Case Study 2: Retail ShopEverything

Names: Kiruthika Venkatachalam & James Ko

BrainStation
Cybersecurity Course

CONTENTS

EXECUTIVE SUMMARY

ShopEverything is a large department store chain and e-commerce platform that offers a marketplace for select, approved vendors to sell their products, with over 500 stores across the country.

- It’s main threat was a Phishing Email (Social Engineering)
- Threat actors are described as malicious individuals, likely cybercriminals, who successfully conducted a phishing attack by posing as an IT manager.
- Data was highly sensitive due to PPI (Private Personal Information) & unencrypted data
- Installation of backdoors, potential data breaches
- Customers, company operations and employees were all affected

INCIDENT ANALYSIS

SECURITY
COMPANY

The main cause was poor practices by people and technology. The company stored PPI and passwords in plain text with no encryption.

The following element(s) of the CIA triad were comprised:

- Confidentiality – Unauthorized access to sensitive customer data (PII) and potentially internal company information.
- Integrity – The installation of backdoors by threat actors may allow unauthorized modification of data or systems, compromising data integrity.

The incident happened because of the following factors:

- Impersonation: The group of malicious individuals posed as an IT manager and created a highly targeted phishing email.
- Social Engineering: The threat actors exploited the recent company update of new technology to send the phishing email.

INCIDENT ANALYSIS

Phishing Email: The email was sent to company's Operations Leads to reset their work email password and it has a link leveraging as a legitimate company website.

Credential access: The Operation Lead used a very weak password and it made publicly available and make easy for the threat actor to access it.

The threat actors and the company's Operation Lead are the **people** involved in this attack and the **process** they used is the email communication and password reset. The **technology** involved in this attacks are Emails, Password Management, Security tools and access control system.

There were several technology components of the information system are relevant:

1. **Email System**
2. **Database Management System – Place where employee's sensitive data is stored**
3. **Web Applications – The fraudulent site mimicked as legitimate company web page**
4. **Access Control Systems – The system grants varying levels of access to users based on the job role**
5. **IT Security Infrastructure – Protective measures in place, which appear to be minimal based on the case**

INCIDENT ANALYSIS

There were few defense systems in place as ShopEverything had limited number of access to handle the customer's sensitive data and it was evidenced that one of the few IT security individual who reported the issue.

However, the effectiveness of those defenses appears to be lacking given the breach. To enhance security and prevent incidents the company could have implemented several key measures like **Multi-Factor Authentication (MFA), Strong password policies, Advanced Email Filtering technology (Gmail Spam Filter) Access Controls and Proper Employee Trainings.**

COMMUNICATION

The breach was discovered by one of the company's few security employees, who presumably reported the issue internally within the general IT department this meant there was a lack of a structured internal communication process delayed proper detection and response.

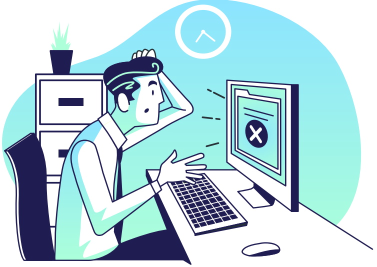
This should have been disclosed and should have been more customer trust, and will be at risk of reputational damage if the breach becomes public. Non-disclosure may lead to penalties under GDPR (General Data Protection and Regulation) or CCPA (California Consumer Privacy Act)

Recommendation for Future Communication

The company should establish a clear escalation process for reporting and handling security incidents across departments.

They should issue a public statement acknowledging breaches to maintain transparency and customer trust. Communication protocols should be in the Incident Response Plan (IRP) for timely customer updates and notifications.

RISK MANAGEMENT & BUSINESS ANALYSIS



Analysing the incident, the likelihood of this incident happening again is **high,** as employee training on security awareness is inadequate**.** If ShopEverything doesn't mitigate the issues to its Cybersecurity practices, it could be targeted again as Phishing Attacks are the most common type of attack.

Also, with the lack of Encryption and security policies and weak passwords, the occurrence of incidents are very high.

It should be included in the future risk registers to manage the ongoing risk and monitoring it to mitigate the risk by applying safeguard measures in place.

- The company should be aware of the following risks: **Data Breach, Online Security Risk, Financial Risk, Reputation Risk and Compliance Risk**

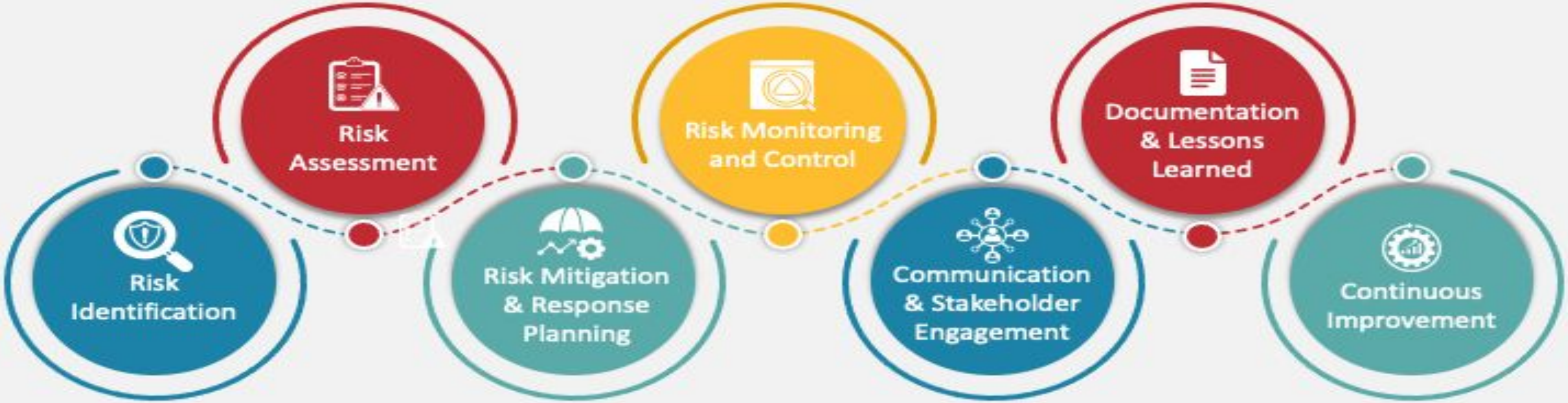
RISK MANAGEMENT & BUSINESS ANALYSIS

Note: Some other companies are monitoring similar risks-

1. **Cyber Risk –** Cyber Risk is a top concern among North America businesses now, and is expected to remain to be high in the near future as ransomware attacks continue to grow**.**
2. **Supply Chain and Vendor Risk –** Companies (and consumers) continue to face persistent supply shortages, delays, and rising commodity costs.
3. **Warehousing and Logistics Issues** – The retail company could run out of stocks while orders are coming in, a product shipment might be delayed, or a parcel could be delivered to the wrong recipient.
4. **Intellectual Property Issues –** Companies website images, product descriptions, logos, videos, music, as well as their products, could be copied by others, or violate someone else's intellectual property.

RISK MANAGEMENT APPROACH

Key Components of a Risk Management Approach



Risk Identification

Risk Assessment

Risk Mitigation & Response Planning

Risk Monitoring and Control

Communication & Stakeholder Engagement

Documentation & Lessons Learned

Continuous Improvement

RISK MANAGEMENT APPROACHES

The following risk management approaches would enhance the system security of Shop Everything:

Encryption: Encrypting customer data would protect against unauthorized access.

Access Control: By granting appropriate level of access control to authorized personnel and denying access to unauthorized functions or individual.

Password policy: Enhancing strong password policies and regular password changes.

Incident Response Plan: Develop and test an incident response plan ensure to prevent or take alternate actions if another breach is happens.

Internal Audits: Conduct regular security assessments and penetration testing to identify vulnerabilities.

Training: Implement regular security awareness training to educate employees about phishing emails and strong password practices and conducting webinars about cyber security threats and alters could gain knowledge and we could mitigate the risk.

Transparency with Customers: If a breach occurs, be transparent about the situation to maintain customer trust.

RISK REGISTER

Risk	Priority (Likelihood x Impact)	Risk Management Approach	Solution
Data Breach (unencrypted data storage)	High	Preventative measures	Encrypt all sensitive data in transit
Phishing Email Attack	High	Email filtering, employee training, anti-phishing tools	Conduct phishing awareness sessions
Weak Passwords (use of plaintext)	Medium	Increase password strength	Use Hash and better authentication (lockouts, CAPTCHA)
Malware/Ransomware Attack (lack of detection)	Medium	Antivirus,	Deploy endpoint detection and EDR tools

RISK REGISTER

Risk	Priority (Likelihood x Impact)	Risk Management Approach	Solution
Insider Threats	Medium	Implement tighter access controls, monitoring, and behavior analysis	Establish strict vendor management policies and limit data sharing
Third-Party Risks	High	Establish strict vendor management policies and limit data sharing	Minimize data sharing to only necessary information. Conduct regular security audits of vendors. Implement third-party contracts with clear data-handling guidelines

APPROACH & ACTION PLAN

ShopEverything has limited cybersecurity maturity based on its weak practices: storing sensitive data in plain text, lack of encryption, weak password policies, and poor access controls.

To address the identified risks, the key actions are: implementing Data Encryption, strengthening Access Control, and Enhancing Phishing Protection.

The required resources include:

- **People:** CISO, Employee Training Programs
- **Technical:** SIEM and Intrusion Detection Systems, Encryption Tools, Multi-Factor Authentication (MFA)
- **Capabilities:** Incident Response, Continuous Monitoring

APPROACH & ACTION PLAN

In terms of NIST Framework, all of the elements could be improved (Identify, Protect, Detect, Respond, and Recover and is summarized below:

- **Identify:** Improve risk management and asset classification.
- **Protect:** Enhance data security through encryption, access control, and employee training.
- **Detect:** Implement real-time monitoring systems like IDS and SIEM for better threat detection
- **Respond:** Establish an incident response plan with clear communication protocols.
- **Recover:** Develop a recovery plan and focus on continuous improvement post-incident with also a Disaster Recovery Plan and regularly backup all critical data.

After analyzing this, it's crucial to prioritize **Protect** (encryption, MFA, access control) and **Detect** (real-time monitoring) measures to prevent breaches and detect threats early.

INDUSTRY BEST PRACTICES & KEY IMPROVEMENTS

- **Data Encryption & Access Control:** Implement encryption for customer data and enforce multi-factor authentication (MFA) and role-based access controls (RBAC) to secure sensitive systems.

- **Implement Real-Time Monitoring:** Deploy SIEM (security information & event management) and network intrusion tools for continuous monitoring and early detection of suspicious activity.

- **Train Employees on Cybersecurity Awareness:** Regularly train employees on phishing, password security, and data handling, and conduct phishing simulations.

- **Learning from Other Companies:** Get inspiration from financial, healthcare, and tech companies like Google, Microsoft, and Amazon for best practices in proactive security and risk management (zero trust, regular training, access controls).

KEY TAKEAWAYS

Implementing Clear Security Policies and Response Plans

- **Recommendation:** Establish a comprehensive incident response plan (IRP) and create clear data governance policies to manage customer data responsibly.

Strengthening Security Awareness

- Employees are vulnerable to phishing and social engineering attacks due to lack of awareness.
- **Recommendation:** Implement mandatory *security awareness training* for all employees, focusing on recognizing phishing attempts and handling sensitive data securely.

Upgrading Security Infrastructure

- Critical gaps exist in data protection, access controls, and threat detection.
- **Recommendation:** Encrypt all sensitive data, implement multi-factor authentication (MFA), role-based access control (RBAC), and deploy real-time monitoring tools like SIEM and IDS.

Proactive Approach to Future Threats

- No proactive risk management practices in place to prevent future incidents.
- **Recommendation**: Incorporate the identified threats into a **Risk Register**, prioritize them, and conduct **regular risk assessments**.

APPENDICES & ASSUMPTIONS

- The security team is small and operates under a general IT department, indicating that security is not yet a top priority.

- The company does not have a strong incident response process and decided not to disclose a significant breach, which may indicate a lack of a risk-aware culture.

- Recommend that the company build a dedicated Cybersecurity team with a Chief Information Security Officer (CISO) to drive security strategy.

- Company could benefit suggested improvements (more personnel, budget for security tools and training).

Thank you!

REFERENCES

Liu, H., & FTC, S. at the. (2022, October 6). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework#:~:text=NIST%20is%20the%20National%20Institute,The%20Framework%20is%20voluntary.