

CS6501 Assignment 1

2231290

ANDREW GRAFF

Dr Manish Singh

Table of Contents

Introduction.....	2
Part One.....	3
Lab 1.2 Cryptography	4
Lab 1.3 Cryptography (Continued)	6
Lab 1.5 Security Policies.....	10
Lab 1.1 McCumber Model	13
Part Two	16
Qualitative Risk Management.....	17
References.....	20

Information Security Assignment 1 CS6501

1. **Purpose: Why am I doing?**
2. **Motivation: Why am I doing this?**
3. **Clarity – What are sections of my report / What am I delivering?**

Talofa lava,

In this report we will venture in the broad field of information security and understand the various complex nature of how we perceive security of how we secure, protect, and analysed important information and data. It is vital for anyone delving into the security field of information technology to grasp a conceptual understanding, by not only practical measures but a level of security awareness thinking alike.

An increased presence of online users prompts an accompanying option to perform virtually any duties remotely. These are the inevitable shifts to an interactive world. We understand whilst the transition is global, it also increases the potential of risk. Exploring practical techniques and methods to help reduce these risks to protect ourselves and others are motivating factors.

There are two main sections of this Information security report that will give us a brief idea of the practical methods and techniques of applying protection to data and adapting cognitive security thinking. The first part is lab analysis and evaluation, where we show the understanding of what was performed in the lab and analysing by providing reference to the lectures covered in weekly sessions.

The labs I have selected are; *Lab 1.2 Cryptography, Lab 1.3 Cryptography Continued, Lab 1.5 Security Policies and Lab 1.1 McCumber Cube Information Security Management Model*. These will be in separate sections throughout the report.

The last section is Qualitative Risk Management where we perform some calculations using formulas to be able to measure and weigh out the importance against what is determined as valuable.

We conduct a risk assessment using these techniques and establish an outcome to see what is worth considering to cover given financial restraints.

Part One: Lab Analysis and Evaluation

Exercise is to provide evidence that you understand the concepts behind lab activities in this course, providing reference to the lectures that are covered in the weekly sessions.

You are to complete ONE mandatory lab plus THREE of the selected labs to demonstrate your understanding of the subject matter, and you will analyse and compare the lab material to the corresponding lecture notes.

Lab 1.1 McCumber Cube Information Security Management Model

Lab 1.2 Cryptography

Lab 1.3 Cryptography

Lab 1.5 Security Policies

Lab 1.2 Cryptography

1. We will detail the account of activities undertaken in the lab, including interesting or unexpected findings
2. The central concept behind the lab activity, and its alignment with understanding Information Security Principles
3. An overall review of the lab, with suggestions for additions, and/or improvements. This should include extension activities

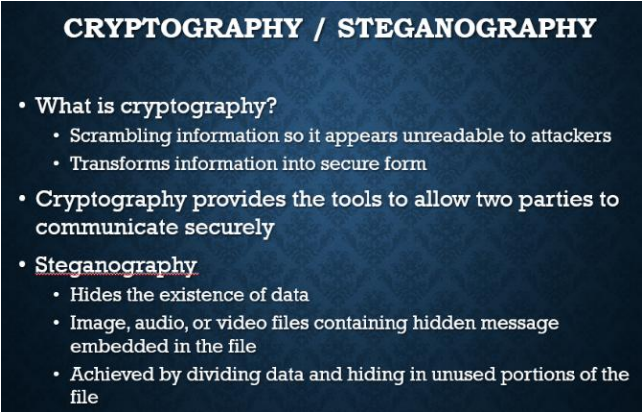
Lab 14: Cryptography Concepts

In this lab we used steganography techniques using various tools. As per lecture slides, we find steganography involves concealing messages in images, audio or video files. We learn this is achieved by dividing data and hiding in used portions of this file. This is where plain text is converted into binary form,

The purpose of steganography is to covert communication to hide a message from a third party.

Cryptography is the art of secret writing which is intended to be unreadable by a third party.

During this lab the activities undertaken were creating a secret message txt file and hiding this in an image.



CRYPTOGRAPHY / STEGANOGRAPHY

- What is cryptography?
 - Scrambling information so it appears unreadable to attackers
 - Transforms information into secure form
- Cryptography provides the tools to allow two parties to communicate securely
- **Steganography**
 - Hides the existence of data
 - Image, audio, or video files containing hidden message embedded in the file
 - Achieved by dividing data and hiding in unused portions of the file

We learn something interesting called the “steghide” command which is a powerful steganography tool to hide messages or files within an image, video or audio file.

We found an image to use and check how much space we can use to conceal a message. We then check the size of this txt file to ensure it is operable and confirm sha1 hash value for comparison later. Then begin the steganography process

```
steghide info top_secret.jpg
du -b secret.txt
sha1sum top_secret.jpg
steghide embed -cf top_secret.jpg -ef secret.txt
```

steghide: tool to hide message, **embed**: mode is used to hide data inside the file, **-cf**: cover file, the image file you will use to hide inside and **-ef** embed file, the file you want hide) So we see **top_secret.jpg** and concealing **secret.txt** – the txt file we created earlier. (Alim, 2022). We then enter a passphrase to lock this information.

```
kali@kali: ~/Desktop/steg
File Actions Edit View Help
(kali@kali)-[~/Desktop/steg]
$ echo "The password to the WinOS is NDGLabpass123\!" > secret.txt
(kali@kali)-[~/Desktop/steg]
$ cat secret.txt
The password to the WinOS is NDGLabpass123!
(kali@kali)-[~/Desktop/steg]
$ steghide info top_secret.jpg
"top_secret.jpg":
  format: jpeg
  capacity: 119.1 KB
Try to get information about embedded data ? (y/n) n
(kali@kali)-[~/Desktop/steg]
$ du -b secret.txt
44      secret.txt
(kali@kali)-[~/Desktop/steg]
$ shasum top_secret.jpg
85527a71b0612b06fd4b9535c96765c97f8a1a59  top_secret.jpg
(kali@kali)-[~/Desktop/steg]
$ steghide embed -cf top_secret.jpg -ef secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "top_secret.jpg" ... done
(kali@kali)-[~/Desktop/steg]
$
```

As concealing the secret message is equally as important as extracting the secret message. We simply use;

steghide extract -sf top_secret.jpg

extract: mode and **-sf:** specify the file with secret message.

Enter the passphrase and you will obtain the secret message. As it is in a text file, we check the contents by cat command.

```
(kali@kali)-[~/Desktop/steg]
$ cat secret.txt
The password to the WinOS is NDGLabpass123$
```

We were also able to hide multiple files within an image file using basic Linux commands, very similar to what we used to hide a text into an image. As per the above, we ensure we can see the size of the files (ls -lh command) ls command to list files and lh command to list human-readable sizes.

A command was used to create a zipped (zip) archive file to contain a text file and an image file, then redirecting this to a new created file using (cat) command and redirecting this (>) to the named file. In Linux, you can almost create any type of file by the CLI, showing versatility and simplicity. Below were the two functional commands.

kali@kali\$ zip secret_files secret.txt top_secret.jpg

kali@kali\$ cat cyber_monday.jpg secret_files.zip > cybersec.jpg

The central concept behind this activity and the alignment with understanding Information Security Principles is:

The use of Steganography and how this tool can be used to send files with hidden messages. We learn techniques of what commands are used and how it works in Kali Linux. In this activity we hide a message in an image file, hide multiple files within an image (by creating a zipped file and cat) and observed the avalanche effect in hashing operation. We see how hash functions is affected in cryptography to indicate the significance of its encryption security by seeing/testing the many different conversions and output of plain text. These protect confidentiality one of our important information security principles to ensure there are no third party intrusions to deliver a message for an intended recipient only.

An overall review of the lab, with suggestions for additions, and/or improvements. This should include extension activities

An interesting lab, learning how files are created, embedded, extracted etc. A hands-on approach given step by step and breaking these down slowly in a way for myself to understand. It was my first time seeing the practical applications of how we can protect information. The lab had a timer and the request for extension was limited to what could be explored. It did in a way feel the comprehensive understanding would be restricted given progress could not be saved and continued.

Lab 1.3 Cryptography Continued

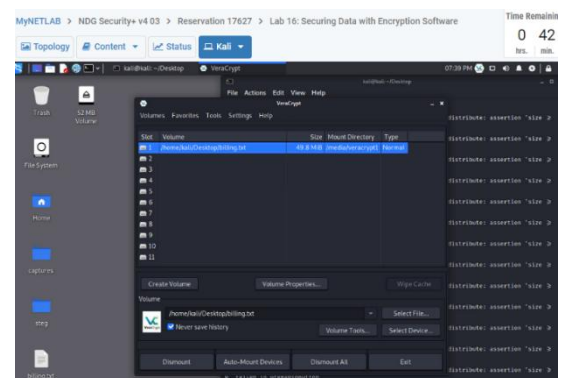
1. We will detail the account of activities undertaken in the lab, including interesting or unexpected findings
2. The central concept behind the lab activity, and its alignment with understanding Information Security Principles
3. An overall review of the lab, with suggestions for additions, and/or improvements. This should include extension activities

Detail the account of activities in the lab, interesting or unexpected findings

Lab 16: Securing Data with Encryption Software

In Kali Linux, we learn to use Veracrypt container as a tool to secure files. This was a way by having an accessible software in our desktop to simply drag files to encryption. The following steps was how this was conducted.

We used the CLI to perform our operations and found it was interesting we could simply access veracrypt by typing this in the terminal.



A txt file was created (we will use to encrypt)

touch billing.txt to create a text file

veracrypt

(Launches the application) create volume, create an encrypted file container, standard veracrypt volume, select the billing.txt file as volume location and replace. Encryptions algorithm is at AES and Hash algorithm at SHA-512, volume size at 50mb, password set on the container with FAT as default settings. Moving the mouse randomly generated a higher cryptographic strength of encryption keys for the Volume Format.

Learning about the encryption algorithm, as per our lecture slides. We see there are two ways to notate the use of a specific key: $C = EK(M)$, $C = E(K, M)$

C = cipher, E = encryption, K = key, M = message. So the first way indicates Ciphertext is obtained where the encryption key (EK) is used to encrypt or decrypt a message (M). This is symmetric algorithm. The second is encrypting both the key and message $E(K, M)$

Symmetric involves private key encryption so both encryption key and decryption key are the same. Asymmetric involves public key encryption, so both keys are different.

In the instructions, we set Encryption Algorithm at AES (this is symmetric key encryption algorithm) and Hash algorithm at SHA-512. AES converts blocks of data into encrypted data. “SHA is widely used for data integrity verification, digital signatures, and password storage while AES is commonly used for data encryption, VPN and TLS/SSL encryption, and disk encryption”, (Miller, 2023).



“The encryption key is a piece of data utilized in cryptography to transform plaintext into cipher text (encryption) and vice versa (decryption). Its complexity defines the difficulty of the decryption process for unauthorized parties”, (Moes, 2023).

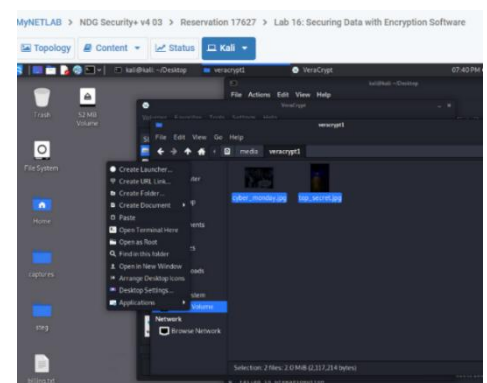
We created an encrypted volume container (a place where files could go to be secured in an encrypted hard drive on disk)

These were the instructions showing me what to do during this lab. It was being familiar of the processes and why we create a volume and these settings for an encrypted container. “We achieve these results by leveraging computational assumptions, not just for encryption but, more interestingly, to hide volumes themselves,” (Kamara et al 2019)

We created a VeraCrypt container (billing.txt) and can now select this and mount on an available drive slot in the VeraCrypt application. We enter the password set for billing.txt container. Drive is successfully mounted as we see the drive on desktop

We then copy and paste two images in the veracrypt container

It was interesting to know encryption software such as VeraCrypt could easily be created and mounted to the desktop. Where any files dragged to this disk will be automatically encrypted.



The central concept behind this activity was encryption and how we can secure our data using encryption software. The alignment to Information Security Principles is confidentiality by protecting files and ensuring it is only readable by the intended recipient. This type of encryption appears to be symmetric encryption with the generation of one key and bulk encryption. We secured the files in a container with a password.

SYMMETRIC VS. ASYMMETRIC		
	Symmetric	Asymmetric
Algorithm	Manipulation of bits	Mathematics
Number of Keys	One	Two
Key distribution	The key has to be shared "out-of-band" before encryption.	No prior arrangement is necessary. Just use the recipient's public key
Authentication	Cannot pinpoint the sender if key is shared by more than two people.	Can trace the message to the owner of the related private key.
Use	Bulk encryption	Key distribution Digital signature
Speed	Fast	Slow

A lecture reference to the left, seeing the differences between the keys. The VeraCrypt we used in the lab was symmetric keys. We know this because the same key used to encrypt is the same key we use to decrypt.

The review of this lab was a step-by-step process, although unable to get explanations for why the settings were set when building the encryption folder. We used one tool which was VeraCrypt. A way to improve would be having another way of encrypting files to see what a scenario of an asymmetric key will unfold or other software that operate similar to VeraCrypt.

Lab 1.5 Security Policies

1. We will detail the account of activities undertaken in the lab, including interesting or unexpected findings
2. The central concept behind the lab activity, and its alignment with understanding Information Security Principles
3. An overall review of the lab, with suggestions for additions, and/or improvements. This should include extension activities

Detail the account of activities in the lab, interesting or unexpected findings

In this Security Policies lab, we are to identify similarities and differences between the ICT Computer Acceptable Use Policies at WelTec and Whitirea.

Similarities		Differences	
Weltec	Whitirea	Weltec	Whitirea
Both Policies/Procedures are due for a review		Policy effective since 2009	Procedures due for review since 2016
Weltec: 3h & Whitirea 5.2: Emails must meet the same standards of published documents.		9. Personal use: Relevant Policies, including but not limited to this policy, policies on EEO, Harassment, intellectual Property, Code of Conduct, are observed.	Relevant policies are observed.
Both institutes recognise the principles of academic freedom by the principles set out in the ETA.		Weltec Business Policy articulates principles and guidance governing the use of Weltec production network.	Whitirea ICT Procedures outline the acceptable use of ICT resources and services.
Both documents relate to Information Communications Technology (ICT).		Security, efficiency, activities through the use of ICT consistent with code of practice	Acceptable use and standard of conduct
Documents applies to staff and students who use ICT services.		Weltec has internet policy guidelines	Whitirea has regulatory standards around ICT
Personal Use sections in both documents			

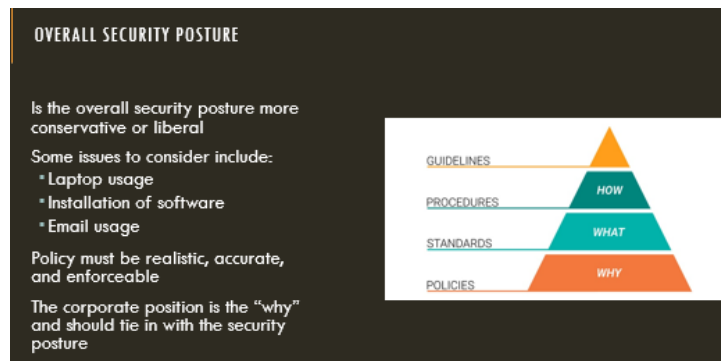
		resources except Internet.
	There is a request for access to restricted Internet sites form	No request for access to restricted internet sites form
Documents list Information Security and user emails are similar documents Whitirea Procedures 11.1 Users of email is similar to Weltec Policy Guideline 4.b	Not enlisted in procedures	Authorisation to use broadcast electronic communication
Weltec 6. Statement of Responsibility is similar to Whitirea 15. Responsiibilities of ICT Services.	ICT resources must be used in support of teaching, education and research, consistent with the education objectives of the institute and for business related purposes.	ICT resources at discretion of a manager full time or part time proportional or contract employee may be given access to either a shared or dedicated resource.
	Weltec document has a contents and 19 pages.	Whitirea has no contents given shorter document of 7 pages.

I will then provide suggestions regarding development of a common policy document. Suggestions will be to incorporate both a policy and procedures document, contents page with regular checks to ensure its validity and is up to date. This will harmonise both documents together with a nice user-friendly modern look. Clarity of document, with the intent and purpose, main policy statements, structure formality and meeting any legal requirements.

The findings in this security and policies labs were being able to identify and understand the difference between policy and procedures. Policy revolves a lot more around regulatory requirements that are mandatory and must be followed. Procedures are step by step guidelines to accomplish an activity or task. In this case, procedures do compliment policy.

“By providing your employees with clear guidelines in well-defined documentation, you can be confident that your organization is prepared to face today’s threats confidently”, Lane, 2023).

The central concept behind this Security Policies activity was grasping a conceptual view of how documents are important towards security ensuring not only proper use but also keeping organisation data secure.



The above image is a lecture note reference of the overall security posture. Whilst this particular lab activity leans towards Policy and Procedures, we can see a simplified way of the approach when it comes to different important areas: Guidelines, Procedures, Standards and Policies.

Information security is a broad field and having these documents in place reinforces the aspects of what end users should be aware with guidelines to follow. These are standard practices given the legality involved thus policy documents revolving carefully and providing reference. These helps reduce any risks or threats to the organisation. Walls between legislation that govern the policies and rules set by the institute.

Overall review of the lab and suggestions are having other documents to also examine and view so we can see how policies work for different institutions. It was interesting to see what the policies and procedures were as a student.

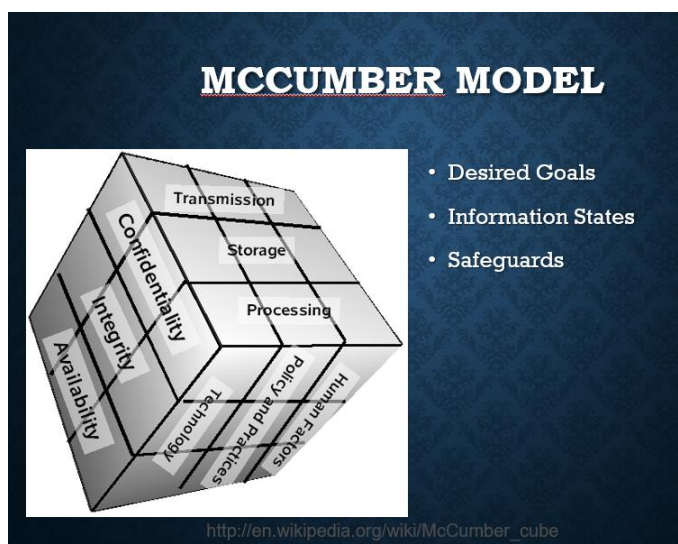
Lab 1.1 McCumber Cube Information Security Management Model

1. We will detail the account of activities undertaken in the lab, including interesting or unexpected findings
2. The central concept behind the lab activity, and its alignment with understanding Information Security Principles
3. An overall review of the lab, with suggestions for additions, and/or improvements. This should include extension activities.

Detail the account of activities in the lab, interesting or unexpected findings

The activities in this lab, were about the McCumber Cube Information Security Management Model. A model used to help see what needs to be addressed to secure a system. In this activity we apply this model to address our practices that intersect three cells. The three cells being Confidentiality, Integrity and Availability and the others, that make up the McCumber cube. We used this method to see what we would do for our Security folder in the One Drive and ways to better secure.

We are familiar with CIA model and the importance towards Information Security. The McCumber Model adds another layer to this in a re-evaluating another way to better secure a system. It was revisiting these concepts; Confidentiality to ensure the data is only accessed by authorised users, Integrity the accuracy and unaltered data and Availability ensuring information is accessible when needed.



What interests me about this model, is the way each layer intersects like a Rubix cube signifying the many multiple combinations that could be made.

These are all important that it securely compliments each other.

Desired Goals: *Confidentiality, Integrity, Availability*

Information States: *Transmission, Storage, Processing*

Safeguards: *Human Factors, Policy and Practices and Technology.*

This McCumber Model has more than 3 attributes than our CIA triad model. Here we have 9 attributes that are all important to discussing security issues.

Confidentiality: Authorisation of information (Non-disclosure)

Integrity: Data/Information (Accuracy)

Availability: Information available

These are our important principles from the CIA triad model and are recognised as the foundation to Information Security. These are known as the desired goals and are part of one dimension of the McCumber Model.

Transmission: Transferring information

Storage: Storing information

Processing: Processing information (making information available to the unit with likely modifications)

These are the states and movement of data in three ways: Data in transit, Data at rest or in storage and Data in process as per lecture notes. It is important to protect the data in the three different possible states to avoid any data from being leaked or at risk of being accessed by any unauthorised persons. This is the second dimension of the McCumber cube model.

Technology: Technological solutions

Policy and Practice: Rules around Information Assurance (“what and when” is policy & “how” is practice)

Education: Training and awareness

Lastly, the safeguarding of data. The information or awareness for end users, or those in the space of information to have education and guidelines on how to safe keep information. These are sensitive to the law, protection abiding by legislation or corporate regulations.

We could now formulate a way to cover the intersecting cells and we apply this to securing course material. The lab required a brief statement on each sentence. An example would be: Confidentiality – Policy – Transmission: “Only authorised students with current student ID and logins can access course material”.

This lab relates closely aligns with Information Security Principles CIA model. Equipping the mindset of a security analyst/policy writer to see all areas of what needs to be covered which is the central concept of this activity. Building strong practices with good practices. The McCumber Model was developed by John McCumber (early cybersecurity expert).

“The Cybersecurity Cube identifies the three types of skills and disciplines used to provide protection. The first skill includes the technologies, devices, and products available to protect information systems and fend off cybercriminals”, (Golovatenko, 2018).

An overall review of the lab, it was the first lab presented and kicked started Information Security 2 course. Completing the McCumber Model had its own challenges but was fun to explore and realising how this is important if venturing in the field of chasing a security analyst/cybersecurity role. These are global definitions that aren't restricted to studying institutions as these are real life scenarios.

An action could cover two dimensions of the cube. Examples would Confidentiality, Policy, and Storage to implement a policy or news to students when uploading assignment to Moodle to zip and encrypt files to protect from any interception. These same practices could be applied to a financial institution environment and writing articulate policies that reflect the safeguarding of important data/information.

Part Two: Risk Management Exercise

Qualitative Risk Management

Compile a list of information you store on your personal computer or online using the provided information asset template from the Open University, which I will make available as a separate document. For example, you may have personal correspondence, photographs, work documents or personal details such as an identity document, insurance policy details and passwords for online services.

Introduction to Cyber Security

Information asset list

Information Type	Location (device / online service)	Value (High / Medium / Low)	Relevant Threats
Media (Photo/Video)	Device and Online	High	Malware Attacks
Work Documents	Device and Online	Medium	Malware Attacks
Identity Details	Online	High	Phishing (Social Engineering Attack)
Passwords Online	Device and Online	High	Password Attacks
Applications	Device	Low	DDoS Distributed Denial of Service
Laptop	Device	Medium	Physical Attacks
Software Tools	Device	Low	Zero Day exploits – unknown vulnerabilities
Files	Device	Medium	Malware Attacks
Social Logins	Online	High	Social Engineering Attacks
Email	Online	High	MitM Attacks (Intercept communication)
Online Banking	Online	High	Malware/Password Attacks
Shopping	Online	Low	DDoS

For each type of information, think of its value to you. Label the most valuable types of information as ‘High’, the least valuable as ‘Low’ and those that are in between as ‘Medium’.

The value could be the cost to replace the information, in time or money, or the impact of its loss on your reputation, for example, all your emails or photographs could all be published online.

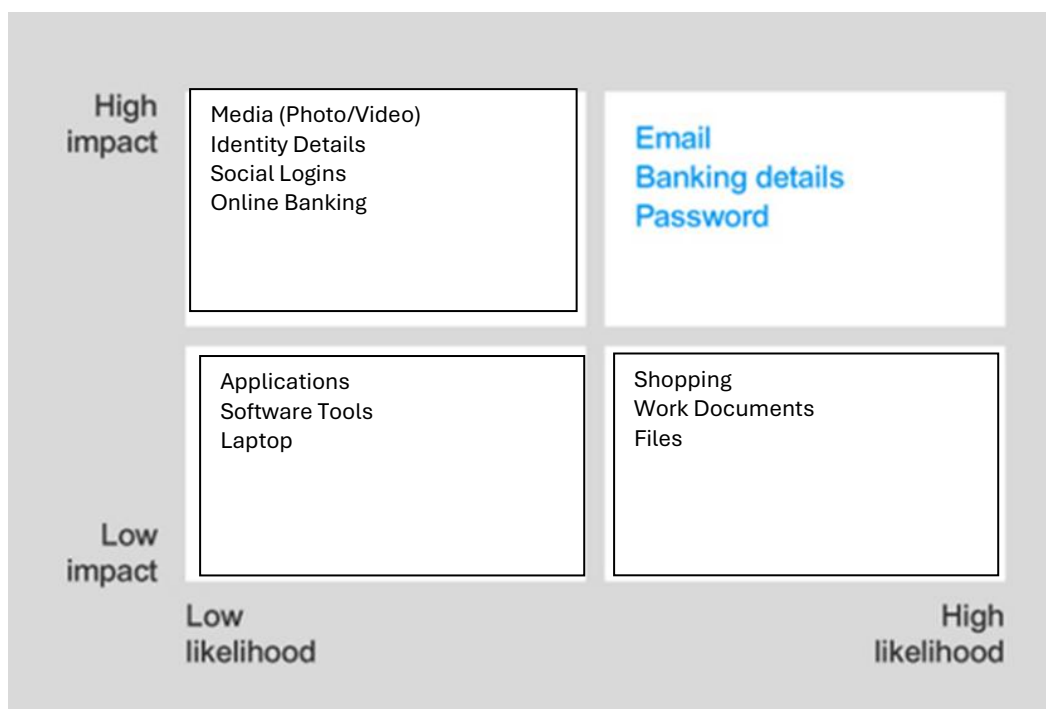
Do the same exercise for the online activities you engage in. For example, you might use online banking, shopping or social media. This time, label each one with a value based on the potential cost of an unauthorised person gaining access to it.

The main technique for a qualitative analysis of risk is to construct a likelihood–impact matrix in which the likelihood and impact of each risk event are assessed against a defined scale and then plotted on a two-dimensional grid. The position on the grid represents the relative significance of each risk. The simplest matrix is formed by classifying both likelihood and

impact as either high or low, which leads to a 2 by 2 grid. This basic classification of a high or low value leads to the following rank order for tackling risks:

1. high-impact, high-likelihood risks
2. high-impact, low-likelihood risks
3. low-impact, high-likelihood risks
4. low impact, low-likelihood risks.

By way of an example, assume that when you compiled a list of information stored on your personal computer or online, you identified email correspondence, banking details, and password information as information assets. Any successful attack on email, banking details and password information likely will have high impact and there is a high likelihood that these attacks will be targeted due to their high value. So, they should go in the high impact-high likelihood box.



Populate the impact-likelihood matrix with your identified e information assets.

Low-impact, low-likelihood risks are probably not worth expending much effort on. You can then look at the high-impact or high-likelihood risks one by one to determine whether there are ways either to reduce the impact if the risk occurs or to reduce the likelihood of the risk occurring, or both.

Quantitative Risk Management

- The following threat statistics have been gathered by a risk manager. Based on these calculate the ALE for each threat:

Threat	Cost per Incident	Occurrence Frequency	SLE*ARO	ALE
Software piracy	\$600	1 per month	$600 * 12$	\$7200
Computer virus / worm	\$2,500	1 per month	$2500 * 12$	\$30,000
Information theft (hacker)	\$3,500	1 per 3 months	$3500 * 4$	\$14,000
Information theft (employee)	\$6,000	1 per 4 months	$6000 * 3$	\$18,000
Denial-of-service attack	\$11,000	1 per 2 years	$11000 * 0.5$	\$5,500
Laptop theft	\$4,000	1 per 5 years	$4000 * 0.2$	\$800
Web defacement	\$1,500	1 per 2 years	$1500 * 0.5$	\$750
Fire	\$500,000	1 per 10 years	$500000 * 0.1$	\$50,000
Flood	\$300,000	1 per 15 years	$300000 * 0.066$	\$20,000

- Using the figures you calculated above, determine the relative ROSI (return on security investment) for each of the same threats with the following controls in place. Copy the values in the ALE column in the table above to the ALE₁ column below.

Threat	Cost per Incident	Occurrence Frequency	Control	ALE ₁	ALE ₂	Control Cost	ROSI
Software piracy	\$500	1 per 4 months	Anti-piracy protection hardware	\$7,200	\$1,500	\$15,000	-\$9,300
Computer virus / worm	\$1,300	1 per 5 months	Anti-virus	\$30,000	\$3120	\$5,000	\$21880
Information theft (hacker)	\$2,000	1 per 3 months	IDS	\$14,000	\$8000	\$30,000	\$1000
Information theft (employee)	\$7,000	1 per 18 months	Access Controls	\$18,000	\$4666.66	\$10,000	\$3333.3

Denial-of-service attack	\$4,000	1 per 10 years	Firewall	\$5,500	\$400	\$15,000	-\$9900
Laptop theft	\$5,000	1 per 10 years	Physical security	\$800	\$500	\$25,000	-\$24700
Web defacement	\$1,500	1 per 5 years	Firewall	\$750	\$300	\$15,000	-\$14550
Fire	\$75,000	1 per 10 years	Insurance	\$50,000	\$7500	\$30,000	\$12,500
Flood	\$50,000	1 per 15 years	Insurance	\$20,000	\$3300	\$30,000	-\$13,300

Grouping Controls

Control	Threat(s)	Savings $ALE_1 - ALE_2$	Cost of Control	ROSI
Firewall	DoS, Web defacement	5100-450: \$4,650	\$15,000	-\$10350
Insurance	Fire, flood	42500-16700: \$25,800	\$30,000	-\$4200

3. Remember that a single control may affect more than one threat, and you need to take this into account when calculating the ROSI. Based on your calculations, which controls should you recommend be purchased? Briefly justify your answer.

Controls to be purchased:

Purchasing the below controls will mean the company's net profit will be higher than sales revenue. Indicating the company is operating at a profit covering expenses for these controls. Where the cost of the other controls will lose profit. This is our cost benefit analysis.

Computer virus / worm

Information theft (hacker)

Information theft (employee)

Fire

References

(Alim, 2022)	Alim, A. 2002. Steghide – A beginners tutorial. Steghide — A beginners tutorial. Welcome. by Ashraful Alim System Weakness
(Lane, 2023)	Lane, S. 2023 Dec 5. The Purpose of Policies and Procedures What Are Policies & Procedures? Policy vs Procedure Explained (kirkpatrickprice.com)
(Kamara and Moataz, 2019).	Kamara, S., Moataz, T. (2019). Computationally Volume-Hiding Structured Encryption. In: Ishai, Y., Rijmen, V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science(), vol 11477. Springer, Cham. https://doi.org/10.1007/978-3-030-17656-3_7
(Moes, 2023)	Moes, T. 2023. What is an Encryption Key? Types You Need to Know What is an Encryption Key? Types You Need to Know (softwarelab.org)
(Miller, 2023)	Miller, T. 2023, April 19. SHA vs AES: What's the Difference? SHA vs AES: What's the Difference? - TechColleague
(Golovatenko, 2018)	Golovatenko, I. 2018, Dec 13. The Three Dimensions of the Cybersecurity Cube. The Three Dimensions of the Cybersecurity Cube - Swan Software Solutions