STP Limited

Networking Project

2017

9/16/2017

# Executive Summary

The objective of this report is to assess the networking environment which is recently implemented in STP Ltd. Company. The focus of the report is on the environment and its connections with the company employees. The report explains the background information of the project and its objective which is to streamline the business operations of the company such that the employees can be equipped with the tools that would help them serve the growing base of customers. Because of the new installation, the company is likely to face certain security issues and thus, STP needs to use its people, products and policies in a cooperative manner such that the business remains protected. Policies have to be implemented in order to keep the company data secure. Moreover, the procurement processes used in the company must cause minimum disruption to the networking environment if the company has to make the most out of the development. All these measures would help keep the business continuity of the company intact. Business continuity reflects upon the endurance capacity of a business. First, a backup of the organizational data has to be taken for business continuity post which disaster recovery plans have to be formulated for the physical security of the infrastructure. The report discusses these steps involved in business continuity planning including succession planning. Risk management details are provided in the report to explain how STP can manage risk scenarios and identify the risk categories. For protection of the STP assets, security policy has to be defined and implemented and thus, the same has also been discussed. Finally, the report presents a list of recommendations that aim to make the implementation successful for a long term.

Table of Contents

[Executive Summary 8](#_Toc495342439)

[Introduction 10](#_Toc495342440)

[Project Background 10](#_Toc495342441)

[Project Scope 10](#_Toc495342442)

[Project Goals 11](#_Toc495342443)

[Strategic Alignment of the Project 11](#_Toc495342444)

[Network Security 12](#_Toc495342445)

[Ideal Branch-Office Security Solution 13](#_Toc495342446)

[Securing data 14](#_Toc495342447)

[Mobile device security 15](#_Toc495342448)

[Wireless Local Area Network (WLAN) attacks 15](#_Toc495342449)

[BYOD risks 15](#_Toc495342450)

[Plan for Hardware Purchases 16](#_Toc495342451)

[Acquisition of new hardware 17](#_Toc495342452)

[End user feedback and reviews 17](#_Toc495342453)

[Purchasing strategies 18](#_Toc495342454)

[Asset register 18](#_Toc495342455)

[Business continuity 19](#_Toc495342456)

[Risk management 20](#_Toc495342457)

[Risk Management Strategy 20](#_Toc495342458)

[Risk Identification 20](#_Toc495342459)

[Risk Responsibilities 20](#_Toc495342460)

[Risk Assessment 20](#_Toc495342461)

[Risk Response 20](#_Toc495342462)

[Risk Mitigation 21](#_Toc495342463)

[Tracking and Reporting 21](#_Toc495342464)

[Security Policy 21](#_Toc495342465)

[OBJECTIVE 21](#_Toc495342466)

[The security policy ensures that: 21](#_Toc495342467)

[Training and awareness 23](#_Toc495342468)

[Integration technology 23](#_Toc495342469)

[Conclusions 24](#_Toc495342470)

[Recommendations 24](#_Toc495342471)

[References 27](#_Toc495342472)

# Introduction

STP Limited is an organization that is based out of Wollongong and has its head office in the same city. The organization manufactures cabinets and is expanding to the other regions as well. The sales and revenue are going good for the organization and as a result, it recently bought office premises in Bathurst and Lithgow. They have also set up a new office in Sydney. The company is currently located in four locations and has warehouse machines and other equipment installed in these locations. Networking has become a major area of concern for the company because of the need to come up as an integrated unit to provide good quality services to the customers.

# Project Background

There are new networking and communication technologies that are being used by STP Limited to enhance its connectivity and integration capabilities. Every office of the company is equipped with a modem and a switch and the Internet connection is made active with the aid of ADSL. The members of the staff are allowed to Bring their Own Devices at work which is also known as the BYOD scheme. The wireless connections are also made enable by the organization.

With the use and application of new networking channels and mediums in the organization, there can be a lot of growth and development that the organization may witness. It is because of the reason that the enhanced network connections will allow the employees to be connected with each other at any hour of the day. It will aid in the resolution of the problems and conflicts in a timely manner and will make it possible to experience enhanced efficiency and productivity of the employees. The customers will also be able to contact the organization in case of any query or complaint. There will be enhanced help and assistance services provided which will make it easy to increase the levels of customer trust and engagement (Cisco, 2008).

## Project Scope

The scope of the project is to develop the measures that may enhance the integration and security of the new networks and communication channels.

It will include the design, development and deployment of these measures so that the enhanced networking mediums are implemented. Privacy is one of the essential properties that are required to be maintained in association with the information and networks. The efforts will also be implemented to make sure that the privacy of the information and the communication networks is not disturbed or violated.

## Project Goals

* Ability to make sure that all the office locations and units of STP Limited are integrated with each other as a single unit.
* Ability to ensure that the security of the networks and the information channels is maintained along with the assurance of privacy (Pareek, 2011).
* Ability to make sure that enhanced revenues and customer engagement is earned with the improved networking and communication medium.

## Strategic Alignment of the Project

|  |  |
| --- | --- |
| Alignment Perspective | Description |
| Strategic Execution | * The strategies to implement the networking mediums and communication channels are in line with the organizational goals of achieving enhanced revenues and customer engagement. * The design, development and deployment of the networking integration measures will be done to achieve the goals. * The design, development and deployment of the security and privacy measures will be done to achieve the goals. |
| Technological Potential | * The wireless connections and networking equipment that have been set up are compatible with the organizational systems and applications. * The integration and security solutions that are proposed are feasible on the basis of technical feasibility study. |
| Competitive Potential | * Network security and privacy is a much in demand trend in the market. * The quality of the services is enhanced with the use of the advanced networking and communication mediums. |
| Service Level | * A networking strategy has been designed and determined by the Project Manager so that the organization goals are met. * Resources have been allocated to the project tasks and activities at the operational and managerial levels. |

# Network Security

There are various issues that must be addressed from the point of view of network security. It must be made sure that there are enough human resources in the department of local IT as the support staff. It would be necessary to understand the significance of remote management of the security controls and mechanisms which will involve roles such as network administrator, security analyst etc.

The device configuration that is set up shall be allowed to be accessed with the means of HTTP, HTTPS, Telnet, SSL and likewise. Remote management must provide the capability of remote configuration and management with minimal errors.

In a nutshell, the security solutions that are set up at the branch office must target the needs and requirements of the office sizes and these shall also be easy to deploy and economical in nature. Apart from the security services and solutions, the set of appliances at the branch office must also include the enhanced network capabilities such as secure routing, WAN connections etc. This will eliminate the requirement of installing separate networking devices and equipment.

Another condition that must be considered is the changing landscape of the security threats and attacks. There is a change of technology that is being witnessed with each passing day which leads to the emergence of new forms of threats and risks. There may be some extremely severe implications of these attacks and threats. For instance, in the year 2003, Slammer worm infected 90% of the susceptible hosts in 10 minutes with the doubling rate of 8.5 seconds. There are signature based countermeasures that are being implemented in the organizations which cannot be updated at such a short period of time (Canavan, 2001).

The effectiveness of the security solutions at the branch office would therefore need supplementing of the reactive countermeasures that may have the ability to prevent the uncertainties and security attacks that are not predicted earlier. The use of network focussed defence mechanisms shall also be used for preventing the security attacks associated with application layer and services.

## Ideal Branch-Office Security Solution

At a broader level, the following set of features and mechanisms shall be present in the ideal security solution at the branch office.

* It shall provide a fast and safe VPN connection based on the site-to-site connectivity. This would provide secure access to the centrally operated applications and services along with the support for remote access and management for the employees.
* A direct and secure access to the internet shall be provided. This would be significant in the avoidance of unknown Internet traffic re-directed through any of the regional headquarters location.
* Improved security services and solutions shall be provided for the internal services and network connections. It will be beneficial for the branch office and will also provide indirect benefits to the other connected sites and locations (Alabady, 2009).
* It shall be easy to use and shall also be cost-effective in nature. There shall be system qualities such as performance, reliability and usability maintained.

## Securing data

* Virtual Private Networks: The establishment of IPSec VPNs will be a prime necessity for the branch security solutions and services. There shall be maintenance of more than 100 simultaneous tunnels along with encrypted throughput, such as, greater than 100 Mbps. The use of secure encryption algorithms, such as tripe DES and AES shall be used with key exchange and user authentication protocols (Joshi and Karkade, 2015). NAT traversal and Microsoft VPN clients shall also be made available for the maintenance of security.
* Firewall: Firewall is one of the most significant measures for the security of the data. It should just not stick to the basic networking controls and access control at the transport layer. The access to only the traffic that is secure and as per the policies and regulations eliminates the possibility of many of the security threats and attacks. The effectiveness of firewalls can be realized only by the mode of application of the same, for instance, the implementation of firewall at the network layer only will not be able to prevent the security risks associated with the application layer.
* Attack Protection: There is certain amount of traffic that passes through even with the set up of the firewalls. It also does not identify certain types of security risks and attacks. Intrusion detection and prevention is a technology that comes in the picture to identify and prevent the entry of the bad elements. There are anomaly based, signature based, network based and behaviour based intrusion detection and prevention systems that have been developed for preventing many of the denial of service, flooding and integrity attacks (Strebe, 2004).
* Advanced Content Filtering: There are many of the anti-malware packages that are present such as, anti-viruses, anti-spyware etc. these are completely reactive in nature but have the capability to control the file based attacks and many of the known threats and attacks. There are also some of the serious malware such as Keylogger Trojans that can be prevented and controlled with the aid of this mechanism. There is Web/URL filtering measure that may focus on the outbound traffic and prevent the access to the web sites that are not safe (Soriano, 2011).
* Segmentation & Security Domains: Internal security at the branch office may be improved with the aid of this measure. It makes sure that the associated appliances have the capabilities such as multiple LAN interfaces along with VLAN connections. A unique security policy is enforced on the basis of the users and the computing resources.

## Mobile device security

Mobile devices have become a crucial part of the IT infrastructure of a small business. However, it also presents certain risks to the company that is not always identified at the time of first implementation. Mobile devices give flexibility and mobility but are also faced with issues like limitations of the hardware and security concerns rising from downloading of un-trusted content. Small businesses show more agility towards innovation through the use of technology but these companies rarely take a strong security stance for getting protection for prevention of the financial losses. Some concerns that the company would dace due to BYOD devices and Wireless LAN systems are listed here.

A security strategy shall be developed and implemented to ensure the safety and security of the mobile devices. There are also unknown devices that may be connected to the office network with the use of BYOD technology.

## Wireless Local Area Network (WLAN) attacks

Currently there are many staff at the company that are connecting wirelessly with a mobile device such as a laptop. The risk of such an environment is significant as the asset that holds the most value is very attractive to those who wish to steal or damage vital information. Capturing wireless data is one of the most common enterprise attacks external of the enterprise while rogue access points and evil twin access point are internalized. WLAN attacks can be overcome by proper configuration of devices and employee training programs.

## BYOD risks

Currently, the staff of STP Ltd can connect to the organization’s wireless network through their personal devices. This option has less financial constraints which is convenient for the company but at the same time, it is also exposed to greater risks. While this option is practical to organization as it relieves the business of additional financial constraints, there are risks associated with such a position. The confidential information of the company can get exposed because of user actions. Malicious software can also attack the device or the network affecting the security baseline of the organization. Thus, for the use of personal devices, minimum security requirements must be defined and the employees must be trained on the aspects of data protection and security so that they become better equipped to handle risky situations.

There are some essential tools that may be used for further enhancing the mobile device security.

* **Fingerprinting:** It is a mechanism that enhances and inspects the characteristics that are associated with the mobile devices to understand the type of the device, operating system installed in the device, browser version and so on. It may highlight the unsafe devices and their presence in the networks (Souppaya, 2013).
* **Network Access Controls:** It is commonly abbreviated as NAC and is a measure that may be used for advanced device management by the organizations. An in-depth analysis of the device is done under NAC to highlight the presence of any intruders associated with the device, anti-virus and anti-span packages and so on. If the necessary security solutions are not present in the device, then access of the same is limited in the corporate environment.
* **Authentication:** This is the security solution that comes after the fingerprinting and NAC. It authenticates the users on the basis of the WLAN standards such as 802.1x standard. The combination of the three controls will provide the organizations with the required set of security controls and network management (Sujithra and Padmavathi, 2012).

# Plan for Hardware Purchases

If the organization wants to have a competitive advantage then proper planning needs to be done for hardware procurement. Procurement strategy is an important area of operations of an organization as it keeps the operations going on. Purchase planning is vital for a company. Research can be used for aligning purchase processes with organizational strategy. This can improve financial and operational performance of the business. Hardware purchases would put some financial burdens to the organization and thus, contingency plans are required to be developed for ensuring that business operations remain continued.

## Acquisition of new hardware

Purchase of new hardware cannot be avoided as it can result from causes like loss, failure, or damage to the devices. As the Gympie store is located in an area which is flood prone and thus, it can be a concern for the company. STEP limited has deferred the procurement risks by insuring its business assets. However, for preparing to deal with circumstances, certain documents and assets such as asset register, budget forecasts, emergency plans, policies, procedures, reviews and strategies can be created and maintained. This would empower the company staff to know what can be done in case an unforeseen circumstance is faced to reduce disruption or the loss of productivity.

## End user feedback and reviews

An understanding of how the hardware is used by the employees must be considered while making procurement plans. There can be situations where a hardware used by an employee is outdated or overloaded and thus, software applications used over it are not able to show their full potential. A review from employees as users of the hardware system can help identify such concerns. It can also be known if the user is downloading or running certain applications on the devices causing load to the system unnecessarily. Reviews can be scheduled for evaluation of the hardware performed such that the management can take more informed decisions about procurement. The review would help management identify current issues as well as potential risks that can be faced in future.

## Purchasing strategies

It’s essential that procurement strategies must be aligned with the strategic position of the company. The management must make sure that the company has enough funds for the hardware purchase which needs a careful, cash flow planning. Small organizations like the current one is more likely to have close coordination between employees and thus, strategic alignment would be better. If the organization needs to take the advantages of purchasing hardware at low price, suppliers have to be identified appropriately and the business needs have to be understood through exploration of the business requirements.

## Asset register

It is important for accountants to identify assets to understand their protection needs which can be done using an asset register. This asset register can also be used for tracking any additions or replacements of the IT assets used by the organizational employees. It can record the hardware which is replaced and assess the risk that result from this replacement.

. There are many equipment necessary for installation and testing purposes. Some of the necessary hardware may include the following:

* Computer Systems: These may be required for accessing the tools and applications for the purpose of installation and testing.
* Servers: There are web and file servers that may be required for accessing various information sets along with the database servers as well.
* Peripheral Equipment: Networking equipment such as switches, bridges, routers, hubs, gateways would be required for establishing and maintaining network connections.
* Simulators and Emulators: It would not be possible to carry out testing activities on all the devices and these tools will come into the picture for gaining a virtual experience and testing purposes.
* Diagnostic Equipment: The troubleshooting and diagnostic processes will be carried out for network management and security using this equipment.
* Communication Devices: These will be necessary for the sharing of information and data.

# Business continuity

Data Backup

If the company makes use of cloud based applications then the need for creating backup on the local devices is eliminated. However, the data that gets exchanged over the POS and other non-cloud applications is also the company’s responsibility. Thus, an offsite backup of the store has t be created such that data can be retrieved in case the site is damaged so that the business can be continued without interruptions. A cloud based system can be used for creating this backup which would ensure that most valuable assets are well protected from any losses. Cloud based backup is both efficient and cost effective as it does not require maintenance that is needed in the case of physical backup. Multi-general backups can be created by administrators who would be responsible for the management of the departmental servers.

Physical security

The internal and external environment of the organization affects its physical security. The organizations physical infrastructure could be located in a place that is prone to security risks such as network failures, power outages, road blocks, and floods. Thus, disaster recovery planning is essential such that staff can be made prepared to deal with such situations and ensure that business operations continuity is still maintained. Another concern to the physical security of the business environment comes because of the insider threats as these threats can overtake all the regular security measures as insiders can have greater access authority to system usage. In such a situation, it is the responsibility of the administrator to ensure that the systems remain secure and protected from insider threats.

Succession planning

There can be situations when an important employee or the owner of the organization is unable to work because of unforeseen situations such as injuries from accidents. The company must remain prepared to deal with such situations. Planning must include the details of the roles and the process for appoinmtne of the other people who can take over the work in such circumstances. The comapny must know what financial impacts would be caused as a result. For suscessful implementation of such a plan, company must have the knowlege, skills and capabilities of all the potential replacement employees identified. Their strengths and weaknesses may be assessed and development opportunities may be identified through monitoring, support and evaluation.

# Risk management

Risk is defined as any event that may have a probability of occurrence associated with it and it may have a positive or a negative impact. Risk management is defined as a process that may include the measures for the identification, assessment and treatment of the risks.

## Risk Management Strategy

### Risk Identification

A risk register will be prepared by the Project Manager covering all of the possible risks and attacks.

### Risk Responsibilities

The responsibility of dealing with the risks shall be distributed to all of the stakeholders. The risk responsibility shall be allocated for each of the risk that is identified. The mapping of the stakeholder must be done on the basis of the type and category of the risk (Berg, 2010).

### Risk Assessment

The assessment of the risk shall be done on the basis of its impact and likelihood along with the various factors that may be associated with the risks. The risk ranking shall be applied and assigned to every risk.

### Risk Response

A response strategy shall be defined for every risk that is identified and assessed. The response may include different treatment strategies and measures. There are various methods that may be applied for the risks, such as, avoidance, acceptance, transfer and mitigation (Crane, 2013).

### Risk Mitigation

It shall include the activities for the control of the risk along with the contingency plan associated with the same. The risk mitigation strategies as identified in the risk response process shall be applied and implemented for every risk (Dcu, 2015).

### Tracking and Reporting

The risk mitigation strategy shall be applied and the same shall be tracked and reported by the Project Manager. There shall also be a weekly report that must be prepared to keep a track of the same and the senior management must carry out monitoring and control activities (Debono, 2016).

# Security Policy

A security policy can be used for protecting the assets of an organization as well as for providing a baseline for the user conducts in a workplace. A security policy is not sufficient for complete protection of a small organization but it can definitely act as a tool that creates awareness in the people and help in building a culture that is supportive for the organization in terms of security.

## OBJECTIVE

The objective of defining an information security policy is to ensure that the ABC Company is able to keep its business continued in any situation of damage by any incident and the impact of such damages is minimized. The policy can protect the assets of the organization against internal, external, accidental as well as deliberate threats to some extent. The security policy is approved by a CEO or MD.

## The security policy ensures that:

* Information is protected from unauthorized personnel’s
* Confidentiality of the data is maintained
* Integrity of the information is maintained
* Information availability is ensured at all times
* Regulatory or legislative compliance needs are managed
* Business continuity plans are developed, tested and maintained
* Security related training is given to all employees
* Security breaches are reported to security managers
* An acceptable use policy must be created with acceptable usage terms for system and networking equipments.
* Acceptable use policy

Outlines acceptable and unacceptable use while accessing systems and networking equipment.

* An Antivirus policy must be developed containing details of procedures used for minimizing dangers of virus attacks in computers.
* A Data policy can be developed for outlining of the process for storage of data, its retention and disposal which would be helpful as mobile devices are most susceptive to data theft.
* An Email policy would be used for identifying how email services may be used and how much of the information can be shared with the third party
* An Ethics policy can capture the details of openness of culture, integrity issues, trust factors, ethical practices and impacts on unethical behaviour.
* Password management: Identification of the minimum requirements for creation and management of passwords.
* Privacy policy: It can be used to tell how data can be used by the organization maintaining the privacy of users or others who are associated with the organization.
* Security-related HR policy: This policy takes care of new hires and also includes policies and procedures used for termination. This is useful for management of privileges.

This policy relates to newly hired employee orientation and also termination policies and procedures. This is especially important for privilege management.

* VPN security policy: It highlights the necessary actions that are required to be completed for gaining access to the virtual private network remotely.
* Wireless communication policy: This policy outlines the standards to be used for wireless systems for connecting to the network of the organization
* Managers have to be thoroughly investigated.
* Policies must support the procedures like virus control, password protection and business continuity planning
* Business needs for information and system availability would be met
* The policy must be maintained and supported by the Information Security Manager
* The responsibility of implementation of polices and ensuring that all employees follow the compliance procedure is with all the managers.
* Everyone working in the organization must comply with the Information Security Policy

## Training and awareness

Creation of awareness in employees of STP ltd can have some challenges as well as benefits if training is used as the approach. There can be three elements as defined in the risk model that can be used for managing risks effectively and these include prevention, detection, and correction. It is recommended that all the staff members are trained on security aspects such that they are able to deal with security challenges posed by web presence. Training can also foster a compliance program by pushing employees to use certain practices that can ensure that security threats are minimized.

## Integration technology

If the information systems are integrated to provide real time reporting, it can give the company more capabilities than the case of Software as a Service model of adoption. Integration between applications is something like the web pages mashups in which external sources can be combined on the platform as a service (PaaS). For instance, Force.com is an example of the PaaS system which provides capabilities to build applications to independent software developers or vendors. SalesForce is one such application which is already used by the company. Third party integration gives many opportunities to the organization but also raises some security concerns and interoperability issues such as responsibility of individual parties for ensuring security and guarantee service provision at all times. Thus, it is essential that a service level agreement is developed and used between parties outlining their obligations.

# Conclusions

Brach offices along with the personnel working in the offices are critical assets for the organization at the strategic level. It is essential to make sure that the security of these branch offices is ensured by developing and implementing the measures for security the data and mobile devices. There is an enhanced network management that must be carried out for securing the information and for maintaining the business continuity. The threat landscape is changing at a rapid pace and the corresponding countermeasures that are developed shall be in accordance with the same. There must be system qualities that must be maintained which shall include reliability, availability, performance and usability.

# Recommendations

Network security:

* Third party testing process should be used and implemented
* WLAN access logs should be compared so that risks and attacks associated with the unknown devices are uncovered
* Determination of the usage of the app usage associated with the network tools
* Use and implementation of an identify-centric security model for the purpose of mobility

Evaluation of the level of infrastructure integration:

* The set of applications, cloud services and devices that is available and visible in an unified manner.
* The identification of the set of appliances that are old and make use of obsolete technology.
* Estimation of the people hours that may be saved from the IT staff for using a wired or a wireless network.

Mobile population of the company:

* The number of employees that tele-commute an d the mediums that they use
* The number of employees that are present in this field
* VPN capabilities that are associated with the same

WLAN usage and the population of the devices:

* The number of the inventory device types that are used
* The number of form factors along with the operating systems that are used
* Site survey for the determination of the current usage of geographies and hotspots
* WLAN capacity that will be required along with the factors that contribute in the growth of tablet and the usage of Smartphones
* Evaluation of the VoIP and related latency sensitive applications that may assist in the development or building of the WLAN requirements and applications.
* Evaluation of the 802.11ac. If the use of 802.11ac the costs and architecture associated with it will be required to be developed.

Other recommendations

**Recommendation 1:** Implement procedures and policies for supporting the business continuity through consideration of the security aspects such as data protection in business strategy development.

**Recommendation 2:** The use of LAN and mobile devices must be limited till additional protection measures are taken that can be used for covering the mobile device access points.

**Recommendation 3:** An asset register may be maintained for supporting business continuity through the use of risk management processes.

**Recommendation 4:** A cloud based backup system can be created as an offsite solution such that the data remains safer and more reliable without the need of having physical backups**.**

**Recommendation 5**: Key employee roles that can replace other important employees critical for work must be identified in the succession planning to take over. They must be monitored, evaluated and supported in learning and take over process.

**Recommendation 6**: A training program must be run to make the employees aware of the security aspects and risk scenarios that are associated with business transactions**.**

# References

Alabady, S. (2009). *Design and Implementation of a Network Security Model for Cooperative Network*. [online] Available at: http://www.iajet.org/iajet\_files/vol.1/no.2/Design%20and%20Implementation%20of%20a%20Network%20Security%20Model%20for%20Cooperative%20Network.pdf [Accessed 18 Sep. 2017].

Berg, H. (2010). *Risk Management: Procedures, Methods and Experiences*. [online] Available at: http://ww.gnedenko-forum.org/Journal/2010/022010/RTA\_2\_2010-09.pdf [Accessed 18 Sep. 2017].

Canavan, J. (2001). *Fundamentals of Network Security*. [online] Available at: https://whc.es/Network/Fundamentals%20of%20Network%20Security.pdf.1.pdf [Accessed 18 Sep. 2017].

Cisco (2008). *Wireless and Network Security Integration Solution Overview*. [online] Available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sec\_wireless\_overview.pdf [Accessed 16 Sep. 2017].

Crane, L. (2013). *Introduction to Risk Management*. [online] Available at: http://extensionrme.org/pubs/IntroductionToRiskManagement.pdf [Accessed 18 Sep. 2017].

Dcu (2015). *Introduction to Risk Management*. [online] Available at: https://www.dcu.ie/sites/default/files/ocoo/pdfs/Risk%20Mgt%20Training%20Slides.pdf [Accessed 18 Sep. 2017].

Debono, R. (2016). *Project Risk Management*. [online] Available at: http://www.isaca.org/chapters11/Malta/Documents/Events/210416%20-%20Mark\_Debono%20-%20Understanding\_Risk\_in\_the\_Field\_of\_Project\_Management.pdf [Accessed 18 Sep. 2017].

Joshi, M. and Karkade, R. (2015). *Network Security with Cryptography*. [online] Available at: http://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf [Accessed 18 Sep. 2017].

Pareek, R. (2011). *Network Security: An Approach towards Secure Computing*. [online] Available at: https://www.rroij.com/open-access/network-security-an-approach-towards-secure-computing-160-163.pdf [Accessed 16 Sep. 2017].

Soriano, M. (2011). *Information and Network Security*. [online] Available at: http://improvet.cvut.cz/project/download/C2EN/Information\_and\_network\_security.pdf [Accessed 18 Sep. 2017].

Souppaya, M. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [Accessed 18 Sep. 2017].

Strebe, M. (2004). *Network Security Foundations*. [online] Available at: https://imcs.dvfu.ru/lib.int/docs/Networks/Security/Network%20Security%20Foundations.pdf [Accessed 18 Sep. 2017].

Sujithra, M. and Padmavathi, G. (2012). *Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism*. [online] Available at: http://dl.icdst.org/pdfs/files/35dc646a4630971fd27c6b2d32661555.pdf [Accessed 18 Sep. 2017].