Tutorial 2 - Risk management (2.5%)

Due date: 19 August 2020,

Group members: Jaimee Mullins, Sanjana Manocha, Alex Jackson, Harrison Compton, Lavanya Sajwan

XYZ Company

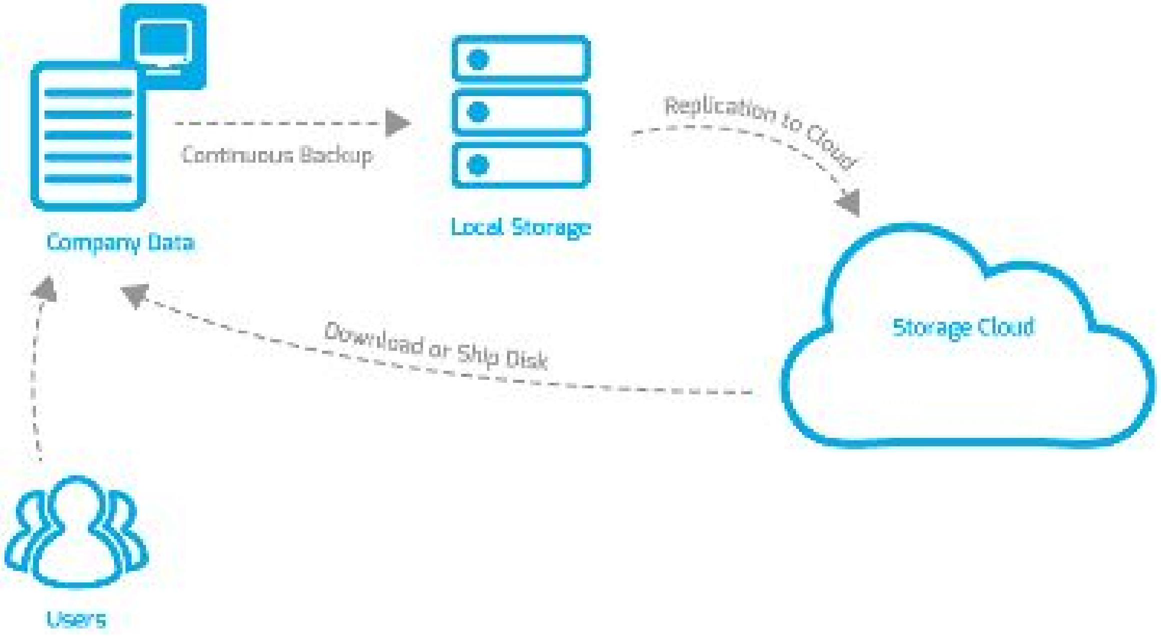
Figure 1 depicts the user access and backup processes for XYZ Company. XYZ employees can access the company's files and documents from their **local designated systems** within the company's office. **Employees** can only read the **documents** uploaded by the management and the system administrator and, shared with the rest of the company. Employees are however not allowed to modify those documents. There is "common" **folder** in which each employee is assigned a designated folder which can be used to store **files** of their own. The "common" directory has a sticky bit permission set.

Each employee is issued a username and a randomly generated password by the system. Employees are not allowed to change their passwords. The passwords are automatically changed every 6 months and employees are informed of the changes. The XYZ Company does not allow remote access to its files and resources. All employee PCs run on Windows 10 and updated regularly and use the built-in firewall and antivirus. The designated PCs do not provide **local storage**. **All files are saved on a network attached storage system (NAS)** installed within the office in a locked and secured cabinet. **This storage is referenced as local storage within the company. The company has a contract with "ADrive" (https://m.adrive.com/) cloud backup and storage service** by which the XYZ Company **updates synchronizes the NAS drive with the cloud storage every day at 6 pm when the company's office is officially closed**. In case any issue with the **local storage** arises, **the synced files can be downloaded from the cloud storage provider and/or can be shipped using tapes and through postage** depending on the scale of the recovery and the size of the data.

Tasks and submissions:

Create a word document which includes the following tasks. The document should include the full name of the group members and submitted individually by each member, using the submission system on the course website.

1. Identify all the assets of the depicted information system
2. Identify all the threats and vulnerabilities in the system and using domain knowledge, assign qualitative ranking ((including definition of the ranking system)
3. Create a risk register with appropriate entries including current and proposed controls
4. You may use the provided classification, ranking system and risk matrix where appropriate
5. You may use the provided template as part of the assignment 1 to complete this work


Company Data
Continuous Backup
Local Storage
Replication to Cloud
Storage Cloud
Download or Ship Disk
Users

Overview of XYZ Company’s Information System

Value	Description
Confidential	Used for the most sensitive corporate information that must be tightly controlled, even within organisation. It requires a greater level of protection.
Internal	Used for Information that can be viewed by internal employees, authorised contractors and third parties. It requires less level of protection than Confidential.
External	Used for information that has been approved for public release or use. It requires proportionately less protection than Confidential and Internal.

Likelihood	Description
Certain	It is easy for a threat to exploit the vulnerability
Highly probable	It is feasible for a threat to exploit the vulnerability.
Possible	It is achievable for a threat to exploit the vulnerability.
Possible but unlikely	It is feasible but would require significant skills or resources for a threat to exploit the vulnerability.
Almost never	It is difficult for a threat to exploit the vulnerability.

Impact	Description
Severe	There is economic loss. There is loss of life. Legal liabilities and/or breach of SLAs. There is loss of corporate or public image. Communications and recovery must be shared with customers.
Significant	It causes major disruption of business operations. There is loss of corporate or public image. There are additional costs involved. Communication and recovery is shared with customers.
Moderate	
Minor	
Minimal	

Categories	Description
Hardware	Systems and peripherals, security devices, data centres, networking components
Data	Information transmission, processing and storage, databases, hardcopy, intellectual property
People	The organisation's colleagues or employees or contractors
Procedure	IT and standard business
Software	Applications, Operating systems, security components

Classification	Description
Confidential	Used for the most sensitive corporate information that must be tightly controlled, even within organisation. It requires a greater level of protection.
Private	Information that can be viewed by internal employees, authorised contractors and third partie It requires less level of protection than Confidential.
Public	Used for information that has been approved for public release or use. It requires proportionately less protection than Confidential and Internal

Impact	Severe	15	19	22	24	25
	Significant	10	14	18	21	23
	Moderate	6	9	13	17	20
	Minor	3	5	8	12	16
	Minimal	1	2	4	7	11
		Almost never	Possible but unlikely	Possible	Highly probable	Certain
		Likelihood				

Asset ID	Asset Name	Category	Classification	Loss of Confidentiality	Loss of Integrity	Loss of Availability
001	NAS (network attached storage)	Data/Hardware	Private	High, if compromised lots of information could be leaked	High, if tampered with in terms of hardware or digitally	High, the company will likely rely on a lot of this data so they will not be able to operate
002	A Drive (cloud)	Data/Hardware	Private	High, if compromised lots of information could be leaked	High, if tampered with in terms of hardware or digitally	High, the company will likely rely on a lot of this data so they will not be able to operate
003	Engineers	People	Public	Medium, some employees may leak more information than others	Low	Medium, losing employees to other companies
004	CEOs	People	Public	Medium,	Medium	Medium
005	Tapes	Data/Hardware	Private	Medium to high, these tapes could be intercepted and leaked	Medium, the tapes could be intercepted and tampered with	Medium, tapes could be stolen before reaching destination
006	PC's	Hardware	Private	Low to medium as they can only be accessed onsite and not remotely. So for someone to gain access they have to be within the site grounds.	Low to medium as someone would likely have to break in to tamper with these PCs	Low to medium because most of the important sotarge should be on the cloud

007	Local Storage	Hardware/ data	Private	High, as someone could be storing personal information which they only want on their computer	High, if accessed by a third-party, in terms of hardware or digitally.	High, employees will not be able to access their own files and projects that aren’t backed up
008	Employee Username and Passwords	Data	Confidential	High, could provide insights to other password in the company	High, if accessed by an unauthorised individual as they could log on to an employee’s account	Low to medium as they would have to get their password reset
009	Personal Employee Details	Data	Private	Medium, could reveal company secrets	N/A	N/A
011	Documents	Data	Private			
012	Shared files	Data	Private			
013	Continuous backup	Procedure	Private			High because if data gets corrupted then it is non-recoverable
014	Download	Procedure	Private			
015	Shipping of the Tape	Procedure				

Key	Low	Medium	High
	0.1 - 0.4	**0.5 - 0.7**	**0.8 - 1.0**

Asset ID	Asset Name	Impact to time	Impact to profitability	Impact to public image	Weighted score
001	NAS (network attached storage)	High	0.8	0.8	
002	A Drive (cloud)	Medium-High	0.8	0.8	
003	Engineers	High	0.5	0.5	
004	CEOs	Very High (explain)	0.8	1	
005	Tapes	Medium	0.4	0.4	
006	PC’s	Medium	0.4	0.5	
007	Local Storage	Medium	0.4		
008	Employee Username and Passwords	Low		0.9	

009	Personal Employee Details	Medium-High		0.8	
010	Documents	Medium		0.5	
011	Shared files	Medium	0.6	0.5	
012	Continuous backup		0.5	0.2	
013	Download		0.4	0.2	
014	Shipping of the Tape		0.3	0.5	
015					

Asset ID	Threats and Vulnerabilities	Gross Risk			Existing safeguards	Recommended Controls	Residual Risk		
		Impact	Likelihood	Risk Rating			Impact	Likelihood	Risk Rating
001									
002	Technological Obsolescence - Bad cloud technology.								
003	Risk of human error - employees and contractors can potentially cause issues in the system just as failure of backup or leakage of documents.								
004	Risk of human error - cause issues in the system just as failure of backup								

	or leakage of documents.								
005									
006									
007									
008									
009									
010									
011									
012									
013									
014									
015									