Information Security Risk Management Project

Part 1: Research Report

Introduction

Confidentiality, Integrity, and Availability, or the CIA trinity, have historically been at the centre of information security roles in enterprises. To secure sensitive data, businesses mostly relied on standard precautionary measures like firewalls, antivirus software, and password regulations. For example, banking firms have always used strong firewall defences to stop outsiders from accessing client data. But as the digital world has developed, these fundamental defences are no longer adequate to fend off more complex cyberattacks.

Conventional Information Security Methods

Antivirus software, firewalls, and intrusion detection systems (IDS) are the mainstays of conventional security procedures. Businesses frequently ignored the dynamic nature of threats in favour of concentrating exclusively on erecting a defensive perimeter around their data. One such instance is the 2013 Target data breach, which resulted in the exposure of millions of consumers' personal data. Target was susceptible even with standard defences like firewalls and antivirus software because of its reliance on antiquated technologies. The hack demonstrated the shortcomings of these protective measures and made it clear that businesses needed to reconsider their security plans considering contemporary dangers.

Changing Environment of Threats

Numerous new security dangers, such as ransomware, insider attacks, and advanced persistent threats (APTs), have been brought about by the digital transition. These difficulties are exemplified by significant events during the last five years. For example, the 2017 WannaCry ransomware assault used weaknesses in out-of-date software to infect over 200,000 systems worldwide. The incident made it clear how important it is to have reliable cybersecurity procedures and timely patch management. Organisations discovered that a heavy dependence on conventional defences was no longer practical after being taken off guard. Businesses need to modify their security strategy to effectively tackle the contemporary difficulties posed by the ever-changing threat landscape.

Defend to Enable" Theory

The idea of "Protect to Enable" signifies a change in the way businesses view information security. Companies today see security as an opportunity to foster innovation and commercial growth, rather than only as a protective measure. Microsoft, for instance, has incorporated security into its cloud services, resulting in increased customer trust and revenue development. With this strategy, businesses can innovate with confidence since they have strong security safeguards in place to safeguard client data. Businesses can foster an environment that fosters innovation and security by emphasising security as a business enabler.

Section 2: Risk Management for Security Risk Identification and Evaluation for Proposals

Attacks by Phishing: Phishing is still a serious issue for businesses of all sizes. Sensitive patient data was exposed because of an increase in phishing attacks targeting the healthcare industry in 2020 during the COVID-19 pandemic. Businesses must take strong precautions against phishing since it can result in loss of money and harm to their reputation.

Ransomware: Due to high-profile events like the Colonial Pipeline attack in 2021, which interrupted fuel supply along the U.S. East Coast, ransomware attacks have grown more common. Attacks of this nature have the potential to seriously impair operations and result in large financial losses, especially for businesses that rely largely on digital infrastructure.

Insider Threats: Organisations are at danger from insider threats, whether intentional or unintentional. For example, in 2021, a former employee of a financial services company disclosed confidential client information, which led to legal action and a decline in client confidence. Insider attacks can have a significant impact by compromising the integrity of important data and causing data breaches.

Strategy for Risk Mitigation

Organisations should put these methods into practice to address the risks identified:

Phishing Prevention: To help staff members spot phishing efforts, businesses should regularly train them in security awareness. For instance, Google has made two-factor authentication (2FA) a requirement for all workers, which has greatly decreased the number of illegal access attempts. Furthermore, phishing drills that are simulated can support instruction and get staff members ready for actual attacks.

Ransomware Defence: To effectively combat ransomware, organisations should implement a multi-layered strategy that includes advanced endpoint detection and response (EDR) tools, timely software patches, and routine data backups. Following a ransomware assault in 2018, the City of Atlanta made investments to strengthen its incident response protocols and backup procedures, thereby fortifying its defences against such attacks in the future.

Insider Threat Mitigation: Organisations can identify possible insider threats early by putting in place stringent access controls and keeping an eye on user behaviour. Additionally, businesses want to foster a culture of security that gives staff members the confidence to report questionable activity. For example, Capital One, a financial services company, strengthened its security posture by improving its monitoring capabilities, which effectively detected and reduced insider threats.

Alignment of Businesses

The suggested risk-reduction tactics support the company's overarching business goals by upholding operational effectiveness and fostering customer confidence. Organisations can foster a culture where security fosters rather than impedes growth by incorporating security measures into routine business operations. For instance, Amazon Web Services (AWS) has successfully struck a balance between innovation and strong security measures, enabling clients to grow and develop their businesses without worrying about data breaches. This strategic alignment highlights the fact that security is an essential enabler of corporate success as well as a cost centre.

**References**

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Bishop, M. (2021). Computer Security: Art and Science. Addison-Wesley.

McKinsey & Company. (2022). The Future of Cybersecurity: Protecting Business Value. McKinsey & Company.

National Institute of Standards and Technology. (2021). Framework for Improving Critical Infrastructure Cybersecurity.

Ponemon Institute. (2022). Cost of a Data Breach Report 2022. IBM Security.