

Company IT Security Plan

**“Identify relevant legislation for the resulting company and identify individual responsibilities arising from these laws.”**

IT Security Management March 2017

Student:

[**Gheorghe**](https://vle.tower.ac.uk/user/view.php?id=4338&course=8493) **Mitrea**

Tutor Assessor:

[**Paul Grainger**](https://vle.tower.ac.uk/user/view.php?id=4338&course=8493)

Table of Contents

[1. Task 1 Understand Risks to IT Security 5](#_Toc483214040)

[1.1 Identify and Assess Business Risks Generally and Specifically for SS Ltd 5](#_Toc483214041)

[1.1.1 Security Risks for Physical Resources 5](#_Toc483214042)

[1.1.2 Security Risks to User Accounts 6](#_Toc483214043)

[1.1.3 Security Risks to Authenticate the Users 7](#_Toc483214044)

[1.1.4 Data Security Risks 7](#_Toc483214045)

[1.1.5 Security Risks of Data Transmission 8](#_Toc483214046)

[1.1.6 Perimeter network security risks 16](#_Toc483214047)

[1.1.7 Factors that Can Cause Security Risks 16](#_Toc483214048)

[1.2 Existing Security Procedures and Security Policy 18](#_Toc483214049)

[1.2.1 Security Policies 18](#_Toc483214050)

[1.2.2 Security Procedures 21](#_Toc483214051)

[2. Task 2 Understand mechanisms to control organisational security 23](#_Toc483214052)

[2.1 Explain the process for completing a risk assessment and findings for SS Ltd. 23](#_Toc483214053)

[2.2 Explain how Data Protection laws affect SS Ltd. and its IT security policy 32](#_Toc483214054)

[2.3 Consider the physical security issues associated with SS Ltd. IT setup 34](#_Toc483214055)

[3. Task 3 Be able to manage organisational security 37](#_Toc483214056)

[3.1 Draft for security policy 37](#_Toc483214057)

[3.2 Evaluate the suitability of the tools used in an organisational policy 46](#_Toc483214058)

[3.2.1 Draft in detail and further improvements 46](#_Toc483214059)

[3.2.2 Further improvements and development 50](#_Toc483214060)

[3.3 Impact of security policy 51](#_Toc483214061)

[CONCLUSION 51](#_Toc483214062)

***Table of Figures***

[Figure 1 DOS attack 9](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213952)

[Figure 2 DDOS attack 10](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213953)

[Figure 3 Masquerade (Source: Masquerade, 2017) 11](#_Toc483213954)

[Figure 4 MAC Address spoofing (Source Internet 2007) 12](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213955)

[Figure 5 Backdoor attack 13](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213956)

[Figure 6 Security attack (Source Internet 2007) 14](#_Toc483213957)

[Figure 7 IT risk components for SS Ltd. 24](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213958)

[Figure 8 Sources of human threats at an information system 27](#_Toc483213959)

[Figure 9 Examples of vulnerabilities 28](#_Toc483213960)

[Figure 10 Establishing the probability of risk in the organisation 29](#_Toc483213961)

[Figure 11 Analysing the impact of SS Ltd. 30](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213962)

[Figure 12 Matrices of a risk for SS Ltd. 31](file:///D:\IT%20Security%20Management%20Assignment\Gheorghe_Mitrea_IT%20Security%20Management_Assgnment_final.docx#_Toc483213963)

#### INTRODUCTION

Today, organisations are using information technology to increase the communication and production in a cost-effective manner. Networks are used in businesses to share and manage the work efficiently.

Networking and connectivity to the Internet can cause additional risks of unauthorised access to data or even fraud.

Technological development has been accompanied by security solutions, equipment manufacturers and technical protection applications, including methods of increasing performance. However, while information technologies change is exponential, the human component remains unchanged. Therefore, securing information security cannot be achieved solely through technical measures but is primarily a human issue.

Most security incidents are caused by inadequate management and organisation and less due to the failure of security mechanisms. It is important that SS Ltd. understand the risks associated with the use of technology and information management and take a positive approach to this subject by an awareness amongst employees of the importance of information security, understanding the typology of threats, risks and vulnerabilities of specific environments and applying computerised control practices and policies.

The report will identify and evaluate the security risks to the organisation. Alongside this, it will also analyse the organisational security procedures. A risk assessment method and impact of data protection law and regulations will be discussed along with the physical security issues of the organisation. The report will draft the security policy and identifies the area identification of improvements and impacts. Human resources and security auditing related impacts of the new policy will be discussed. The report will use the case study of SS Ltd for better understanding.

To achieve an efficient security program requires policies, procedures, practices, standards, descriptions of duties and responsibilities of service, as well as the overall security architecture. These controls should be implemented to achieve the specific objectives of security and in general of the organisation.

It is important that each organisation be able to identify their own safety requirements. For this it must appeal to the three main sources:

* risk analysis
* existing legislation
* standards and internal procedures

The first step will be to evaluate the potential risks of the newtork security for SS Ltd..

# Task 1 Understand Risks to IT Security

## Identify and Assess Business Risks Generally and Specifically for SS Ltd

Risk management facilitates the efficient and effective achievement of the objectives of the organisation. Potential attackers are people within the organisation and accidents, or natural disasters are the main sources of risks to information systems. External factors are also an important source of risk because they are, in some cases, more motivated and harder to detect and investigate than people in organisations.

The security risk is the threat or vulnerability that may materialise at a time. Threats come from different directions: from an attacker who knows what they want to achieve; from bad or poorly configured applications; from users who exceed their duties. Threats sometimes become attacks.

### Security Risks for Physical Resources

An attacker who has access to the physical resources - computers, buildings, server rooms - could penetrate very easily the network and might have access - by default - to the confidential information and business secrets of the organisation (Peltier, 2016).

The protection software is no longer sufficient if the attacker will have physical access to computers or the network components. For this reason, the following protection should be in place: all the organisation’s buildings, internal areas of the company's buildings, network connections, hardware. Without the physical protection, the attacker might load a Trojan Horse program to send typed characters (primarily passwords) somewhere to a location on the Internet.

The usual threats at the level of the physical resources are:

* theft
* installing applications on computers
* subversive sabotage

***Threats Posed to Computers Lifecycle are***:

* initial installation: the lack of antivirus protection, incorrect configurations, weak passwords for staff accounts
* initial security settings: layouts using unverified default layouts
* additional settings, depending on the role of the computer: it could be inaccurate, inadequate, incomplete tested
* applying security updates for operating systems and applications: without serious testing
* close of business, beware of equipment that maintains information on hard disks that can be reused remaining maliciously

### Security Risks to User Accounts

If an intruder attacker gains access to a privileged account, then he gets an authorised access to network resources. Main vulnerabilities for user accounts are:

* Passwords - could be too weak, identical to multiple accounts, unchanged in time, stored locally, on paper and forgotten
* When staff leave the organisation, failing to remove their authorise access
* Privileges - too big and too many users related the tasks and actions
* The use of the accounts - Administrator account used when is not needed, active accounts even if no longer used

### Security Risks to Authenticate the Users

Most common vulnerabilities are:

* passwords transmitted in clear (unencrypted)
* programs to intercept passwords Trojan horse
* older software using weak authentication methods
* weak encryption
* intercepting authentication packets

### Data Security Risks

Potential attackers could, in certain circumstances, to override its permissions to control access to data. The data (information) within an organisation are vulnerable to internal and external threats, mostly through:

* incorrect permissions configuration
* insufficient physical security of data and access to data carriers
* damage to the data (alteration, incorrect encryption)

### Security Risks of Data Transmission

Data is vulnerable when transmitted; the vulnerabilities of the best known in this situation are connected with the execution of malicious operations. The threats to information systems can be classified as follows:

* Direct Threats
* Fundamental threats
* Threats which facilitate

1. ***Direct Threats***

***Disclosure***: Important information that should remain confidential and undisclosed accessed by unauthorised persons or exceed their powers. Since some information has great value, that value will be considerably reduced or lost through breach of confidentiality, this type of attack can have adverse consequences and be extremely serious for SS Ltd.

***Altered information:*** Information is entered into the system without authorisation, modified or overwritten by any unauthorised person (or people paid by unauthorised persons) or exceeding their powers. Due to the fact that some decisions or actions depend decisively on information from this type of attack this presents a great potential danger for the company.

***Repudiation:*** The ability of a person or action to deny the identity of a sender, content or time of communication or transmission of an electronic message. It is important that SS Ltd. provides non-repudiation them because messages or electronic communications have great importance.

***Denial of service attacks (DOS):*** attacks of this type consume a computerised information system resources, resources for serving legitimate users. There are two main sub-categories of attacks in this category: logical attacks and flooding attacks.

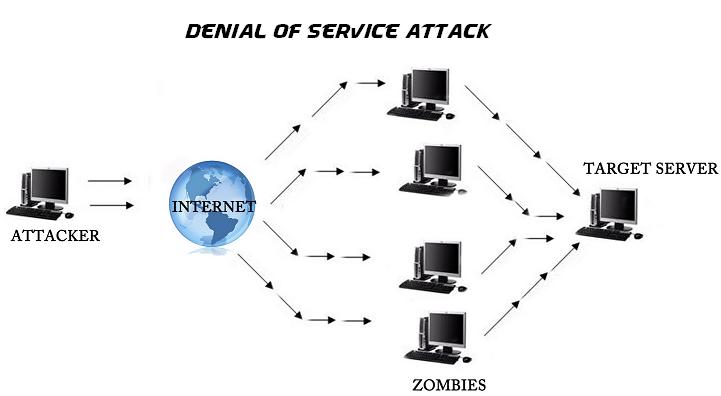


Figure 1 DOS attack

Source: Internet https://www.blackmoreops.com/denial-of-service

***Denial-of-Service Distributed attacks (DDoS):*** This is a type of attack that is used in dozens or even thousands of compromised computers to automate data transmission systems, which can flood the targeted attack. These compromised attacks of computers which are controlled remotely by planting viruses most commonly Trojans Horses, which produces a group of zombie computers. These attacks are dangerous because they are tough to counteract.

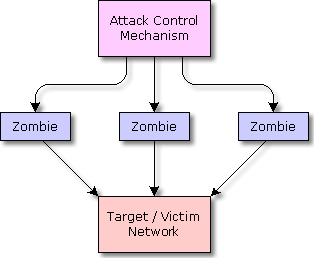


Figure 2 DDOS attack

Source Internet: http://www.understandingcomputers.ca/articles/grc/drdos\_copy.html

***Illegitimate use:*** The information is used by unauthorised persons or for unauthorised purposes. Since some information (research results or details of customers) can have significant value, this action endangers important for the organisation.

1. ***Threats Which Facilitate***

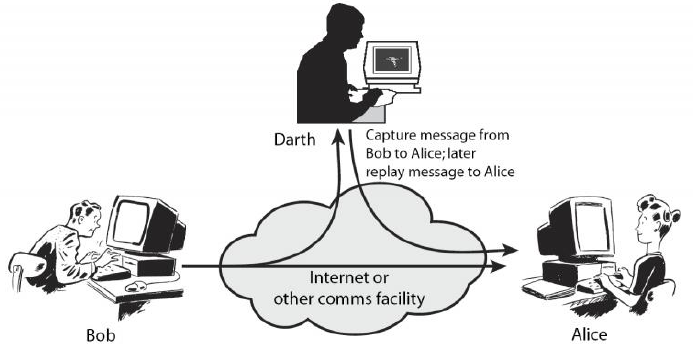
If existing security measures are in place, attackers will not be able generally to jump to the fundamental threats, so they will execute threats that facilitate the positioning. Such issues are risks that provide access to fundamental threats. Facilitating threats can be categorised as follows: masquerade, malicious code, circumvent security measures, violating approval (Bays, 2015) and are discussed in the following subsections.

***Masquerade***: This attack is made at the Network layer of the OSI model.

Authentication of a user identity based upon one or more of the following:

* Something only the user knows (secret password)
* Recognised physiological characteristics of the user (fingerprint, hand geometry, retina scheme, typing rhythm or tone of voice)
* Something the user has exclusively (for example, a card or magnetic chip).

It is possible that attacker assumes IP address of a trusted system and pretends as a valid user to get access to resources and network capabilities. Masquerade attacks allow unauthorised users in networks due to poor identification schemes. SS Ltd has security risk of masquerade attack in wireless connections where most of the devices are identified by their IP addresses and information is saved on the devices to auto authorise them on the network. If the devices lost are locally stored, others occupy authentication detail, then it is possible to have a risk of unauthorised accessed (Cheminod, 2013). However, the internal wired network is limited to IP addresses, and the user also needs to provide authentication. Therefore, the wired network has dual security. There is a high risk of information disclosure in wired devices with masquerade attack.



*Figure 3 Masquerade (Source: Masquerade, 2017)*

***MAC address spooﬁng:*** This is what happens when a villain changes the MAC address in such a way as to match in the MAC address of a device on the network. Allows a hacker to pretend that the hardware belongs to a different person

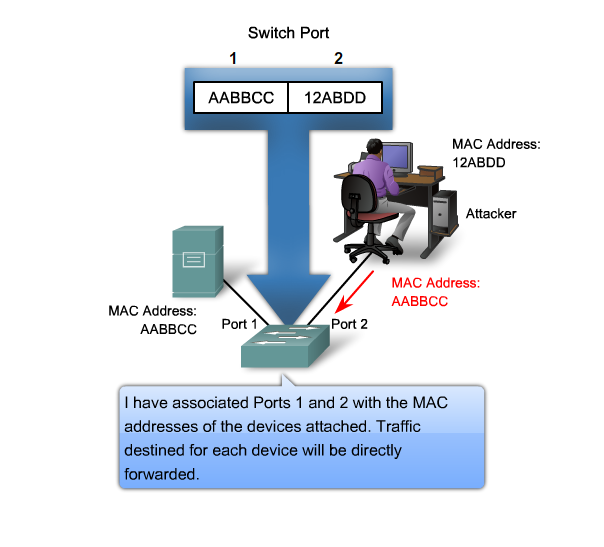


Figure MAC Address spoofing (Source Internet 2007)

***E-mail spoofing*** is the action that the email address of the sender message is altered so that the email would look like it came from another source. Email spoofing is most often used in phishing messages to falsify the origins of the email.

**Backdoors**: This attack is made at the Presentation layer of the OSI model. Security mechanisms of computer information systems are in place to prevent unauthorised access or unauthorised insertion of data or programs. Backdoor is a mechanism that allows access restrictions infringement or writing to disk, allowing violation of confidentiality of the information, unauthorised modification of information, planting Trojans Horses.

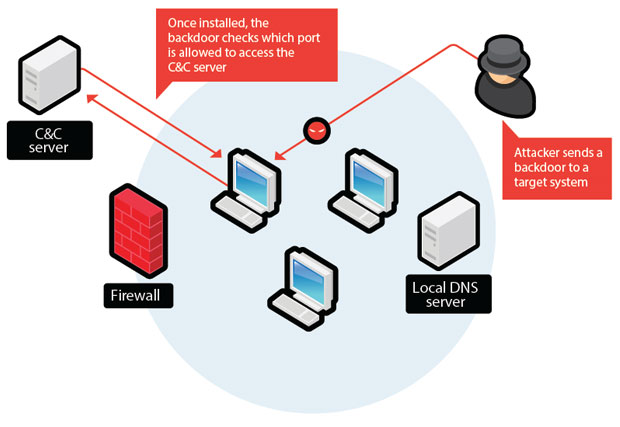
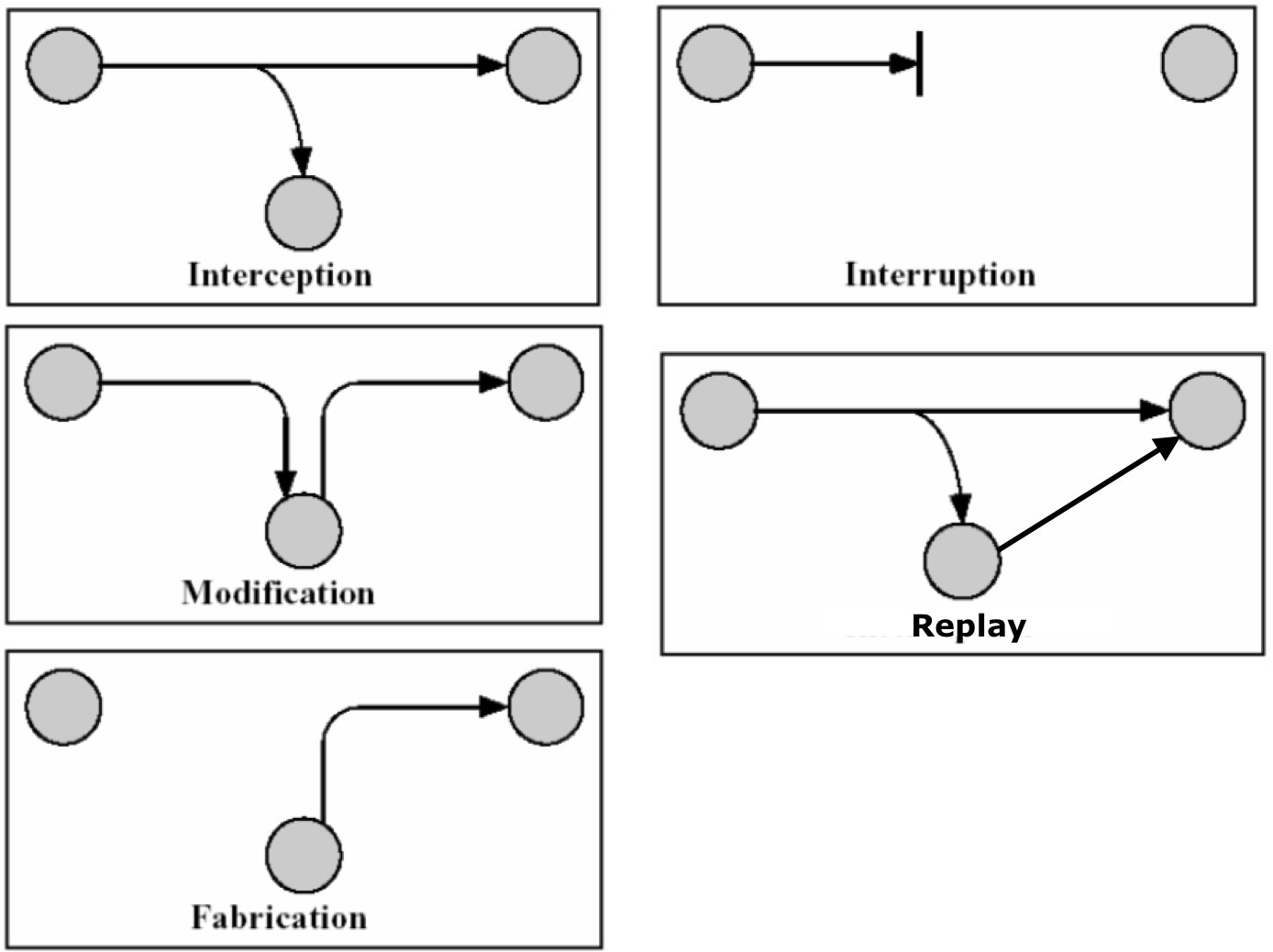


Figure 5 Backdoor attack

###### Source: Internet

***Interception-based attacks -*** Data during the transmission is captured and listened to by attackers to intercept the authentication information of users. Attackers can read, modify or corrupt the information being transmitted in the network. In this manner, financial transactions can be malfunctioned or data can be altered for benefits. **Replay attacks** are also part of interception based attacks in which the data packets of the network are captured and later retransmitted to gain access to user data through the server. Various social and technical approaches can be used to intercept the information (Zhu, 2014). Notably, the addition of new router devices in the network has offered connectivity to mobile devices, but the improper security on authentication and encryption can lead to risks for the organisation.



*Figure 6 Security attack (Source Internet 2007)*

Attackers can influence the wireless router and associated devices due to improper security on passwords. It is possible to capture the user data packets and then replay the same sequence again to obtain the data from the server. The data can be altered in financial tasks due to easy connectivity with wireless routers. If an attacker gets success to intercept the router due to poor security, it is possible to get and intercept the data from associated mobile devices. However, internally wired connections are secure with packet filtering, access control list and dedicated connections with a limited number of IP address only.

***Malicious code -*** Unauthorised user programs and data packets in the network may perform unwanted functions like a collection of keystrokes and transmission to a remote location. Various malicious codes and virus programs need to be treated seriously as they can corrupt or delete the data. The security risk of data disclosure and corruption is high with malicious codes in the network (Peltier, 2016). There is need of firewall systems with adequate filtering to remove the malicious codes. Anti-virus programs are also useful to prevent the malfunctioning and data security compromises.

1. ***Indirect Threats:***

These threats derive from the basic features of the Internet and information infrastructure. The following sub-categories can be viewed in this section: interception, scavenging, indiscretion and administrative error.

***Administrative mistakes***: Errors of administration of a computerised information system (i.e., misconfiguration, keeping a user account on the system after the dismissal of the account holder, setting the wrong authorisations, etc.) can create the possibility of triggering action or obtain unauthorised access unauthorised.

***Interception:*** Programs that allow 'sniffing' passwords (password sniffers, key loggers) monitors and records their usernames and passwords. After obtaining this information, attackers can impersonate an authorised user and access confidential information, alter information or launch different programs or existing orders that can cause damage.

***Scavenging***: This is the use of tools to recreate the information on magnetic media after they have been deleted or overwritten (Mythen, 2014). Another form of this action is looking for information that could be useful in places where the bins or other information printed on paper are thrown (is not shredded).

***Indiscretion***: This category includes actions that lead to the disclosure of passwords or techniques authentication used, leaving the computer without concluding a work session or social engineering - addressing naive attempts at obtaining passwords through techniques like "I need the password X to carry out configuration " or "I forgot my password ".

### Perimeter network security risks

Known vulnerabilities come from that area is the area with the highest exposure to public Internet, remote access, connections with offices (branches, subsidiaries) remote. The vulnerabilities arise through (Feng, 2014):

* intentional or unintentional exposure of information about the network:
* port scanning, TCP / UDP, ICMP perimeter scanning, analysis packages
* incomplete control over the infrastructure: Web servers unauthorised forgotten connections, VPN clients uncontrolled, uncontrolled applications
* voluntary or involuntary exposure to computers: the aftermath of service attacks, display account information, e-mail worms, unauthorised access to data, data destruction.

### Factors that Can Cause Security Risks

The next factors of SS Ltd. company can cause security problems of computer information systems:

***Employees*** - They are invested with trust and have access to the information system, which allows knowing the weaknesses of systems, operations that may be detrimental to those organisations and erasing digital records;

***Consultants / System Maintenance personnel*** - These people often have access to sensitive areas of information system, which allows them to carry out diverse operations;

***Customers*** - Their motives are not economic in some cases congruent with those of the organisation and, in some cases, can perform certain actions that may pose security risks;

***Competitors*** - Other individuals or organisations that will benefit from the losses caused by attacks on the organisation's information system;

***Crackers*** - People who illegally penetrate information systems and intentionally causing damage motivations are different;

***Experts in espionage*** - Persons who are specialised in obtaining information that will benefit other organisations. This person is a high level of technical knowledge, they are well paid and can often perform actions without being detected;

***Accidents/natural disasters*** - this can cause considerable damage to the hardware equipment, to the data and the information.

Most often of the attacks are carried out by respecting the same model:

* ***Fingerprinting*** - at this point the attacker studies the network. The attackers get all the information publicly available about the organisation, leadership, employees, will scan ports on all computers of SS Ltd. have access to all the resources available through the Internet.
* ***Penetration*** - After identifying and locating vulnerabilities are trying, testing and network access to network resources. The most exposed place: the web server.
* ***Assessment privileges*** - after penetrating the network is evaluated the privileges: an attacker will try to gain administrative privileges or system component level.
* ***Possibly trying*** to use a system account to create a new user account with privileges administration. Often the default settings give enough freedom to the attacker to gain access to the network without much effort.
* ***Exploitation*** - after obtaining the necessary privileges, the attacker exploits the situation.
* ***Deleting traces*** - finally, the attacker will try to cover his tracks to not to be detected shares. They will delete the created accounts and relevant journal entries.

## Existing Security Procedures and Security Policy

As it was specified on the assignment records, the network implemented by SS Ltd. is now giving a secure network conditions for the company as well as giving a right answer to the users. However, there is no written security policy to control all the security areas and establish controls that should be followed by the whole staff of the firm.

This part will discuss the SS Ltd needs to provide a Security Policy which should include the following:

### Security Policies

***Description of SS Ltd Responsibilities Following UK Legislation***

The organisation must comply with UK regulations to continue to be legal since it is using a sensitive information; SS Ltd. must follow the next laws and acts:

* UK Data Protection Act 1998
* Regulation of Investigatory Powers Act (RIPA) 2000
* Computer Misuse Act 1990

**Risk assessment**

1. The next risk assessment model comprising the following seven steps:
2. Identification of protected values;
3. Identification of unwanted security events;
4. Determination of the frequency of occurrence of unwanted security events (probabilities, possibilities);
5. Determining the consequences of unwanted events;
6. Establishing solutions to minimize risk;
7. Assessing the effectiveness of implementing risk minimization solutions;
8. Cost/security level determination.

Depending on the size of the cost/security level, the decision to deploy security solutions or resume the evaluation is taken until an acceptable report is provided.

The resumption of the assessment may occur at any stage, depending on the acceptance or non-acceptance of the result obtained at that stage.

The successive loops of the model provide great flexibility in response, but make it difficult to conduct the evaluation process. Therefore, it is necessary to establish a compromise between the accuracy of the evaluation and the time and the assessment forces.

**The policy of confidential information transfer:**

* The policy defines how the confidential data of SS Ltd is handled and transferred to users without being the knowledge and accessibility to attackers. It also defines a set of rules needs to be followed during the transmission (Manhart, 2015). The policy has objective to establish the secure and authenticated connection between users to share the information effectively.

**Network connection policy:**

* The policy clarifies the users, those who can use the specific kind of networks like wired network and wireless. Only the certain specific devices are granted to have wireless connectivity, and each device has to follow the rules to get connected with the internet from the mode of connection.
* The network has high security using firewall and filtering services. All connections are directed towards the network firewall to check their packets for proper encryption and authentication. In the same manner, the incoming packets are being checked at the firewall for their authentication and destination in the network. It helps to achieve the security. Also, the routers and switches are configured to eliminate the attacks of the unwanted request and access to them. The network is effective to close all the open holes in security.
* Wi-Fi access is limited to known users only as WPA encryption is strong enough to prevent the assumptions and brute force cracking to penetrate the network. Intruders also need to know Wi-Fi SSID to connect with the hidden network. Internal mobile users know the SSID and WPA security so that they can connect safely. Encryption helps to prevent the data during transmission, access and sharing.

**Monitoring and logging policy:**

* The policy of SS Ltd for monitoring and logging of network activities has to be established, as the policy is just maintained on computer devices through an administrator account.
* Application and access control policy: the policy defines the access control in network and usages of applications. The policy is effective to set the guidelines and instructions for access control in the network.

**Conditions to use IT services:**

* SS Ltd has the policy to use the resources and IT services of the network to high performance and quality which can be achieved and the resources which can be utilised effectively (Coventry, 2014). The conditions also include the variable for software usages and data migrations through IT services.
* Security is achieved through proper configuration of disabling the USB functionality inside the wired network of the company for possible vulnerabilities as data theft or forming bridges with public Wi-Fi networks.

### Security Procedures

SS Ltd is following two major procedures for the security implementation and monitoring: log duration management and non-standard user accounts expiration. Both procedures are strictly in actions to ensure the security of the network:

***Log duration management***

The duration for which a user account was active in the network is logged so that recovery based activities can be made simple and efficient. Access to particular resources is logged for the time stamp so that security and authentication can be ensured. The inbuilt system in computers to log the information about the user session and events helps the organisation to review the information on demand. The administrative unit of the organisation reviews the monthly report on user sessions and events to determine the permissions and access to certain resources for security reasons.

***Non-standard user accounts expiration***

The security procedure of the SS Ltd uses the concept that the password of standard users should be newer and strong whereas the guest user accounts need to be expired after the specific time. Non-standard user accounts like administrative accounts should need to follow the password policy of the organisation (Jaferian, 2014). The newer password should not be same as previous and must contain alphabets with at least one uppercase letter, one digit and one special symbol along with the minimum length of 20 characters. Every password expires after one month.

# Task 2 Understand mechanisms to control organisational security

## Explain the process for completing a risk assessment and findings for SS Ltd.

The system generates new risks for the organisation to ensure the effective protection of information; it is necessary to develop a complex process of study and analysis of the risks.

Practical the reality requires addressing risk information in the light of three factors: ***threats*** of events or activities (generally outside of the auditory system) that can affect the ***vulnerabilities*** existing in any system causing ***impact***, which has been considered as a loss or a consequence term short, medium or long supported the organisation.

Networking and Internet connection also induce additional risks of unauthorized access to data or even fraud. Ensuring information security cannot be achieved solely through technical measures is primarily a human issue. Most of security incidents are caused by inadequate management and organization, and less due to failure of security mechanisms.

The risk to the organisation cannot be removed; it will always exist a risk, the management of the company is responsible for its reduction to an acceptable level.

In this regard, the below figure put in correspondence different elements that need to be taken into account to reduce the risks:

**Threats**

**Vulnerabilities**

**ulnerabilities**

Impact on Society

Privacy/Integrity/Availability

**Information system assets**

Increase

Reduce

Increase

reduce

Increase

which protect

limited by

causing

cause loss

expose the

exploits

Figure IT risk components for SS Ltd.

increase

Implemented Controlled Measures

In this context, risk information can be characterised by the following elements:

* Threats and vulnerabilities processes and assets
* Impact on assets based on vulnerabilities and threats
* The frequency of threats.

Once identified, the risks must be assessed according to the seriousness of the effects they produce.

The speciality defines risk management as the process of identifying vulnerabilities and threats within an organisation and to develop measures to minimise their impact on information resources. The methodological approach of this process includes the following steps:

* Characterisation of the information system
* Identify the threats
* Identify the vulnerabilities
* Destinations of the hazards and process
* Analysis the existing controls of the system
* Determine the probability of successful threats
* Impact analysis
* Assess the risk and make the decisions of the actions
* Make a record
* Review risk assessment

#### Step 1: Characteristics of the information system

At this stage, the auditor will analyse the activity of collecting information about the information system, information that will cover hardware, software, system interfaces, user’s system, data and applications, important sensitivity data and system to assess the level protection that is needed to be done to ensure the integrity, confidentiality and availability of data.

Most investigative techniques used for collecting this information are questionnaires, interviews, documentation system, the use of scanning tools automatic information system (SATAN is just one example of such an instrument that allows detecting vulnerabilities of a network). The results of this phase will provide a picture of the environment computerised information system boundaries analysed.

#### Step 2: Identify the threats

Risk assessment starts with the identification of the hazards or problems those may damage the desired outcome with network infrastructure. For example, SS Ltd has to find identify the problems within wireless network and routers those can lead the issues of data loss or security breaches in network.

An essential element in this stage is represented by determining the probability of making such threats element to be analysed by the company according to:

* Source of the threat:
* natural (earthquakes, fire, tornado, etc.)
* human (network attacks, unauthorised access to confidential data)
* environmental (long-term power outages, pollution, humidity)
* Potential vulnerability
* Existing controls.

The table below reveals the various sources of threats generated by human actions on SS Ltd. network:

|  |  |
| --- | --- |
| **The Source Threat** | **The Action Threats** |
| Hackers, crackers | System intrusions, hacking attacks, unauthorised system access |
| The computerized crime | Fraudulent acts, actions of spoofing, system intrusions. |
| Terrorism | Penetration of the system, interfering destructively system. |
| Commercial espionage | Penetration of the system, unauthorized access, capture data from an unprotected communication line. |
| Employees attacks | Fraud and errors, data corruption, introducing false data, unauthorized access to the system, introducing viruses, trojans, etc. |

Figure 8 Sources of human threats at an information system

#### Step 3: Identify the vulnerabilities

The aim of this step is to generate a record of system vulnerabilities (flaws or weaknesses) that can be exploited sources of potential threat. In this context for example, it is necessary for SS Ltd. to analyse the vulnerabilities - exemplified threats in a limited way in the table below:

|  |  |  |
| --- | --- | --- |
| Vulnerability | **The source of the threat** | **The action of the threat** |
| The identifier (ID) of fired employees is not removed from the system | Fired employees | Connecting to the corporate network and access its data. |
| Corporate firewall allows access to the system via Telnet | Unauthorised users (hackers, terrorists, fired employees) | Using Telnet allows access to files on the system |
| One partner of the company has identified weaknesses in the design of system security of SS Ltd., the system itself giving the partner various methods to deal with them. | Unauthorised users | Gaining illegal access to sensitive system files, based on well-known vulnerabilities. |
| Automatic data processing center uses sprinkles of water against fire, which may adversely affect the hardware. | The fire, person’s negligence | Automatic activation of the extinguishers of fires. |

Figure 9 Examples of vulnerabilities

#### Step 4: Destination of hazard and process

SS Ltd has to find who will be getting affected from the problems and how the problem will affect the users and organizations to complete their objectives. Let consider that wireless connection related issue may prevent the user to get connected with wired users and overall transactional or informational communication may be constraint (Bahr, 2014). Therefore, the destination and the methods of impact should be clear.

#### Step 5: Analysing the existing controls of the system

In order to minimise or eliminate hazards SS Ltd. has to implement technical or non-technical control methods that may cover:

* Access control mechanisms
* Identification and authentication mechanisms
* Data encryption methods
* Intrusion detection software
* Security policies
* Operational procedures and personnel

#### Step 6: Determine the probability of successful threats

To determine an overall probability rates, indicating the probability that a potential vulnerability be exercised in the model associated with threats, for example SS Ltd. needs to consider the following factors (Bahr, 2014):

* ability and motivation of the source of threat
* nature vulnerability
* the existence and effectiveness of current controls

This element can be appreciated by the qualification "High", "Medium" and "Low" in the following conditions:

* "High" - the source of the threat is highly motivated and sufficiently capable and the checks for the prevention of these exploits are ineffective.
* "Mid" - the source of the threat is highly motivated and sufficiently capable, but the checks can prevent the vulnerability.
* "Low" - the source of the threat is devoid of motivation, or the controls are there to prevent.

|  |  |
| --- | --- |
| Probability of occurrence | Description |
| High | Certainly. Occurs once or several times per year |
| Medium | Probable. Event that may occur at least once or twice or three times a year |
| Low | Unlikely. Event cannot occur in the next three years |

Figure 10 Establishing the probability of risk in the organisation

#### Step 7: Impact Analysis

The financial impact is defined as the estimated value of the entity's losses as a result of exploitation by system weaknesses threats. For example, this impact may have two components related to the risks assessment of SS Ltd.: a short-term impact and long-term impact.

Impact and it can be expressed through qualification "High", "Medium" and "Low".

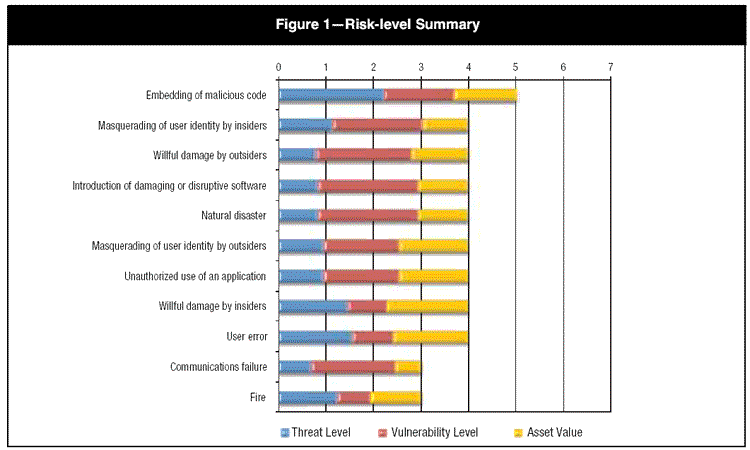


Figure 11 Analysing the impact of SS Ltd.

###### Source: Internet

#### Step 8: Assess the Risk and make the Decisions of the Actions

SS Ltd has to assess the risk strictly and to determine the effective action which can resolve the issue or mitigate its impact on user and regular operations.



Figure Matrices of a risk for SS Ltd.

*Source: Internet*

Organization has to determine the effective actions from the set of solutions towards the problem but it needs high understanding and research with issue.

#### Step 9: Make a Record

The findings of the action implication should be recorded so that same information can be used later to mitigate the impact of such issues in effective time. For example, the organization needs to record the methodology, resources and requirements to deal with particular problem in wireless and wired infrastructure.

#### Step 10: Review Risk Assessment

The step ensures that the actions and practices are in continuous routine to avoid such issues back into organization (Rausand, 2013). It is also required to introduce the new working practices and safety actions on the basis of solutions with particular problems.

## Explain how Data Protection laws affect SS Ltd. and its IT security policy

The organisation must comply with UK regulations to continue to be legal since it is using a sensitive information; SS Ltd. must follow the next laws and acts:

* UK Data Protection Act 1998
* Regulation of Investigatory Powers Act (RIPA) 2000
* Computer Misuse Act 1990

Data Protection Act or laws ensure the valid usage of user information by the organization as the personal as well as professional information of the user cannot be shared, reused and modify without the knowledge of users. Law guides the organizational practices to use the user information fairly and lawfully and to ensure the safe handling and storing of information. In this manner, Data Protections law has following effects on SS Ltd and its IT security policy:

1. ***Sensible data must be honestly and legally adopted***

Accordingly, processing of personal data is legal only if:

* + is in compliance with the law;
  + pursues a legitimate aim

1. ***Sensible data must be applied only when is needed for a particular purpose***

Individual data must be taken only for one or more detailed and legal views and will not be more controlled in any way contrary to that view.

1. ***Sensible data must be handled when is important and never being abused***

Individual data will be fair, appropriate and not unreasonable about the mission for which it is prepared.

1. ***Sensible data must be correct and modernised when is needed***

Private data must be valid and where is needed, stored up to date.

1. ***Sensible data must be collected just for a definite time, as long as is needed***

Any prepared private data for any goal or goals will not be held for larger time than is needed for that plan or those plans.

1. ***Sensible data must be managed based on people’s records protection rights***

Individual data must be treated by the rights of data subjects under Data Protection Act.

1. ***Sensible records must be stored in a protected location***

Private data must be kept in a safety place.

1. ***Delicate records are not a matter of being given outside of European Union without proper security***

Individual data must not be given to a nation or area outside of EEA, except that nation or area guarantees a high level of security for the rights and privileges of data subjects about the processing of individual data.

In this manner, the organization has impact of IT security policies as user data should be protected during sharing and storing process. There is need of adequate security on local storage and web based sharing so that right user and destination can be determined. Non-repudiation is enforced by the Data Protection Act to recover the data and its misuse to the maximum possibility (Vanderdonckt, 2016).

## Consider the physical security issues associated with SS Ltd. IT setup

It will be evaluated according to the information gathered, relating to: existing security systems, fire detection and alarm systems, protection systems against power outages, equipment protection against theft, protection against natural disasters (floods, earthquakes) protection physical storage medium, leaving the backup in a different location than where it operates organization.

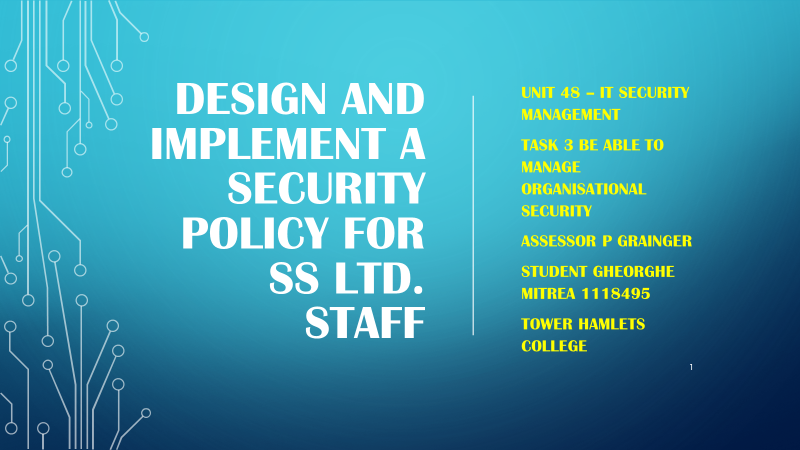
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criterion**  **No.** | **Questions** | **Yes** | **No** | **Comments** |
|  | **Prevent incidents, flooding and power outages** |  |  |  |
| 1 | The environment in which it operates SS Ltd is properly protected against fire:  - There detection systems and fire alarm?  - No automatic fire extinguishing systems?  - The place where the storage medium is fire resistant?  - There are fire extinguishers?  - The staff has been trained on when it should alert the team to prevent incidents? |  |  |  |
| 2 | The reports on the occurrence of incidents are provided by the management? |  |  |  |
| 3 | The equipment is protected against floods? |  |  |  |
| 4 | There are protection systems against power outages? |  |  |  |
| 5 | Systems and technical equipment are secured against theft? |  |  |  |
|  | **Physical factors and facilities** |  |  |  |
| 6 | Is it controlled the physical access to the IT department? |  |  |  |
| 7 | There is a place to protect the storage medium outside the company headquarters? |  |  |  |
| 8 | There are procedures on how to store confidential information? |  |  |  |
| 9 | The programming documents, system is stored in a safe place with restricting access by unauthorised persons? |  |  |  |
| 10 | The backups of the documentation are in a safe place? |  |  |  |
| 11 | Are the servers in a separate room? |  |  |  |
| 12 | Is the communication equipment properly protected? |  |  |  |
|  | **CONTROL ACTIVITIES AFTER WORK PROGRAMME** |  |  |  |
| 13 | There is one level of control after the end of the program? |  |  |  |
| 14 | Are computers secure after hours’ work? |  |  |  |
| 14 | Are secure the keys and the access cards? |  |  |  |
| 16 | Are monitored the teams of cleanliness and maintenance? |  |  |  |
| 17 | There is a log to identify the persons who had access to the computer system outside of office hours? |  |  |  |

Physical security of the network of SS Ltd is good to meet the requirements of the organization but from the point of external users and attackers. Following are key physical security issues associated with IT infrastructure of organization:

* *Security of components*: SS Ltd has used servers, switches, routers and workstations to enhance the connectivity and internet sharing but there is no physical security as the resources are open to be accessible from any one. The data as well as values of the resources may be compromised by external entities by doing damaging activities. Organization has to protect the resources from physical access of unauthorised users and external entities by using wall mounts, locks and racks. Server rooms are not isolated from network so their issue of access and modification in files those are concurrently shared among users.
* *Issue with portable:* storage drives are portable in network so that the network has issue of theft (Peltier, 2016). Portable devices in network need proper surveillance and monitoring for the resources. Addition to it, the workstations in network needs to protect the computers from accepting the portable drives and storage devices to prevent the theft of data.
* *Lack of surveillance*: physical devices in network need surveillance so that theft and damage can be prevented (Feng et.al, 2014). For example, monitoring of resources helps organization to know the issues like fire and theft in workplace and helps to prevent from extension to other devices.

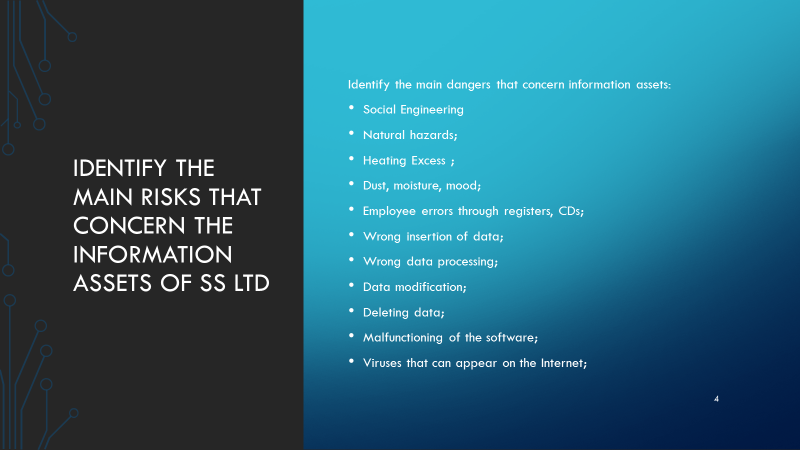
# Task 3 Be able to manage organisational security

## Draft for security policy

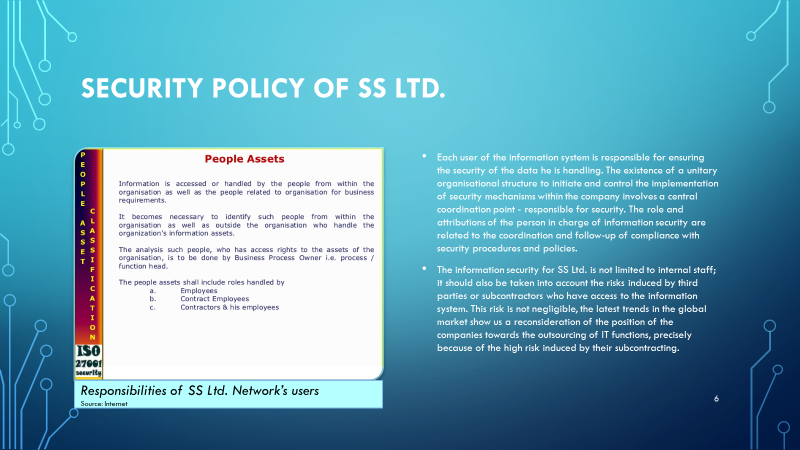




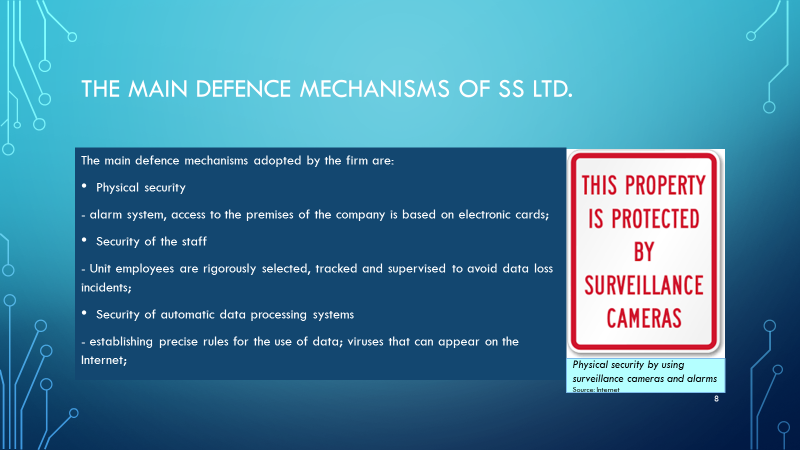




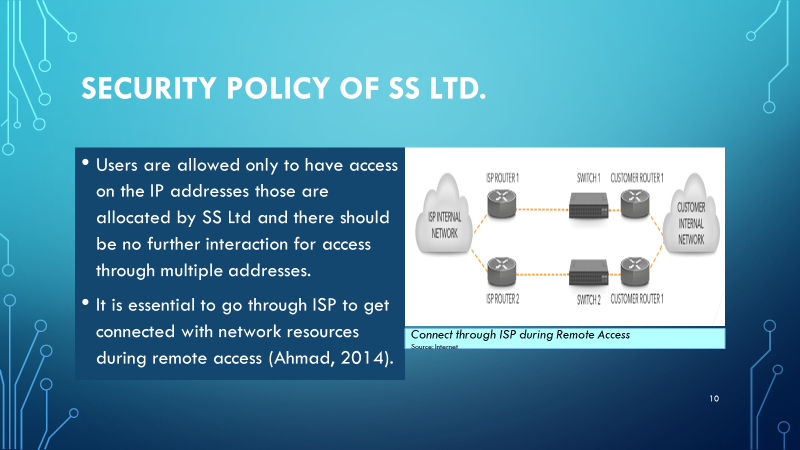




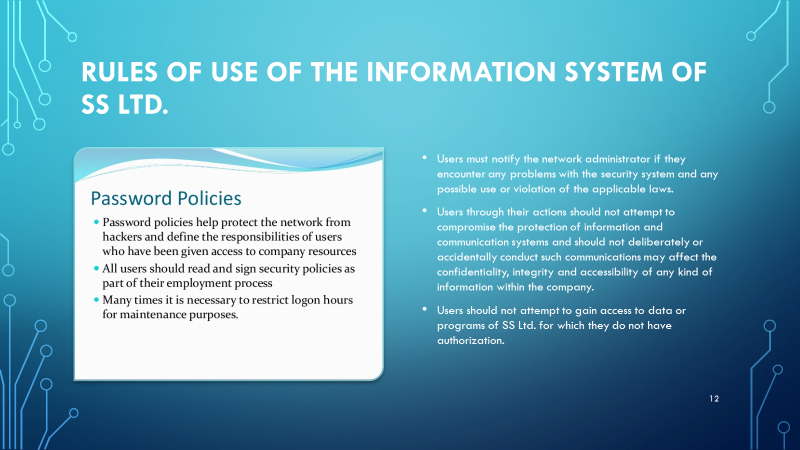


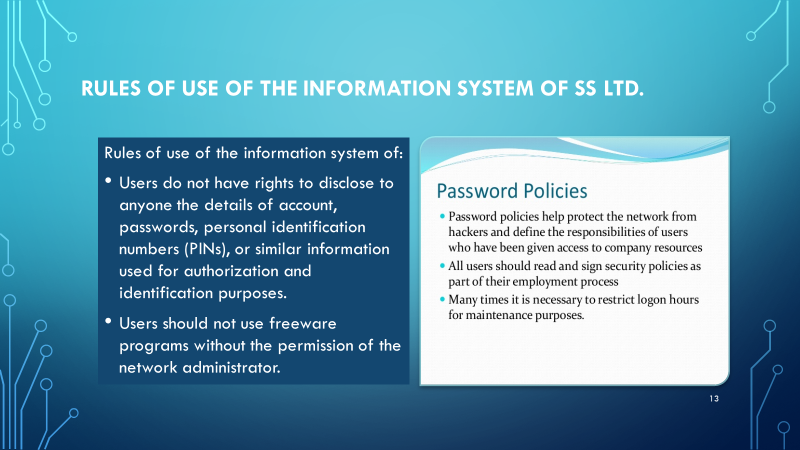


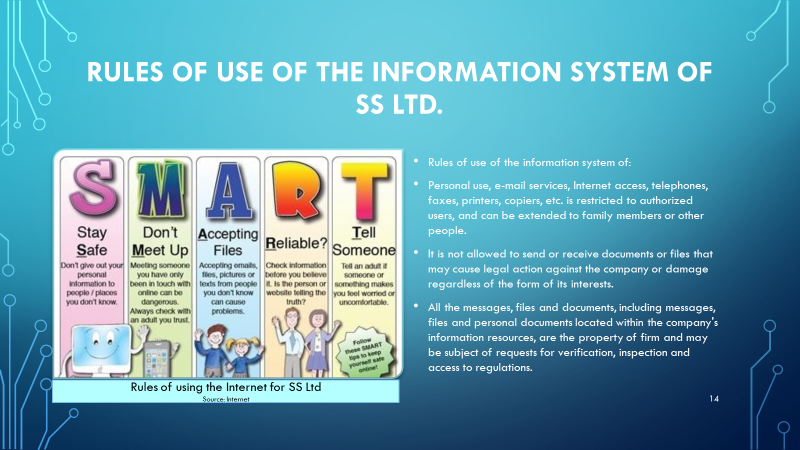


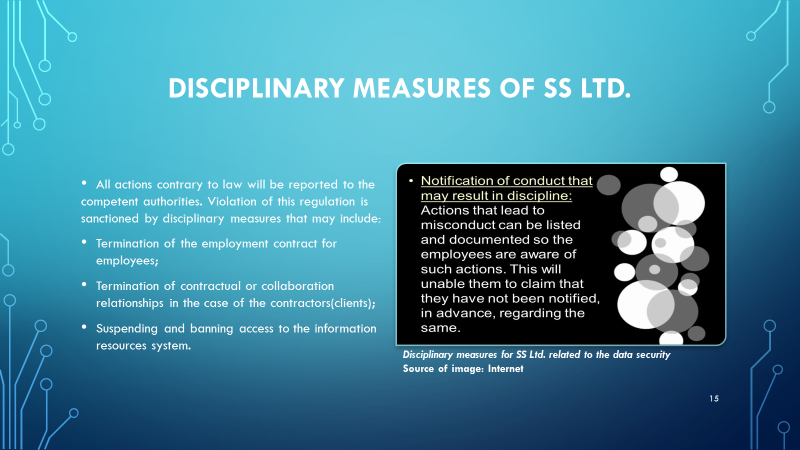


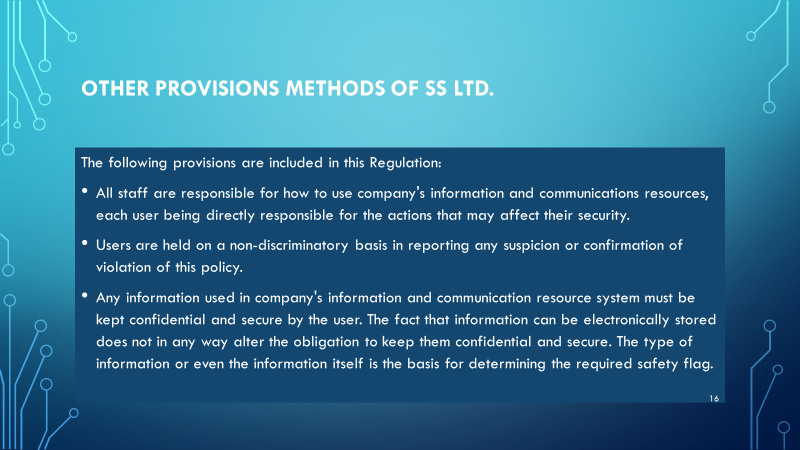


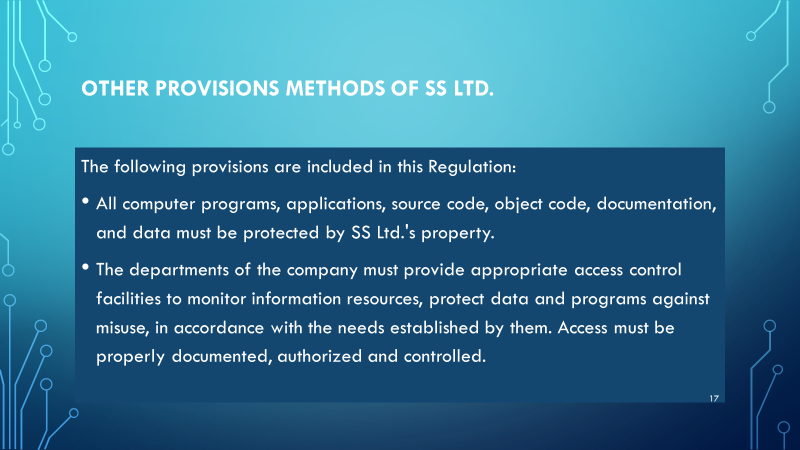












## Evaluate the suitability of the tools used in an organisational policy

### Draft in detail and further improvements

The draft is designed to guide the users and technical staff in implementation of network computers for security implementation. The policy clearly defines the practices that need consideration for the security and access to resources. The draft policy defined many activities like access and installation of resources, modification in network services and products and usage of remote access from external sources. The policy strictly ensures that the activities towards the access and modification in network should be under the pin of control of authority in SS Ltd. Network access standards define the practices those can be used during the communication with external network device (Botta, 2014).

***Security policies***

The information security program policy is the roof under which technical security policies, standards and enforcement rules will be implemented. Here are some of the company's security policies:

***Information protection policy***

Through such a policy, users are made aware of the conditions for the processing, storage and transmission of sensitive information. The primary purpose of this policy is to ensure that the information is properly protected against unauthorized modifications or disclosures.

***Password management policy***

It is often the heart of security policies in an organisation. As a rule, it regulates the expiration of passwords, their length, and other necessary checks. Here are some recommendations to be surprised by such a policy:

* + the minimum length of a password must be at least eight characters long;
  + the password should not be a word in the dictionary;
  + it must be a combination of special letters and symbols;
  + the password must expire after a predetermined period;
  + network administrator passwords must expire much faster and need to be longer;
  + organisational passwords must be different from those used in other systems.
  + a list of old passwords must be kept preventing reuse (the last six passwords must not be repeated);
  + new user passwords must be unique and hard to guess.

***Internet usage policy***

The Internet use policy often referred to as the Internet Acceptable Use Policy (IUPA), is the document detailing how the users of SS Ltd.'s network must use the public Internet service. The policy will describe the software used for filtering and blocking to protect the organisation, but also the specific activities allowed, as well as who are the beneficiaries of these access rights and to whom it is forbidden.

1. *Electronic mail*

This refers to all the company's email forms, defining what is acceptable to use, declaring the software used for filtering and scanning. It should highlight the specific requirements for non-email data and the procedures to follow if a user receives messages of this kind. This policy should also provide for measures taken in the event of non-compliance with the conditions for the use of e-mail;

1. *Searching the Web*

The policy will provide specific conditions for Web traffic. As long as WWW (World Wide Web) uses the HTTP (HyperText Transport Protocol) to transfer information, this policy will clearly define the types of websites that are strictly forbidden, such as porn, gambling, and so on.

1. *FTP*

By allowing users to access File Transfer Protocol (FTP), it opens the way for easily downloading viruses into the organisation's system, as well as transmitting confidential information to servers outside the organisation. Organization FPs must be provided with an FTP access level for file downloads to update existing software, but this policy must establish FTP usage permissions;

***SS Ltd. User obligations***

User is bounded in certain actions towards IP addresses and changes in products and services to implement the security. The objective behind the policy is to enhance the services in network and to make the users liable for the performance, quality and reliability in network. Access factor is focussed in network policy to guide the users toward standard practices.

A final user is considered any person, operator, employee, outsider, who uses the information. He is considered a data consumer who needs daily access to information to fulfil his service obligations.

User obligations are:

• follow the operating procedures defined in the organization's security policies and comply with the published rules on the use of information;

• pay full attention to the maintenance of information during the activity performed, as stipulated in the policies for the use of information issued by the owner organization. They must ensure protection against unauthorized access to classified information;

• to use the company's information resources only for the purpose of it, not for personal purposes.

Access control in the system is implemented to reduce the risk to systems and reduce possible losses. Control can be preventive, detective or corrective.

Controls aim at empowering people accessing sensitive information. Accountability is accomplished through access control mechanisms that also require the use of identification, authentication and auditing functions.

The controls must be in full compliance with the organisation's security policy and the insurance procedures are designed to demonstrate that the control mechanisms implement security policies for the whole life cycle of the information system correctly.

Controlling a user's access to an object involves establishing access rules. These rules can be categorised into three categories or models: mandatory access control, discretionary access control, and non-discriminatory access control.

The security system has to discern who is the authorised person, who are the visitors and who are the unauthorised categories. Authentication can be done by the security body, other access control or automated systems.

The firewall policy used to control access and the routes that the information circulates;

### Further improvements and development

Feedbacks are collected from the users and technical staff of the organization in which it is noted that the network security and access policy needs some changes as shown below:

* Firewall usage: users are expecting to secure the network access through firewall when they are connecting to external environment. Therefore, it is recommended to improve the firewall system for the network so that users simultaneously can access the network resources as well as firewall rules. It is required to improve the security and access. In order to manage the external environment and SS Ltd network interaction, it is suggested to use the access control list and filtering for authenticated users.
* The network can be extended to support multiple platforms so that policy can grant the users to have connection with various mobile devices like laptops, smart phone and tablets (Aromaa, 2016). Policy has to modify for the user interaction through wireless connections.
* Financial transaction: it is recommended to use the wired network connection for the transaction and to ensure that the firewall rules and policies are available to protect the user transaction.

## Impact of security policy

Human resources and security auditing approaches of network gets the influences of security policy as it defines the constraints as well as freedoms of the users to interact with the network. SS Ltd has impact in the form of training of employees for new rules, guidelines and practices to monitor the implementation and improvements in outcomes (Zadek, 2013). Human resources have changes in their practices to meet the objectives of communication, remote access and data management. Employees of the organization have to understand their rights and roles to interact with hardware, software and their operations in network. At other side, the security auditing team has to know the breaches and threats to security policy from the employees’ interaction. Auditing team has to identify attacks those are possible in network to have access in resources and data. Data sharing and effectiveness of the network access management also needs to be measured effectively by the auditing team. Overall impact is positive on the organization to make network secure and reliable.

# CONCLUSION

The report has been identified and evaluated the security risk and existing security procedures for organization. The report has been competed the risk assessment and determined the key findings. It has been discussed how data protection law affects organization and how physical security issues are occurring in network. The report has been drafted the security policy and discussed in depth for further improvements. It has been forces how security policy affect the human resources and security auditing.

##### Bibliography

Ahmad, A. B. R. a. S. R., 2014. *Protecting organizational competitive advantage: A knowledge leakage perspective.,* s.l.: Computers & Security, 42, pp.27-39..

Aromaa, S. a. V. K., 2016. *Suitability of virtual prototypes to support human factors/ergonomics evaluation during the design.,* s.l.: Applied ergonomics, 56, pp.11-18..

Bahr, N., 2014. *System safety engineering and risk assessment: a practical approach,* s.l.: CRC Press.

Bays, L. O. R. B. M. G. L. a. M. E., 2015. *Virtual network security: threats, countermeasures, and challenges.,* s.l.: Journal of Internet Services and Applications, 6(1), p.1..

Botta, A. D. D. W. P. V. a. P. A., 2014. *On the integration of cloud computing and internet of things.,* s.l.: n Future Internet of Things and Cloud (FiCloud), 2014 International Conference on (pp. 23-30). IEEE..

Cheminod, M. D. L. a. V. A., 2013. *Review of security issues in industrial networks.,* s.l.: IEEE Transactions on Industrial Informatics, 9(1), pp.277-293..

Coventry, L. B. P. J. D. a. v. M. A., 2014. *Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment,* s.l.: In International Conference of Design, User Experience, and Usability (pp. 229-239)..

Feng, N. W. H. a. L. M. 2., 2014. *A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis,* s.l.: Information sciences, 256, pp.57-73..

Jaferian, P. H. K. S. A. V.-R. M. a. B. K., 2014. *Heuristics for evaluating IT security management tools,* s.l.: Human–Computer Interaction, 29(4), pp.311-350..

Layton, T., 2016. *Information Security: Design, implementation, measurement, and compliance.,* s.l.: CRC Press..

Manhart, M. T. S. a. M. R., 2015. *The Ends of Knowledge Sharing in Networks: Using Information Technology to Start Knowledge Protection.,* s.l.: In ECIS.

Mythen, G., 2014. *Understanding the risk society: Crime, security and justice,* s.l.: Palgrave Macmillan.

Panko, R., 2004. *Corporate Computer and Network Security, 2/e.,* s.l.: Pearson Education India.

Peltier, T., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management,* s.l.: CRC Press.

Peltier, T., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management.,* s.l.: CRC Press.

Rausand, M., 2013. *Risk assessment: theory, methods, and applications (Vol. 115),* s.l.: John Wiley & Sons.

Vanderdonckt, J., 2016. *Accessing guidelines information with SIERRA,* s.l.: In Proc. of IFIP Conf. on Human-Computer Interaction Interact (Vol. 95, pp. 311-316).

Zadek, S. E. R. a. P. P., 2013. *Building corporate accountability: Emerging practice in social and ethical accounting and auditing.,* s.l.: Routledge..

Zhu, M. a. M. S., 2014. *On the performance analysis of resilient networked control systems under replay attacks,* s.l.: IEEE Transactions on Automatic Control, 59(3), pp.804-808..