UK Based University Risk Assessment

Security Management

Adam Cooper

up2009045

word count: 2120

2023

Contents

[Introduction 2](#_Toc151473767)

[*What constitutes an information security risk?* 2](#_Toc151473768)

[*Risk Metrics* 2](#_Toc151473769)

[*Nature of business* 2](#_Toc151473770)

[Executive Summary 3](#_Toc151473771)

[Context 3](#_Toc151473772)

[Methodology 3](#_Toc151473773)

[Key Identified Risks 3](#_Toc151473774)

[Key Risks 3](#_Toc151473775)

[Key Controls 3](#_Toc151473776)

[Recommendations 3](#_Toc151473777)

[Organisational Benefit 4](#_Toc151473778)

[Risk Assessment 0](#_Toc151473779)

[Threat & Vulnerability Identification 0](#_Toc151473780)

[Cloud software – Theft of documents 1](#_Toc151473781)

[Operating Systems – Brute force attacks 1](#_Toc151473782)

[Operating Systems – Malware attacks 1](#_Toc151473783)

[Internal Systems – Device failure 1](#_Toc151473784)

[Risk Treatment/Control 3](#_Toc151473785)

[Multifactor authentication and enforcement of strong password policies/file encryption 4](#_Toc151473786)

[Update: Software, hardware, firmware, operating systems 4](#_Toc151473787)

[Staff training for data security, sensitivity, and social engineering scenarios 4](#_Toc151473788)

[Correct configuration of systems and services 4](#_Toc151473789)

[Recommendations 6](#_Toc151473790)

[Appendices 7](#_Toc151473791)

[Figures 15](#_Toc151473792)

[Tables 16](#_Toc151473793)

# Introduction

The aim of this report is to undertake a security risk assessment of a typical university which would be based in the United Kingdom to define areas where security can be improved further or any current threat areas that need to be followed up.

Following on from this, this report will follow these main objectives. Firstly, identifying assets of a UK university. Secondly, the threats associated with each of these assets. Lastly, the vulnerabilities associated with the threats. This will give us a good overview of the threat landscape and allow us to produce a risk score based on the impact and likelihood of each individual threat to an asset.

After the initial risk score has been calculated, treatment/controls will be suggested, and a reviewed risk score will be generated to act like these changes were actioned and threats had been remediated.

### What constitutes an information security risk?

An information security risk is based on anything which breaches the CIA triad, thus breaking either confidentiality or integrity, or preventing the availability of information.

### Risk Metrics

A screenshot of a graph

Description automatically generated

Risk score will be calculated following ISO 27005 requirements of impact × likelihood and an enhanced risk matrix for the calculation of risks where 1 is notable and 25 is potentially catastrophic.

### Nature of business

The typical UK based university has a primary focus of providing education, public or private sector with the production of two main outputs graduates and research.

# Executive Summary

### Context

The main purpose of this risk assessment is to verify the university’s risk compliance via identifying and evaluating threats and vulnerabilities, assessing them against the ISO 27005 standard. Both asset owners and extended management team members will find this report useful endeavouring to reduce and remediate risk.

### Methodology

Curating a qualitative asset-based approach along with the application of binary risk analysis, we calculated the impact/likelihood of individual threats to each identified asset. This produced our risk register providing an overview of the university’s threat landscape.

### Key Identified Risks

To calculate risk, we used the risk matrix calculation defined in ISO 27005 requirements of impact × likelihood and an enhanced risk matrix for the calculation of risks where 1 is notable and 25 is potentially catastrophic. Below are both key risks discovered and controls most needed in accordance with frequency along with recommendations for going forward.

### Key Risks

* Improper access control.
* Out of date software/hardware for current/backup systems and software.
* Data theft.
* Insufficient password management.

### Key Controls

* Multifactor authentication.
* Update: Software, hardware, firmware, operating systems.
* Staff training for data security, sensitivity and social engineering scenarios.
* Enforce strong password and encryption policies for files.

### Recommendations

The following controls are those which are recommended, can be implemented quickly with no impact to current services in the estate and would have an overall benefit most risks identified.

Multifactor authentication – Remediates brute forcing and unauthorised access to accounts.

Update software/operating systems of both current and backup equipment – Reduces system vulnerabilities.

# Organisational Benefit

The overall benefit of this risk assessment to the university is to identify the vulnerabilities which are currently present within the organisation, weaknesses which can be controlled sufficiently and security measures which can be implemented to ensure best remediation of any threats which remain and pose the greatest risk.

As the university compiles personal data, research data along with dealing with other sensitive information i.e., financial information, it is of the utmost importance that the university complies with all applicable industry regulations and standards like HIPAA for ensuring that sensitive health information is kept confidential, this would apply to any student with a disability, EC claims, the University dentist and surgery. GDPR to protect the confidentiality of student and staff information, PCI for processing payments i.e., the student union and compliance with ISO27001 for risk management against data being handled, processed and any potential risks towards assets within the university. Carrying out the risk assessment successfully demonstrates compliance towards these standards and regulations avoiding any legal actions or other adverse actions by not abiding.

This security risk assessment will also provide a better vision and understanding of Return of Investment (ROI) allowing for enhanced strategic planning with more identifiable goals and achievements for security in the future. ROI for security is not easily identified without a risk assessment leaving justification of security investments, stakeholder communication and quantification of potential losses to be a mystery or lacking. Conducting this risk assessment allows for the quantification of potential loss comparing to what can be invested at that time and providing a justification for investment, how security controls will help, what threats/vulnerabilities they will remove and how potential loss or damages to the organisation will be reduced.

# Risk Assessment

## Threat & Vulnerability Identification

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Assets | Threats | Vulnerabilities | Description | Inherent Risk | | |
| Impact | Probability | Risk Level |
| Operating Systems | Improper access controls | Malware - Brute force attacks | Brute force attacks on operating systems with incorrect access controls such as MFA present the risk of attackers gaining access | 3 | 5 | 23 |
| Cloud Software | Theft of documents | Open S3 buckets | Misconfigured S3 buckets which are open potentially allow data theft via internal staff or external threat actors if completely open | 5 | 4 | 21 |
| Operating Systems | Malware attacks | Unchanged superuser credentials | Standard superusers i.e., admin:admin are well known and easily guessed by attackers | 5 | 5 | 25 |
| Internal Systems | Device failure | Outdated operating system / Software | Old OS/Software versions can produce incompatibility issues, performance issues or system failure | 4 | 5 | 24 |

Table 1 – Table containing example risks of the highest threat to the university.

Table 1 displays four risks which pose the highest threat to the university across various areas covering cloud applications, operating systems, and internal systems. These all present a risk to one of more aspects of the CIA triad and are substantial enough that they can generate or contribute to other risks present within the risk register leading to potential catastrophic consequences.

### Cloud software – Theft of documents

Misconfigured S3 buckets (AWS) or equivalent dependent on cloud services the university is using (e.g., blob storage for Azure) creates an access point to stored documentation and the network. Focusing on S3 buckets, providing these are open, this allows anyone, threat actors or current employees to access them without any verification needed.

Should any sensitive documentation be stored in these S3’s, this creates confidentiality, integrity, and availability issues. The free access to this documentation can allow for data manipulation, destruction and access to sensitive data which would otherwise be locked down to certain staff members.

### Operating Systems – Brute force attacks

Improperly enforced access controls on operating systems such as poor password policies and/or lack of multi-factor authentication for user accounts will lead to successful brute force attacks by threat actors. These attacks open risk to confidentiality and integrity of sensitive documentation and the integrity of the systems themselves.

This is rated as a highly likely threat due to the risk being relatively simple following misconfigured controls with a medium impact score as although this would leave the threat actor with potential access to documentation and the ability to brake systems, administrative controls and individual file encryption would lessen the impact of this.

### Operating Systems – Malware attacks

Similarly, to brute force attacks, both windows, Linux and OSX systems have standard admin users which have common username and password combinations such as admin:admin. This is one of the very first areas a threat actor will attack to escalate privileges within a network hence why this is rates as five for both impact and probability as it could not only allow them admin access to a number of services such as active directory but potentially a large knock-on effect throughout the entire estate.

### Internal Systems – Device failure

Systems, components, and services with out-of-date software open the university up to device failure via compromised integrity. These old software versions introduce compatibility, performance, and security issues. This has been rated at five for probability as this is a common recurrence and is something which regularly presents threats to internal systems. Also presenting significant impact to internal systems, due to not only the loss of integrity but also the loss of availability potentially affecting the entire estate.

The affect on controlling these risks whether through remediation or risk reduction could dramatically lower the domino effect of other assets such as personally identifiable information, sensitive documents and infrastructure components being affected and further reducing compromise of CIA.

Figure 1 - Inherent risk level before controls have been implemented.

# Risk Treatment/Control

The most identified risk controls fall in-line with risks associated with the highest threat towards the university’s estate and found to be potential remediations, reductions or avoidance of multiple risks throughout separate asset groups also preventing collateral damage via a chain of consequences.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Unauthorised access | Lack of multifactor authentication | Systems lacking MFA are wide open to attacks which allow unauthorised access to the network | 4 | 3 | 14 | Implement Multifactor authentication such a SDO and Fido | 2 | 2 | 7 |
| Equipment Failure | Outdated server software/operating system | Improperly maintained server could lead to lack of availability following equipment failure | 5 | 4 | 21 | Implement regular update for both software and operating systems. | 3 | 3 | 13 |
| Compromise of data confidentiality via social engineering | Lack of staff training in social engineering scenarios i.e., phishing | Staff with improper training will not be able to easily recognise social engineering scenarios and therefore are more likely to hand out sensitive information | 4 | 3 | 14 | Dedicate training time to staff towards social engineering to increase social awareness within these scenarios | 4 | 2 | 9 |
| Lateral Movement | Server misconfiguration | Misconfiguration can easily allow threat actors to bypass security controls or gain access to high level accounts | 5 | 2 | 11 | Ensure server is configured as expected, applications/services are setup correctly | 3 | 2 | 8 |

Table 2 – Table containing example risks associated with highest frequency controls.

Table 2 displays four risks to the university across various areas. These again all present a risk to one of more aspects of the CIA triad and are substantial enough that they can generate or contribute to other risks present within the risk register leading to potential catastrophic consequences. Attached are the controls and re-calculated risk score in accordance with these controls being applied

### Multifactor authentication and enforcement of strong password policies/file encryption

Implementing multifactor authentication into the university’s estate instantly provides an extra layer of security whether this be something you have such as a soft or hard token, something you are i.e., FIDO key or something you know i.e., personal identification number. Usually these are forms of authentication an attacker would not be able to guess or brute force making gaining access near impossible without specific knowledge.

Pairing MFA with strong password policies for accounts and encrypted files significantly reduces both the impact and probability of a risk.

### Update: Software, hardware, firmware, operating systems

Multiple threats identified within the risk registers are related to poor maintenance of computer systems and hardware. Creating a maintenance schedule to carry out important hardware, software and firmware updates will reduce the overall risk score and remediate any previous vulnerabilities to systems.

### Staff training for data security, sensitivity, and social engineering scenarios

Providing training for staff on data security and social engineering scenarios to increase awareness of threat actors attempting to gain information, for example by acting as the person in question or a trusted third party the university deals with, greatly reduces the probability of compromised confidentiality. Although the impact score of this doesn’t necessarily change, the significant impact this threat would originally introduce to the estate prior to staff training can easily be avoided.

### Correct configuration of systems and services

Ensuring systems, servers, services, and applications are configured and setup correctly is paramount to preventing high level threats such as lateral movement. When working with cloud service providers, this risk must be shared as the university won’t have full control over some settings.

Figure 2 - Inherent risk level post control implementation (significantly reduced)

# Recommendations

The main controls which would have the most success and be effective in preventing threats within the university are the combination of multifactor authentication and frequent organisational updates. MFA provides an extra layer of security to systems throughout the estate which preventing attacks and also ensuring the user who is accessing the account or service is the user who should have access.

Secondly the frequent updates reduce system and network vulnerabilities significantly lowering the routes a threat actor can take to exploit and gain access to confidential information, implementing a schedule to carry out these updates will further enforce this.

Lastly the combination of both MFA and regular updates significantly reduces the probability of many risks found throughout the risk register, making it drastically more arduous to not only gain access to the network and its systems, but access PII/sensitive documentation and modify, destroy or exfiltrate.

# Appendices

A green screen with white text

Description automatically generated

Figure 3 - Risk Register

A green screen with white text

Description automatically generated

Figure 4 - Risk Register

A green screen with white text

Description automatically generated

Figure 5 - Risk Register

A green screen with white text

Description automatically generated

Figure 6 - Risk Register

A green screen with white text

Description automatically generated

Figure 7 - Risk Register

A green screen shot of a computer screen

Description automatically generated

Figure 8 - Risk Register

A green screen with white text

Description automatically generated

Figure 9 - Risk Register

A green screen with white text

Description automatically generated

Figure 10 - Risk Register

# Figures

[Figure 1 - Inherent risk level before controls have been implemented. 2](#_Toc165137344)

[Figure 2 - Inherent risk level post control implementation (significantly reduced) 5](#_Toc165137345)

[Figure 3 - Risk Register 8](#_Toc165137346)

[Figure 4 - Risk Register 9](#_Toc165137347)

[Figure 5 - Risk Register 10](#_Toc165137348)

[Figure 6 - Risk Register 11](#_Toc165137349)

[Figure 7 - Risk Register 12](#_Toc165137350)

[Figure 8 - Risk Register 13](#_Toc165137351)

[Figure 9 - Risk Register 14](#_Toc165137352)

[Figure 10 - Risk Register 15](#_Toc165137353)

# Tables

[Table 1 – Table containing example risks of the highest threat to the university. 0](#_Toc165137354)

[Table 2 – Table containing example risks associated with highest frequency controls. 3](#_Toc165137355)