CYS 2310
Policy, Legal, Ethics and Compliance

Lecture # 6
Essential Cybersecurity Standards and Controls

Learning Objectives:

Upon completion of this lecture, you will be able to learn about:

- ✓ Cybersecurity controls issued by the NCA
- ✓ Network Security Controls
- ✓ Access Control
- ✓ Incident Response and Management
- ✓ Security Awareness and Training
- ✓ Health Insurance Portability and Accountability Act (HIPAA)
- ✓ ISO 27001
- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Conclusion

Cybersecurity controls issued by the NCA

- The National Cybersecurity Authority (NCA) in Saudi Arabia has issued several cybersecurity controls to protect critical infrastructure and information systems.
- While the specific controls may vary, here are some common areas covered by the NCA's guidelines:

Network Security Controls

- The NCA provides guidance on implementing robust network security controls, including firewalls, intrusion detection systems, intrusion prevention systems, and secure configurations for network devices.

Access Control

- The NCA emphasizes the need for strong access controls to ensure authorized user access and prevent unauthorized access to sensitive systems and data.
- This includes implementing secure authentication mechanisms, access management policies, and least privilege principles.

Incident Response and Management

- The NCA encourages organizations to develop and implement incident response plans and procedures to effectively detect, respond to, and recover from cybersecurity incidents.
- This includes establishing incident response teams, conducting regular drills, and establishing communication protocols.

Security Awareness and Training

- The NCA emphasizes the importance of cybersecurity awareness and training programs for employees to promote a security-conscious culture.
- This includes educating staff about common cyber threats, phishing awareness, and secure practices for handling sensitive information.

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA is a U.S. standard that focuses on safeguarding protected health information (PHI) in the healthcare industry.
- It sets requirements for data privacy, security, and breach notification.
- While HIPAA is not specific to Saudi Arabia, organizations that handle PHI for U.S. entities may need to comply with HIPAA regulations.

ISO 27001

- ISO/IEC 27001 is an international standard for information security management systems (ISMS).
- It provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system.
- Organizations in Saudi Arabia can adopt ISO 27001 as a best practice for managing their information security.

Payment Card Industry Data Security Standard (PCI DSS)

- PCI DSS is a set of security standards established by the Payment Card Industry Security Standards Council (PCI SSC).
- It applies to organizations that handle payment card data, such as merchants, banks, and payment processors.
- Compliance with PCI DSS ensures the protection of cardholder data and the secure processing of payment transactions.

Conclusion

- It's important to note that compliance with these standards and controls may be mandatory or voluntary depending on the industry, sector, and specific regulatory requirements.
- Organizations should consult the respective standards and local regulatory bodies for detailed information and specific compliance obligations.

Review

- Cybersecurity controls issued by the NCA
  - Network Security Controls
    - Access Control
    - Incident Response and Management
    - Security Awareness and Training
    - Health Insurance Portability and Accountability Act (HIPAA)
    - ISO 27001
  - Payment Card Industry Data Security Standard (PCI DSS)
- Conclusion

End of Lecture