University Risk Assessment

DO NOT SHARE

Content

Executive summary

The potential for risk in Information technology (IT) is expected; having these risks at a university could cause many impacts on confidentiality, integrity and availability and increase the likelihood of dangerous attacks. Undertaking a risk assessment will allow me to make an ideal template for what the university should undertake to ensure that its security information systems are fully protected to enable it to fulfil CIA requirements. I will dissect different assets, how they can be affected, the impact, and the likelihood and give them an overall risk score. Doing this will show the places where the university needs to improve its security.

The scope of this report will be to understand the university's potential assets. I will analyse the university as a whole and its potential threats to its information security. The list of possible investments that can be affected is high for a university since it will all be running off databases, accounts, and computers. So, ensuring that I see the different threats from every asset as a whole for the university will allow us to keep an idea of ways I can better security.

For this report, I will follow a “quantitative, asset-based risk assessment”. The idea of this being that it being quantitative allows me to use data to measure the likelihood and impact of each risk. The asset-based section allows for that specificity of individual assets that let me entirely focus on everything. This means I can individually evaluate each asset, provide many different controls, and ensure that asset risk needs to be focused. For this risk assessment, I will follow the guidelines proposed by ISO 207005 Risk Management Framework [2].

In this report I have identified four sectors of the university where there is potential for attack, I have identified multiple asset groups with given vulnerabilities represented with their retrospect risk scenario. All of these different threat scenarios have all been given their retrospective risk value and treatment method. At the risk value table you will find a justification for each likelihood and impact. No controls will be given to an asset scenario with a risk value of 0-12 that will **retain** (retain the risk without any further action) or **avoid** (withdraw from a set of activities or change the way it operates) that risk. I identified this value using the risk matrix represented below. If the risk level is above 10 in the 13-25 range I will provide a form of treatment: **reduce** (Risk should be handled by eliminating or changing controls, allowing the risk to be reviewed) or **transfer** (transfer risk to another party that can help reduce the risk). All controls represented in this report will have a justification of why they will help bring down the likelihood and impact of that risk.

The risk value table identifies many scenarios, many of which are above our 0-12 risk value threshold. Finance and human resources account for the majority of the findings. Twelve of the set risks are either way above or slightly above our entry. These scenarios reveal three distinct attack methods: phishing, malware, and poor encryption. Using these critical identifiers, we can see a pattern with the vulnerabilities for the attacks.

Vulnerabilities:

Phishing: Found the potential for successful phishing scams to be high; this will expose vulnerable information to attackers

Outdated software: Obsolete software will lead to many potential malware attacks, allowing information to be leaked or stolen.

Poor access controls: A few sectors found poor access controls, providing risk to unauthorised access, leading to potential data theft, data leaks, and unauthorised data modification.

Lack of authentication: Authentication measures were not taken place, which can lead to unauthorised modification of data

These were some of the most common vulnerabilities across the risk assessment. I suggest taking action against these risks to help mitigate the overall risk score. Patching these risks will help the university tremendously when it comes to protecting its information.

In the final segment of this report, there is a controls section; you will find that I have provided controls for all significant threats above the defined threshold. The recommended controls aim to address the risks and systematically reduce the university risk score.

Controls:

Phishing:
- Implement annual phishing awareness and testing
    - This will allow the staff to get more familiar with phishing and possible ways to identify it; the testing will allow you to see who is most at vulnerable and maybe be more focused on helping that individual

Outdated software:
- Update all forms of software: possible implement automatic software updates
    - This allows the system to be at its best and ensures that all past vulnerabilities for the software are now up to standard.

Poor access controls:
- Aline user privileges with the responsibility of their role at the university
    - This means that only specific people can access the files are in relation to them

Lack of authentication:

- Implement two-factor authentication
    - This makes it a lot harder for someone to just access an account hosted by the university since they will need either the user's phone or email.

These are just a few of the overall controls I have recommended, but these were some of the most important since they have come up in multiple sectors of the university.

Overall, from the research conducted, this university is facing some potential risks to its assets and data for information security. These findings show the importance of achieving this risk assessment for the university now it can allow them to protect the assets and data that they hold fully. A risk assessment for this university should be something other than a one-time thing. There should be another one soon after putting all the prevalent controls in place to see if there are any other risks I have not identified.

Risk matrix

[1]

			Likelihood				
			Rare	Unlikely	Moderate	Likely	Almost certain
			1	2	3	4	5
Impact	servere	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5

Asset Identification table

Sector	Asset group	Description	Assets	Threat scenarios reference	Vulnerability	Consequences [2]	Reference
Human resources	Student Information	This information is related to students enrolled in the university. This information is all personally identifiable information. There are many different things in this address information to health.	Name, Address, Email, Phone number, Family contact, medical information, birthday,	**TS.1**	• Lack of student awareness to potential phishing attacks • Lack of staff awareness • Weak authentication • No two-factor authentication • Lack of data protection policy	• Investigation and repair time • Health and safety • Financial fine • Damage to student trust • Damage to teacher trust	**HR.1**
				TS.2	• Lack of session management • Lack of student awareness	• Investigation and repair time • Image and good will damage • Health and safety • Financial fine • Damage to student trust	**HR.2**
				TS.3	• Lack of device protection • Outdated software • Lack of data protection policy	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial fine • Health and safety • Damage to student trust	**HR.3**
				TS.4	• Weak access control • Lack of backups	• Investigation and repair time • Image and good will damage • Damage to student trust •	**HR.4**
				TS.16	• Lack of encryption • Lack of data protection policy	• Investigation and repair time • Image and good will damage • Health and safety • Financial fine	**HR.5**
	Staff Information	Staff information: is the details about the employee within the university. These details can include: birthdays, address, emails, contact numbers, social security numbers, job title, department and more.	Name, Address, Email, Phone number, Family contact, medical information, birthday, performance data, engagement data	**TS.1**	• Lack of Staff awareness to potential phishing attacks • Weak authentication • No two-factor authentication • Lack of data protection policy	• Investigation and repair time • Image and good will damage • Health and safety • Financial fine	**HR.6**
				TS.2	• Lack of session management • Lack of student awareness	• Investigation and repair time • {Operational} time lost • Financial fine • Damage to employee fine	**HR.7**
				TS.3	• Lack of device protection • Outdated antivirus software	• Investigation and repair time • {Operational} time lost • Image and good will damage • Health and safety • Financial fine	**HR.8**

				TS.14	• Improper access control	• Investigation and repair time • Image and good will damage • Financial fine • Health and safety • Damage to employee trust • Damage to student trust	**HR.9**
				TS.16	• Lack of encryption • Lack of data protection policy	• Investigation and repair time • Image and good will damage • Health and safety • Financial fine	**HR.10**
Technology systems	Virtual learning Environment	Virtual learning environments (VLEs) or learning environment managers (LEMs) are online platforms universities use to hold instructional materials and manage assignment submissions.	The virtual learning environment, Modules/lessons, Announcements pages, Student data, Employee data, server	**TS.5**	• A lack of bandwidth and resources capable of handling a large number of network requests, which a lack of DDoS protection cannot exacerbate • Lack of device protection	• Investigation and repair time • {Operational} time lost • Image and good will damage • Damage to employee trust • Damage to student trust	**TechS.1**
				TS.6	• Lack of backups • Lack of authorisation	• Investigation and repair time • Image and good will damage	**TechS.2**
				TS.7	• Lack of access removal	• Investigation and repair time • Image and good will damage	**TechS.3**
				TS.8	• Maintenance of hardware is not kept up • Lack of back up protection	• Investigation and repair time • {Operational} time lost • Image and good will damage • Reputation damage	**TechS.4**
				TS.24	• Lack of password policy • Lack of authentication • No two factor authorisation	• Investigation and repair time • {Operational} time lost • Image and good will damage • Damage to employee trust • Damage to student trust	**TechS.5**
	Network systems	The data is relevant to the management of the network. This includes network devices like routers, switches and servers and information about the overall network and who is connected.	Physical breaches, Software version, network passwords, network usernames, network servers, Network configuration	**TS.23**	• Lack of physical forms of security, giving access to physical network servers	• Investigation and repair time • {Operational} time lost • Image and good will damage	**TechS.6**
				TS.1	• Lack of network team awareness to potential phishing attacks • Weak authentication • No two-factor authentication	• Investigation and repair time • {Operational} time lost • Image and good will damage	**TechS.7**
				TS.9	• Poor access controls • Lack of monitoring • Lack of back ups • Poor authentication • No intrusion detection system	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial cost	**TechS.8**
				TS.10	• Poor access controls • Lack of monitoring • Lack of back ups • Poor authentication	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial cost • Damage to employee trust	**TechS.9**

						• Damage to student trust	
				TS.11	• Non standard data encryption • Weak password policies • Password sharing	• Investigation and repair time • {Operational} time lost • financial cost of specific skills to repair the damage	**TechS.10**
	Physical devices	These are devices that can be used by employees/students; these are also components that run a lot of the university and let it function to its fullest	Desktops, Laptops. Server, databases	**TS.18**	• Lack of physical security • Lack of back up protection	• Investigation and repair time • financial cost of specific skills to repair the damage	**TechS.11**
				TS.19	• Outdated antivirus software • Lack of back up protection	• Investigation and repair time • {Operational} time lost • financial cost of specific skills to repair the damage • Damage to employee trust • Damage to student trust	**TechS.12**
				TS.8	• Maintenance of hardware is not kept up • Lack of backup protection	• Investigation and repair time • {Operational} time lost • Image and good will damage	**TechS.13**
				TS.20	• Lack of physical security • Lack of backup protection	• Investigation and repair time • {Operational} time lost • Image and good will damage • financial cost of specific skills to repair the damage	**TechS.14**
Financial	Financial statements	These are written/typed statements that detail the university's expenses and financial performance.	Balance sheets Income statements, Financial statement notes, footnotes,net assets statements	**TS.1**	• Lack of network team awareness to potential phishing attacks • Weak authentication • No two-factor authentication • Lack of data protection policy	• Investigation and repair time • Image and good will damage • Damage to employee trust • Damage to student trust • Financial fine	**F.1**
				TS.12	• Access rights • Weak authentication • Lack of backups	• Investigation and repair time • Image and good will damage • Financial fine • Damage to employee trust • Damage to student trust	**F.2**
				TS.13	• Outdated software • Downloading stuff online • Lack of device protection	• Investigation and repair time • Image and good will damage • Health and safety • Financial fine	**F.3**
	University finance records	These are records that show the university's financial activity.	Account details, account numbers, credit card numbers, online credentials, Finance statements	**TS.1**	• Lack of network team awareness to potential phishing attacks • Weak authentication • No two-factor authentication	• Investigation and repair time • Image and good will damage • Damage to employee trust • Damage to student trust	**F.4**
				TS.14	• Lack of access controls • Lack of authentication	• Investigation and repair time • Image and good will damage • Financial fine	**F.5**
				TS.16	• Lack of encryption	• Investigation and repair time	**F.6**

					• Lack of data protection policy	• {Operational} time lost • Image and good will damage	
				TS.22	• Lack of Access controls • Lack of authentication	• Investigation and repair time • Image and good will damage • Damage to employee trust • Damage to student trust	**F.7**
	University staff payroll/tax information	Payroll data encompasses all information on an organisation's employees and their compensation. Tax information refers to details about a person's or organisation's tax responsibilities.	Tax records Employee records Employee details	**TS.1**	• Lack of network team awareness to potential phishing attacks • Weak authentication • No two-factor authentication	• Investigation and repair time • Image and good will damage • Financial fine	**F.9**
				TS.14	• Lack of access controls • Lack of authentication	• Investigation and repair time • Image and good will damage • Financial fine • Damage to employee trust • Damage to student trust	**F.10**
				TS.17	• Weak access controls • Lack of back ups • Poorly defined data policies • Inefficient employee training • Outdated software	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial fine • Damage to employee trust • Damage to student trust	**F.11**
				TS.13	• Outdated software • Downloading stuff online • Lack of device protection • Lack of authorisation	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial fine • Damage to employee trust • Damage to student trust	**F.12**
				TS.4	• Lack of access controls • Lack of backups • Lack of authorisation	• Investigation and repair time • {Operational} time lost • Image and good will damage • Financial fine • Damage to employee trust • Damage to student trust	**F13**
Academic	Intellectual property	This is an intellectual creation: software, algorithms, patents.	Student projects, lectures/course material, Software, algorithms. Research paper, publications, patents	**TS.13**	• Outdated software	• Investigation and repair time • {Operational} time lost • Image and good will damage • Damage to employee trust • Damage to student trust	**A.1**
				TS.7	• Lack of backup/copies • Lack of access control	• Investigation and repair time • Image and good will damage • Damage to employee trust • Damage to student trust • {Operational} time lost	**A.2**
				TS.16	• Lack of encryption	• Investigation and repair time • Image and good will damage	**A.3**

				TS.21	• Lack of access control • Lack of authentication • Lack of backups	• Investigation and repair time • {Operational} time lost • Damage to employee trust • Damage to student trust	**A.4**
				ts.25	• Lack of backup • Lack of contracts	• Investigation and repair time • {Operational} time lost • Damage to employee trust	**A.5**

Threat scenario reference table

Threat scenario	Reference
Loss of **confidentiality**: A data leak via Phishing	**TS.1**
Loss of **confidentiality**: Data leak due to a device being left logged in/unattended	**TS.2**
Loss of **confidentiality:** Data leak via malware stealing data from university provided device	**TS.3**
Loss of **integrity**: Due to unauthorised modification of records made by an attacker	**TS.4**
Loss of **availability**: DDoS attack made to the university systems	**TS.5**
Loss of **availability**: Modification of data stored on the VLE by a rogue employee	**TS.6**
Loss of **availability**: Modification of data by an malicious ex-employee	**TS.7**
Loss of **availability:** Due to critical hardware failure	**TS.8**
Loss of **availability**: Rouge employee makes unauthorised configuration to systems	**TS.9**
Loss of **confidentiality**: Rouge employee makes data leak via network attacks	**TS.10**
Loss of **availability**: Due to account compromisation	**TS.11**
Loss of **availability**: Due to accidental deletion by employee	**TS.12**
Loss of **availability**: Data being held by ransomware	**TS.13**
Loss of **integrity**: Due to the unauthorised modification of records by an malicious employee	**TS.14**
Loss of **confidentiality**: Due to poor data encryption for storage of data	**TS.16**
Loss of **confidentiality**: Data leak by an employee	**TS.17**
Loss of **availability**: Due to physical destruction of a university device	**TS.18**
Loss of **availability**: Due to software failure induced by malware on a university device	**TS.19**
Loss of **availability**: Destruction of device due to natural disaster	**TS.20**
Loss of **integrity**: Due to modifications made by a student	**TS.21**
Loss of **confidentiality**: Due to data leak by a rogue employee	**TS.22**
Loss of **integrity**: Due to critical hardware failure	**TS.23**
Loss of **integrity**: due to account compromisation	**TS.24**
Loss of **confidentiality**: Due to partnership sharing of projects	**TS.25**

DO NOT SHARE

Risk Value table

Reference	Scenario	Likelihood	Impact	Treatment	Likelihood Justification	Impact justification	Risk value
HR.1	**TS.1**	L	S	**Reduce & transfer**	Phishing attacks are one of the most common attacks carried out every year. There are millions reported every single year. Since the attack is very easy, there is a lot of motivation behind the outcome of stealing the data. Attackers can gain financially and commit other crimes of the data received.	If Student data is leaked, this is a privacy violation, potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	20
HR.2	**TS.2**	R	S	**Retain**	An attacker might do this attack since it's an easy attack and will provide them with information they could potentially sell. But, this type of attack is hazardous and not the easiest to pull off.	If Student data is leaked, this is a privacy violation potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	5
HR.3	**TS.3**	M	S	**Reduce**	Malware attacks can be a really easy attack for attackers to perform and give the attacker lots of data that they can use later on. This type of attack can provide a financial incentive. I have it as moderate likelihood because there are many different things an attacker must know before committing this type of attack. Outdated software provides a strong stance on the attack being successful.	If Student data is leaked, this is a privacy violation potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	15
HR.4	**TS.4**	R	Mo	**Retain**	An attacker gaining access to a system to modify data is going to be rare since the only benefit they gain from this type of attack is the disruption of operations.	Modifying student data can diminish students' trust in the university. This data is essential to the university since teachers and students rely on this data to ensure the credibility of the student. The repair of the data deletion will lead to operational damage since there will be time taken to replace the data that has been changed.	3
HR.5	**TS.16**	L	S	**Reduce**	Decryption of encrypted hashes in a database system is a common attack, if this data is decrypted will provide an attacker with a lot of financial gain since they can sell the data. Due to the nature of the attack it can be common to see attacker try it a lot	The decryption of student data will cause many potential consequences for the university. This will reveal a massive privacy violation, potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	20
HR.6	**TS.1**	AC	S	**Reduce & transfer**	Phishing attacks are one of the most common attacks carried out every year. There are millions reported every single year. An attacker would phish for staff data because it can provide them with some financial gain.	If Staff data is leaked, this is a privacy violation potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be	25

						lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	
HR.7	**TS.2**	UL	S	**Retain**	An attacker may try and use a personal device to get information on the user. But, this form of attack is quite risky to pull off.	If Staff data is leaked, this is a privacy violation potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	10
HR.8	**TS.3**	M	S	**Reduce**	Malware attacks can be a really easy attack for attackers to perform and give the attacker lots of data that they can use later on. This type of attack can provide a financial incentive. I have it as moderate likelihood because there are many different things an attacker must know before committing this type of attack. Outdated software provides a strong stance on the attack being successful	If Staff data is leaked, this is a privacy violation potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	15
HR.9	**TS.14**	UL	Mo	**Reduce**	Insider threats provide potential security hazards to data security. An employee with malicious intent to modify data may seek to delete/change/manipulate data for various reasons, including personal vendetta or financial gain. However, this approach may be less popular because it is specialised and does not provide the most advantageous income for the attacker.	Having incorrect or no information about an employee can lead to potential disinformation of the accuracy of an employee. Loss of trust from the staff if they find out that data can be tampered with, potentially impacting staff credibility.	6
HR.10	**TS.16**	L	S	**Reduce**	Decryption of encrypted hashes in a database system is a common attack, if this data is decrypted will provide an attacker with a lot of financial gain since they can sell the data. Due to the nature of the attack it can be common to see attacker try it a lot	The decryption of staff data will cause many potential consequences for the university. This will reveal a massive privacy violation, potentially affecting the health and well-being of the students. This will cause the university many legal issues, fines, penalties, and potential legal action. The reputation of the university will be lost due to data being leaked. This can also halt day-to-day operations for the university as they try to find methods to teach about these issues and prevent them.	20
TechS.1	**TS.5**	M	S	**Reduce**	Educational platforms can be alluring to attackers, given the importance of the platform since this platform can be critical for students' learning. Since there aren't great benefits for the attacker to take down a platform, there is a moderately high likelihood, but they can be taken down for political reasons to cause chaos.	Having incorrect or no information about an employee can lead to misinformation about the person's accuracy. Employees may lose faith if they discover that data can be manipulated, potentially affecting staff credibility. The university's workflow will be hampered because feeding the data into the system will take time, potentially resulting in downtime.	15
TechS.2	**TS.6**	R	Mo	**Retain**	A rogue employee would gain nothing from committing an attack like this unless it was potentially politically motivated	Having data be modified/manipulated can cause issues for the university when trying to deliver teaching to the students, so there may be a reputation loss with the students and teachers. There may be downtime when trying to recover the data that has been modified.	3
TechS.3	**TS.7**	R	Mo	**Retain**	A malicious ex-employee would gain nothing from committing an attack like this unless it was potentially revenge motivated	Having data be modified/manipulated can cause issues for the university when trying to deliver teaching to the students, so there may be a reputation loss with the students and teachers.	3

						There may be downtime when trying to recover the data that has been modified.	
TechS.4	**TS.8**	UL	MA	**Retain**	VLE is controlled by a server that is constantly running; depending on the quality of hardware, there is a chance that a vital part of the system that runs the system fails, causing an outage of that system, meaning no one can use it.	This will mean the university will have to take time to go and fix the issue at hand and reset the system, disrupting the normal flow of activities. It will lose the trust of students and staff, disrupting the ability for them to learn and teach.	8
TechS.5	**TS.24**	UL	MO	**Reduce**	The university password policy may allow students/staff to enter passwords that would not be compatible with today's standard, creating a scenario of weak authentication.	Account compromise can cause a user to be unable to use their account, losing trust in the university because they can no longer complete tasks. This will cause operational time to be lost since they must fix the issue. That can lead to other consequences depending on what the attacker does after compromising the account.	6
TechS.6	**TS.23**	UL	S	**Retain**	VLE is controlled by a server that is constantly running; depending on the quality of hardware without constant maintenance, there is a chance that a vital part of the system that runs the system fails, causing an outage of that system, meaning no one can use it.	This can have drastic financial consequences for the university if the system fails, the repair cost to gain the data back from partitions, and revenue lost from courses. This also has a chance to cause mass data loss if these services can not be brought back. This will cause a reputation loss with the students and staff since the downtime caused will impact them a lot.	10
TechS.7	**TS.1**	L	MA	**Reduce**	Phishing attacks are one of the most common attacks carried out every year. There are millions reported every single year. Since the attack is very easy, there can be a lot of motivation by gaining access to a network account leading to potential data breaches.	This means other people can access the network via the account, meaning operation time to fix the issue. The network would have to go into downtime to repair this issue, losing trust with the students and teachers. This will cause some financial problems since the server needs to be run to provide people with their services.	16
TechS.8	**TS.9**	R	S	**Retain**	The ability to do this type of attack is rare since you would need access to the network configuration, the ability for a random employee to gain that access would be hard, unless it was a network employee.	In this event, it would cause downtime for the university systems as they try to get their network black to its original configuration. They are driving trust with the students and employees to be lost. Financial costs for the university will be lost due to the systems being down.	5
TechS.9	**TS.10**	UL	S	**Retain**	The chance of a employee wanting to commit malicious intent against their workplace is unlikely	Leaking of network data can mean the network infrastructure can be identified and potentially lead to more attacks on the university. This will cause drastic issues for the university because they will need to bring down the network to fix any problems there could be so other attackers can gain access, and they will need to change all network accounts. Student and employee trust will be lost since it can also affect service availability.	10
TechS.10	**TS.11**	L	S	**Reduce**	A network account provides a lot of access for an attack they can make drastic changes to a system. It is likely that a network account is targeted	Account compromisation of a network account can lead to many onset effects, such as data tampering, falsification, and data leaks. This can lead to the university's reputation going down since they would have to make some changes and can erode trust in the university security practice.	20
TechS.11	**TS.18**	UL	Min	**Retain**	Physical damage can be dropping or purpose destruction, there is a chance of it happening but it will not be often.	This could mean an employee could struggle to complete work since they do not have a system to work on, which may cause some financial cost for the university since they may need to buy backup plans if they are provided	4

TechS.12	**TS.19**	M	S	**Reduce**	The possibility of user being unaware of what they are installing onto a machine and this could potentially be a software fatal malware	This could cause machines routinely utilised by students and faculty to fail, potentially impairing their capacity to learn/teach. This could be a significant concern for the university regarding providing software and new devices to restore lost data and avoid future data loss. Software failure could cause issues with day-to-day operations because it will prevent the completion of procedures.	15
TechS.13	**TS.8**	R	S	**Retain**	Depending on circumstances the chances of a piece of hardware failing. But, there are some potential factors: hardware age/use, the type of hardware in use, and maintenance factors. These can all lead to hardware failing but it is rare.	This will cause trust issues with employees and students since they need help to use the systems. The cost of replacing the hardware and now hiring staff to maintain it will cause some financial loss. This issue could also lead to data loss depending on what fails, and getting that data back can cost a lot for the company.	5
TechS.14	**TS.20**	R	MA	**Retain**	The chance of a natural disaster is really rare	If a natural disaster happens and destroys a piece of hardware necessary for a function or just general hardware used by students, it will cause issues. Since this hardware is no longer available, it will disallow access for students/staff, losing their reputation since they can't use the services. Financial loss will be prominent since they must spend money fixing the issue and possibly restoring data.	4
F.1	**TS.1**	M	S	**Reduce & transfer**	Phishing being one of the most common attacks and easiest to do will provide a somewhat high likelihood for someone to commit the attack. An attack will definitely go for these files since it can provide a high financial gain.	Financial statements being leaked will cause many issues for the university: the potential for fraudulent transactions, etc. The leaking of this data could lead to the compromisation of financial accounts, leading to more data potentially being leaked—the university's reputation with its students and employees with potential data leaks. The operation would need to be halted since the company will need to work on fixing that issue before anything else.	15
F.2	**TS.12**	R	s	**Retain**	The possibility that an employee accidentally deleted and important file is going to be relatively rare	Deletion of financial statements can cause many issues for the university. This can be an availability issue because the university will be following compliance with the modification of these statements, which means they won't be tracking compliance, which will lead to fines for the university that could also lead to legal issues. When the university checks its financials, there would be issues if there needs to be more data. This will be an operational disruption for returning these statements and ensuring all their information is correct.	5
F.3	**TS.13**	M	S	**Reduce**	An attacker may use malware to grab data and hold it ransom because these statements are really important to a university, holding these statements provides an attacker with potential financial gain. This type of attack though is quite slow, not everyday is an attacker going to be able to get malware onto a system.	The university will be following compliance if the files they need are unavailable, which will lead to many legal concerns and financial loss. The issue could cause a loss of reputation with a few groups: stakeholders, students, and employees since they may think the university can not keep this confidential information safe. Getting the data back to where it needs to be will take a long time and cause disruptions in day-to-day operations.	15
F.4	**TS.1**	AC	S	**Reduce & transfer**	Phishing attacks are one of the most common attacks carried out every year. There are millions reported every single year. Fishing of a finance account can provide the attacker with a lot	University finance records being leaked will cause many issues for the university: the potential for fraudulent transactions, etc. This could lead to the compromisation of financial accounts,	25

					of gain; they can perform many different attacks with these details.	leading to more data potentially being leaked—the university's reputation with its students and employees with potential data leaks. The compromisation of funds for students and employees could happen if these records are leaked, leading to fines. The operation would need to be halted since the company will need to work on fixing that issue before anything else.	
F.5	**TS.14**	UL	MA	**Retian**	Modification of these records does not provide an employee with much benefit, unless they are doing it to get back at the university and maybe some potential financial gain. Overall do not gain a lot	Unauthorised modifications of these files are destructive. Having these files modified could lead to issues with financial reporting, which can cause problems with the university's financial health. Loss of reputation & credibility since this is misleading information. There could be legal consequences since this lack of compliance can also lead to fines.	8
F.6	**TS.16**	AC	S	**Reduce**	Decryption of encrypted hashes in a database system is a common attack, if this data is decrypted will provide an attacker with a lot of financial gain since they can sell the data. Due to the nature of the attack it can be common to see attacker try it a lot	If university finance records get compromised, it will cause many issues for the university: the potential for fraudulent transactions, etc. This could lead to the compromisation of financial accounts, leading to more data potentially being leaked—the university's reputation with its students and employees with potential data leaks. The compromisation of funds for students and employees could happen if these records are leaked, leading to fines. The operation would need to be halted since the company will need to work on fixing that issue before anything else.	25
F.7	**TS.22**	UL	S	**Retain**	An employee main leak financial data because it can allow them to gain financially	University finance records being leaked will cause many issues for the university: the potential for fraudulent transactions, etc. This could lead to the compromisation of financial accounts, leading to more data potentially being leaked—the university's reputation with its students and employees with potential data leaks. The compromisation of funds for students and employees could happen if these records are leaked, leading to fines. The operation would need to be halted since the company will need to work on fixing that issue before anything else.	10
F.9	**TS.1**	AC	S	**Reduce**	Phishing attacks are one of the most common attacks carried out every year. There are millions reported every single year. Fishing of a finance account can provide the attacker with a lot of gain; they can perform many different attacks with these details.	If an attacker gets payroll/tax information, they could commit many crimes: identity theft, tax fraud, and fraudulent transactions leading to a loss of reputation for the university and its employees. Since this data is being stolen, it will lead to financial fines and possible legal consequences for the university and its employees. The university will need to investigate what caused this issue, which will halt operations for the university for the time being.	25
F.10	**TS.14**	UL	S	**Reduce**	Modification of these records does not provide an employee with much benefit, unless they are doing it to get back at the university and maybe some potential financial gain. Overall they do not gain a lot so this attack is not going to be that common.	Unauthorised modifications of these files are destructive. Having these files modified could lead to issues with financial reporting, which can cause problems with the university's financial health. Loss of reputation & credibility since this is misleading information. There could be legal consequences since this lack of compliance can also lead to fines.	10

F.11	**TS.17**	R	S	**Retain**	An employee accidentally leaking data is going to be rare, the only way this would be possible is if they didn't know the system and accidentally did something they didn't realise. However, I thought that if there is no authentication in place it could be accidentally leaked without warning the user.	If an attacker gets payroll/tax information, they could commit many crimes: identity theft, tax fraud, and fraudulent transactions leading to a loss of reputation for the university and its employees. Since this data is being stolen, it will lead to financial fines and possible legal consequences for the university and its employees. The university will need to investigate what caused this issue, which will halt operations for the university for the time being.	5
F.12	**TS.13**	L	S	**Reduce & transfer**	An attacker may use malware to grab data and hold it ransom because these statements are really important to a university, holding these statements provides an attacker with potential financial gain. This type of attack though is quite slow, not everyday is an attacker going to be able to get malware onto a system.	Payroll/tax information being held for ransom will lead to many different consequences. Financial loss for the university is prominent since the attacker may demand money for the data to be released. Also, the fines the university will face due to the lost data will cause an issue with compliance for finances, which could also cause legal problems for the university. The data loss could lead to employee payment issues and loss of reputation with the employees.	20
F.13	**TS.4**	R	MA	**Retain**	An attacker may modify payroll/tax information because the attacker could potentially add their own details to the payroll to try and gain financially, but if they are caught there details are on the system to be able to identify them	This would be a significant issue because the university would be actively paying an attacker to their system, meaning they are losing since they are actively giving this person money.	4
A.1	**TS.13**	UL	S	**Retain**	An attacker may use malware to steal IP because it can provide them a potential financial gain for the university to pay the ransom to get the property back, and cause they could potentially leak the IP. However, this attack does take a lot of time to actually commit.	Intellectual property being held at ransom could cause financial loss for the university if they have to pay the ransom and have no other way of getting their IP back. It could make a reputation with the students and staff since this is sensitive research they can not keep safe. This could pose legal and ethical risks since safeguarding IP can cause the university to face fines and penalties.	10
A.2	**TS.7**	UL	MA	**Retain**	Modification of IP does not provide an employee with much benefit, unless they are doing it to get back at the university and maybe some potential financial gain. Overall and employee maliciously changing an IP does not benefit them at all so it's not going to be common.	If this IP revolves around research or an algorithm changes to this IP, it will lead to a mass integrity issue if the study is altered. Trust in the university will be lost, especially with students and employees. Financial loss could also be present since the university could face fines and penalties.	8
A.3	**TS.16**	UL	S	**Retain**	The decryption of encrypted hashes in a database system is a widespread attack; if this data is decrypted, an attacker can make a lot of money by selling the data. Because of the nature of the attack, it is usual to see attackers try it multiple times.	Intellectual property being decrypted will lead to potential Ip theft or malicious attackers using the stolen IP for their gain. This will cause damage to partners and other relationships the university has. This could lead to potential legal issues if the university fails to create a good data protection policy.	10
A.4	**TS.21**	UL	M	**Retain**	A student could use university IP for research misusing/modifying this IP could be possible accidental or malicious. But, the university should be protecting forms of their IP with access controls to editing rights.	The changing IP could lead to operating time in the university coming to a halt since they will need to work on getting the information back to where it was, which could take a while. Trust in the university would be lost, especially if sensitive research was needed, which could drastically affect the users.	6
A.5	**TS.25**	M	S	**Reduce**	Since the nature of intellectual property is based on collaborative work for the university there may be private/ sensitive information so the university would want to make sure this is a trustworthy institute they are working with. It isn't that likely that someone will steal it but there is a chance it can	If the university has put effort into discovering the creation of a potentially stolen algorithm, this can result in financial loss. The university's reputation will suffer, particularly among its students, teachers, and stakeholders. Any data stolen from a university will result in legal ramifications. The university must	15

					happen if outcomes change.	enforce intellectual property rights, and failure to do so may result in some companies suing the university.	

Control table

Reference	scenario	L	I	RV	Control	Control justification	L	I	NRV
HR.1	**TS.1**	L	S	20	Annual students are informed with presented guidelines on the university website.	Having students and staff become more familiar with the idea of phishing shall decrease the likelihood there will be a successful attack.	R	M	3
					Implement a password policy	A more robust password policy will mean students can not use non-standard passwords.			
					Activate two factor authentication	Implementing two-factor authorisation means an attacker can not access the account without the users giving them a code. This will make it much harder for an attacker to access an account.			
					Transfer data to cloud provider	Having data on a secure cloud provider because it provides more security and can help with potential disaster relief			
HR.3	**TS.3**	M	S	**15**	Make sure that devices are up-to-date with all applications and anti-virus software	Having all devices be up-to-date, will minimise all ways a malware can be used to gain information	R	S	5
HR.5	**TS.16**	L	S	20	Implement stinger encryption	Having stronger encryption means that data will be harder to decrypt making the access of data not possible	R	S	5
					Implement a strong data protection policy	Stronger password policy stops the ability to enter non secure passwords			
HR.6	**TS.1**	AC	S	25	Annual students are informed with presented guidelines on the university website.	Having annual staff training will provide staff in constant reinformation of what phishing looks allowing them to spot it before it happens.	R	M	3
					Implement a password policy	A more robust password policy will stop the ability to set weak passwords on the system.			
					Activate two factor authentication	Implementing two factor authentication will make it harder to access accounts since there is a extra layer of protection			
					Transfer data to cloud provider	Having data on a secure cloud provider because it provides more security and can help with potential disaster relief			
HR.8	**TS.3**	M	S	15	Make sure that devices are up-to-date with all applications and anti-virus software	Having all devices be up-to-date, will minimise all ways a malware can be used to gain information	R	MA	4

TechS.1	**TS.5**	M	S	15	Implement cloud protection	Cloud protection is design to handle mass amount of traffic, it will scan the traffic and determine what is legitimate and allow it through the network	R	MA	4
					Implement a physical firewall	Firewalls allow for traffic filtering they can try and put a stop to a mass traffic attack trying to take down your network			
TechS.7	**TS.1**	L	MA	16	Annual staff training and testing Student informed and shown guidelines on how to stop potential phishing attacks	Having students and staff become more familiar with the idea of phishing shall decrease the likelihood there will be a successful attack.	UL	MO	6
					Implement a password policy	A more robust password policy will mean students can not use non-standard passwords.			
					Activate two factor authentication	Implementing two-factor authorisation means an attacker can not access the account without the users giving them a code. This will make it much harder for an attacker to access an account.			
TechS.10	**TS.11**	L	S	20	Implement stronger encryption	Stronger encryption can stop the ability of passwords being cracked	UL	MA	10
					Impalement a password policy	Stronger password policy stops the ability to enter non secure passwords			
					Inform staff on password sharing	Teach staff about the vulnerabilities of sharing passwords			
TechS.8	**TS.9**	L	S	20	Implement proper access control	Access controls will make it so only specific staff members can perform specific actions	R	MA	4
					Implement a audit log	Audit logs will allow a admin user to see what actions have been performed by who			
					Implement back up controls	Having back up controls allows a team to reset back to a point where everything worked without having to completely remake it			
					Implement two factor authentication	Implementing two-factor authorisation means an attacker can not access the account without the users giving them a code. This will make it much harder for an attacker to access an account.			
					Implement intrusion detection	Implementing intrusion detection will inform any admins of an intrusion meaning they can quickly work on patching and getting the intruder out before any serious consequences happen.			
TechS.12	**TS.19**	M	S	15	Make sure that devices are up-to-date with all applications and anti-virus software	This will stop any potential malware getting onto the system and causing long lasting damage to any of the software	R	M	3

					Implement backup protection	Backup controls will allow users to reset the device to a point in time where the system was running perfectly.			
F.1	**TS.1**	M	S	15	Annual staff training and testing	Annual staff training and testing allows staff to understand what fishing is and see examples of it. The testing will test staff to see where potential holes are and people who may need specific training.	UL	Min	4
					Implement a password policy	Having a strong password policy makes it so there is no way a staff member can have a weak password			
					Activate two factor authentication	Two factor authorisation makes it so the user must enter a code given to them by either phone number or email, mitigating potential breaches through just an user account			
					Transfer data to cloud provider	Having data on a secure cloud provider because it provides more security and can help with potential disaster relief			
F.3	**TS.13**	M	S	15	Make sure that devices are up-to-date with all applications and anti-virus software	Having all software up-to-date will reduce the ability for malware to enter the system and steal from the system	R	Min	4
					Implement a firewall	Having some physical security like a firewall allows for an admin to monitor specific traffic and block certain downloads they may think are dangerous			
					Implement backup protection	Having back up protection for their network can allow them to go back to a point before being attacked and allow them to have the network up and running again.			
F.4	**TS.1**	AC	S	25	Annual staff training and testing	Annual staff training and testing allows staff to understand what fishing is and see examples of it. The testing will test staff to see where potential holes are and people who may need specific training.	UL	Min	4
					Implement a password policy	Having a strong password policy makes it so there is no way a staff member can have a weak password			
					Activate two factor authentication	Two factor authorisation makes it so the user must enter a code given to them by either phone number or email, mitigating potential breaches through just an user account			
					Transfer data to cloud provider	Having data on a secure cloud provider because it provides more security and can help with potential disaster relief			

F.6	**TS.16**	AC	S	25	Implement stinger encryption	Having stronger encryption means that data will be harder to decrypt making the access of data not possible	R	S	5
					Implement a strong data protection policy	Stronger password policy stops the ability to enter non secure passwords			
F.9	**TS.1**	AC	S	25	Annual staff training and testing	Annual staff training and testing allows staff to understand what fishing is and see examples of it. The testing will test staff to see where potential holes are and people who may need specific training.	R	S	5
					Activate two factor authentication	Two factor authorisation makes it so the user must enter a code given to them by either phone number or email, mitigating potential breaches through just an user account			
F.12	**TS.13**	L	S	20	Make sure that devices are up-to-date with all applications and anti-virus software	Having all software up-to-date will reduce the ability for malware to enter the system and steal from the system	R	Min	4
					Implement a firewall	Having some physical security like a firewall allows for an admin to monitor specific traffic and block certain downloads they may think are dangerous			
					Implement backup protection	Having back up protection for their network can allow them to go back to a point before being attacked and allow them to have the network up and running again.			

References

[1] Group, T. A. (n.d.). *ERM | RISK ASSESSMENT PHASE TWO: RISK ANALYSIS*.

Info.thealsgroup.com. https://info.thealsgroup.com/blog/erm-risk-assessment-phase-two-risk-analysis

Page 3: Risk value table

[2] *BSOL British Standards Online*. (n.d.). Identity.bsigroup.com.

from https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030412541

Consequences

[3] *Access Manager*. (n.d.). Sso.port.ac.uk.

https://moodle.port.ac.uk/pluginfile.php/4645087/mod_resource/content/2/Security_Management_23_L4_.pdf

For the risk tables

DO NOT SHARE