Tutorial 1 - Risk management (3% total)

Due Date: 28 July 2024
Weight: 3% of the final grade (1% group work + 2% individual work)
Submission: ECS Submission System

Student's full name: Thomas Green (300536064)

Other group members' full names: Did not attend tutorial

Instructions and Tasks:

- In groups of four (4), complete the group work tasks below.
- Document your answers and **submit it together with your own answers to the individual work**, using the submission system on the course website. Name the document as YOURSTUDENTID.docx/pdf
- **All members will be receiving the same mark for the group work.**

---

1. **Group Work [1 Mark]**
   A. **[0.5 Mark**] Define impact and ranking criteria. You may use the provided classification, ranking system and risk matrix if applicable.
   B. **[0.5 Mark]** Identify all the assets of the depicted information system
2. **Individual Work [2 Marks]**
   C. Identify all the threats and vulnerabilities in the system using your domain knowledge and assign qualitative impact and likelihood rankings

***Asset valuation and classification is missing from this template and is not required for this tutorial session only. They are however crucial part of a risk assessment process.

XYZ Company Case Study

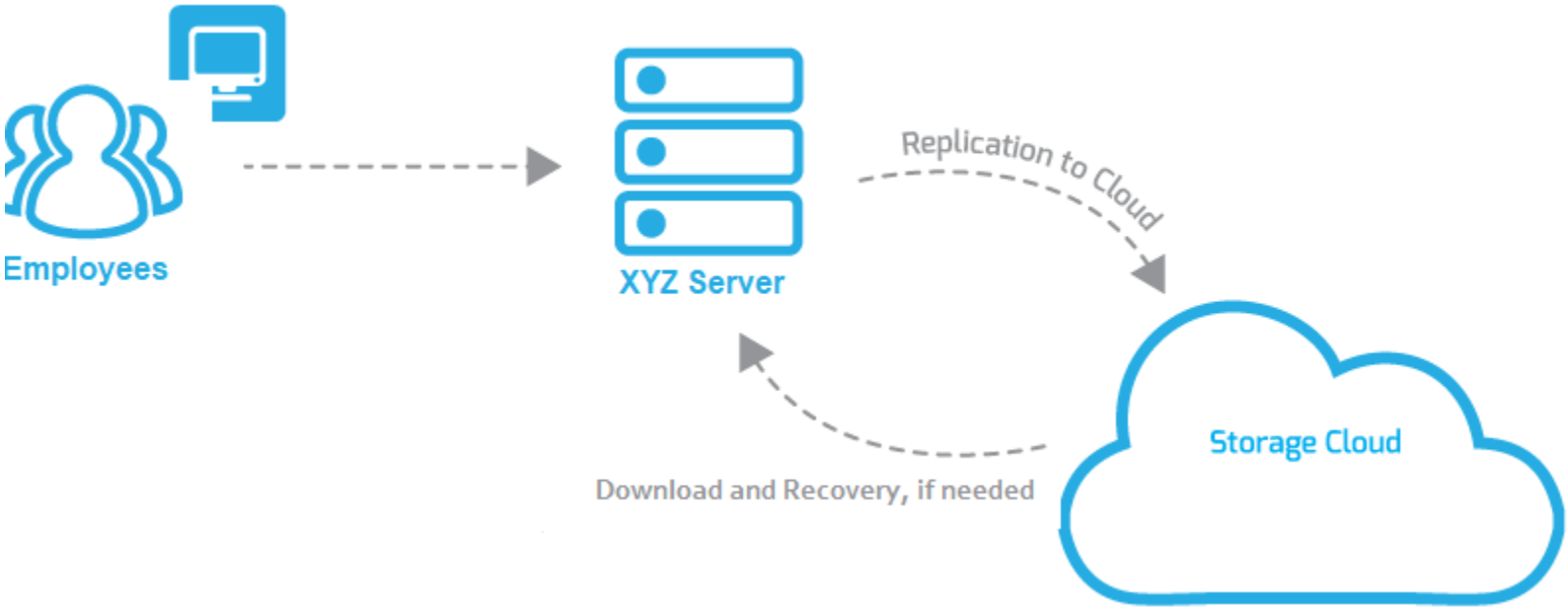
Figure 1 depicts the user access and backup processes for XYZ law firm Company. XYZ employees can access the company's files and documents (legal forms, legal documents) from their local designated PCs within the company's office through a network mapped folder (called **Legal Files**) which is mapped to a folder on **xyz server**. Employees can only read the documents uploaded by the CEO and the system administrator and, shared with the rest of the company. Other employees are however not allowed to modify those documents.

The server was purchased from Dell (https://www.dell.com/en-nz/work/shop/cty/pdp/spd/poweredge-r7515/per7515tm0112nzoo). The server is secured in a locked cabinet which is also fixed to the floor.

Employees access to the office is monitored by Bob who is the security guard and receptionist at the company. Bob has a desk in front of the main (only) access door to the office. Employees have access to their own desktop PCs at the company's office. They have a limited/restricted account on their Desktop PCs which means they are not allowed to install/remove any applications, disable services, change firewall settings or change any operating system settings and configurations. They can write to their own user account folder (e.g. C:\users\<username> which includes subdirectories such as Desktop, Documents and Downloads"). Employees have full access on their user folder and subfolders (similar to home directory for a user on Linux).

Each employee is issued a username and a randomly generated password by the administrator to access their desktop PCs. Employees are allowed to change their passwords (8 letters, must include a capital letter). All employees (excluding the CEO and administrator) are forced to change their passwords every 6 months.

The XYZ Company does not allow remote access to its files and resources. All employee PCs run on Windows 7 and updated regularly and use the built-in firewall and antivirus. The company has a contract with "ADrive" (https://m.adrive.com/) cloud backup and storage service to ensure company's data are backed up in case of an incident or a disaster. A script file on the XYZ server executes automatically at 11:59 pm every day and synchronizes the server's data with the cloud storage service.



Overview of XYZ Company's Information System

Ratings, rankings and criteria definitions

Likelihood	Description
Certain	It is easy for a threat to exploit the vulnerability without high-level skills or resources. The threat occurs frequently. No current control in place to prevent or detect threats.
Highly probable	It is feasible for the threat to exploit the vulnerability with minimal skills or resources. The threat is likely to occur frequently. Current control is in place but unlikely to prevent or detect threats
Possible	It is feasible for a threat to exploit the vulnerability with moderate skills or resources. The threat is possible to occur. Current control is in place and can prevent or detect threats
Possible but unlikely	It is feasible for a threat to exploit the vulnerability but would require skills or resources for it to occur. The threat is unlikely to occur. Current control is in place and makes it unlikely for threats to occur.
Almost never	It is difficult for the threat to exploit the vulnerability. The threat is not expected to occur. Current control is in place and makes it not expected to occur through prevention and detection

Impact	Description
Severe	The company suffers severe corporate and public damage that is not easy to recover from. There is a loss of life public and/or staff. There is a severe H/S incident involving the public and/or staff. Legal liabilities and/or breach of SLAs. Severe economic loss. Severe risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without external funding. Communications and recovery must be shared with customers/stakeholders. Disruption of operations requires severe recovery efforts.
Significant	The company suffers significant corporate and public damage. There is a significant H/S incident involving the public and/or staff. Significant Economic Loss. Potential legal liabilities and/or of SLAs Significant risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without re-prioritisation of internal processes.

	Communications and recovery must be shared with customers/stakeholders. Disruption of operations requires significant recovery efforts.
Moderate	The company suffers limited corporate and public damage. There is a significant H/S incident involving staff and/or limited public. Moderate Economic loss. Possible legal liabilities and/or SLAs. Moderate risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without re-planning some internal processes. Disruption of operations requires moderate recovery efforts.
Minimal	Reputation is not affected from a corporate/public standpoint. No loss or significant threat to health and safety involving staff and/or the public. There is minor economic loss. Limited risk impacting company objectives, service delivery, and productivity. The impact can be managed with current resources and no re-planning. Minor disruption of operations, quick recovery

Risk rating matrix

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 inventory and categorization

Provide at least 9 entries (excluding the example provided).

Asset ID	Asset Name	Category	Other Information?
001	Server	Hardware	Manufacturer: Dell Model: PowerEdge R7515 Price: 22,000 Processor: AMD EPYC Memory: 32GB
002	Employee PC	Hardware	Manufacturer: Various. OS: Windows 7 Role: Employee Restricted Access: Yes
003	CEO PC	Hardware	Manufacturer: Various OS: Windows 7 Role: CEO Restricted Access: No
004	Server Data Backup Process	Process/Procedure	Sync of server data to cloud service (ADrive) run at 11.59 pm
005	PC Policy	Process/Procedure	Restriction on employee PCs at workstations -> Apps to not be uninstalled or removed as well as no changes to set settings or OS.
006	Script for backup	Software	Performs daily synchronization of server data with cloud service (ADrive)
007	Legal Files/Documents	Data	Location: XYZ Server. Access: Read only -> employees. Write: CEO and Admin
008	Office Access Control	Physical	Bob -> security guard and receptionist at the company, he is positioned in front of the main access door to the office, and the desk is located in front of the door. In charge of office security and monitors access to restricted areas.

009	Employee user folders	Hardware	Desktops used by users. Can write to user account folder (e.g. C:\users\<username>) which includes subdirectories(Desktop, Documents, Downloads). Access is fully enabled for these directories for that employee.
010	Password changes	Process/Procedure	Changes to employee passwords (exception for CEO and administrator) are to be done every 6 months. Passwords are required to consist of 8 letters which must include a capital letter.
011	Firewall and Antivirus Software	Service, Software	Service to mitigate viruses from being injected into network, server, and cloud. Protects company data and information. Updated regularly. Built-in on Windows 7 pcs.

Threat and Vulnerability Assessment

Provide at least 1 entry for every asset listed in the inventory.

Asset IDs	Asset Name	Asset Category	Threat	Vulnerability	Risk and Consequence	Impact	Likelihood
001	Server	Hardware	Theft	The server is small in size and can be stolen by an employee The location of the server is known to all employees	Most of the company operations will be disrupted The company's data will be leaked resulting in significant damage to the reputation Damage to Intellectual property	Significant	Possible but unlikely
001	Server	Hardware	Theft	The server is small in size and can be stolen by an outsider	Most of the company operations will be disrupted The company's data will be leaked resulting in significant damage to the reputation Damage to Intellectual property	Significant	Almost never
001	Server	Hardware	Hardware Failure	The company only has one server	The server could fail due to hardware failure which means most of the company operations will be disrupted	Significant	Medium
002	Employee PC	Hardware	Malware	Employee PC runs on Windows 7 which could potentially lead to outdated software to counteract malware and viruses.	Employee operations will be disrupted. This leads to loss or unauthorized data access	Moderate	Possible but unlikely
003	XYZ Server Data	Server	Limited Encryption or access controls	Legal information and documents could lead to a leak of private confidential client information.	Potential legal liabilities through non-disclosure of private information of legal documents. Major impact on public and corporate image	Significant	Possible

004	Employee Credentials	Data	Unauthorized Access	Failure to update passwords regularly enough or not long enough passwords. Passwords are easily guessable.	Unauthorized access by internal or external threats that lead to theft of information, defamation, or disruption of services.	Moderate	Possible
004	Employee Credentials	Data	Credential Theft	Unauthorized access to employee PC (e.g. leaving desktop unlocked) employees not following password policy or insecure storage of employee information.	Leading to data breaches and disruption of services. Malicious employees can obtain sensitive documents that they do not have access to. Attacks carried out by a malicious/disgruntled employee. This could result in operational dysfunction and/or services.	Significant	Highly probable
005	Backup Script	Software	Power outage	Cloud service (ADrive) needs to be available for backup to be efficient	Cloud service experiences an outage, resulting in backups being incomplete. This could cause data loss and disruption.	Significant	Possible
006	Legal Documents	Data	Data Corruption	Lack of proper backup procedures or safeguard	Critical documentation and files are corrupted and lost, resulting in potential legal liabilities and impact on public/corporate image.	Moderate	Possible but unlikely
007	ADrive Cloud Backup and Storage	Service	Data Loss	Failure to synchronize with cloud service or issues with script execution.	Loss of backup data resulting in not being able to recover	Moderate	Possible but unlikely
008	Bob - Office Access Control	Physical	Unauthorized Entry	Lack of supervision or monitoring of entry of company office OR Bob may be a malicious insider and allow unauthorized access.	This can lead to unauthorized or malicious outsiders to gain access to the company building. Can lead to theft or damage to company assets	Minimal	Possible but unlikely
009	Workstations	Hardware	Data loss	Lack of regular backup of employee workstations	This leads to loss of work done by employees and can result in operational delays and recovery costs	Moderate	Possible but unlikely
010	Antivirus Software	Service, Software	Outdated Software	Antivirus software not updated regularly	Risk of not being able to mitigate new modern threats that can pose a risk to the business. Increase risks of malware and infections to PCs. Causes operation dysfunction and loss of data	Significant	Possible (new threats)

The criteria for grading are:

- **Completeness** – Did you complete all the tasks and how comprehensively? Did you Provide explanation where necessary?
- **Accuracy** - How well did you complete the tasks?
- **Presentation** - Did you use the right terminology? Please check for readability.

Letter grades

- **A-range:** Complete, accurate, and well presented. Shows good knowledge and good understanding of subject. Well-argued. Where required, contains good original input from the student.
- **B-range:** Mostly complete, mostly accurate, and well presented. Shows a good knowledge and good understanding of the subject but either fails to complete some parts of the tasks or is unclear or is poorly argued.
- **C-range:** Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the subject or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.
- **D-range:** Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.
- **E-range:** Well below the required standard.