Developing the Corporate Strategy for Information Security

[Name of the Student:]

[Name of the Institution:]

Developing the Corporate Strategy for Information Security

## Specific Functions of the CISO

 The Chief Information Security Officer (CISO) is a senior executive in a company who is responsible for protecting the systems, assets, and communications of a company from potential and existing threats. These threats can be external as well as internal. The CISO develops and implements programs for information security and evaluates their performance after installation. The CISO has a competent team of professionals who depict various skills needed to complete the project and run it successfully. This information security program is implemented across the organization, and no information can go outside or come inside without being screened through the system.

The CISO works as with the top management of the company to determine the risk factors associated with the system (Hooper & McKissack, 2016). The main function performed will be to assess the acceptable level of risk for the information security system of the organization. The policies for the company's information security will be established consequently. This function will be performed at the start of building a security system.

The CISO will be controlling the security operations in his/her supervision. Any threats liable to harm the company in any sense (information breach, assets exploitation, etc.) will be noticed by the CISO’s team immediately. Any attempts of theft or accounts hacking would become highlighted in the information security system, and the necessary action will be taken in response. Possible threats will be simulated and developed to allow the employees to understand and beware of the real threats. Certain scans, tests, and security assessments will be performed periodically to maintain security. This function will be performed before, during, or after a threat to the security system is noticed.

The CISO is responsible for empowering the information security system in a way that ensures full compliance with the national cyber laws. This is a great responsibility, as complying with the country's law related to cybersecurity is a critical issue, and if not met with successfully can cause serious issues for the company. The compliance activities are mainly performed at the startup of an enterprise. However, with time, there arises the need of formulating strategies and modifying running programs according to the regulatory instructions.

## Competencies of the CISO

Among the key competencies of a CISO is to manage the data security of the company. The CISO will develop security programs to ensure data security such that all possible threats are known to the IT professionals beforehand. The CISO will take necessary measures to protect the digital privacy of the company. He/she has to ensure the security of data from any unauthorized access.

The CISO is responsible for incident management in the company. Any incidents that have occurred in the company related to the data theft or misuse will be tackled to prevent future occurrences. The threatening incidents will be identified, analyzed and rectified to make the security system more capable.

The CISO must demonstrate competency in risk strategic management. The security operations are designed and developed according to the strategic planning accomplished by the higher management of the company. The CISO must be capable of working with the top management in a way that their collective efforts result in comprehensive and effective strategies to provide a useful security framework.

## Functions of a CIO

The Chief Information Officer (CIO) is a senior executive who is responsible to manage various functions related to the IT needs at an executive level in a company. The CIO generally oversees the IT needs of the company, partly involving in the IT operations of the company.

Among the various functions performed by a CIO is to manage data security in alliance with other executive managers. Data security is a big issue and very critical as well. The CIO will recognize the principle vulnerabilities to a security system. Further, the CIO will conduct periodic employees’ training programs related to the issue. These programs will create awareness among the employees about the potential threats to security. The CIO will indulge in attaining the information related to data security and disseminate it across the different levels of employees’ hierarchy according to their needs.

The CIO will involve in risk management along with the senior executives. The CIO will place the competent professionals for work at risk management. Providing them with adequate resources and necessary authorities to complete their tasks will fulfill their job requirements. The CIO will engage in creating the risk assessment criteria and development of relative strategies (Haffke, Kalgovas, & Benlian, 2016).

Further, the CIO will engage in strategic management at the senior-most level in the company. People at the workplace will be made aware of the strategic context of the organization to better cope with the data risk issues. The CIO will be involved in planning out security, audit, and compliance for the company. He or she has to understand the business requirements and develop strategies aligning with them.

## Security Assurances achieved by the CIO

The security assurances can be classified by considering different factors in information security management. Two important security assurance issues are authenticity and confidentiality. The CIO is responsible to achieve these security assurances. The CIO will make sure that whether the information is received or sent by the actual user. It means that the information system will be capable of ascertaining if the information generator or receiver is the same individual or entity as it has introduced itself. The CIO will develop training programs to make employees aware of this issue. Another security assurance achieved by the CIO is confidentiality. This implies information security to make sure that the right person has access to certain information. This also implies that no other irrelevant persons or entities can access a particular piece of information. To establish confidentiality, the CIO will develop programs for monitoring issues related to confidentiality in information systems. Techniques used in assuring confidentiality would be encryption, and different types of data management during acquisition, utilization, and saving.

## Ways to certify Security Functions & Data Assets

The CIO will use certain methods, technologies, and processes to certify the security functions and data assets of the organization daily. He or she will make use of the necessary software and programs to protect confidential information. The new hires will be screened for security purposes. The authentication procedures have to be deployed to avoid any data thefts. The network of computers in the organization needs to be established using LAN wherein enclaves are segregated by firewalls. The CIO will assign responsibilities to the related staff for ensuring the security of the systems. Every department's information will be under scrutiny of the information security team. The systems will be designed safely to automatically detect possible threats. The employees should be trained for preventing data risks and secure information processing. Scanners should be run and background checks made to ensure safety. A virus scanner and software update are recommended to make potential attacks ineffective. The sensitive data of the company should be protected with special care and must be saved in the owned systems only.

## Role of Digital Forensics in Information Security

Digital forensics refers to the examination of digital devices so that the information can be extracted from them for investigation purposes. The recovered information can have clues to certain specific or sensitive information that can be used as evidence. This field of forensic science has its applications in the digital- or cyber-crimes investigation where useful evidence can be generated by identifying data breaches that involve corporate data thefts. Digital forensics processes can be categorized in four steps. To collect digital forensic data, all related equipment and devices will be seized, and sent for investigation. The seized data will be examined and analyzed to assess the necessary information. Digital forensics also involves obtaining the evidence related to the events or history, such as recovering the deleted browsing data and emails to find out possible suspects involved in the crime.

## Operational Duties of Digital Forensic Personnel

Digital forensics personnel are involved in collecting, analyzing, and reporting information from the digital devices to find evidence of certain digital crime. They recover information from computers, mobiles, servers, etc. depending upon the sensitivity of the issue. They recover data like confidential documents, situational photos, or emails to find the relevant clues (Frecks, Curry, Lynn, & Bland, 2015). They search through the Internet browsing histories, word-processing documents, photos, and other files. They use certain sets of developed, technical skills that help them identify the points of data breach, and retrieve relevant hidden information.

## Technical Resources available to Digital Forensics Professionals

There are various technical resources available to digital forensic professionals at their disposal. Software tools such as Encase, COP, X-ways, Linux DD, etc. that will help them collecting, indexing, and executing a detailed analysis of the digital data. Encase is a software that is used for various purposes including forensics, cybersecurity, etc. Another popular tool is digital detective that is used to develop advanced forensic analysis software. They can use packet analyzers or sniffer tools to analyze network traffic.

Works Cited

Frecks, A. P., Curry, A. W., Lynn, D. G., & Bland, C. J. (2015). *Systems and methods for digital forensic triage*. Google Patents.

Haffke, I., Kalgovas, B. J., & Benlian, A. (2016). *The Role of the CIO and the CDO in an Organization’s Digital Transformation*.

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585–591.