Audit Report: Analysis of Data Breach Incident Response and Change Management Effectiveness at RMC Consultancy
Prepared by: Cybersocialdefend Team
Date: March 4, 2025

Roles & Responsibilities

- **Lead Auditor (Miguel)**: Oversees the entire audit process, ensures compliance with security standards, and finalizes the report.
- **Technical Auditor (Gulshan)**: Focuses on security configurations, incident response effectiveness, and cloud security assessments.
- **Compliance Auditor (Bhupender)**: Reviews policies, training effectiveness, and adherence to industry regulations.

Executive Summary

RMC Consultancy, a financial services firm with 10 employees, has experienced multiple cybersecurity breaches due to social engineering attacks, including phishing, vishing, and business email compromise (BEC). Despite existing security measures, weaknesses in incident response and change management strategies have contributed to repeated breaches. This audit evaluates RMC Consultancy's incident handling processes and change management practices related to data breaches. The focus is on identifying gaps in their current approach and recommending strategies to enhance security, mitigate future incidents, and improve overall resilience.

Findings indicate deficiencies in several areas, including incident reporting, training effectiveness, automated response capabilities, and access control mechanisms. Change management processes do not systematically enforce follow-ups on security improvements, leading to persistent vulnerabilities. This report presents an in-depth analysis of these issues and provides actionable recommendations for the CEO of RMC Consultancy to strengthen the company's security posture and incident management processes.

Audit Scope and Objectives

This audit assesses RMC Consultancy's ability to detect, report, and mitigate social engineering threats while examining how its change management processes can be leveraged to enforce long-term security improvements. The specific objectives of the audit are as follows:

- Evaluate the effectiveness of current awareness training on phishing, vishing, and business email compromise (BEC).
- Identify weaknesses in the incident response process.
- Assess the role of change management in addressing security vulnerabilities.
- Examine data security controls, including encryption, access policies, and cloud security.
- Provide structured recommendations to reduce the risk of future breaches through improved incident handling and change management.

Audit Methodology

The audit employed a combination of qualitative and technical assessments to evaluate RMC Consultancy's security posture:

- **Interviews with key personnel:**
  - **IT Security Staff** – Assessed security protocols, incident response, and change management.
  - **Employees** – Conducted surveys to evaluate awareness of social engineering threats.
- **Policy and incident review:**
  - Analysed incident response policies, change management records, and past phishing, vishing, and BEC incidents.
- **Security controls assessment:**
  - Evaluated cloud security configurations, access controls, MFA implementation, and encryption practices.
- **Simulated phishing tests:**
  - Tested employee responses to phishing attempts to measure training effectiveness.

Audit Findings

3.1 Incident Handling Deficiencies

- **Delayed Threat Recognition:** Employees often fail to promptly identify and report phishing attempts, increasing the risk of successful attacks.
- **Ineffective Training Retention:** Despite regular security training, employees continue to fall for social engineering scams, indicating gaps in training effectiveness and reinforcement.
- **Absence of Automated Security Controls:** The organization lacks automated threat detection and response mechanisms, leading to delays in isolating and mitigating cyber threats.
- **Poor Incident Documentation:** Incident records are inconsistently maintained, making it challenging to track trends, analyze root causes, and implement effective countermeasures.
- **Weak Data Protection Measures:** Inadequate encryption protocols, weak firewall configurations, and the absence of robust Data Loss Prevention (DLP) policies have led to unauthorized access incidents.

3.2 Change Management Gaps

- **Lack of Structured Security Enhancements:** Change management processes do not require systematic follow-ups on security training effectiveness or enforce corrective measures for identified vulnerabilities.
- **Absence of Continuous Security Monitoring:** There is no proactive evaluation of security measures to detect and adapt to emerging threats in real time.
- **Insufficient Employee Accountability:** Employees who repeatedly fail security tests are not required to undergo additional training, monitoring, or corrective action.
- **Weak Enforcement of Policy Updates:** Security policies are revised periodically but are not consistently enforced, monitored, or effectively communicated to employees.

Recommendations

4.1 Strengthening Incident Response

- **Automate Threat Detection & Email Security**
  Implement AI-based threat detection with SPF, DKIM, and DMARC email authentication to block phishing and BEC attempts. Solutions like Iron scales can provide phishing simulations and training to reinforce awareness.
- **Enforce Multi-Factor Authentication (MFA)**
  Require MFA for all sensitive systems (email, cloud storage, internal apps) to enhance access security and reduce the risk of unauthorized logins.
- **Clear Incident Reporting & Real-Time Response**
  Establish a one-click email reporting button for phishing attempts and a dedicated vishing hotline. Implement real-time alerts and automatically isolate compromised accounts to minimize exposure.
- **Enhance Network Security with Fortinet Firewall**
  Purchase and deploy a **Fortinet firewall ($100 per user per month)** to improve perimeter security, enforce web filtering, and protect against advanced threats.

4.2 Improving Change Management

- **Integrate Security Changes into Change Management:** Ensure all security-related changes are documented, tested, and enforced as part of the formal change management process to maintain consistency and security.

- **Conduct Regular Security Audits:** Perform regular audits to assess the effectiveness of implemented security changes and ensure they are functioning as intended.
- **Mandatory Response Plans for Employees:** Implement a mandatory Standard Operating Procedure (SOP) for employees, especially those who fail security tests, including additional training and monitoring to improve compliance.
- **Enforce Strict Access Control Reviews:** Include routine access control reviews as part of security policy updates to prevent unauthorized access.
- **Implement Least Privilege Access Model:** Apply the least privilege model to restrict access, ensuring employees have the minimum necessary access to resources.

4.3 Policy and Compliance Enhancements

- **Recurring Security Awareness Training:** Establish mandatory recurring training with performance tracking to ensure retention and build a stronger security culture.
- **Zero-Tolerance for Policy Non-Compliance:** Implement a zero-tolerance policy for employees who fail to follow security protocols.
- **Data Encryption Policies:** Enforce strict data encryption for all sensitive financial and customer records to ensure data integrity.
- **Cloud Security Configuration Enhancements:** Strengthen cloud security by improving access controls and adding anomaly detection capabilities.

Change Management Action Plan

Phase	Action	Timeline	Responsible Party
Immediate	Update incident reporting procedures and require prompt reporting of threats.	1 Month	IT Security Team
Short-Term	Implement phishing and vishing simulations and track employee responses.	3 Months	IT & HR
Medium-Term	Strengthen cloud security configurations and restrict access controls.	6 Months	IT Security Team
Long-Term	Automate incident response and integrate AI-driven threat detection tools.	12 Months	IT & Management

Ongoing	Conduct continuous security audits and policy enforcement reviews.	Continuous	IT & Compliance

Phishing & Vishing Incident Response Workflow

Current Process Issues:

- Employees receive a phishing email or vishing call but may not report it.
- Incidents are only investigated if manually reported.
- No proactive threat isolation or prevention mechanisms in place.

Proposed Enhanced Process:

- Email and phone monitoring tools to detect potential phishing and vishing attempts.
- Employees report threats using an easy-to-use reporting tool.
- Automated security tools isolate potential compromised accounts immediately.
- Incident response team investigates and mitigates threats.
- Findings are documented, and security policies are updated accordingly.

Chart summary audit finding and Recommendation with tools list :

Audit Finding	Recommendation	Tools & Price (Small Business, 10 Employees)
Absence of Automated Security Controls	Implement Real-Time Alerts & Automated Threat Isolation	- **Fortinet Firewall** - Approx. $100 per user/month (for small businesses, consider alternatives)
		- **Microsoft Defender for Endpoint** - Starts at $5 per user/month
		- **CrowdStrike Falcon** - Approx. $8-$12 per user/month
		- **Webroot DNS Protection** - Approx. $4 per user/month
		- **Darktrace** - Custom pricing, typically starts at $100 per user/month
Lack of Structured Security Enhancements	Integrate Security into Change Management	- **Microsoft Teams** - Free or $5-$12/user/month depending on features
		- **Microsoft Planner** - Free with Microsoft 365, or $5/user/month for advanced features

		- **Trello** - Free, or $12.50/user/month for business plans
		- **Jira Software** - Approx. $7 per user/month
Absence of Continuous Security Monitoring	Conduct Regular Security Audits & Continuous Monitoring	- **Microsoft Sentinel** - Starts at $2.94 per GB of data ingested/month
		- **Splunk** - Starts at $150 per month (for basic plans)
		- **SolarWinds Security Event Manager** - Starts at $2,800/year for 10 users
		- **LogRhythm** - Custom pricing, usually around $100 per user/month for small businesses
Weak Enforcement of Policy Updates	Enforce Policy & Access Control Reviews	- **Microsoft Intune** - Approx. $6 per user/month
Insufficient Employee Accountability	Mandatory Response Plans for Employees	- **Microsoft Viva Learning** - Part of Microsoft 365 subscription (depends on the plan)
		- **KnowBe4 Security Awareness Training** - Starts at $24 per user/year
		- **Cofense Phishing Simulation** - Approx. $2,000/year for up to 25 employees
		-**Cybersocialdefend Security Awareness Training** -Starts at $14.99 per user/year for Security Awareness - Starts at $799/year for up to 30 employees for phishing simulation
Weak Data Protection Measures	Improve Data Encryption & Access Controls	- **Vormetric Data Security Platform** - Custom pricing, typically around $2,500/year for small business setups
		- **Symantec Data Loss Prevention (DLP)** - Approx. $30 per user/month
		- **Digital Guardian** - Custom pricing, generally starts around $40 per user/month

Cost Summary (for 10 Employees):

- **Fortinet Firewall**: Approx. $100/month (or one-time depending on purchase model)

- **Microsoft Defender for Endpoint**: Approx. $50/month (for 10 users at $5/user)
- **CrowdStrike Falcon**: Approx. $80/month (for 10 users at $8/user)
- **Microsoft Teams**: and **Microsoft Planner**: Free (with Microsoft 365 subscription) or $50/month for full Microsoft 365 Premium plan)
- **Microsoft Sentinel**: Approx. $2.94/GB/month (depending on volume of data ingested)
- **Microsoft Intune**: Approx. $60/month (for 10 users at $6/user)
- **Cybersoscial Security Awareness Training**: Approx. $149.99/year (for 10 users at $14.99/user/year)
- **Vormetric Data Security Platform**: Approx. $2500/year (for basic setup)
- **Huntress US$ 10 per user, per month**
- **Iron scales US$ 10 per user, per month**

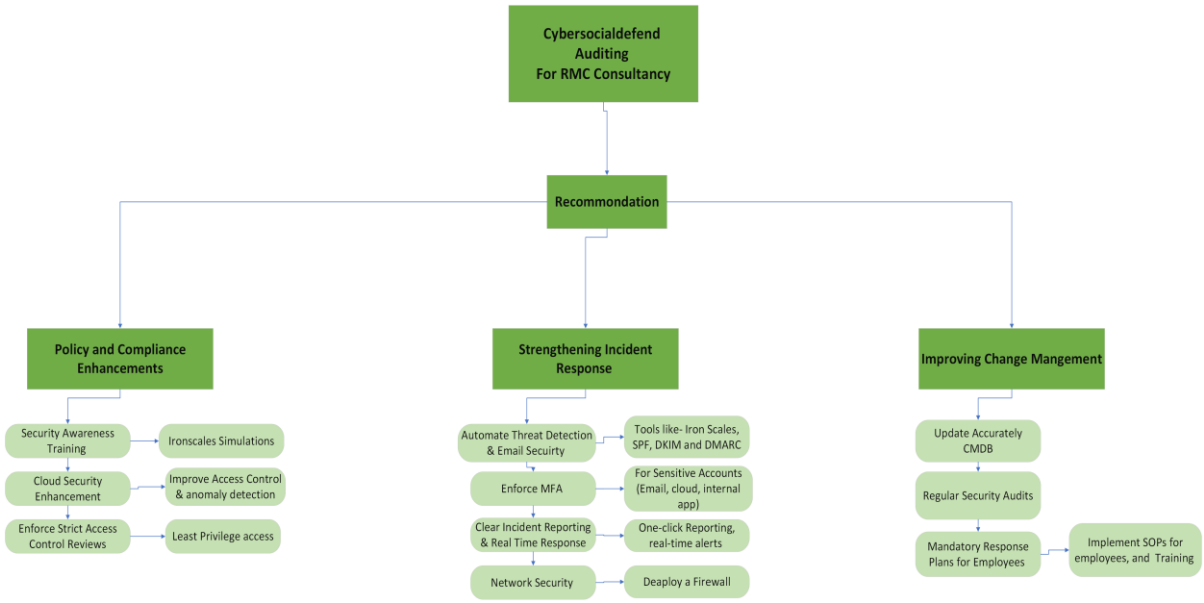
- **Implement Iso 27001 for Security and Risk Management**
- **Implement Iso 27002 for Change Management**
- **Implement Iso 27035 for Incident Management**

Total Approximate Monthly Cost for 10 Employees:

Basic setup with essential tools (Fortinet Firewall, Microsoft Defender, Teams, Planner, Intune): Approx. **$300 - $520/month** depending on your Microsoft plan choices. For ISO implementations, we provide documentation, best practices and recommendations from these frameworks, along with one year of follow-up. The service includes 4 hours per month at a rate of US$100 per hour, with a minimum of 2 hours per month.

Conclusion

RMC Consultancy needs to enhance its cybersecurity posture by addressing key gaps in incident handling, employee training, and change management processes. The audit revealed weaknesses in threat detection, incident response, and policy enforcement, which have contributed to repeated security breaches. By implementing automated threat detection systems, enforcing stronger accountability, and integrating security improvements into the formal change management process, RMC Consultancy can significantly reduce its exposure to threats. These improvements will not only mitigate risks but also bolster the company's overall resilience against future cybersecurity incidents.



Prepared by: Cybersocialdefend
Date: March 4, 2025