Module 9: Homework 9

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

October 22, 2023

Review Questions

1. **Briefly differentiate between information security governance and information security management.**
    - Information security governance refers to the overall strategy, policies, and oversight of an organization's information security program. It focuses on aligning security with business objectives and managing risk. Key activities include establishing security policies, setting standards, defining roles and responsibilities, and monitoring compliance. The board of directors and executive management typically lead security governance.
    - Information security management refers to the day-to-day operational aspects of implementing an information security program. It focuses on executing the policies, controls, and procedures defined under security governance. Key activities include risk assessments, implementing technical controls, security monitoring, incident response, awareness training, and ensuring compliance with regulations. The CISO and security team typically lead security management.

    In summary, security governance provides high-level direction and oversight, while security management handles the hands-on work of running security operations and implementing controls. They work together to ensure an effective information security program. Governance defines the what and why, while management focuses on the how.

2. **List and describe the responsibilities of typical C-level executive positions.**

    C-level executive positions and their main responsibilities:

    - Chief Executive Officer (CEO): The CEO is the highest-ranking executive and leader of the entire company. They are responsible for setting the overall vision, strategy, and direction of the organization. The CEO manages the executive team and makes major corporate decisions.
    - Chief Financial Officer (CFO): The CFO oversees all financial matters in the company. Key responsibilities include financial planning and analysis, accounting, tax, treasury, budgeting, auditing, reporting, and investor relations. They manage cash flow and risks.

- Chief Operating Officer (COO): The COO is responsible for the daily operations and execution of business plans. They oversee day-to-day activities across business units to drive growth and operational excellence. COOs manage execution of strategy set by the CEO.
- Chief Information Officer (CIO): The CIO leads technology strategy and oversees all aspects of information technology in the organization. This includes IT infrastructure, systems, applications, networks, and security. They align IT initiatives with business goals.
- Chief Marketing Officer (CMO): The CMO leads marketing strategy and campaigns. Responsibilities include market research, branding, advertising, media relations, and new product launches. The goal is to drive sales, engagement, and company visibility.
- Chief Human Resources Officer (CHRO): The CHRO heads human resource management including talent acquisition, retention, compensation, diversity, training, and organizational culture and change management. They oversee HR policies and programs.

3. List and describe the responsibilities of typical privacy positions.

- The Chief Privacy Officer (CPO) develops and oversees the organization's overall privacy program, establishing privacy policies, standards, procedures and governance. The CPO manages privacy risk, ensures compliance with regulations, and reports to executives on privacy issues.
- Privacy Counsel provides legal advice on privacy laws and regulations. They review privacy policies, contracts, and agreements and assist with compliance audits and investigations.
- Privacy Analysts conduct privacy impact assessments on new projects and document privacy controls. They support training efforts and help with privacy audits and data subject requests.
- Privacy Engineers implement technical controls to protect privacy in systems and applications. They de-identify data and build automation tools.
- Privacy Auditors perform regular audits and assessments to identify risks and gaps. They validate remediation of issues and measure privacy program effectiveness.

- Privacy Officers or Managers lead privacy teams to execute governance activities like developing processes, coordinating training, and reporting on metrics.

These roles work together to operationalize an organization's privacy program. The CPO establishes the privacy vision while the other roles execute the privacy program and manage risk. Scope varies based on company size and industry regulations.

4. What is a privacy program?

A privacy program is a comprehensive approach that organizations use to ensure the proper handling of personal information and compliance with applicable privacy laws and regulations. The key components of a privacy program typically include:

- Privacy policies and procedures - Documents that outline how the organization collects, uses, shares, secures, and disposes of personal data. Procedures provide guidance for day-to-day privacy operations.
- Governance model - Defines privacy roles and responsibilities. This includes having a privacy/data protection officer and cross-functional team to manage the privacy program.
- Legal compliance - Processes to identify and comply with relevant privacy laws and regulations. Organizations continuously monitor legal changes.
- Risk assessments - Regular privacy impact and risk assessments of products, services, systems, and third party vendors that handle personal data.
- Training - Ongoing awareness training for employees and contractors on privacy policies, legal requirements, and best practices.
- Incident response - Plans and procedures to detect, investigate, and remediate privacy breaches and incidents.
- Vendor management - Selection criteria and oversight mechanisms to ensure vendors and partners handle personal data properly.

5. **Briefly differentiate between privacy program plan, privacy plan, privacy policy, privacy notice, and acceptable use policy.**

    - Privacy Program Plan - An overall roadmap that lays out how an organization will implement and manage its privacy program. It covers governance, resources, controls, processes, and key program elements.
    - Privacy Plan - An action plan focused on a specific initiative like a new product launch or IT system implementation. It assesses privacy risks and documents required controls.
    - Privacy Policy - A public-facing document that discloses how an organization collects, uses, shares, and secures personal information. It informs customers and users.
    - Privacy Notice - A document that provides detailed and specific information to individuals about how their personal data is being handled. Notices supplement privacy policies.
    - Acceptable Use Policy - An internal policy for employees on properly using company systems and technology. It covers permissible activities, security protocols, and handling of data.

    In summary, the privacy program plan is the overarching strategy while policies, notices, and plans address specific privacy activities and disclosures. The acceptable use policy governs employee behavior and system use. Together these documents operationalize and communicate privacy practices.

6. **Briefly describe the OASIS privacy management reference model.**

    The OASIS Privacy Management Reference Model (PMRM) provides a framework for designing and operating a privacy program. Here is a brief overview of its key components:

    - Govern - Establishes the policies, roles, and business processes to manage privacy from the top down. Includes leadership, goal setting, and governance bodies.
    - Comply - Activities to comply with privacy laws, regulations, and commitments. Involves identifying requirements, gap assessments, and monitoring legal changes.
    - Operate - Ongoing activities to operationalize privacy controls and processes. Includes assessing risk, building controls into systems, training, managing vendors, and handling requests.

- Sustain - Measures to continuously improve the privacy program. Focuses on metrics, audits, maturity assessments, and feedback loops for enhancing the program.
- Inform - Covers internal and external communications about privacy practices. Includes awareness training, public notices, statements, and other transparency efforts.
- Enforce - Handles enforcement, sanctions, remedies, and consequences for non-compliance. Includes disciplinary actions and breach notification processes.

7. Briefly describe the OASIS privacy documentation for software engineers.

The OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) provides guidance for building privacy into software and systems. Here is a brief overview:

- Privacy Guided Requirements Analysis - Includes privacy requirements gathering, compliance reviews, impact assessments, and risk analysis.
- Architectural Analysis - Evaluates architecture approaches to integrate privacy controls like encryption, access controls, and data minimization.
- Design Analysis - Incorporates privacy solutions into detailed designs such as pseudonymization, aggregation, validation, and secure storage.
- Implementation Analysis - Applies best practices for handling personal data like logging, testing, configuration management, and security coding.
- Maintenance & Evolution Analysis - Addresses privacy in system upgrades, patches, enhancements, and decommissioning throughout the system lifecycle.
- Documentation - Captures process artifacts like privacy requirements specs, architecture tradeoff analysis, design decisions, and implementation checklists.

References

[1] Freestone, T. (2022, September 3). *A Guide to Information Security Governance*. Kiteworks | Your Private Content Network. https://www.kiteworks.com/secure-file-transfer/security-governance/

[2] *Steps for building a privacy program, plus checklist | TechTarget*. (2021, November 1). Security. https://www.techtarget.com/searchsecurity/tip/Steps-for-building-a-privacy-program-plus-checklist

[3] *Privacy Policy vs. Privacy Notice: What's the Difference - Securiti*. (2023, September 18). Securiti. https://securiti.ai/privacy-policy-vs-privacy-notice/

[4] *OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC | OASIS*. (n.d.). OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC | OASIS. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se