# Enterprise Risk Management: The Role of Leadership

## Executive Summary

Every business is based on trust. Trust is only attained when the participants in a particular transaction feel safe and secure. In the current IT industry, the security of business data and applications acts as the enabler of successful attainment of the set out business goals. One of the main characteristics of technology is constant advancement (Stallings & Brown, 2015). At the same time, hackers and other unauthorized users are constantly devising sophisticated mechanisms or techniques of breaking into computer networks. Because of hacking, different companies have lost finances, business secrets and other crucial information. Hence, IT Security is a major concern for most companies all around the globe (Moeller, 2011). In essence, enterprise risks especially in the IT industry are continuously on the rise. This paper therefore lays major focus on the role of a company leadership in enterprise risk management via an account of Techline Incorporation.

## Introduction

In the current constantly advancing technological world, enterprise risk management has become a subject of great concern. The evolution of technology has been playing a very crucial role in enhancing day-to-day business operations. That is, it acts as the basis for promoting the competitive edge of companies (Moeller, 2011). However, at the same time, hackers and other unauthorized users are constantly devising sophisticated tools for break into information systems and computer networks. Some of the tools include Trojan horses, viruses, worms and Denial of Service attacks. As a result, IT managers, Chief Executive Officers, Business Enterprise Managers, Software Engineers and other stakeholders in the business world are fighting tooth and nail to ascertain that they apply the best approaches in managing risks within their enterprises (Chapman, 2013). As technology advances, the numbers of threats to business operations are also increasing in number and sophistication. This necessitates business leaders to consider coming up with a well-orchestrated mechanisms for the management of enterprise risks. Business leaders’ are the role models and pioneers in implementing the best practices within a business.

At Techline Incorporation, the main business goal is to ensure efficient delivery of business integration solutions for companies. The key operations in the company entail provision of innovative solutions on crucial business areas such as information assurance, cyber security, help desk services, IT and Healthcare knowledge management and Insider Threat analysis. Effective delivery of the above business requirements depends hugely on ascertaining that the organization is well equipped in terms of implementation of up to date information security platforms (Moeller, 2011). Essentially, in order to achieve this objective, especially in the current speedy advancing IT driven business world, staying in touch with relevant technological advancement is paramount.

It is important to note that the use of technology has provided Techline Incorporation with a significant number of business benefits. They include increase in the company’s targeted customer base. This is a consequence of advanced digital marketing and advertisement tools, which help in informing as many customers as possible on the different services at the company. Additionally, through other software modules such as the integrated customer relationship management system, more people get informed on the available services (Chapman, 2013). The increase in customer demand for Techline services has further increased sales hence creating a great platform for attainment of the overall business goal, which is making profit.

Technology has also played a key role in facilitating efficient internal and external communications. Internally, the company staffs enjoy an easy and effective platform for sharing useful business information. Externally, the company continuously enjoys an efficient mechanism for communicating with its customers, potential customers and investors as well as the public (Stallings & Brown, 2015). Most importantly, technology has streamlined the decision making process at Techline Incorporation. The management of the company is able to keep track of the use of key organizational resources such as finances, market status and customer satisfaction. In general, IT has been fundamental in promoting business growth for Techline Incorporation.

Regardless of the benefits, technological advancement has created a considerable number of risks in the day-to-day operations of the company. Risks act as potential threats to the continued successful implementation of the company’s operations (Moeller, 2011). Some of the key risks that Techline must put into close consideration include unauthorized access to the company’s information system, alteration of financial records, alteration of system configuration, theft of business secrets and piracy on the company’s essential business integration software. Other risks are natural and they include floods, fire and other environmental hazards. For our company to succeed in mitigating the various types of enterprise risks, it is important that its leadership comes up with a well-designed platform for enterprise risk management (ERM) (Stallings & Brown, 2015). Failure to have an efficient approach for risk management can result into immense losses. Hence, the adoption of an ERM will play a very crucial role in coming up with a disciplined approach for the selection and management of risks. In summary, enterprise risk management (ERM) is a process that involves planning, organizing, leading as well as controlling activities within an organization to help in minimizing the effects on a company’s capital and resources.

## Definition of terms

Enterprise - It refers to a company or business that is established to run a particular operation with an aim of making profit.

Management - This is a process of organizing and coordinating business activities with an aim of attaining predefined business objective.

Information - This refers to a data set that is processed and presented in a way whereby a user can easily understand it (Stallings & Brown, 2015).

Data - This refers to a representation of facts as well as computer instructions in a way that is formal enough to be interpreted by a computer.

Database - This is a structured collection of related data, which is designed and built to satisfy the required purpose (Moeller, 2011).

Data warehouse - It refers to a well-designed system that collects data from different data sources and presents it in a site where users can easily access (Chapman, 2013).

Software – This refers to a set computer data and instructions aimed at delivering specific functional capabilities.

Risk - This entails any potential failure in technology that can disrupt day-to-day business operations (Moeller, 2011).

Frailty – This is a weakness in a particular computer network or information system that results in the system being weak.

Threat – It refers to anything that can cause harm on an information system or computer network (Chapman, 2013).

Hacker – This entails an individual who makes use of a computer device or tool to acquire unauthorized access into an information system (Grosslight, 2010).

Confidentiality – This is a set of rules as well as security mechanisms, which limit access to a specific set of information hence making it secretive in nature.

Integrity – It is an assurance that information contained in an information system will always remain reliable and exact (Stallings & Brown, 2015).

Availability – This is a guarantee that only the authorized users of a certain information system will benefit from reliable access to the system.

Intrusion Prevention System – It is a unique security software that examines network traffic in order to detect and prevent vulnerability exploits in a system (Slater, 2010).

Intrusion detection system – This is a specific type of security software that is designed to perform automatic alerting of administrators about any malicious activity.

Malware – This is a software that is designed with the aim of damaging a particular computer systems (Grosslight, 2010).

## Current Company Network State

Techline incorporation is composed of a well-configured set of network resources ranging computer devices, work force and infrastructure. It is essential to outline that Techline Incorporation currently operates in a one-storey building located in Hinesville, Georgia. The ground floor is composed of the junior company staff members in charge of the daily business operations (Stallings & Brown, 2015). The first floor hosts the company servers as well as key company officers including the Chief Executive Officer, Chief Information Officer, Network Administrator and the head of the Supply chain Unit. In each of the floors, a specific set of pre configured network devices allow users to share information and develop products that help in attaining the company’s main objectives. Company leaders such as the CEO, CIO and the Network Administrator play a crucial role in ensuring attainment of the set out objectives.

### Main business Objectives

The current main business objectives include provision of high quality software solutions for business integration. Other major objectives under Techline Incorporation is to ensure the delivery of innovative software solutions that include information assurance, data analytics, cyber security, Insider threat analysis, help desk services and systems knowledge management. All around the globe, companies are striving to have the best tools for performing information assurance and data analytics, which is vital in improving their marketing practices for their products (Moeller, 2011). In addition, insider threat analysis and cyber security services are paramount in enhancing confidentiality, integrity and secure availability of business services. Hence, the demand for these services is consistently increasing. In essence, the company objectives are well suited for the current constantly advancing technological world.

### IT processes

As seen above, Techline incorporation operation has a significant number of main objectives that act as the basis for the company’s day-to-day business activities. There is a considerable number of information technology processes that have been facilitating the attainment of the company’s objectives. Firstly, the company has employed around twenty-five staff members with majority of them specializing in the development of software products as well as computer network configuration (Chapman, 2013). The company has two main Local Area Networks (LANs) connected to a Wide Area Network (WAN) that facilitates access to the internet. One of the LAN provides services to the junior staff members on the ground floor while the second LAN is utilized the top leadership of the company.

Several other IT processes help in achieving the main objectives at Techline Incorporation. They include a well-designed set of independent software applications for running the daily activities at the company. These include the information assurance application, data analytics application, an application for insider threat analysis, business suite software, accounting information system, sales management system and a human resource management system, visual studio and the dot Net framework (Moeller, 2011). Visual studio helps in coming up with customized software applications for installation in different businesses or companies. In addition, the company has a five-terabyte database system, which helps in the storage of the ever-increasing data requirements at the company. In general, the availability of these IT processes has been fundamental in ensuring that Techline Incorporation succeeds in satisfying its business goals.

### The need for Information assurance need

As aforementioned earlier, Techline Incorporation specializes in provision of various IT services such as data analytics, development of business software, information assurance, Insider threat analysis, help desk services, cyber security monitoring and computer network configuration (Grosslight, 2010). Considering the constant technological changes, delivery of these services requires the availability of an efficient information assurance practice. In simple terms, information assurance refers to a practice of protecting of IT resources as well as managing risks related to the day-to-day processing, storage and transmission of data across an information system.

Hackers are continuously devising sophisticated tools and mechanisms for breaking into computer systems (Wackrow, 2017). Actually, because of its emphasis on providing secure business integration solutions, Techline Incorporation has experienced a wide set of security threats. Different hacking threats have been experienced in the company, with majority of the hackers motivated by the urge to prove that they are more sophisticated than the company’s technical staff. By use of programs such as Trojan horses, worms and viruses, hackers have continuously tried to break into the company’s IT system (Chapman, 2013).

The availability of a number of well-configured security mechanisms within the network has been vital in enhancing information assurance both for the company itself and for its customers. Additionally, through the leadership of the CIO and Chief Network administrator, the company has developed quality risk identification and mitigation practices.

In essence, the company has developed a risk management practice that emphasizes on guaranteeing the following. First, it is secure availability of services and information within its online information system. It also focuses on delivering integrity-based services, which ascertain that information can only be modified or accessed by the authorized users only. Furthermore, to minimize the risks of having unauthorized system access, the IT team has integrated authentication feature for accessing the company’s information system (Stallings & Brown, 2015). This feature entails a username, password and pre defined access level for every user. In addition, the information system maintains high-level confidentiality, which limits access to the company data. Using an accountability-tracking tool, the system further guarantees non-repudiation where one cannot deny an action done because the system can automatically provide proof (Grosslight, 2010).

In essence, the availability of these features within Techline Incorporation’s information system has been very critical in building customer trust in our products. The company has been able to retain a significant number of loyal customers as well as attracting new ones from all around the globe. This is because most customers who use our products end up being satisfied that their data and applications are always secure from any unauthorized access (Moeller, 2011). That is, the positive information assurance practice has laid a foundation in ensuring that the company succeeds in daily its business operations.

### Network Configuration

It is important to commend the effort made by the company’s IT team in coming up with a well-configured computer network. As a said earlier, the company’s network is divided into two main local area networks (LANs). One facilitates the junior officers on the ground floor while other is for the company’s top leadership on the first floor. The ground floor LAN is connected to fifteen workstations and three printers. For security purposes, each of the workstations is installed with a well-configured software firewall. The software firewall helps in ensuring that viruses from different areas across the internet do not infect the computer.

From the workstation, each LAN network ends at a switch. That is, each LAN is composed of a switch, which connects the workstations within it. The switches are both configured to ensure that specific device MAC addresses can gain access through the network. For data to be transmitted from a junior officer’s workstation to a leader’s workstation, it must follow the following path. From workstation to switch 1 (on the ground floor) via router to switch 2 (on the first floor). It is essential to note that the router is configured with access control lists (ACLs), which filters IP addresses that are not defined. This feature is crucial in protecting the company network from unauthorized access. In addition, just before the router, the IT team has installed a physical firewall, which filters all network packets and authorizes only the ones with right header details (Chapman, 2013). Furthermore, the network contains a pre-configured intrusion detection system to help in detecting and alerting users about any potential system intrusion.

As seen above, the company network is designed in a manner that is of great significance in attaining the set out business goals. In order to support the security needs, the network contains considerable number of security devices that include firewall and intrusion detection systems (Wackrow, 2017). Additionally, for the efficient operation of the IT processes, the network has been configured in a manner where there is efficient and secure flow of information within the company network and over the internet.

### Current network security risks

It is vital to note that upon a thorough analysis of Techline Incorporation’s network configuration and information system, a considerable number of security issues were spotted. To be precise, information from the Network Security Administrator indicates that, in the last six months, a significant number of security incidents have happened within the organizational network (Chapman, 2013). These incidents were identified in the company’s firewall, intrusion detection system and intrusion prevention system. The security incidents portrayed a considerable set of security risks at Techline Incorporation. Below is a summary of the incidents as seen from the desk of the network security administrator.

One of the key incidents is defacement of the company web. In this case, it was noted that a hacker used a virus to gain access into the company’s main website. Upon gaining access, the hacker further configured the viruses to perform complete defacement of the website. This resulted in complete change on the visual appearance of the website. It became black in color with some red writings on it indicating details of the hacker (Moeller, 2011). Although the IT team did immense efforts to restore the website, it was also found out that the different links had been removed or changed from one location to another. Most notably, the company’s main login link had been transferred from the normal central position to bottom left. Hence, there is great need to identify the source of the threat and come up with techniques for mitigating it completely.

The second incident is that, the company’s intrusion detection system has been configured using the misuse detection technique. That is, it operated using signature based form of intrusion detection. This technique uses a central database as a reference point for determining an attack. To be precise, under the misuse detection technique, the IDS utilizes a large central database of different attacks. Whenever, an item tries to access the home network, the IDS performs matching of the attack signature with the ones in the database. When there is match, an alert is made to the network administrator and the attack is denied access. This method is beneficial in that it provides accurate information about attacks instead of providing false positives (Chapman, 2013). However, its main drawback is the inability to detect new forms of attacks that are not in the database. Because of the speedy rising hacker sophistication, the use of this form of an Intrusion Detection System is a great risk to the success of the company in attaining its set out business objectives.

Thirdly, lack of adequate qualified personnel in handling information security matters within the company was found to be a major risk to its success. The company had focused on employing people with ordinary IT skills. Apart from the network security administrator, all the other IT officers had inadequate knowledge in information security. Additionally, none of the staff members was a certified cyber security expert (Stallings & Brown, 2015). In essence, the company lacked a specialist in handling information security matters such as cyber security or information assurance. The availability of a certified cyber security expert within an organization is paramount in ensuring maximum security in a particular network infrastructure. According to the company records, it is indicated that it had earlier outsourced an information security service provider, who was tasked with the installation of the intrusion detection and prevention systems. It was also noted that, one year since the IDS was installed, no security update has been done. As a result, the system had become obsolete in that could no longer detect new forms of security attacks. Lack of up-to-date intrusion detection systems is a great risk to the day-to-day operations of a company.

The fourth network security risk was seen in an incident where the company’s firewall rules were conflicting. Research shows that technology is constantly advancing to meet the ever-changing user needs (Moeller, 2011). At the same time, hackers are developing sophisticated ways of intruding computer network. This necessitates the implementation of consistent firewall rules. In addition, the firewall software has to be updated regularly. However, at Techline Incorporation, it was noted that its firewall policy was last updated in the last three years. Under that old policy, normal users and technical users such as IT professionals had same access privileges. Each was allowed to add or remove a network item in the firewall. In one instance, one of the company sales representatives allowed a cookie packet into the company’s network. The cookie captured and sent the user’s login details for the company’s sales management system to a hacker. Fortunately, it was discovered earlier that there was unauthorized and the issue was resolved. In essence, lack of up to date and clear firewall policy creates backdoor entry points in a network, which is a very risky situation for the company.

## Analysis of how the network reached its current state

Since inception, Techline incorporation focuses on the development of innovative software solutions for businesses. The company has been using common features such as the internet and ecommerce, which exposes it to a wide number of security risks. In addition, as a global developer and user of technological tools, the company’s online boundaries are continuously growing. The increase in the online boundaries results into immense increase in IT risks (Grosslight, 2010). Hence, over the last one year, Techline Incorporation has undergone significant changes in the implementation of information assurance practices.

### Changes made to the network

The company CIO and the Network administrator have been working hand in hand to ensure that they improve the quality of information assurance at Techline Incorporation. In the last one year, the two have pioneered the implementation of a number of changes in the organizational network to facilitate improvement information assurance. The first change was the introduction of culture of security within the organization (Moeller, 2011). Considering the current world of the internet of things, creation of a culture of security is essential. To attain this culture, the company leadership has played a significant role in rolling out the custom across the department. One of the steps done is conducting of regular employee training on ways of mitigating security threats in the organizational IT infrastructure. As the IT team becomes aware of the new hacking techniques, its first role is to perform immediate sharing of the same to the company to the employees (Stallings & Brown, 2015). Knowledge is power, hence sharing the security issues to the company employees and customers will be vital in enhancing data protection levels. Although majority of the employees were initially reluctant in accepting the culture of security, the leadership made it a success by being proactive in sensitizing all the company stakeholders. The culture has further been enhanced by the introduction of a security tool called Core Impact. This tool is integrated in the network penetration software. In essence, Core Impact performs a thorough testing of the organization to determine if the users are responding properly to different security threats such as phishing mails and fraudulent offers. In general, a top down leadership and bottom up participation of employees to the culture of security has been a major factor in enhancing security at Techline Incorporation.

The other recent change is the utilization of the international guideline for information assurance. To be exact, based on that guideline, the company leadership introduced a security checklist that has to be implemented in the execution of the daily duties. The guideline is based on six fundamental principles, which are awareness, responsibility, response, risk assessment, security design and implementation and reassessment. About awareness, the guideline laid emphasis on the general personnel issues mainly training on the best security practices. The company put in place weekly campaigns to raise the levels of security (Wackrow, 2017). Through awareness, almost every stakeholder was enlightened on the various required security practices at the company. However, specific security configuration as well as network architecture has always been kept secret (Chapman, 2013). On responsibility, the guideline focuses on the importance of involving the senior management in matters related security as well as development of security policy. That is, all security matters need to gain support right from the highest level of organization. In order for security to be assured, it requires the provision of clear instructions right from the top leadership. Regarding the principle of response, the company introduced an incidence response unit. This unit is in charge of attending to all the security incidents within the organization. Whenever, an employee detects a malicious activity, he or she is not supposed to attend to it. Instead, she immediately has to alert a member of the prescribed incident response unit. The incidence management team is responsible for recording and reporting all procedures taken in solving different security matters at the company.

On the subject of risk assessment, the guideline clarifies that, all decisions taken in addressing risks and their mitigation must involve the top management of the company. That is, they must involve, the CEO, CIO and the Network security administrator. All the risks that relate to the daily business operations must first be, identified, prioritized and then have action plans agreed to by all responsible parties (Stallings & Brown, 2015). For a company to succeed in attaining its set out business goals, all the risks must be mitigated. Therefore, this action plan is paramount in mitigating any potential security threats. Essentially, in order to ensure that appropriate priority is given ICT-related risks, they all have to be integrated in the assessment of the overall corporate risks.

On security design and implementation, the guideline outlines that information security assurance has to be an essential part of the day-to-day ICT solutions. This guideline is very important in the delivery of the required services at Techline Incorporation. According to the guideline, any company that is involved in designing and configuring ICT related components must always build in security features that are appropriate to the company needs. On this regard, the consideration made by the company included balancing of issues related to costs and the overall risk assessment plan (Moeller, 2011). On reassessment, the guideline helped in ensuring that there is maximum stakeholders’ participation and compliance to the legal functions of the company. In addition, the stakeholders must work together to facilitate efficient reassessment of all the risk management plans.

The third change in the company entails, full involvement of suppliers, partners, and customers in enhancing security and gain a better understanding the security challenges faced while utilizing the company’s products. The involvement of suppliers is helpful in gettig their feedback on the security challenges they experience while accessing data from the company website (Grosslight, 2010). As aforementioned earlier, Techline incorporation develops different innovative solutions, data analytics and business integration solutions for different customer categories. The success of any IT company depends on the availability of high quality security features within its IT infrastructure (Chapman, 2013). Therefore, in order to attain better security, the company products are now designed with integrated security features as well as manuals. In addition, customer awareness has been raised especially on the importance of security and the need to be part of the culture of security at the Techline Incorporation.

### Impetus behind the changes

There are different factors that drove the need for changes within the company’s IT infrastructure. These factors include operating in line with the international IT security standards. It is important to clarify that, time after time, renowned IT security organizations across the globe come up standards for implementing security within organizational IT platforms. Most companies that do not follow the international security standards are always prone to attacks or unauthorized access. These standards contain the guidelines that help in mitigating risks associated with the development and use of IT tools (Moeller, 2011). They also help on how to come up with strategies for enhancing employee awareness and improving a company’s reputation on the global IT industry. In order to succeed in the current IT world, the leadership of Techline incorporation found it necessary that the company makes use of the international IT security guidelines. The use of international standards is also crucial in mitigating not only local but also global IT security threats. As a result, the significant changes made at Techline Incorporation were driven by the need to ensure compliance with the new International IT security standards.

Another major driving factor towards the implementation of the changes is the subject of increase in insecurity within the company network. As aforementioned earlier, the company has recently been a victim of a considerable number of insecurity issues. They include defacement of the company’s main website to a black interface with red writings about a certain hacker’s details. Although the website was later restored, the company’s top leadership became very concerned. Hacking of a company’s main website results into significant loss in reputation as well as lowering of the customer trust levels (Stallings & Brown, 2015). In this incident, an urgent security meeting was held to ensure that the situation does not happen again. In another incident, a hacker gained access across the organizational computer network and altered a number of key financial documents. Although the incident did not reach the public domain, it resulted into much concerns on the ability of the company’s IT security system to withstand future attacks. The company’s top leadership also became highly concerned on whether they operated using the best security mechanisms. Upon holding of a number of IT security meetings, it was unanimously agreed that changes were necessary.

Last but certainly not least, the need to handle huge data volumes was crucial in the implementation of the changes. Some of the key services at Techline incorporation include information assurance and data analytics. In fact, data analytics is done for the company itself and for its customers (Moeller, 2011). In simple terms, data analytics is a process of extracting and categorizing data to identify patterns based on company requirements. This process is useful in analyzing the marketing practices of a company and coming up with improvements. Currently, the company operates using a 5-terabyte database system. However, considering the consistent rise in data requirements, it has become a big challenge for the company database to withstand. An overloaded database is always prone to attacks. In other words, processing large data volumes is always a huge threat to the security of a company’s IT resources. Consequently, this necessitated the implementation of changes in the company’s security practices.

### Anticipated benefits

A considerable number of anticipated benefits always drive the implementation of changes in a company’s IT operations. Hence, it is fundamental to outline that there are several anticipated benefits behind the implementation of changes. They are categorically divided into organizational, operational, strategic and tactical benefits (Moeller, 2011). The organizational benefits are improved shareholder value and attainment of a competitive advantage. As a result, the company acquired significant increase in shareholder value. However, the company has not realized any significant edge over its competitors. The anticipated strategic benefits are better governance and increase in company sales. Because of the changes, Techline Incorporation was successful in realizing considerable increase in sales. In addition, governance of the company was enhanced enough to improve the customer trust levels. The anticipated tactical benefits were easier compliance, better understanding of business opportunities and commitment from business partners and customers (Stallings & Brown, 2015). These benefits were well realized at the company. For example, upon implementation of the changes, the company introduced the provision of innovative solutions for promoting information assurance within integrated business solutions (Slater, 2010). This was achieved through a better comprehension of the available business opportunities. Through the introduction of international guidelines for IT security, it became easier for the company and its staff to comply. The company has experienced a significant rise in the number of loyal customers as well as consistent rise in number of new customers. In essence, the changes played a very crucial role in enhancing the trust levels of all the company stakeholders thus enhancing the commitment from partners and customers.

### Important lessons learnt

There are several important lessons learnt because of changes that were made at Techline Incorporation. Firstly, it was learnt that increase in organizational data requirements increases the company’s IT risks. In essence, as an information system processes and stores a lot of data, more viruses and other malicious information tend to gain access (Moeller, 2011). This is because, it is always easier to maximize security when dealing with little information compared to when dealing with high data volumes. In essence, as the data requirements in an organization increases, it is paramount to consider improving the security mechanisms and tools.

It was also learnt that efficient management and monitoring of all privileged users of company’s information system is crucial in attaining maximum security as well as compliance to the set out policies. There are special international policies and guidelines for information security. In order for users to comply with the guidelines, adequate control features have to be integrated. Moreover, once a company creates a privileged user account in its information system, it is necessary that routine monitoring and auditing is done. This is to ascertain that every user is held accountable for their actions. Once, users understand about their accountability in using the system, they do all their best to ensure compliance (Chapman, 2013). As a result, a company benefits from better service delivery and improved data and network security.

The third important lesson learnt is that maximum security of a computer network and other IT resources can be achieved through the implementation of security awareness programs. Awareness should be done to the staff, suppliers and even the customers. By enlightening staff members on matters related to IT security, it helps in minimizing their chances of being victims of different hacking tricks such as social engineering. IT security awareness acts as the basis in ensuring that employees are always fully alert on matters that can cause failure in protecting a company’s network from unauthorized access (Moeller, 2011). A company with staff members who are well trained on security awareness has great chances of improving its customer base as well as enhancing supplier trust levels. In essence, majority of customers always feel more confident to working with a business, which they understand that their employees are well trained to avoid any form of security breaches. In general, security awareness programs play a significant role in enhancing customer trust hence facilitating improvement of a company’s competitive edge. By having a great competitive edge, Techline incorporation will have a great chance of being successful in the current global market for innovative IT solutions.

It has also been learnt that top leadership support is a fundamental requirement in ensuring that there is a successful culture of security. As said earlier, it is through a top down leadership and bottom up participation by employees that facilitates attainment of a consistent IT security culture. Right from the CEO, through CIO and Network Administrator, the culture of security has to be given top priority (Stallings & Brown, 2015). In other words, leaders have the responsibility of leading by example. For example, if an IT security policy or guideline has been proposed. It is the role of the company top management to start practicing based on the new guideline. Moreover, it is essential that the company leadership instill the concept that IT security belongs to everyone. At first, most employees were of the opinion that IT security was a responsibility of the security team. However, in the implementation of this culture, it was learnt that sustainable IT security culture requires the participation of every stakeholder. Every company stakeholder must feel like a security person (Moeller, 2011). By adopting this mindset, then, there is a security culture for everyone. Furthermore, they should sensitize the junior staff members on the importance of giving their best in delivering the requirements of the new practice. Under the same subject, it was also learnt that, for all employees to give their best, there is great need for leaders to look for opportunities for celebrating success. This can be achieved by giving rewards to those people who do right things for security. By celebrating security success, employees will be placed in a great position to accept security as one of the fundamental elements of the organizational culture.

## Anticipated future business needs and network demands

At Techline Incorporation, the delivery of high quality and innovative business integration has always been one of the most essential goals. To be exact, the main anticipated future business need is the ability to process over ten terabytes of data and applications using the data analytics tool. Another major business need is the ability to provide 24/7 services to the customers from all around the globe (Chapman, 2013). The ability to deliver the above needs will be fundamental in raising the company’s competitive edge.

In order to achieve the above business needs, it is necessary that a considerable number of network demands are ascertained. The first network demand is the implementation of analytics and cloud technology. Cloud technology refers to a service model where the processes and data is presented through a public or private cloud network. For Techline Incorporation, the services will be available via a public cloud portal. A public cloud is a crucial feature in providing efficient access to data and applications aimed at attracting different customer groups across the internet.

Primarily, Techline Incorporation’s need for analytics and cloud technology is driven by the need for database expansion to withstand the ever-rising data and applications. To ensure efficient operation, it is necessary that the technology is implemented in the form of analytics-as-a-service integrated with cloud network connectivity (Stallings & Brown, 2015). Analytics and cloud technology will also play a key role in facilitating efficient disaster recovery. Practically, it is always a big challenge to anticipate when a disaster may happen in a computer network or IT infrastructure (Slater, 2010). Therefore, instead of using the ordinary complex recovery techniques, cloud computing offers an online virtual storage space where organizational data can be recovered at ease. In essence, the implementation of this technology will be vital in attracting a large customer base.

It is vital to note that one of the key network changes that have been proposed for Techline Incorporation is the adoption of a virtual private network (VPN). The company focuses on delivery of innovative business solutions along with data analytics services. In the execution of these services, the company staff have to login into an information system and share very sensitive information (Moeller, 2011). Furthermore, considering the anticipated transformation into using a cloud network, it is necessary that maximum security is delivered. Through a VPN, the company staff and customers will be able to enjoy specialized access to the information system from anywhere around the globe. A VPN is also a key network feature in guaranteeing confidentiality, integrity and secure availability of data across a network. This feature is vital in minimizing IT security risks and improving the level information assurance.

It is important to outline that the above IT infrastructure has put the subject of information assurance and network management into very close consideration. Information assurance involves a assuring and managing the risks that relate to the use, processing, storage and transmission of data across a network (Stallings & Brown, 2015). To ensure efficient handling of the information assurance and network management matters, the plan has included the utilization of a number of key tools such as cloud network and virtual private network. Via the cloud network, it is easier to handle several risks involved in the processing, storage and transmission of data. The cloud network provides virtual storage spaces where company data and applications can easily be recovered even in cases of a huge disaster. On the other hand, through the integration of a virtual private network the company has a great mechanism for minimizing the risks of unauthorized access. A VPN simply entails a technology used to create a safe and encrypted connectivity over a less secure network, such as the public cloud network. The technology allows remote information system users to enjoy secure access to the company applications and data.

It is however, essential to note that, there is one issue of network management that is yet to be properly addressed. It entails the need to recruit the right set of network security experts for managing the planned network growth. For efficient management of the company’s computer network, there is need for the recruitment of certified cyber security experts and information assurance professionals.

The main technical information assurance issues at Techline Incorporation include lack of certified Information Assurance officers. This makes it challenge to determine whether the company is operating as per the required information assurance standards. Secondly, considering the complex IT environments, lack of tools for measuring the level of information assurance is a key issue for the company. The company is therefore unable to determine the level or quality of information assurance within its computer network and IT infrastructure at large (Stallings & Brown, 2015). For the company to succeed in delivering maximum success there is need for the integration of adequate tools for measuring information assurance. Another major information assurance issue is the subject of blended threats. A blended threat entails a software exploit that in turn applies a combination of attacks against various network and information system vulnerabilities. An example of a blended threat involves a worm, a Trojan horse and virus exploiting multiple techniques to attack a particular computer network and propagate. Practically, it is an immense and challenging issue to manage such attacks in a computer network.

Several information assurance issues conflict the aforementioned business plans. Part of the business plans is ensure compliance with the ever changing international standards for managing data and handling IT related content (Moeller, 2011). However, the major conflicting matter is that, as more business compliance elements are defined, more time and effort is then required to deliver the best form of information assurance. That is, it results into significant increase in the amount of time and effort that is need to maintain the proper levels of compliance. Difficulty in the comprehension and management of IT security risks is also a key issue facing IT and network in the company. In actual fact, it is always very challenging to prevent data breaches, which ascertaining that there is no impact on the company’s daily business operations.

## Recommendations

Techline Incorporation has made significant efforts to enhance the quality of IT security within its ICT infrastructure. However, as seen earlier, several gaps exist in its daily operations. In order to ensure that the company succeeds in the current speedy advancing business world, there is need for the following recommendations to be put into implementation.

A thorough analysis of the company staff has revealed that none of them is certified in information assurance or cyber security (Stallings & Brown, 2015). The company plans include integrating advanced technological components such as analytics, virtual private network and cloud network connectivity. Cloud network allows transmission of data over the internet while the virtual private network provides a secure platform for accessing online services. Configuration, installation and maintenance of the above technologies is very complex and is constantly updated to accommodate new innovations. At the same, data requirements for the analytics tool are constantly rising, hence, increasing security risks. In this sense, for the company to enjoy efficient utilization of the above technological tools, it is paramount that recruitment of information assurance and cyber security experts is done.

Techline Incorporation specializes in the provision of a wide number of services including data analytics, information assurance and business integration solutions. Considering the speedy advancing technological world, the number of customers at the company has also been on a speedy rise. Moreover, with the planned introduction of cloud network connectivity, the data requirements are going to rise by a very huge margin (Chapman, 2013). Currently, the company operates on a five-terabyte database system. However, for the company to withstand the ever-increasing data requirements, it hereby recommended that a data warehouse is installed. The use of a small database system to process and store data, results into it being overloaded or congested. It is always very challenging to deliver maximum information on an overloaded database system. Therefore, the introduction of data warehouse will facilitate efficient service delivery in terms of information assurance.

It is also recommended that the leadership of the company adopt the most recent international guideline for information assurance (Stallings & Brown, 2015). Under the new guideline, an organization is provided with a well-structured security checklist. This checklist recommends a company to utilize three main categories of principles for information assurance. These are the foundation principles, social principles and security lifecycle principles. The foundation principles are awareness, responsibility and response while the social principles are ethics and democracy. In addition, the security life cycle principles are risk and risk assessment, security design and implementation, security management and reassessment. In essence, the implementation of these guidelines will play a very crucial role in promoting successful attainment of the set out company goals.

## Conclusion

Trust is an essential thing in promoting success of a business. Customers, suppliers and other stakeholders have to feel safe and secure while interacting with the business. To achieve IT security information assurance is fundamental.

Techline Incorporation has been doing all its best to ensure that the best information assurance practices are put in place. Through the leadership of the Chief Executive Officer, Chief Information Officer and a Network administrator, the company is providing a considerable of number of services. These services include information assurance, data analytics, cyber security, Insider threat analysis, help desk services and systems knowledge management. To enhance the levels of information assurance, the company has implemented a considerable number of changes. These changes include the introduction of a culture of security, full involvement of all the other stakeholders on security matters and the implementation of international guideline for information assurance.

In order to ensure better service delivery, it is hereby anticipated that Techline incorporation introduces the use of analytics and cloud technology. These features will play a very important role in widening the company’s customer base. It is also anticipated that, for the cloud network to work effectively, adoption of a virtual private network is paramount.

Finally, it is recommended that Techline Incorporation recruits the right set of information security professionals. They include certified information assurance and cyber security experts. Moreover, for the cloud network and analytics to work effectively in attaining information assurance, introduction of a data warehouse is also essential. Furthermore, the company leadership must consider implementation of the recent international security guideline, which is based on three main principles. These are the foundation principles, social principles and security lifecycle principles. In general, by improving the quality of information assurance practices, Techline Incorporation will enjoy a great opportunity for improving its competitive edge.

## References

Chapman, R. J. (2013). *Simple tools and techniques for enterprise risk management*. Hoboken, N.J: Wiley.

Grosslight, K. (2010). *Minimize risk by maximizing accountability: Risk management compliance, Wells Fargo*.

Moeller, R. R. (2011). *COSO enterprise risk management: Establishing effective governance, risk, and compliance processes*. Hoboken, N.J: Wiley.

Slater, D. (2010). *Enterprise risk management: Get started in six steps.*

Stallings, W., & Brown, L. (2015). *Computer Security: Principles and Practice, Global Edition*.

Wackrow, J. (2017). *The evolving role of the Chief Security Officer: Rethinking effective risk*

*management for 2017.*