September 19, 2022

Security Frameworks

Activity

Read the article by Barafort et al (2018) and the blog by Kirvan (2021). Review the websites listed in the blog and then answer the following questions:

1. Which of the frameworks do you think would be applicable to the following organisations:
    a. International bank

        → General Data Protection Regulation (GDPR)

        → PCI-Security Standards

        → Sarbanes-Oxley Act (SOX)

    b. Large hospital

        → General Data Protection Regulation (GDPR)

        → HIPAA

        → PCI-Security Standards (depending)

    c. Large food manufacturing factory

        → General Data Protection Regulation (GDPR)

        → PCI-Security Standards

2. Summarise the tests and recommendations you would make to the owners/ managers for each of the above businesses to help them use the frameworks and comply with industry standards
    a. International bank

        → Governance structure

        → Discern between personal and sensitive data

        → Encryption to protect data (transport and storage)

        → Access control policies/procedures/measures

        → Role privileges and segregation of duties

        → Password policies (MFA and encryption type)

        → Patch management protocols/procedures/policies

        → System monitoring (IPS and IDS)

        → Incident management policy and plan

        → Business Continuity Plan and Recovery Plan

        → External Audit

        → Employees training and awareness

        → Physical security management

        → Information management policies

        → Financial reporting (periodic and audited by independent auditors)

        → Internal controls (policies and procedures)

        → Real-Time Issuer Disclosures

        → Whistleblower Protections

        → Criminal Penalties

        → Data Security Standard

→ PIN Transaction Security (PTS)

→ Software Security Framework

→ Point-to-Point Encryption (P2PE)

→ Mobile Standards

→ Secure Network and System

→ Protect Account Data

→ Vulnerability Management Program

→ Monitoring and Testing Networks

→ Information Security Policies

b. Large hospital

→ Governance structure

→ Discern between personal and sensitive data

→ Encryption to protect data (transport and storage)

→ Access control policies and procedures

→ Role privileges and segregation of duties

→ Role rotation, vacation

→ Password policies (MFA and encryption standards)

→ Patch management protocols/procedures/policies

→ System monitoring (IPS and IDS)

→ Incident management policy and plan

→ Business Continuity Plan and Recovery Plan

→ External Audit

→ Employees training and awareness

→ Physical security management

→ Information management policies

→ Privacy Rule: limit use of patient information with prior authorisation, access to copy of the patients' records

→ Security Rule: technical safeguards, physical safeguards, administrative safeguards

→ Breach Notification Rule

→ Omnibus Rule

→ Enforcement Rule

c. Large food manufacturing factory

→ Governance structure

→ Discern between personal and sensitive data

→ Encryption to protect data (transport and storage)
→ Access control policies and procedures

→ Role privileges and segregation of duties

→ Password policies (MFA and encryption type)

→ Patch management protocols/procedures/policies

→ System monitoring (IPS and IDS)

→ Incident management policy and plan

→ Business Continuity Plan and Recovery Plan

→ External Audit

→ Employees training and awareness

→ Physical security management

→ Information management policies

→ Data Security Standard

→ PIN Transaction Security (PTS)

→ Software Security Framework

→ Point-to-Point Encryption (P2PE)

→ Mobile Standards

→ Secure Network and System

→ Protect Account Data

→ Vulnerability Management Program

→ Monitoring and Testing Networks

→ Information Security Policies