UNIVERSITY OF GREENWICH

Mega-Corp Security Enhancement Report

COMP-1608-MANAGING IT SECURITY AND RISK

MSc Computer Forensics and Cyber Security

Table of Contents

Summary

In this age of digitalization and ever evolving technology, Cyber-attacks are one of the most common types of threat for any multination company. Cyber-attacks can compromise a company’s security, integrity or availability. It can disrupt a company’s normal operations, expose sensitive data and damage company’s reputation.

Mega-Corp Security enhancement report outlines the Security enhancements that need to be implemented to reduce risk in case of a cyber-attack. This report is written with a focus on People, Processes, Policies, Procedure and Security standards such as ISO27001, NIST and PCI-DSS.

It includes the threats that are most relevant to the organization and provide security measures to counter those threats. All the steps and procedures to improve perimeter security, physical assets and Infrastructure security, access management control and responsibility of various teams are included in this report.

Task 1: - Five Key areas for Improving the Organization’s Security Posture

1. Cybersecurity awareness trainings and best practices
    - Mega Corp does not follow good cyber security practices. There are no cybersecurity awareness trainings for employees to increase their awareness against phishing, malware or ransomware attacks.
    - Mega Corp does not follow proper onboarding process and does not have standards that employees need to follow.
2. Data Security Policy and Guidelines
    - Mega Corp does not have any security policies relating to their data. Everyone has access to client data. No encryption and backup planning is implemented, also available storage is not sufficient.
    - Mega Corp deals with international customers with products like Food supplements, nutrition but does not have any vulnerability assessment programs or risk assessment in place.
3. Identity Management and Access Control
    - IAM (Identity and Access Management) practices are not being followed. Confidential data cann be accessed by anyone as access control is not enforced.
    - Hierarchy based privileges for access control are not in place. As a result, the chances of data breech increases.
4. Network and Perimeter Security
    - No physical security measures are put in force. Everyone has access to all places. There should be biometric locks for server rooms. Different Id-badge permissions are required for employees and visitors.
    - Network segmentation is not enforced, no separation of dev, test and production environment. No VPN for external users or on-site employees is present.
    - Defence in Depth strategy to secure digital assets and networks should be followed.
5. Monitoring and Incident response.
    - Systems are not equipped with proper monitoring tools. Only web and database server monitoring are in place.
    - Inadequate logging can increase the time required for incident response.

Task 2: - Realistic Action Plan and Team Assignments Using NIST CSF

Action	Area of Improvements
Identify	Asset Management
	Risk Assessment and Strategy
Protect	Employee awareness and training
	Identity Management and Access Control
	Perimeter Security
	Network Security and Data Security (Defence in depth strategy)
Detect	Security Information and Event Management (SIEM)
	Security Operation Centre (Continuous monitoring and detection)
	Vulnerability Assessment and Penetration Testing
Respond	Incident Management and Response Planning
	Incident Analysis and Mitigation
	Improvements
Recover	Disaster Recovery Planning
	Keep records of backups.
	Backup operations procedures

2.1 Identify

- Create an Asset Management team to identify and label assets, track device allocation to employees, and monitor their usage.
- Keep track of critical assets, data and their respective location.
- Establish data governance specific to location and data and take measures to ensure compliance.
- Create onboarding and training policies for business requirements. Human resources team should be responsible for hiring and assigning job titles to employees to effectuate hierarchy.
- Identify risks associated with development related changes especially in production environment. Establish policies for users access to dev and test environments. The Change Management team must verify code and functionality before the changes are deployed in production.

2.2 Protect

Defence in depth is a strategy that involves implementing a series of measures to protect our network/systems. Multiple tools, mechanisms, and policies are simultaneously implemented, with the idea that if one fails, others can protect the system (Fruhlinger, 2022).

Administrative controls

- System Administrators team should be responsible for managing and creating Active Directory (AD) groups and policies according to the organization hierarchy.
- 2FA for Outlook email access should be implemented. Password policies also need to be enforced.
- Client data on the shared network drive should be encrypted and only required users should have access to it.
- Create an IT support team for VPN, software, and installations related issues in compliance to ISO27001 standards.
- Implement automatic update and patch management.

Physical controls

- Issue photo ID cards and make it mandatory for employees to wear. Establish a guest sign-in system with visitor ID cards.
- Install security cameras, maintain video backups, and use third-party contractors for improved physical security.
- Restricted areas should have with biometric locks, allowing only authorized personnels. Have security staff for guarding entrances and exits.

Technical controls

- Have an IAM team responsible for managing the JML (Joiner, Mover, Leaver) process, email assignments, and user access by utilizing automated tools such as SailPoint or Saviynt.
- Put together an NOC team responsible for managing Networks Activities, configuring Firewalls (FortiGate-5001A-SW-G), managing switches, routers, and data centre. They should also manage VPN (rv340) configuration for external data access.
- The NOC team should implement network segmentation, separate client and organization data, set up DMZ, IDS/IPS, establish subnets for different departments, and ensure secure connections to Azure and AWS.
- Risk Management team should be responsible for defining policies for Data access, Data storage and data encryption as per security standards.
- Vulnerability management and penetration testing should take place once a year and, also when systems or application are updated to help detect any threat or loopholes.

Security Awareness

- Cybersecurity awareness training for all employees should be made mandatory and recurring sessions (quarterly or yearly) should be conducted. Fostering a culture of vigilance and responsibility towards cybersecurity risks help maintain a secure environment.
- Perform security drills (or table-top exercises) to check awareness and preparedness of employees/teams in different situations.
- Identify knowledge gap and provide yearly cross-skilling sessions, also allocate budget for industry level certifications.

2.3 Detect

- Proper logging should be enabled on all systems. Allocate separate storage and systems for log analysis.
- Use IBM QRadar or Splunk tools for log analysis and detecting malicious behaviour.
- Install IDS at network level to identify malicious activity at network level and ensure every Host equipped with HIDS (Host Intrusion Detection System).
- Install DLP (Data Loss Prevention) or EDR (Endpoint Detection and Response) tools at device level to monitor data breach.
- SOC (Security Operation Center) team should be responsible for maintaining all the above functionality and continuous monitoring.

2.4 Respond

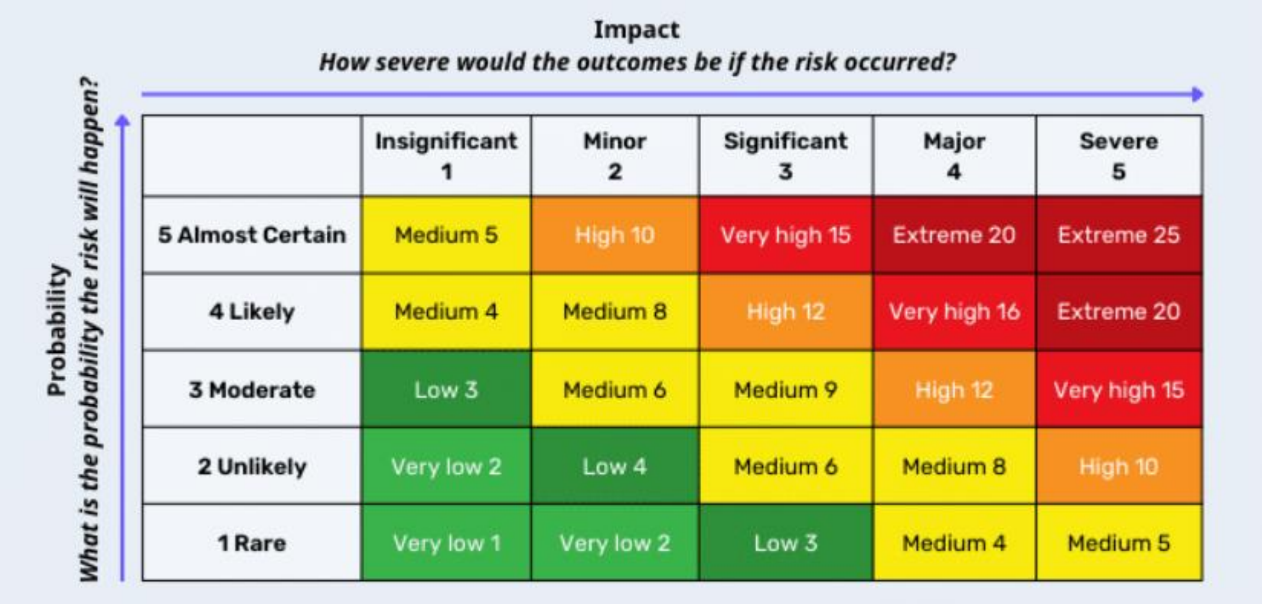
- Create a structured plan for identifying, managing and responding various incidents. Create procedures to handle and respond to incidents.
- Incident Management Team should analyse and understand the nature and impact of incidents. Once identified, team should respond to incidents and prevent further damage. This includes finding RCA (Root Cause Analysis) and implementing solutions to prevent similar incidents from occurring in the future.
- Post Incident, Incident Management team should assess and enhance security plans.

2.5 Recover

- DR team should be responsible for proper data backup and ensuring that enough storage is available for backup.
- DR team should take regular backup, schedule verification and restore processes to ensure that data can be recovered in case of a disaster.

Task 3: - Risk Analysis of Security Threats to the Organization.

Below graph represents the Risk Assessment of Mega Corp company.



Impact
How severe would the outcomes be if the risk occurred?

Probability
What is the probability the risk will happen?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Figure 1: - Risk Metrix of MegaCorp

Threat	Asset	Likelihood	Impact	Risk Metrix
1. Phishing Attacks	Users and relevant data.	3	4	12
	Scenario: - Employee should receive email appearing from trusted source, tricking them to click on the link or revealing confidential information leads to unauthorized access, compromise of confidential data and sometime cause financial loss. Mitigation: - Introducing cyber awareness training related to phishing mail for employee and ensure availability of email filtering tool for blocking malicious mail. Conduct exercise related to phishing attacks to know the level of awareness.			
2. Broken Access Control	Confidential Data, Servers	2	5	10
	Scenario: - joiner's onboarding process is not standardised & employee does not have proper Job Title. Joiners often learn on the job, from shadowing to trial and error. As a result, leaving employees unaware of security protocols and best practices. Mismatch between job roles and access rights, allowing employees more access than necessary. Mitigation: - Create AD group & group policy to restricted access and Implement Role base access control. Create a team that supports JML (Joiner, leaver, mover) process, conduct access reviews (called certification in IAM). Establish training sessions, covering both general security awareness and job-specific skills.			

3. No standardized software development practises	Company's product & Infrastructure	5	5	25
	Scenario: - Developers are testing code in production. No network segmentation of Dev, test and production environment. No change management in practise. Leads to exploits vulnerabilities exploitation and service interruption. Mitigation: - Use best SDLC procedure. Ensure Dev and Test environment are only accessible into private network . Developer can not access production environment until code is approved by change management team for production.			
4. Perimeter Security breach	Data Center, Confidential files, and physical system	4	5	20
	Scenario: - Unauthorized employee can access restricted area like Data Center, Files location that are confidential, Guest can enter without verification and access restricted area increased possibility of theft of physical assets. Mitigation: - Introduce guest verification system and provide visitor badge to guests. Use biometric lock system for restricted area and put guard in entrance and exit. Made mandatory for employee to wear ID-card to identify unauthorized employee.			
5. Inadequate Logging and Incident management	System Failure, Data Leakage, Business Interruption	3	3	9
	Scenario: - Logging is not implemented because of insufficient storage. Company has licence of IBM Qradar but not efficiently used. Mitigation: - Increase the storage capacity for proper log storage. create an Incident management team for proper incident management and response. Having proper action plan and SOPs for frequently occurring incidents.			
6. Insecure Data storge	Confidential data, Storage Devices	2	5	10
	Scenario: - No data separation for client and users. Unencrypted client data on shared storage with improper access control leading to data leak cause loss of reputation in market, heavy financially penalty according to various security standards breach (e.g., GDPR). Mitigation: - Separate network for client and user data. Enforce role base access control and encryption policy for confidential data. Create policy to audit the logs quarterly or monthly to find malicious behaviours related to data access.			
7. Website compromise or security breach	Website, Infrastructure, Product	4	4	16
	Scenario: - Mega Corp doesn't have vulnerability management and penetration testing (VAPT) program are in place and Security Operation Center(SOC) is not operated. That cause vulnerability exploitation by unknown attacker which leads			

	Mega Corp to undetected threats, data breaches and system interruption. Mitigation: - Introduce VAPT program once in a year and while system or product updated or upgraded. Create a and SOC team for continuous monitoring and evaluation which helps to identify breach in a time.			
8. Improper device configuration and management	Network Devices, Servers	4	5	20
	Scenario: - VPN is not used to access internal network. Devices are not encrypted and no administrative controls for software installation. Antivirus, Data loss Preventation tool (DLP) and logging tool are not installed on system which cause malware or ransomware attack. Mitigation: - Configure VPN for remote access users ensuring that connection between users and Mega Corp network is Secure. Install Antivirus, DLP and logging tool which prevent Antivirus and Malware attack and also help SOC team for proper monitoring.			
9. Insecure Network Integration after merger	Network Devices	2	4	8
	Scenario: - Mega Corop recently merger with Initech and integrated its core network equipment but happened rapidly, and a complete list of connected devices is not available. Additionally, integration some Initech staff account moved to Mega Corp's domain to manage newly acquire hardware leading to data breaches, unauthorized access, or disruptions in business operations. Mitigation:- Conduct assessment of integrated network configurations, and potential security risks. Including an audit of admin accounts transferred from Initech. Ensuring that access permissions are necessary and follow the principle of least privilege. Implement robust security controls, such as firewalls, IDS to monitor traffic between MegaCorp's existing network and the newly integrated components.			
10. Lack of centralized patch management system	System Failure	5	5	25
	Scenario: - Mega Corp dependent on manual system patching where user receives email instructions to apply updates. It is possible that user may overlook the email and delay applying patching. Due to lack of centralized patch management, it is difficult to track patching progress. This increases the organization's likelihood to known vulnerabilities and potential exploitation. Mitigation: - Implement an automated patch management system that centralizes the distribution and installation of software updates. To minimize disruptions to operations, create regular and well-defined schedule. Encourage a culture of proactive security maintenance.			

Task 4: - PCI-DSS Compliance: Key Requirements and Implementation Strategies

4.1 Maintain a Vulnerability Management Program and Secure Network

1. **Establish process for addressing vulnerabilities based on risk**
   To address PCI-DSS compliant, Mega Corp needs to create a systematic approach to identify, prioritize, and address vulnerabilities. This process assesses the potential impact and likelihood of vulnerability exploitation, help organization to focus on mitigating critical risks first.

2. **Performing vulnerability assessment and penetration testing quarterly**
   Establish policy to conduct vulnerability assessment and penetration tests quarterly. VAPT helps to identify weaknesses in the software and networks and provide details of vulnerability and CVEs. During software updates this test ensures that any hidden vulnerabilities are discovered and resolved before exploited.

3. **Use Antivirus and DLP Tools for protect Against Malicious Software**
   Mega Corp ensure that their servers and data storage of PCI users are protected from virus and malware using antivirus software such as CrowdStrike and Symantec. This tool prevents, detect and stop malicious activity and help to enhance security.
4. **Encrypt Payment Information and Cardholder Data:**
   Encrypted and Dedicated storage needs us used for storing payment data. Ensure payment data storage and user data storage are in different network segmentation to reduce risk of unauthorized access. This segmentation and encryption add extra layer of security.
5. **Maintain Firewall Configuration**
   Network team needs to make sure that default configuration is not used anywhere. Ensure that all traffic denied by explicitly allowing permitted traffic. It ensures to controlling and monitoring incoming and outgoing network traffic by preventing unauthorized access.
6. **Change Default Password and Device Configurations**
   Default passwords on all the devices, server and network devices need to be changed and force all user to change their password on first login that improve security. unnecessary services and protocols should be disabled to reduce the attack surface and minimize potential vulnerabilities.
7. **Use Encryption Protocols (SSL/TLS)**
   While transmitting cardholder data across open and public networks ensures use of robust encryption protocols (SSL/TLS). This encryption helps protect sensitive information from packet sniffing and unauthorized access during transit.
8. **Use Secure Wireless Networks and VPN Technologies**
   Ensure that wireless networks are secure and use strong encryption algorithms and strong password used to access router configuration. VPN (Virtual Private Network)

technologies are used by employee for secure remote connections to the corporate network for securing and encrypt communication network for remote users.

4.2. Implement Regularly Monitoring and Strong Access Control Measures

1. **Implement Role based access control (RBAC)**
   Mega Corp should follow role base access control policy to ensure that employees have least access sufficing their role. Ensure regular access review and update access permission based on requirements using zero trust architecture.
2. **Standardized Onboarding and Offboarding Processes**
   Ensue that employee's receiver appropriate access and training to understand company's policy and their job responsibilities. Revoke access rights immediately after employees leave the organization that ensure data privacy.
3. **Establish SOC and Security and Event Management (SIEM)**
   Deploy SIEM solution like Splunk across whole network infrastructure, servers, networking devices, storage devices for real-time monitoring and alerting for security events. Implement SOC 24*7 team to monitor and respond to incidents.
4. **Policy for Logging and Monitoring**
   Define policies for logging such as storage device, type of data for logging, retention policy and access to log devices. Configure syslog protocol on servers and devices for secure logging transfer.
5. **Strong policy for Third Party Service Provider (TPSP)**
   While using TPSP for storing encrypted data, ensure that TPSP cannot access any encryption and decryption key and not involve in management of keys. If TPSP use card holder data for processing, ensure strong password policies and access control are in place.

Conclusion

The overall security posture of Mega Corp will improve significantly after the suggested changes are implemented. Steps to reduce risk landscape by evaluating their vulnerability to potential threats and effectively mitigating them have been included in the report. Suggested security measures align with the industry regulations such as PCI-DSS, NIST, ISO 27001 & GDPR . Suggestions to improve Incident Response Capability were also suggested. The importance of user awareness and trainings has also been mentioned. Implementation of Physical, Technical and Administrative controls for restricting access, separation of duties, detecting and preventing unwanted activities is necessary. Continuous monitoring and documentation and reporting also play an important role.

Cybersecurity is an ongoing process and threats evolve with new technology, so it is important to reassess and adapt with emerging threats and maintaining a robust security posture.

References

BasuMallick, C., 2022. *What Is SIEM (Security Information and Event Management)? Meaning, Tools, and Importance.* [Online] Available at: https://www.spiceworks.com/it-security/data-security/articles/security-information-and-event-management [Accessed 27 11 2023].

Fruhlinger, J., 2022. *Defense in depth explained: Layering tools and processes for better security.* [Online] Available at: https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html [Accessed 07 11 2023].

HackerOne, 2023. *5-Step Security Risk Assessment Process.* [Online] Available at: https://www.hackerone.com/knowledge-center/5-step-security-assessment-process [Accessed 27 11 2023].

Harrington, D., 2023. *The 12 PCI DSS Requirements: 4.0 Compliance Checklist.* [Online] Available at: https://www.varonis.com/blog/pci-dss-requirements [Accessed 28 11 2023].

Landsberger, D., 2023. *What Is Network Segmentation and Why Does It Matter?.* [Online] Available at: https://www.comptia.org/blog/security-awareness-training-network-segmentation [Accessed 27 11 2023].

NIST, 2019. *NIST Cybersecurity Framework.* [Online] Available at: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0 [Accessed 27 11 2023].

Owasp, 2021. *Welcome to the OWASP Top 10 - 2021.* [Online] Available at: https://owasp.org/Top10/ [Accessed 27 11 2023].

Karanfil, M. et al. (2022) ‘Security monitoring of the microgrid using IEC 62351-7 network and System Management’, 2022 IEEE Power &amp; Energy Society Innovative Smart Grid Technologies Conference (ISGT).doi:10.1109/isgt50606.2022.9817482.