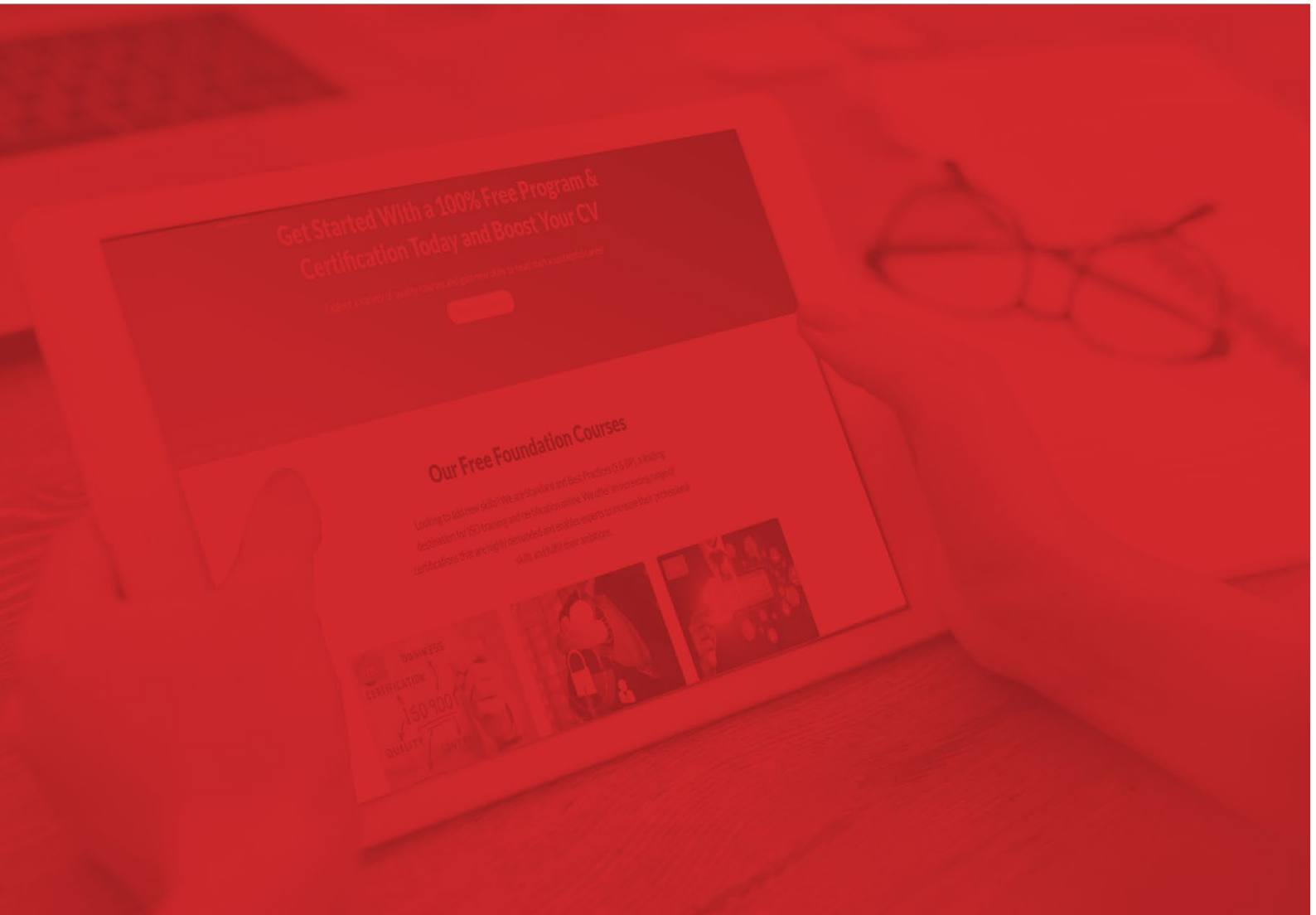
...global validation

SBP ISO 27001:2022 (ISMS) CHAMPION COURSE- CASE STUDIES



CASE STUDY #1

SECTION 5- INFORMATION SECURITY AND ITS SIGNIFICANCE

Case study: Equifax Data Breach (2017)

Background: In 2017, Equifax, one of the three major credit reporting agencies in the United States, experienced a significant data breach that had far-reaching consequences. This breach exposed sensitive personal and financial information of approximately 143 million Americans, making it one of the most substantial and widely publicized data breaches in recent history.

Vulnerabilities and Shortcomings:

1. **Patching Neglect:** One of the key vulnerabilities in this incident was the company's failure to apply a security patch promptly. The breach occurred through a known vulnerability in the Apache Struts web application framework. Equifax had been informed about the vulnerability by the US Department of Homeland Security months before the breach but failed to update the system, leaving it exposed to exploitation.
2. **Inadequate Response:** Equifax's response to the breach was widely criticized. The company took six weeks to publicly announce the incident, during which time the attackers had access to sensitive data. The slow response damaged the company's reputation and increased the risk to affected individuals.
3. **Lack of Encryption:** The breach involved the theft of names, Social Security numbers, birthdates, addresses, and in some cases, driver's license numbers. This data was not adequately encrypted, making it more accessible to the attackers.
4. **Access Control Issues:** There were indications that Equifax may not have had robust access control measures in place, allowing the attackers to navigate within their systems, access sensitive data, and remain undetected for an extended period.

Consequences:

1. **Financial Impact:** Equifax faced significant financial losses, including regulatory fines, legal settlements, and expenses related to incident response and recovery. Its stock price also plummeted, resulting in a substantial market capitalization loss.

2. **Reputational Impact:** The breach severely damaged Equifax's reputation, eroding trust among consumers who entrusted their personal data to the company. Public perception of Equifax suffered greatly.
3. **Operational Impact:** The breach disrupted Equifax's normal operations. It resulted in increased costs for security improvements, legal actions, and compliance measures.

Lessons Learnt:

The Equifax data breach serves as a stark reminder of the consequences of security vulnerabilities and shortcomings. It underscores the importance of information security principles, including confidentiality, integrity, and availability. The breach could have been prevented or mitigated with timely patching, encryption, access control, and a swift and transparent response. This example highlights the necessity of safeguarding sensitive information and the critical role that information security plays in protecting an organization's assets, reputation, and viability.