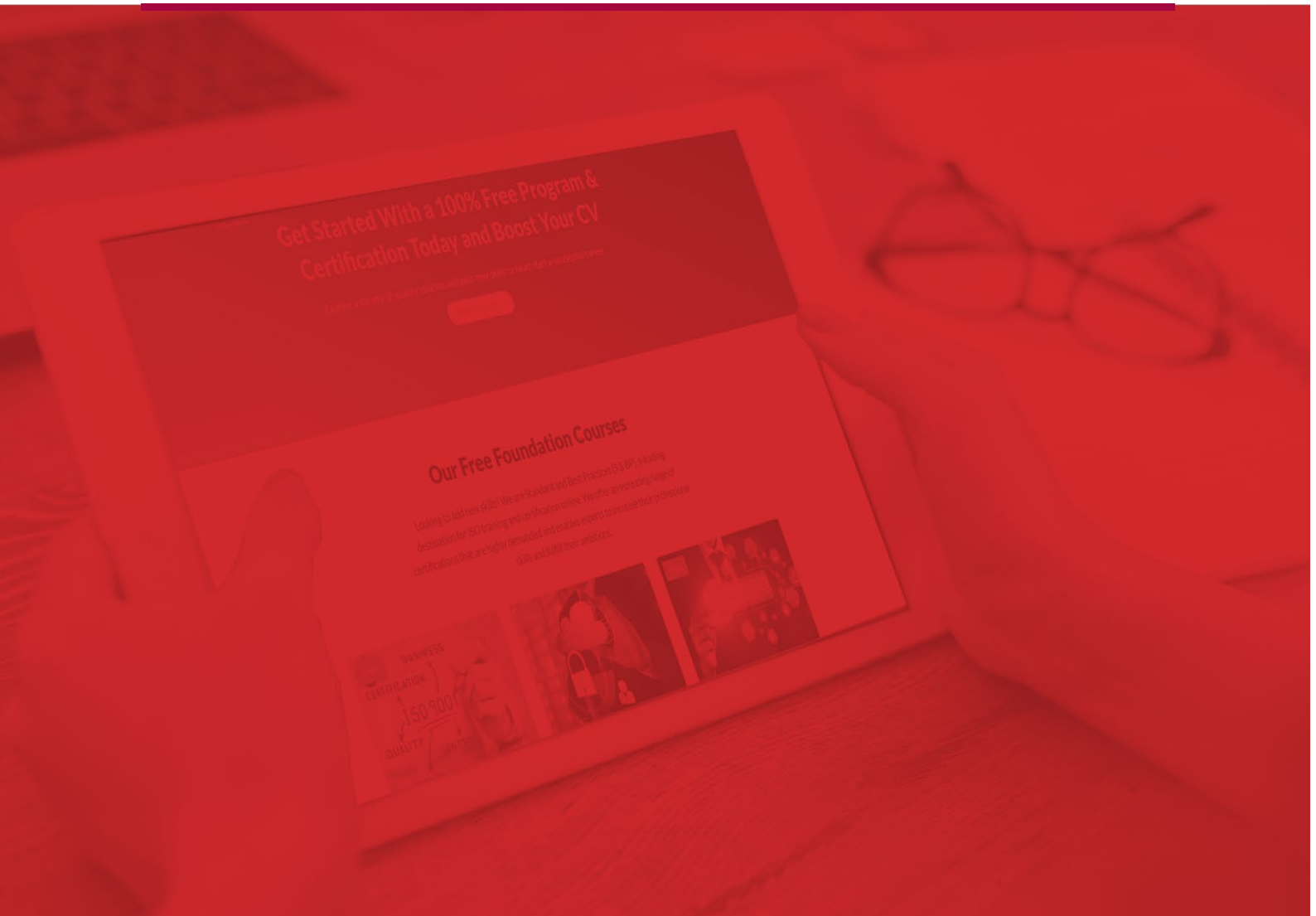
...global validation

SBP ISO 27032:2023 (CYBERSECURITY) MANAGER COURSE- CASE STUDIES



CASE STUDY #1

Credit Information Theft for Online Identity Theft

Background:

ABC Finance, a leading financial institution, faces a significant threat to its clients' credit information being sold on the black market or darknet. The compromise of credit information not only poses financial risks but also facilitates online identity theft.

ISO 27032 Clause Tie-in:

- Clause 8.2 Threats
- Clause 8.3 Vulnerabilities

Scenario:

Malicious actors exploit vulnerabilities in ABC Finance's online systems, leading to the unauthorized access and sale of credit information on illicit platforms. This case study explores the consequences of such threats, emphasizing the importance of addressing vulnerabilities in financial systems to safeguard personally identifiable information (PII).

Learning Objectives:

- Recognize the potential impact of credit information theft on individuals and organizations.
- Implement controls and countermeasures to mitigate vulnerabilities and prevent unauthorized access to sensitive financial data.
- Understand the relevance of ISO 27032 in addressing threats and vulnerabilities associated with online identity theft.

CASE STUDY #2

Cyber Bullying and Exploitation Crimes

Background:

XYZ Social Network, a popular online platform, encounters a growing threat related to cyberbullying, online stalking, and exploitation crimes, including child exploitation and human trafficking.

ISO 27032 Clause Tie-in:

- Clause 8.2 Threats

Scenario:

XYZ Social Network becomes a breeding ground for criminal activities, impacting the safety and well- being of users. This case study explores the diverse threats arising from social networking platforms and emphasizes the need for robust cybersecurity measures to counteract exploitation crimes.

Learning Objectives:

- Understand the various forms of online threats and their potential real-life consequences.
- Implement preventive measures and controls to address cyberbullying and exploitation crimes on social media platforms.
- Relate the case study to ISO 27032's focus on managing internet security risks and protecting users from harm.

CASE STUDY #3

Infrastructure Targeting and National-Level Implications

Background:

LMN Network Solutions, a critical infrastructure provider, faces targeted attacks on its internet-facing systems, affecting the reliability and availability of its services.

ISO 27032 Clause Tie-in:

- Clause 8.2 Threats
- Clause 8.4 Attack vectors

Scenario:

LMN Network Solutions experiences sophisticated attacks aimed at compromising the infrastructure supporting the internet. This case study explores the potential impact on national security and emphasizes the challenges in regulating and controlling illicit activities on the Internet.

Learning Objectives:

- Analyze the repercussions of attacks on internet infrastructure at a national or international level. Implement defence mechanisms against diverse attack vectors targeting critical infrastructure.
- Relate the case study to ISO 27032's guidance on managing risks associated with the internet and defending against advanced persistent threats (APTs).

CASE STUDY #4

Internet Usage Policies Implementation

Background:

XYZ Corporation, a global organization, relies heavily on the Internet for various operations, including web surfing, accessing public cloud services, and conducting e-commerce. Recognizing the unique threats associated with the public network, XYZ Corporation decided to implement comprehensive controls following ISO 27032:2023 standards.

ISO 27032 Controls Tied-In:

- 9.2.2 Policies for Internet security

Scenario:

XYZ Corporation identifies the need to develop and enforce internet usage policies to manage the risks associated with online activities. The policies aim to define acceptable use, determine authorized personnel, and outline security objectives.

Learning Objectives:

- Draft and implement internet security policies in alignment with ISO 27032 standards.
- Ensure policies are approved by management, communicated to relevant personnel, and consistently enforced.
- Define roles and responsibilities regarding internet usage within the organization.

CASE STUDY #5

Strengthening Access Controls for Internet Security

Background:

LMN Technologies, a technology firm, faces challenges related to access controls for their internet- facing systems. Concerns arise about the authentication and authorization processes in place, posing potential security risks.

ISO 27032 Controls Tied-In:

- 9.2.3 Access control

Scenario:

LMN Technologies aims to enhance access controls for users, devices, and applications accessing the internet. The focus is on implementing strict authentication measures, role-based permissions, and regular review of access rights.

Learning Objectives:

- Establish robust access controls for information and assets associated with the internet. Implement secure authentication technologies to mitigate unauthorized access.
- Develop and adhere to policies for reviewing and managing access rights.

CASE STUDY #6

Incident Response in Internet Security

Background:

ABC Cyber Solutions, a cybersecurity firm, encounters an increasing number of security incidents originating from the internet. They realize the importance of having a well-prepared incident response mechanism to address these incidents promptly.

ISO 27032 Controls Tied-In:

- 9.2.5 Security Incident Management

Scenario:

ABC Cyber Solutions establishes an Incident Management Team (IMT) and Incident Response Team (IRT) to assess, respond to, and learn from security incidents originating from the internet. The goal is to detect, report, and manage incidents effectively.

Learning Objectives:

- Formulate an IMT and IRT for internet security incidents.
- Develop incident response procedures considering various cyber-attack scenarios.
- Implement technical solutions for secure information sharing and coordination during incidents.

These case studies provide practical applications of ISO 27032 controls, focusing on internet security policies, access controls, and incident response measures.