assess risk management processes

- Evaluate how information-related risks are identified and managed
  - Otherwise difficult to justify security investments
- How
  - In case of formal risk management processes (RMP), **review outputs** of such processes
  - If no formal RMP, **look for evidence** security team considers risks in decision process

2. Assess risk management processes

- Evidence of risk management process:
  - Periodic, formal threat and risk assessments
  - Third-party testing of security controls
  - Compliance programs
  - Risk-based strategic planning processes
  - Corporate-level risk planning processes
- Guiding question for evaluating process:
  - *How are risks identified, and how does the team align on how to address them?*
  - *What role do business leaders and other stakeholders play in the decision process?*
  - *Are cybersecurity threats considered in the overall organization risk discussions?*

3. Evaluate scope of cybersecurity program

- Determine how the security needs of an organization are met by the program
- How
  - Obtain organization charts or other artifacts describing the structure and function of the security team
  - Interview functional leaders
  - Ascertain separation-of-duties risks

3. Evaluate scope of cybersecurity program

- Minimal scope of a security program:
  - Policy and compliance management
  - Awareness
  - Vulnerability management
  - Security monitoring
  - Incidence response

4. Review the security policy and compliance

- Ensure IT security policies exist and provide adequate coverage
- Determine how policies are communicated
- Determine how compliance is monitored and enforced
- How
  - Verify adequate policy coverage i.e. review based on **industry standards** and **company needs**
    - Review other specific policies i.e. password policy, logical access policy
  - Verify stakeholder buy-in
  - Verify process around the policies i.e. periodic reviews, exemption processes
  - Review monitoring processes for policy compliance

4. Review the security policy and compliance

- Minimum IT security policy coverage:
  - Acceptable usage of company information assets
  - Data classification, retention, destruction
  - Remote connectivity
  - Passwords
  - Server security
  - Client security
  - Logical access

5. Review security awareness and communication

- Review **awareness programs** and **methods to train** employees on security risks and concerns
- How
  - Discuss scope of security awareness program with responsible personnel
  - Review processes for providing general security training to new employees
  - Ensure periodic delivery of security training
  - Review timing and content of training programs
  - Discuss the ongoing security awareness program
  - Review results of phishing exercises

5. Review security awareness and communication

- Security awareness should include
  - General security training for new employees
  - Periodic security training for current employees
  - Ongoing general security awareness
  - Role-specific security training
  - Other specific training i.e. education about malicious emails, phishing email exercises, training about PII

6. Review the vulnerability management process

- Ensure there is awareness of emerging threats and vulnerabilities
- Ensure there is process to identify at-risk systems
- How
  - Review the organization's approach in finding and resolving vulnerabilities
  - An effective program should include
    - Awareness of new threats and vulnerabilities e.g. TZ-CERT, NIST, third-party threat intelligence
    - Vulnerability scanning and other identification methods i.e. timing, tools e.g. Qualys, Rapid7, Tenable
    - Evaluation of discovered vulnerabilities i.e. severity
    - Processes to communicate and track results and actions

7. Assess the security monitoring process

- Review log collection, alert processing, and detection capabilities
- Ensure monitoring group has appropriate systems and is taking necessary action
- How
  - Review processes and technology to collect and correlate log data and alerts i.e. discuss with security operations centre (SOC) team
  - Review SIEM policies i.e. amount of data, sources, retention time
    - Security information and event manager (SIEM) – stores data from different sources e.g. firewalls, proxies, antivirus etc
  - Discuss with SOC how log data is protected
  - Review process for developing alerts from correlated data
  - Discuss how actions/alerts are tracked
  - Ensure mechanism for employees to report security incidents

8. Assess the incident response process

- Ensure the organization can respond effectively to security events
- Review the formal incident response (IR) process to ensure documented process exists and is followed
- How
  - Request copy of the IR process i.e. if unavailable assess organization's response

8. Assess the incident response process

- An effective IR should include
  - Criteria for invoking different response levels
  - Identification of key roles and responsibilities
  - Contacts for decision pints
  - Action guidelines

9. Assess other functions of the security team

- Ensure security team functions meet organization's needs
- How
  - Interviews with security team and document review
  - Security team can also
    - Manage devices and software used to provide technical security
    - Serve as consultants in other IT projects

10. Review data management policies & processes

- Evaluate policies and processes for
  - Assigning ownership of company data
  - Classifying data
  - Protecting data
  - Defining data's lifecycle
- How
  - Review the data classification policy
  - Review evidence of data classification policy implementation i.e. documentation
  - Determine whether data life-cycle information has been created

11. Determine security at organization level

- Ensure various parts of the organization understand security requirements and involve the security team
- How
  - Discuss IT processes with operations/development teams
    - E.g. software patching schedule with dev team
  - Determine how security architecture function engages with other parts of the organization

12. Review security personnel skills and knowledge

- Ensure knowledge and skills of security personnel is current and relevant
- How
  - Review human resource (HR) policies and processes related to security
    - Look for mechanisms to ensure qualified people are hired; existence of continuous improvements
    - Existence of job descriptions
    - Training policies
    - Performance review processes

13. Review MSSPs

- Review processes around the use of managed security service providers (MSSPs) within the security team
- How
  - Review the process of selecting vendors
  - Ensure contract include SLAs, NDAs, right-to-audit clauses

12. Determine effectiveness of security controls

- Ensure that security controls are effective
- Independent assessments i.e. attestations/certifications, external audits, incident response exercises, and penetration testing
- Evaluate the **presence**, **scope** and **frequency** of independent assessments
- How
  - Interviews with CISO and/or delegates
  - Review how results are processes and resolved

Further Reading

- Lecture 7 Reading