Title page

IT security policy

Establishing an effective technology security policy framework is crucial for organizations. The fundamental purpose of an information technology system is to process the data. As every business includes some data processing, the IT security framework deals with critical information such as personally identifiable information. The IT frameworks face the risk of possible theft of its designs, test data, manufacturing and research support applications and its manufacturing capability by suspected foreign entities backing its research partners and civilian competitors (AlHogail & Mirza, 2014). This has encouraged the company to adopt an adequate security strategy that will allow companies to attain security control environment (Stoneburner, Goguen, & Feringa, 2002).

Security framework of NIST and ISO/IEC 27000

The primary process in risk management performed according to NIST and ISO/IEC 27000 framework is risk assessment providing information about the levels of risks involved in the information systems. It reveals the information about the potential threats and the nature that helps the organization to reduce the level of risks by adopting the required measures. This also provides information about the internal control systems and its efficacy. NIST (SP 800-53) identify threats as low-impact, high-impact and moderate-impact.

|  |  |  |
| --- | --- | --- |
| Inventory assets  | Potential impact | Mitigating risks  |
| 1. Hardware
 | High  | HSM codes/ cryptology |
| 1. Software
 | High  | Applications testing |
| 1. Cloud computing
 | Moderate  | cryptology/ HTTP |
| 1. Company’s data
 | Moderate  | HSM code |
| 1. Customer data
 | High  | digital wallet/ merchant software |

Solutions

Based on NIST (SP 800-53) and ISO/IEC 27000 it is critical to deal with important and confidential information so it will adopt certain security measures that are for minimizing the threats associated with the information systems. The activities involved in risk mitigation and integration process is explained below;

|  |  |  |
| --- | --- | --- |
| Phases  |  | Strategies  |
| Initiation  | Expressing requirements for IT system.Defining the purpose of system and documentation. | * Identification of risks.
* Developing and supporting systems.
* Meeting security requirements.
* Implementing the operational strategy.
 |
| Development/ acquisition | Effective designing of IT systems. Purchasing programs and constructing designs where needed. | * After identification, it provides security analysis.
* Developing appropriate architecture for IT systems.
* Meeting database storage requirements.
 |
| Implementation | The security features are configured, tested, enabled and verified. | * Effective assessment of risks.
* Supporting systems implementation and modelling operational environment.
* Critical decisions about systems operations.
 |
| Operation/ maintenance | Effective performance of system functions.Modification of system including hardware and software.Designing policies and recommendations for organizations. | * Periodic systems reauthorization used for risk management activities.
* Operational changes in IT systems when needed.
* Operational enhancement of production environment.
 |
| Disposal  | Disposal of effective information.Controlled use of hardware and software.Discarding confidential information when vulnerable.Scrutinizing hardware and software capabilities.  | * System components disposed or replaced ensuring proper disposal of hardware and software.
* Appropriate handling of residual data.
* Secure conduction of systems migration.
 |

Solutions for securing network administration

System characterization is the initial step for assessing the risks involved in organization systems operations. It determines the scope of threats and available resources and involves delineation of operational authorization. The operational environment is also analyzed in this stage. The system-related information involves the description of characteristics of hardware, software, system interfaces, data and information and using IT system including data criticality and systems information. The functions required for the IT system is also explained in this process and defining the system security architecture. The network diagram is also explained in this process and the technical controls include built-in and add on security products (Stoneburner, Goguen, & Feringa, 2002).

Another important information asset for any organization is cloud computing and NIST and ISO/IEC 27000 attempts to provide maximum security related to cloud computing to protect it from breaches and misuse. It provides increased transparency for assessing the quantity and prevents exposure of sensitive data. e-Security measures are provided by NIST to minimize the risks linked with cloud computing. It also includes effective cytological use for confirming authentication. This will minimize the risks associated with the loss and theft of data and the data remains in safe hands. It maintains compliance and privacy environment for organizations and involves security applications. The migration of sensitive data to clouds remains safe and inaccessible by unauthentic sources (Thales, 2016). The cloud computing security is linked to many organizational benefits as it allows migration of cloud customers to cloud services and enhances the security of cloud services that provide certain levels of assurance related to the security of an organization. Some of the effective applications used by ISO/IEC 27000 are SSL secure socket layer also used for data encryption and enhancing the level of security. SSL establishes a safe link between the main server and the interface thus minimizing the risks of unauthenticated access. HyperText Transfer Protocol HTTP is also used for establishing key encryption authentication and is used for supporting multiple security mechanisms (Thanles, 2016). Hardware is one of the important information assets for any organization and there is a need for minimizing the risks associated with hardware breaches. Security framework will safeguard the intellectual property of organizations and it provides various features for securing the company’s hardware. Cryptology is an advanced feature that protects the confidentiality of information specifically in hostile environments. It involves high levels of integrity and authenticity that can be accessed through electronic document and message. The cryptographic protection uses encryption for maximizing security that reflects the transparent deployment. Network connections are protected via Virtual Private Networks (VPNs) capable of accessing remote locations also. Data- crypto is the backbone of the hardware systems that maximize the level of protection and allowing access only after authentication.

 References

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *IEEE*.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* National Institution of Standards and Technology.

Thales. (2016). *Controlling Fraud and Protecting Intellectual Property: Today's Challenge*. Retrieved 2016 йил 02-october from https://www.thales-esecurity.com/solutions/by-business-issue/controlling-fraud-and-protecting-intellectual-property

Thanles. (2016). *Cloud Computing Security*. Retrieved 2016 йил 02-october from https://www.thales-esecurity.com/solutions/by-business-issue/cloud-computing-security