Project Part 2

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

August 11, 2024

Risk Management

Risk Assessment Report
XYZ Corporation is a global leader in the pharmaceutical industry, it handles sensitive data such as proprietary research, financial transactions, and clinical test data. This report will be an assessment of the potential risk the organization can potentially face.

Risk	Likelihood 1-5	Impact	Risk score (L * I)	Mitigation strategies	Controls Implemented	Responsible	status
Phishing Attack	5	4	20	Cyber Security Awareness training.	Email Filtering, Multi-Factor authentication, phishing simulation training.	IT Security Team	In Progress
Data Breaches	3	5	15	Strong access controls encrypt data at rest and in transit, and strong data policies.	Role-based access controls (RBAC), AES-256 encryption, regular audits on our systems	IT Security Team, Data Governance Council	Planned
Natural Disasters	2	4	8	Create disaster recovery sites and emergency response procedures.	Offsite data backups, disaster recovery site, emergency response playbook, and procedures.	IT and security, compliance team,	In Progress
Malicious employee	2	5	10	Access controls, DLP, Continuous monitoring	RBAC, monitoring of access logs, strong offboarding procedures.	HR & IT Security	In Progress

Careless Employee	3	3	9	Regular Cyber Security training programs	Security awareness training, and regular audits of the training program.	HR & IT Security	In Progress
Supply Chain Attack	3	4	12	Implement supply chain auditing process and procedures	Vendor assessments, secure communications channels	Procurement & IT	Planned
Ransomware	3	5	15	Ensure robust backup and recovery procedures	Endpoint detection and response (EDR), Patch management process	IT Security Team	Planned
DDoS Attack	4	3	12	Network security measure to prevent DDoS attacks	DDoS Protection Services, Monitoring Traffic, Firewalls	IT Security Team	Planned
Software Vulnerabilities	3	4	12	Patch software regularly	Vulnerability scanning and vulnerability management process, patch management processes	IT Security Team	In Progress
Power Outage	2	3	6	Implement backup power solutions	Uninterruptible power supplies, generators	IT	Planned
Espionage	2	5	10	Strict access controls	RBAC, security, monitoring, background checks for	HR & IT Security	Planned

					employees		
Third-Party Vendor Risk	3	3	9	Vendor Risk assessments	Vendor Risk management program and processes, contractual security requirements	IT Security	Planned
Physical Theft of company devices	2	4	8	Physical security and tracking systems	Security locks, asset tracking systems	IT Security, Security Operations	Planned

This list provides a detailed overview of all the potential risks XYZ Corporation is likely to face. It also highlights the mitigation that should be implemented into the mitigation plan within the risk management framework.

Risk Mitigation Plan

Phishing Attack: deceptive emails which have been designed to trick employees into revealing sensitive information or downloading malicious software.

- Mitigation Strategy: XYZ Corporation will implement security awareness training programs as well as advanced email filtering, and finally multi-factor authentication.
    - Security Awareness Training
    - Email Filtering
    - Multi-Factor Authentication (MFA)
    - Regular Updates
- Security Controls Implemented
    - The advanced email filtering solution is: (ProofPoint).
    - Multi-factor authentication (MFA) is: (OKTA)
    - Regular phishing simulations and employee training programs.

Ransomware Attack: malware that encrypts critical data and demands payment for decryption of the data, this will potentially cause operational issues and cause financial loss.

- Mitigation strategy: XYZ Corporation will develop and enforce robust data backup and recovery procedures, It will also implement EDR solutions and ensure regular patching of its software.

    - Data Backup and recovery
    - EDR
    - Software Updates
- Security Controls Implemented
    - EDR (CrowdStrike Falcon)
    - Regular software updates and patch management.
    - Data backups and recovery procedures.

Data Breaches: unauthorized access to sensitive customer or proprietary data theft causing financial loss and reputational damage.

- Mitigation strategy: Implement strong access controls mechanisms and enhance data encryption policies and ensure regular audits.
    - Access control mechanism
    - Data Encryption
    - Regular Audits
- Security Controls Implemented
    - RBAC
    - Data encryption (AES-256) for data at rest and in transit.
    - Regular audits and vulnerability assessments

Unauthorized Access: Intruders who gain access to critical areas which can lead to theft or sabotage of equipment and data.

- Mitigation strategy: enhance physical security measures with access control systems and cameras and security staff
    - Access control systems
    - Cameras
    - Security staff
- Security Controls implemented
    - Access Control systems (Key card)
    - Cameras
    - Security Staff

Supply Chain Attack: compromising a vendor to gain access to the organization's systems and data.

- Mitigation Strategy: implement supply chain security protocols and vendor assessments.
    - Vendor Assessments
    - Contractual Security requirements
- Security Controls implemented
    - Vendor risk management program.
    - Contractual security requirements.

DDoS Attack: involves overwhelming the organization's network with traffic to disrupt services.

- Mitigation Strategy: implement network security measures such as DDoS Protection services, firewalls, and monitored traffic.
    - DDoS Protection Services
    - Firewalls
    - Traffic Monitoring
- Security Controls Implemented
    - DDoS protection services.
    - Firewalls fortinet fortigate
    - Traffic monitoring tools. (Splunk)

Insider Data Theft: employees stealing data for personal gain or for malicious purposes.

- Mitigation Strategy: monitor and control access to any sensitive data using DLP tools.
    - Data Loss Prevention (DLP)
    - Access Controls
- Security Controls Implemented
    - Data Loss Prevention (DLP)
    - Access Controls

Software Vulnerabilities: Issues in the software that can be exploited by attackers to gain unauthorized access or cause damage.

- Mitigation Strategy: update and patch software with patch management process, also scan for vulnerabilities.
    - Patch management process
    - Vulnerability Scanning
- Security Controls Implemented
    - Patch Management system
    - Regular vulnerability scanning process

Power Outage: disruption in business operations due to loss of power this can cause data lass or damage equipment.

- Mitigation Strategy: implement backup power solutions to ensure business continuity.
    - Uninterruptible power supplies (UPS)
    - Backup Generators
- Security Controls Implemented
    - Uninterruptible power supplies (UPS)
    - Backup Generators

Third-Party Vendor Risk: Security Vulnerabilities introduced by vendors and partners that can compromise XYZ organization security.

- Mitigation Strategy: Conduct risk assessment and have a third-party risk management program.
    - Vendor Risk Assessments

    - Contractual Security Requirements
    - Ongoing Monitoring
- Security Controls Implemented
    - Vendor risk management program
    - Contractual security requirements
    - Ongoing team that monitors vendor programs.

Physical Theft of Devices: Theft of devices which involves loss of data or equipment.

- Mitigation Strategy: Implement physical security and asset tracking systems.
    - Security Locks
    - Asset Tracking Systems
    - Security Policies
- Security Controls Implemented:
    - Security Locks on Devices
    - Asset tracking systems
    - Security policies for device handling.

Espionage: individuals or organizations gaining access to sensitive data for malicious purposes.

- Mitigation strategy: strict access controls, employee background checks, and security team monitoring.
    - Access Controls
    - Security Monitoring
    - Employee Background Checks
- Security Controls Implemented:
    - Role-based access control (RBAC)
    - Security Monitoring systems
    - Employee background checks.

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISCO. (n.d.). *Networking, Cloud, and Cybersecurity Solutions*. Cisco. https://www.cisco.com/site/ca/en/index.html

CrowdStrike. (n.d.). *The CrowdStrike Falcon® platform*. Crowdstrike.com. https://www.crowdstrike.com/platform/

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. https://www.fortinet.com/products/next-generation-firewall

ISO. (2023). *ISO/IEC 27001:2022(en)*. Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Lenaerts-Bergmans, B. (2021, December 8). *What is a Supply Chain Attack? | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

NIST. (2020). Security and privacy controls for information systems and organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

paloalto networks. (n.d.). *Global Cybersecurity Leader - Palo Alto Networks*. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/

rockwell. (n.d.). *MES Solutions for Life Sciences | FactoryTalk | US*. Rockwell Automation. Retrieved July 25, 2024, from https://www.rockwellautomation.com/en-ca/products/software/factorytalk/operationsuite/mes/life-sciences.html

SAP. (n.d.). *MES: The Power of Real-Time Data*. SAP. https://www.sap.com/canada/products/scm/execution-mes/what-is-mes.html

SOLARWINDS. (n.d.). *What Is WSUS? Windows Server Update Services Guide - IT Glossary | SolarWinds*. Www.solarwinds.com. https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services