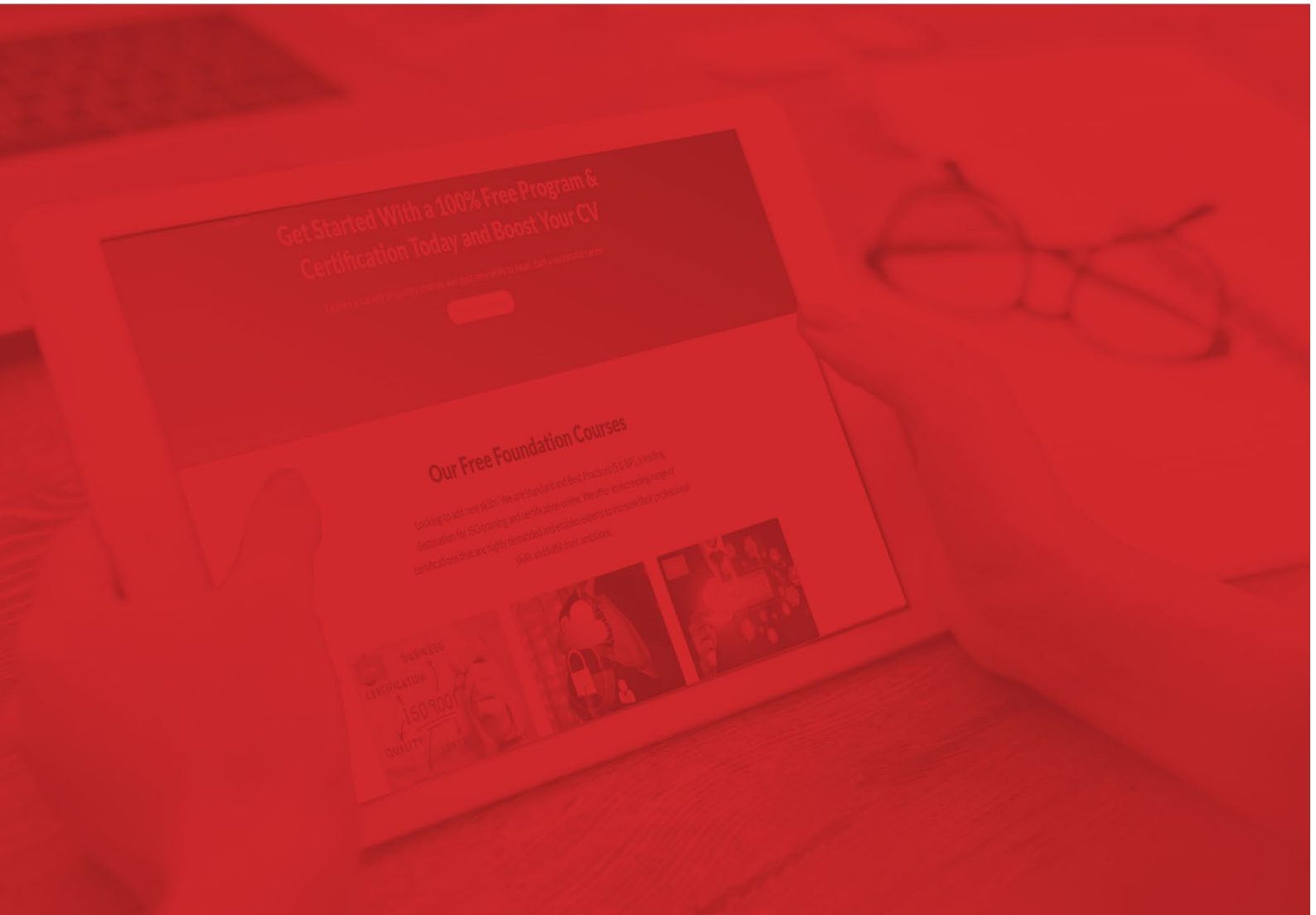
...global validation

SBP ISO 27035:2023 (ISIM) MANAGER COURSE- CASE STUDIES



CASE STUDY #1

Case Study: Cyber Attack on TechCorp Inc.

Background:

TechCorp Inc. is a multinational technology company specializing in cloud computing and cybersecurity solutions. With thousands of customers relying on their services, any disruption could have severe consequences. The company operates a 24/7 Security Operations Center (SOC) to monitor and respond to potential security incidents.

Incident Description: On a Monday morning, TechCorp's SOC detected unusual network traffic on one of their main servers. The anomaly was flagged by their intrusion detection system (IDS) at 03:00 AM. Initial analysis suggested a potential data breach involving unauthorized access to customer data. The SOC team immediately escalated the incident to the Information Security Incident Response Team (IRT).

Scenario Details:

Phase 1: Plan and Prepare

TechCorp Inc. has an established Information Security Incident Management Policy that outlines the roles, responsibilities, and procedures for incident response. The policy is aligned with ISO/IEC 27035:2023 and integrates the company's Recovery Time Objective (RTO) into the incident management framework.

As part of their preparation:

- TechCorp regularly conducts incident response drills.
- The company maintains an updated list of internal and external contact points, including legal advisors, law enforcement, and cybersecurity consultants.
- An Incident Register is in place, where all incidents are documented with details like severity, affected assets, and response actions.

Phase 2: Detect and Report

Detection: At 03:00 AM, the SOC identified the abnormal traffic, triggered by the IDS. The traffic was traced to an external IP address known to be associated with malicious activities. The IDS flagged this as a potential data exfiltration attempt.

Reporting: The SOC immediately logged the event and notified the Information Security Incident Coordinator via the automated alert system. An initial incident report was generated, detailing the time of detection, affected systems, and the nature of the anomaly.

Phase 3: Assess and Decide

Assessment: By 03:30 AM, the IRT convened to assess the situation. The team analyzed the event data, cross-referencing it with threat intelligence feeds. It was determined that the event met the criteria for a high-severity information security incident due to the potential exposure of customer data.

Decision: The incident was officially classified as a critical security incident. The IRT activated the response plan and initiated the response timer, keeping in mind the RTO. Key stakeholders, including the executive management and the legal department, were informed.

Phase 4: Respond

Immediate Actions: The IRT took several actions:

- The affected server was isolated from the network to prevent further data loss.
- Forensic analysis began immediately to determine the scope of the breach.
- The legal team was consulted to understand the potential impact of the breach and to prepare for any regulatory notifications.
- A communication plan was developed to inform customers and the media, if necessary.

Ongoing Response: As the investigation unfolded, it became clear that the attackers had exploited a zero-day vulnerability in TechCorp's software. The IRT coordinated

with the development team to patch the vulnerability and prevent further exploitation.

The incident was escalated to law enforcement, and evidence was preserved for potential legal action against the perpetrators.

Phase 5: Lessons Learned and Follow-Up

Post-Incident Review: After the incident was resolved, a comprehensive review was conducted. The incident register was updated with all actions taken, and a report was prepared for the management, detailing the root cause, the response timeline, and the lessons learned.

Improvements:

- The incident revealed a gap in the company's IDS rules, which was addressed by updating the system to detect similar threats more effectively.
- A new training program was developed to enhance the IRT's ability to respond to zero-day attacks.
- TechCorp also decided to invest in advanced threat detection technologies to improve their incident detection capabilities.

CASE STUDY #2

Case Study: Incident Management at TechSolutions Ltd.

Background

TechSolutions Ltd. is a global technology company providing innovative software solutions to clients across various industries. With offices in multiple countries and a large, distributed workforce, the company handles vast amounts of sensitive data, including personal identifiable information (PII), intellectual property, and client information. TechSolutions Ltd. has a well-established Information Security Management System (ISMS) and is ISO/IEC 27001:2022 certified.

Incident Overview

On a Monday morning, an employee in the Research and Development (R&D) department noticed suspicious activity on their workstation. Files were being accessed and modified without the employee's knowledge. Concerned, the employee immediately reported the activity to the company's Information Security Incident Response Team (ISIRT) via the established reporting mechanism.
The ISIRT, which had been trained and prepared according to the company's Information Security Incident Management Policy, quickly sprang into action. They followed the high-level incident management process flow outlined in the policy: detection and reporting, assessment and decision, response, and lessons learned.

Incident Response

1. **Detection and Initial Assessment:** The ISIRT began by verifying the legitimacy of the reported incident. They conducted a preliminary assessment of the affected systems, identifying the scope of the incident, the type of data involved, and the potential impact on the organization. It was discovered that a sophisticated malware had infiltrated the system, potentially compromising sensitive R&D data, including unreleased software code and client project details.

2. **Containment and Eradication:** Recognizing the severity of the incident, the ISIRT decided to contain the threat immediately. They isolated the affected systems from the network to prevent further spread of the malware. In collaboration with the IT department, the ISIRT initiated a thorough scan of the network to identify any other compromised systems. The team worked closely with external cybersecurity experts to eradicate the malware and secure the network.

3. **Communication and Reporting:** Throughout the incident, the ISIRT maintained clear communication channels with all relevant stakeholders, including top management, the legal department, and the public relations team. The ISIRT also communicated with external partners, including law enforcement and

cybersecurity authorities, as required by the company's legal and regulatory compliance requirements.
An internal communication was sent to all employees, reminding them of the importance of following the information security policies and procedures. Additionally, clients whose data might have been affected were notified in compliance with legal obligations, and the public relations team prepared a statement to manage the company's reputation.

4. **Post-Incident Activities:** After the incident was resolved, the ISIRT conducted a post-incident review. They analyzed how the incident occurred, the effectiveness of the response, and identified areas for improvement. The ISIRT documented all findings and updated the incident management policy to reflect lessons learned from the incident.
   As part of the continuous improvement process, the company initiated additional training and awareness programs to reinforce the importance of information security across all departments. They also reviewed and updated their information security incident management policy to ensure it remained aligned with the latest threats and organizational changes.

Outcome

The swift and effective response by the ISIRT minimized the damage caused by the malware, prevented the loss of critical data, and maintained the trust of TechSolutions Ltd.'s clients. The company's adherence to its Information Security Incident Management Policy, supported by a well-coordinated response and robust communication, ensured that the incident was managed efficiently and professionally.
TechSolutions Ltd. continues to enhance its information security practices, recognizing that a proactive and comprehensive approach to incident management is essential for safeguarding its assets and reputation in an increasingly complex cybersecurity landscape.

CASE STUDY #3

Scenario: Cybersecurity Incident in a Financial Services Organization

Background

Global Financial Corp (GFC) is a multinational financial services organization with operations spanning across various continents. The company handles a vast amount of sensitive customer data, including financial transactions, personal identification information, and confidential business agreements. Due to the critical nature of its services and the regulatory environment it operates in, GFC has implemented a robust Information Security Management System (ISMS) based on ISO/IEC 27035-2:2023 to manage and respond to information security incidents.

Incident Overview

On a typical Monday morning, the IT department of GFC noticed unusual network traffic originating from the internal network. The anomaly was detected by the intrusion detection system (IDS), which flagged it as a potential security threat. The incident involved a significant amount of data being transferred to an unknown external IP address.

Initial Response

The anomaly triggered an automatic alert to the Incident Management Team (IMT) within GFC. The IMT, led by the Incident Manager who reports directly to the Chief Information Security Officer (CISO), immediately initiated the Incident Response Plan. The Incident Manager promptly established an Incident Response Team (IRT) to investigate the anomaly. The IRT was composed of members from the IT department, cybersecurity experts, and legal advisors.

The IRT was tasked with the following:

- **Assessment of the Incident**: The IRT began by analyzing the logs generated by the IDS and other monitoring tools to determine the nature and scope of the incident. They discovered that the data being transferred included encrypted files containing sensitive customer information.

- **Containment**: The IRT immediately took steps to contain the incident by isolating the affected systems from the network to prevent further data exfiltration.
- **Communication**: The Incident Coordinator regularly updated the Incident Manager and other senior executives on the progress of the investigation. They also prepared initial communication drafts to inform external stakeholders, including regulatory bodies, about the potential breach.

Deep Investigation

As the investigation continued, the IRT identified that the data exfiltration was the result of a sophisticated phishing attack that compromised the credentials of a high-level employee. The attacker had gained access to the internal network and used legitimate credentials to bypass several security controls.

- **Forensic Analysis**: The IRT conducted a thorough forensic analysis of the compromised systems. This included analyzing logs, tracing the attacker's steps, and gathering digital evidence. The forensic team also worked on decrypting the exfiltrated files to assess the extent of the data breach.
- **Vulnerability Management**: The IRT identified a lack of multi-factor authentication (MFA) as a significant vulnerability that allowed the attacker to gain access using compromised credentials. They also discovered that certain security patches had not been applied, which contributed to the attack's success.

Recovery and Post-Incident Actions

- **Restoration**: The IRT worked closely with the IT department to restore the affected systems from clean backups. They also ensured that all compromised accounts were secured, and the necessary patches were applied across the network.
- **Communication with Stakeholders**: GFC issued a formal communication to its customers, informing them of the breach and the steps taken to mitigate its impact. The company also worked closely with legal advisors to ensure compliance with data protection regulations.

- **Lessons Learned**: After the incident was resolved, the Incident Manager led a post-incident review session with the IMT and IRT to identify lessons learned. They concluded that the implementation of MFA and regular security awareness training for employees were critical areas for improvement. The review also emphasized the need for regular updates to the incident response plan.

Conclusion

The incident at Global Financial Corp underscores the importance of having a well-structured incident management capability. The proactive measures taken by the IMT and IRT minimized the potential damage, safeguarded customer data, and preserved the organization's reputation. The case highlights the critical role of incident management in ensuring that organizations can effectively respond to and recover from security incidents while continuously improving their security posture.