STRENGTHENING CYBER DEFENSES IN ACADEMIA: A CASE STUDY OF CYBERSECURITY CHALLENGES AND STRATEGIES IN THE APPLIED COMPUTER SCIENCE DEPARTMENT AT THE UNIVERSITY OF WINNIPEG

RESEARCH PROJECT

PRESENTED BY VI LE, SUPERVISED BY DR. VICTOR BALOGUN

ABSTRACT

THE UNIVERSITY OF WINNIPEG

The Applied Computer Science Department at the University of Winnipeg is grappling with heightened cybersecurity threats, an issue that is increasingly prevalent in the open and interconnected realm of higher education. This research presents an investigation into current cybersecurity protocols, highlighting a 44% surge in attacks since 2022, the exploitation of social trust via phishing, and a critical shortage of cybersecurity expertise. Interviews with the university community reveal awareness but also a concerning gap in effective cybersecurity management and policy execution, exacerbated by the BYOD trend and rising IoT use. The study advises bolstering defenses through targeted employee training and a holistic cultural shift towards prioritized cybersecurity, supported by case studies that reveal the severe consequences of breaches in other universities. The urgency for improved security measures is emphasized, with a recommendation for more inclusive future research to better understand and respond to these evolving cyber challenges

BACKGROUND

- “44% increase in cyberattack since 2022” - Checkpoint Blog
- 2200 cyberattacks every day according to research in 2017
- 28778 new vulnerabilities was discovered in 2023, an increase of more than 3000 compared to 2022 according to CVE
- A recent cyberattack at the University of Winnipeg occurred on March 24, 2024

THE UNIVERSITY OF WINNIPEG

CYBER INCIDENTS AT OTHER UNIVERSITIES

- On 11 September 2022, the University of Guelph reported disruption to its IT systems

- The University of Windsor suffered a system outage for two days in June of 2022

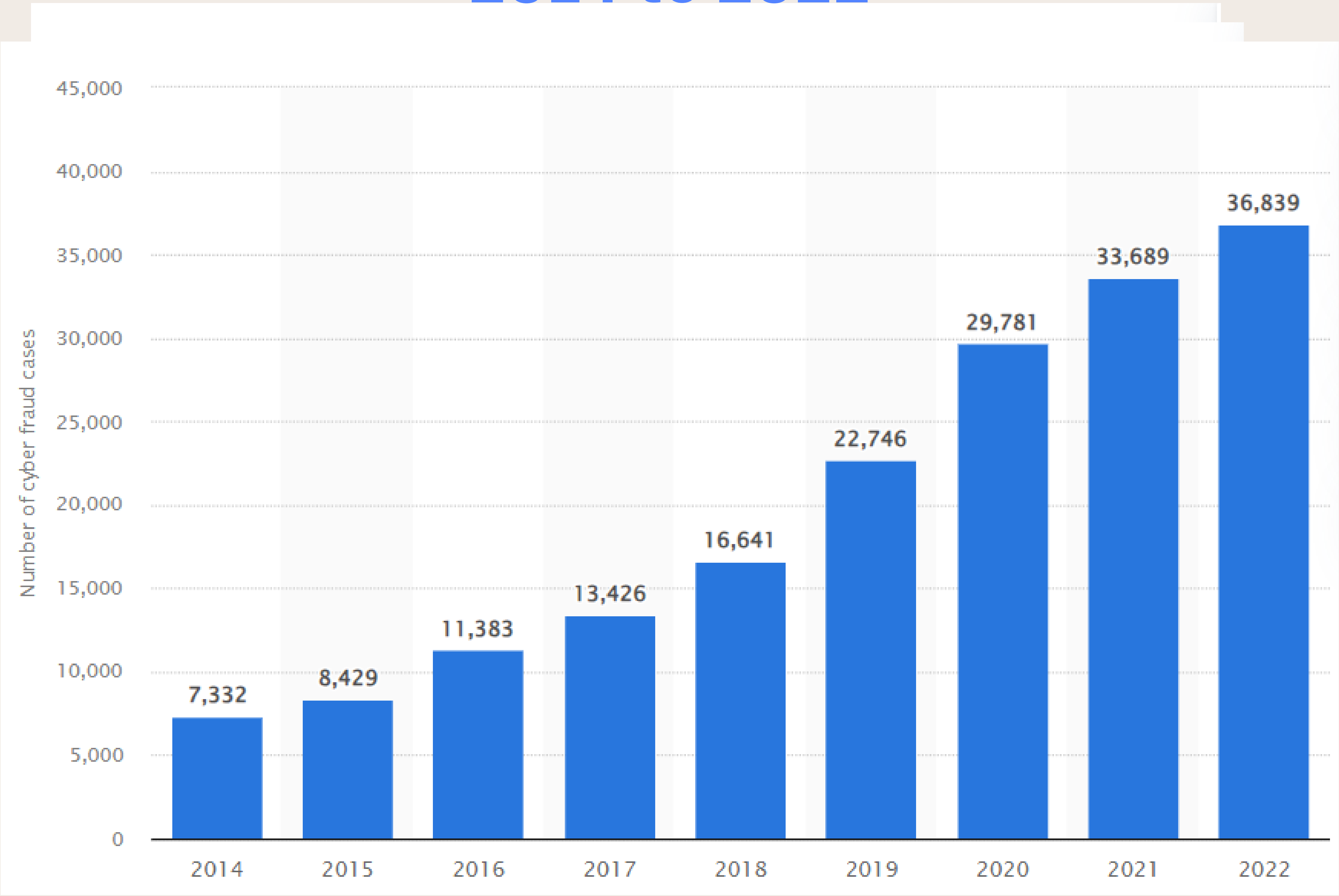
- Simon Fraser University suffered a ransomware attack on 27 February 2020

- Simon Fraser University was attacked again on 5 February 2021

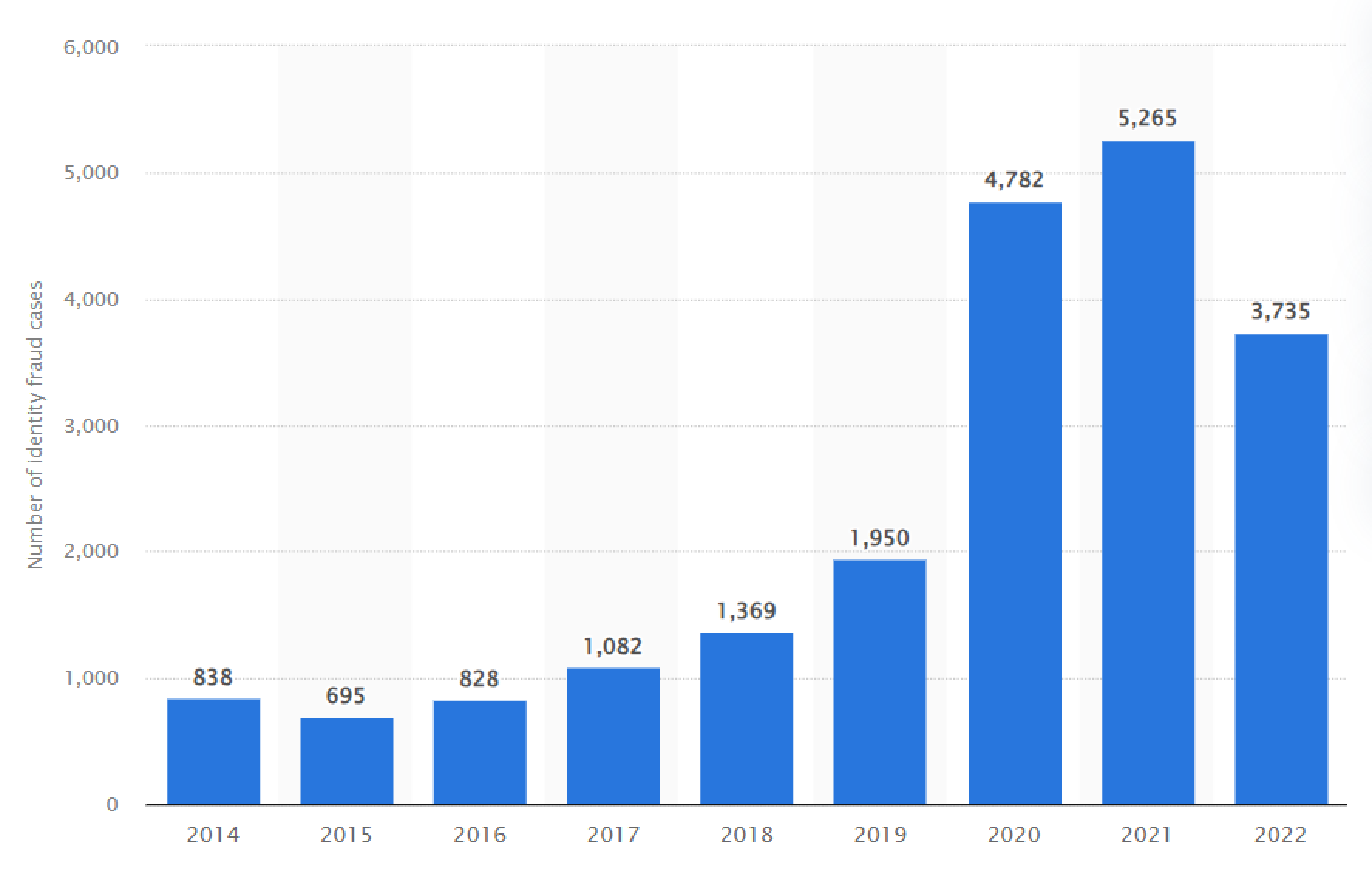
LUX ET VERITAS FLOREANT

THE UNIVERSITY OF
WINNIPEG

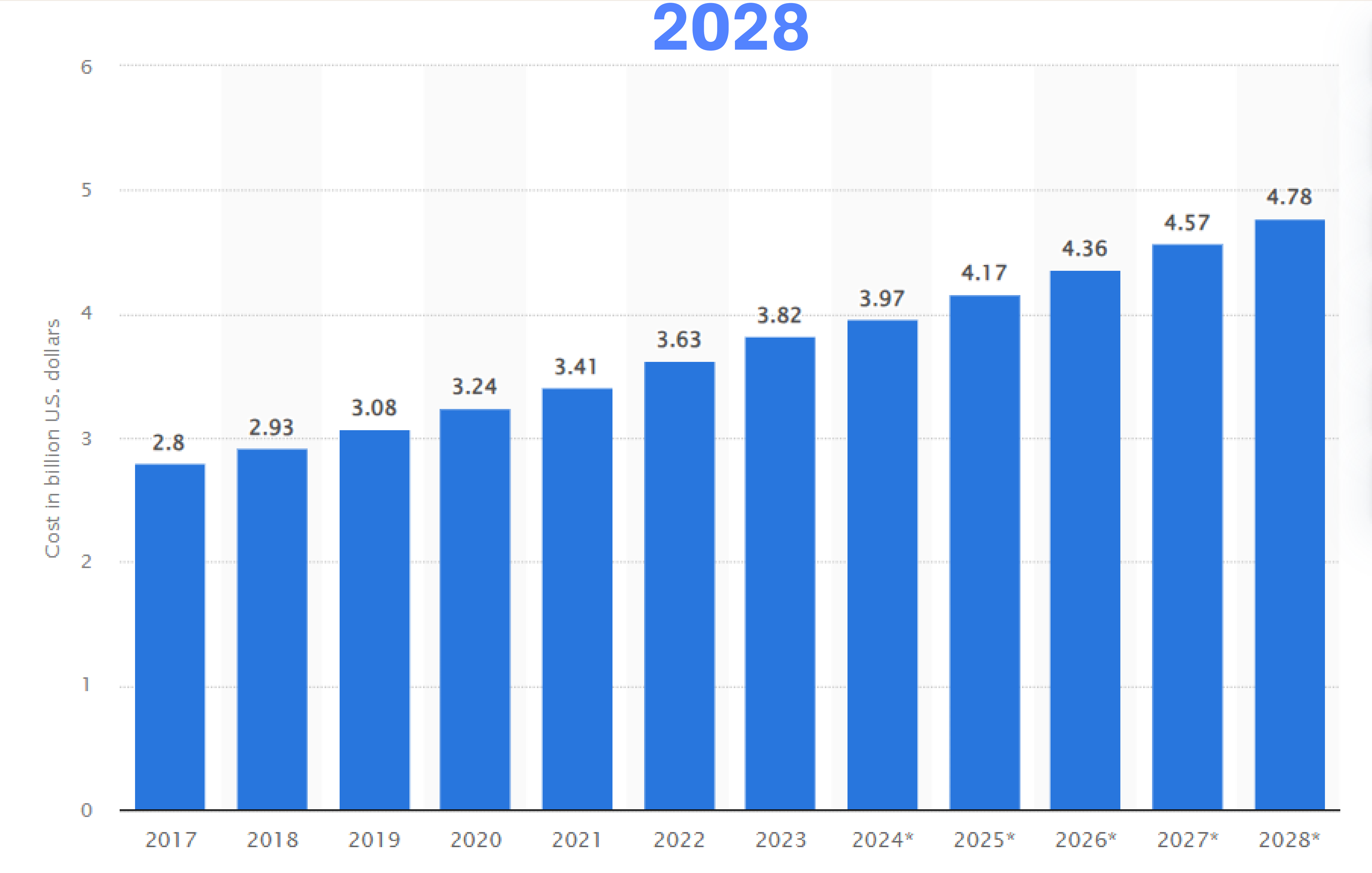
Number of police-reported instances of internet fraud in Canada from 2014 to 2022



Number of police-reported instances of online identity fraud in Canada from 2014 to 2022



Estimated annual cost of cybercrime in Canada from 2017 to 2028



OBJECTIVES

1 Investigate past cyber attacks within ACS department.

2 Analyze attack methods, attack surfaces, and damage caused due to those past attacks.

3 Review current systems, critical assets, and architectural design of ACS department

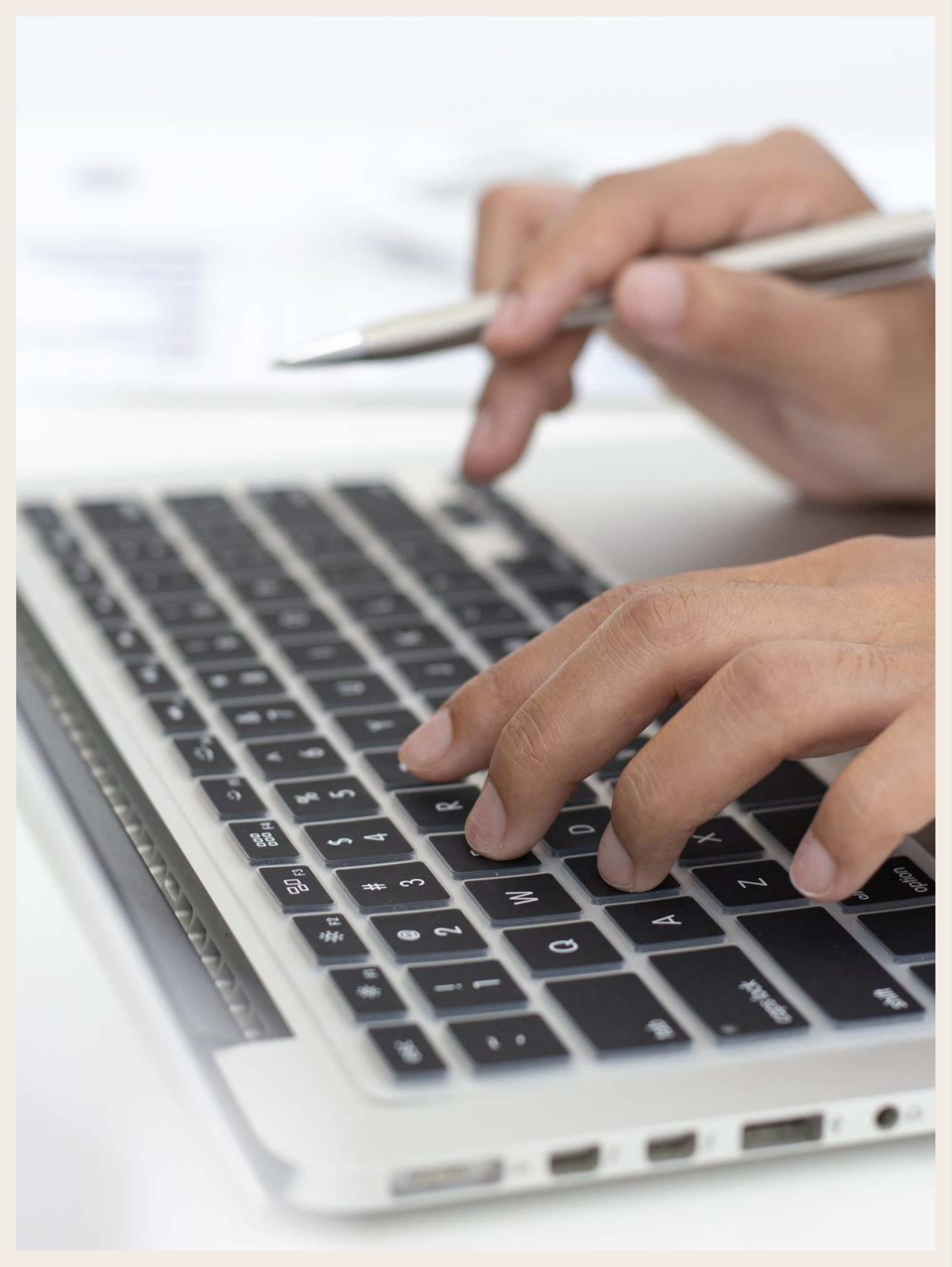
4 Evaluate current protocols, and security policies of ACS department

5 Evaluate the effectiveness of current control mechanisms, defensive measures implemented in ACS department’s system.

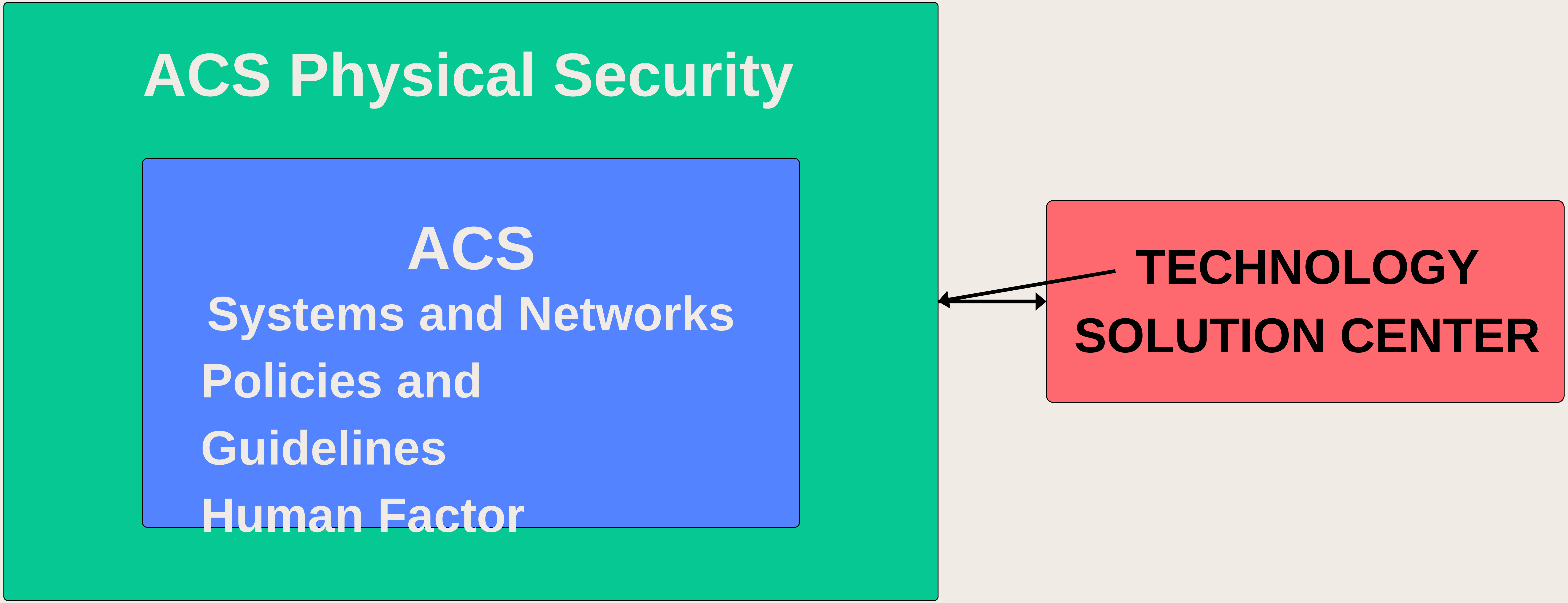
6 Conduct risk analysis and propose strategies to mitigate those risks.

7 Design an incident response plan for ACS department.

8 Design penetration testing plan for ACS department



SCOPE OF RESERACH



ACS Physical Security

ACS

Systems and Networks

Policies and

Guidelines

Human Factor

TECHNOLOGY

SOLUTION CENTER

CHALLENGES UNIQUE TO ACADEMIC SETTING

1. Limited Academic Literatures about Subject

2. Culture of Openess

3. Decentralized Systems

4. Bring Your Own Device Policy

5. IoT Adoption

METHOLOGY

1. Conduct Interviews

2. Do Interview Analysis

3. Create High-level network diagram of ACS

4. Conduct Threat Modeling

5. Risk Evaluation

PARTICIPANTS

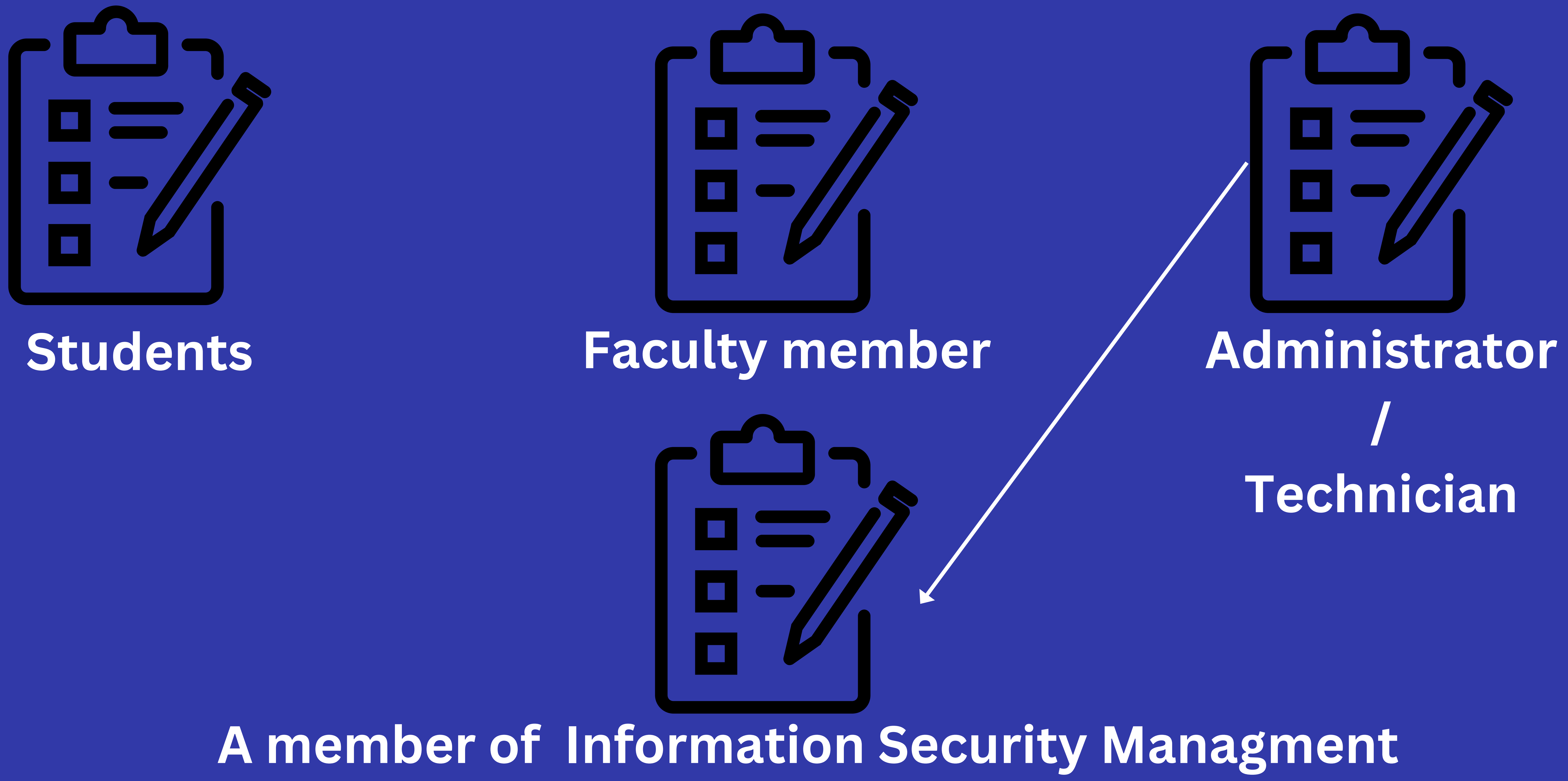
Students

Faculty member

Administrator
/
Technician

A member of Information Security Managment

INTERVIEW QUESTION SETS



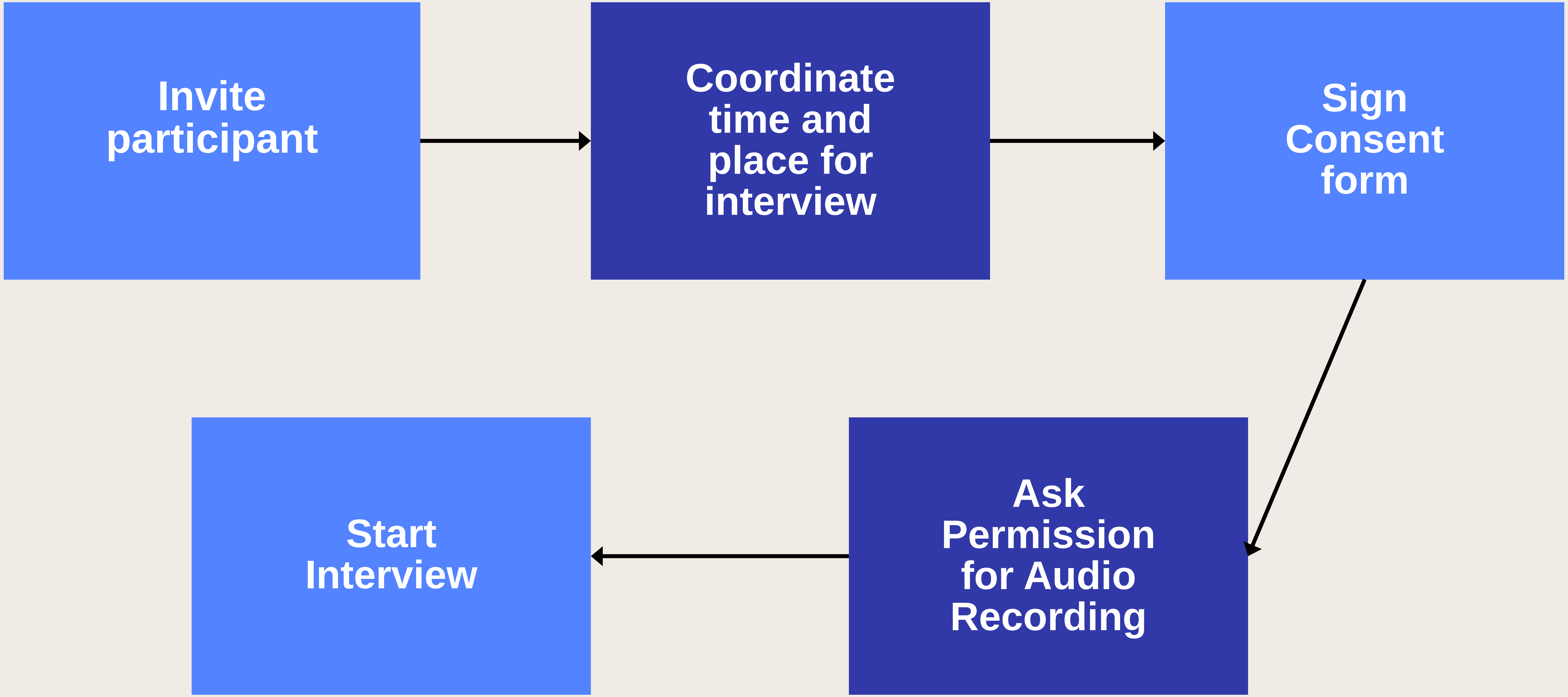
Students

Faculty member

Administrator
/
Technician

A member of Information Security Managment

INTERVIEW PROCESS



Invite participant

Coordinate time and place for interview

Sign Consent form

Ask Permission for Audio Recording

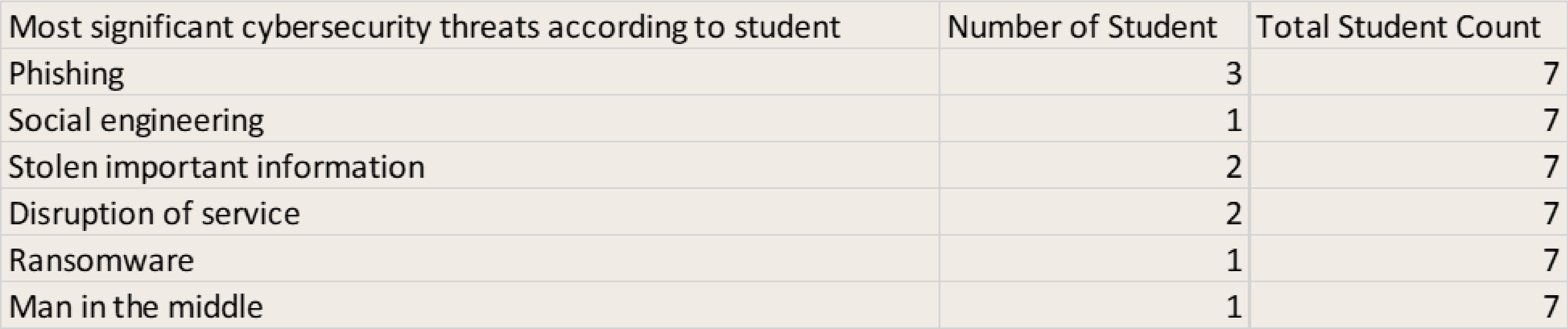
Start Interview

INTERVIEW ANALYSIS

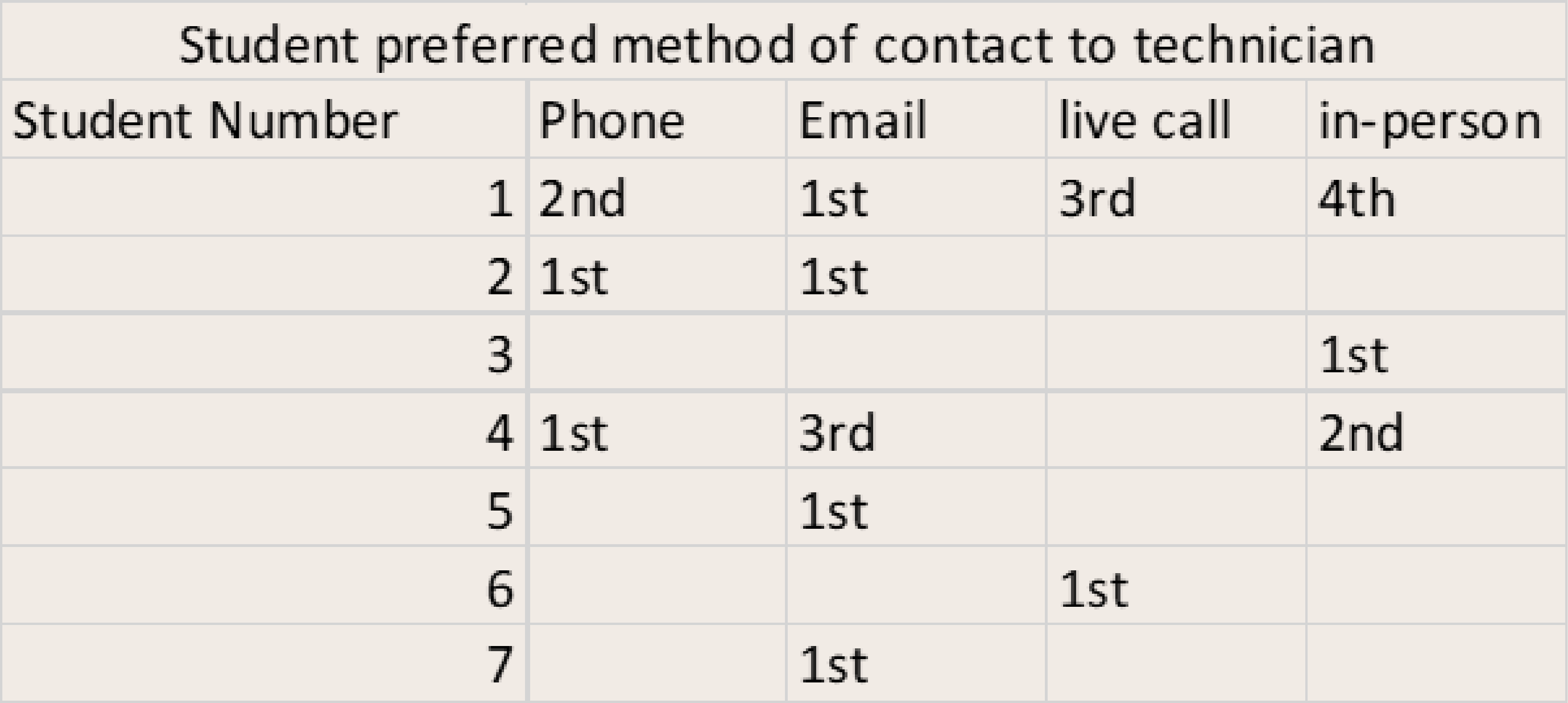
Quantitative Data

Qualitative Data

SOME QUANTITATIVE DATA

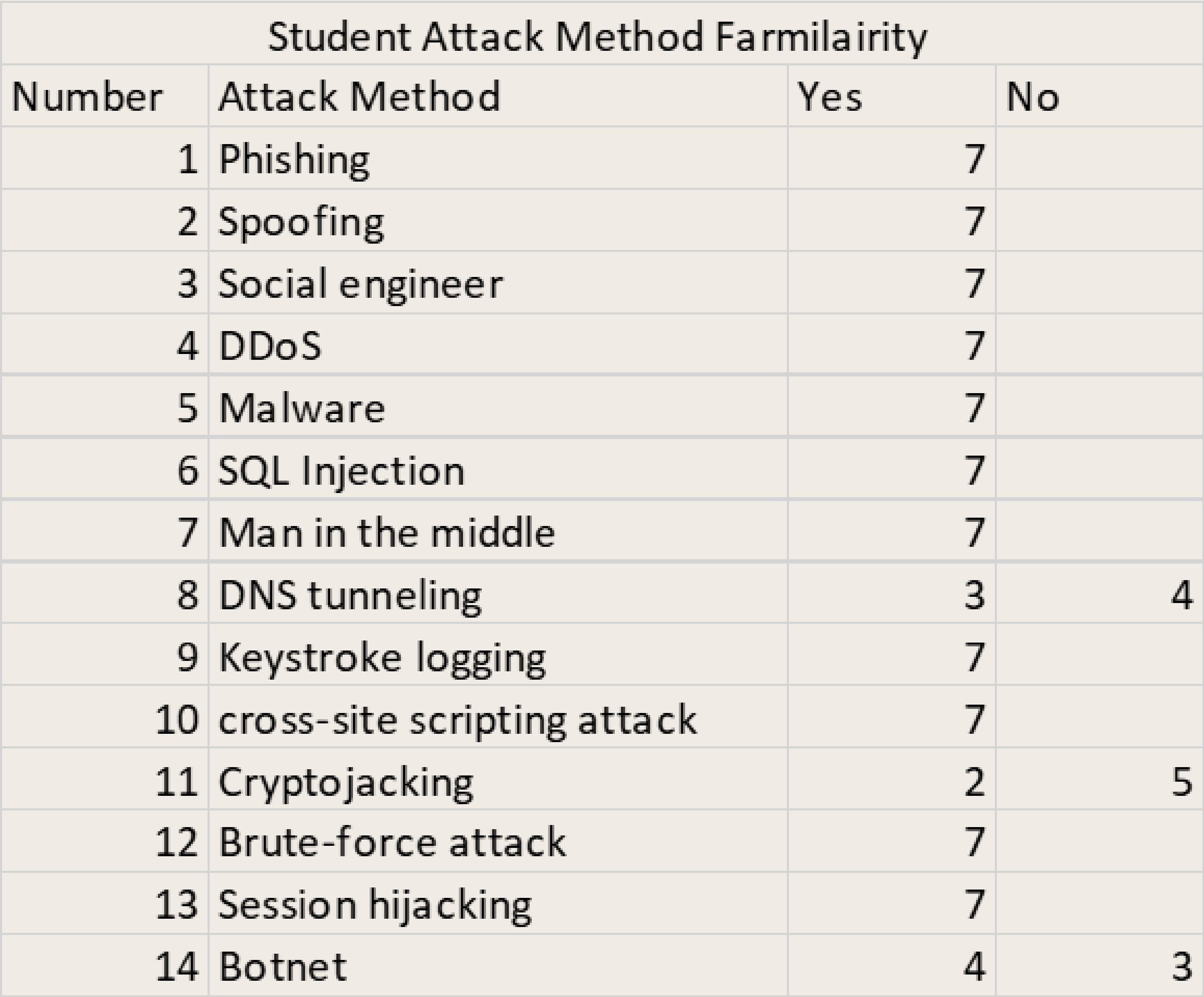


Most significant cybersecurity threats according to student	Number of Student	Total Student Count
Phishing	3	7
Social engineering	1	7
Stolen important information	2	7
Disruption of service	2	7
Ransomware	1	7
Man in the middle	1	7

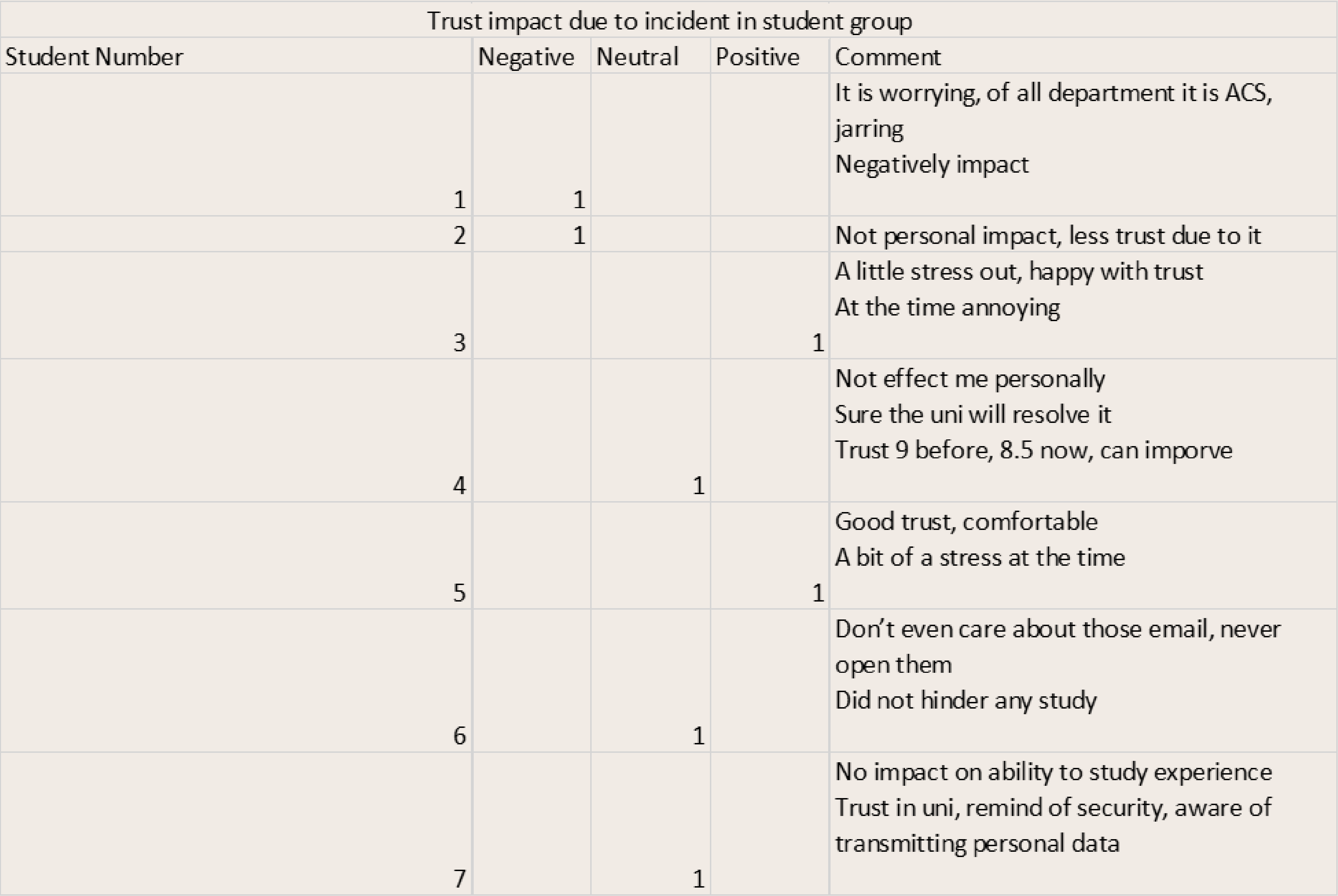


Student preferred method of contact to technician				
Student Number	Phone	Email	live call	in-person
1	2nd	1st	3rd	4th
2	1st	1st		
3				1st
4	1st	3rd		2nd
5		1st		
6			1st	
7		1st		

SOME QUANTITATIVE DATA



Student Attack Method Farmilairity			
Number	Attack Method	Yes	No
1	Phishing	7	
2	Spoofing	7	
3	Social engineer	7	
4	DDoS	7	
5	Malware	7	
6	SQL Injection	7	
7	Man in the middle	7	
8	DNS tunneling	3	4
9	Keystroke logging	7	
10	cross-site scripting attack	7	
11	Cryptojacking	2	5
12	Brute-force attack	7	
13	Session hijacking	7	
14	Botnet	4	3

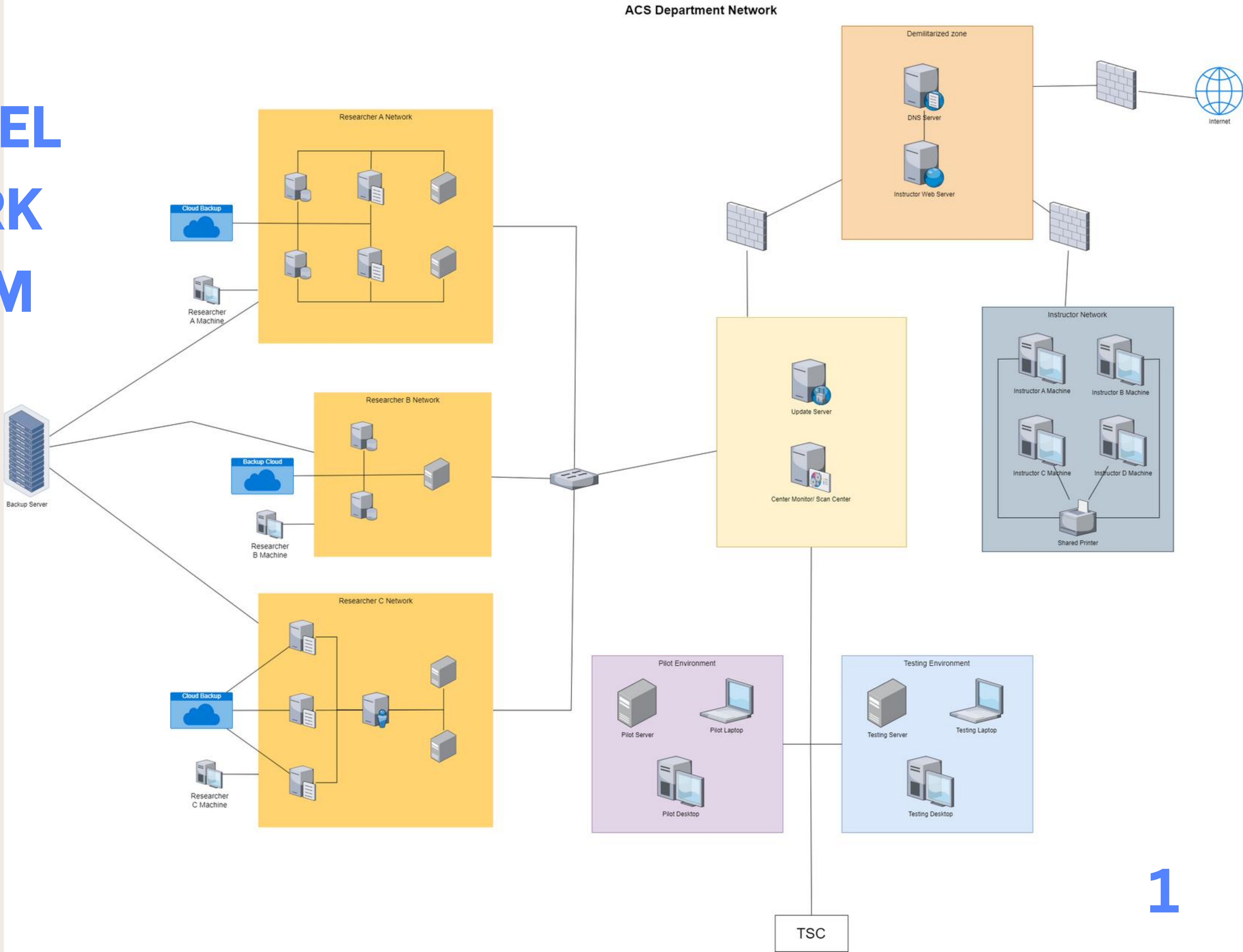


Trust impact due to incident in student group				
Student Number	Negative	Neutral	Positive	Comment
1	1			It is worrying, of all department it is ACS, jarring Negatively impact
2	1			Not personal impact, less trust due to it
3			1	A little stress out, happy with trust At the time annoying
4		1		Not effect me personally Sure the uni will resolve it Trust 9 before, 8.5 now, can imporve
5			1	Good trust, comfortable A bit of a stress at the time
6		1		Don't even care about those email, never open them Did not hinder any study
7		1		No impact on ability to study experience Trust in uni, remind of security, aware of transmitting personal data

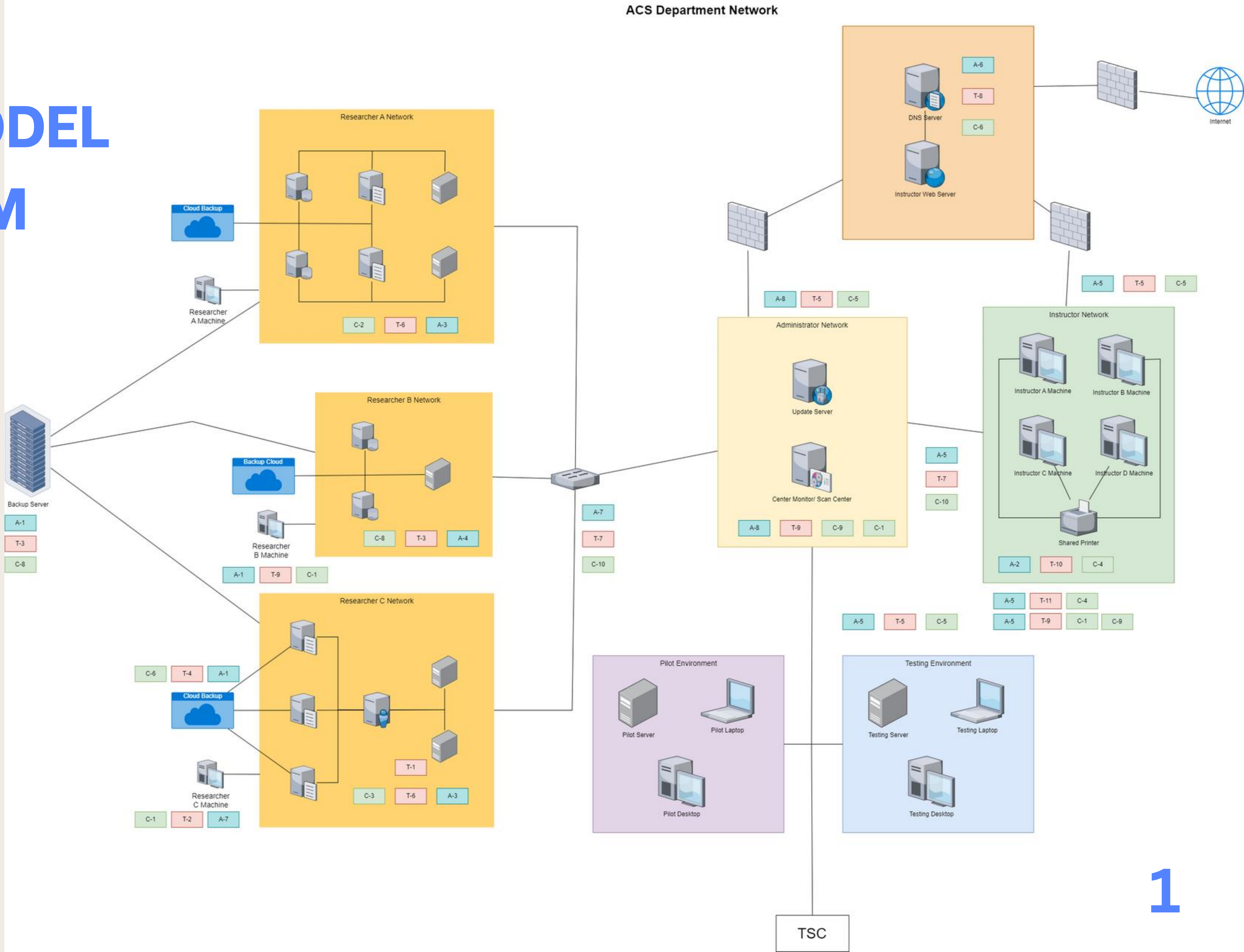
SOME QUALITATIVE DATA

- Student's cybersecurity incident in 2021, multiple students were affected
- "In the middle of class, received a security email about some data breach and they needed to secure the student account. The email asked to verify and make sure to follow instructions"
- The student was not so mindful, windows opened on the side, clicked link that opened a page that was "very professional looking"
- The sender has legitimate domain name as webmail.uwinnipeg.ca
- The student logged in and gave out their password then got logged out of Web Advisor, Nexus and University email.
- "Got sign out from my service and The U of W student email got used for further phishing attacks. I only know of it because my friend texted me and asked yo is this you?"
- The Student's email was compromised and they used personal email to reach out to ACS department
- 15 minutes response time and help personnel did something on ACS end
- Asked to log in with a new password
- The entire thing was done in 30 to 40 minutes, resetting password took 30 minutes
- 50 minutes total to recover from the incident

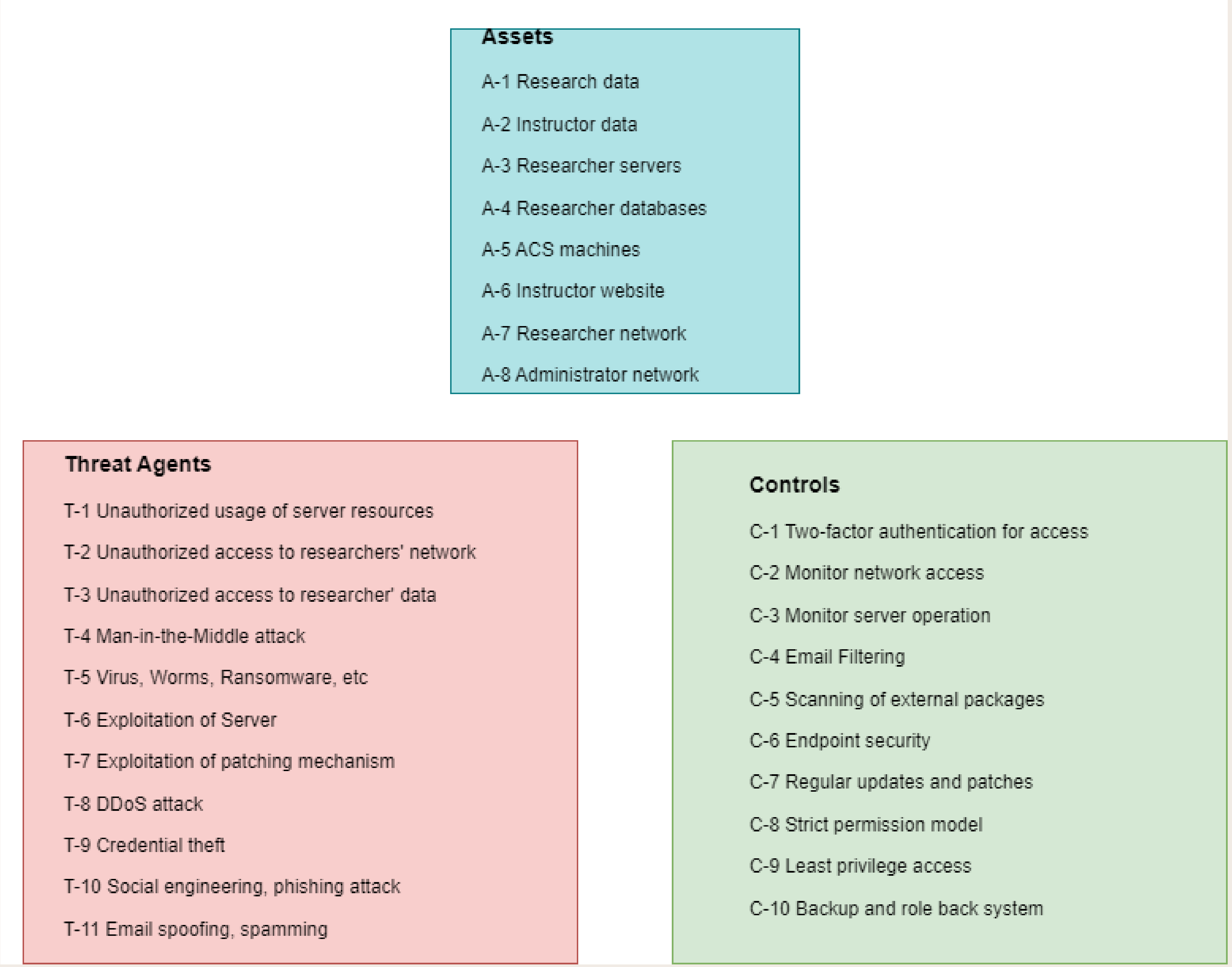
HIGH LEVEL NETWORK DIAGRAM



THREAT MODEL DIAGRAM



THREAT MODEL DIAGRAM



Assets

A-1 Research data

A-2 Instructor data

A-3 Researcher servers

A-4 Researcher databases

A-5 ACS machines

A-6 Instructor website

A-7 Researcher network

A-8 Administrator network

Threat Agents

T-1 Unauthorized usage of server resources

T-2 Unauthorized access to researchers' network

T-3 Unauthorized access to researcher' data

T-4 Man-in-the-Middle attack

T-5 Virus, Worms, Ransomware, etc

T-6 Exploitation of Server

T-7 Exploitation of patching mechanism

T-8 DDoS attack

T-9 Credential theft

T-10 Social engineering, phishing attack

T-11 Email spoofing, spamming

Controls

C-1 Two-factor authentication for access

C-2 Monitor network access

C-3 Monitor server operation

C-4 Email Filtering

C-5 Scanning of external packages

C-6 Endpoint security

C-7 Regular updates and patches

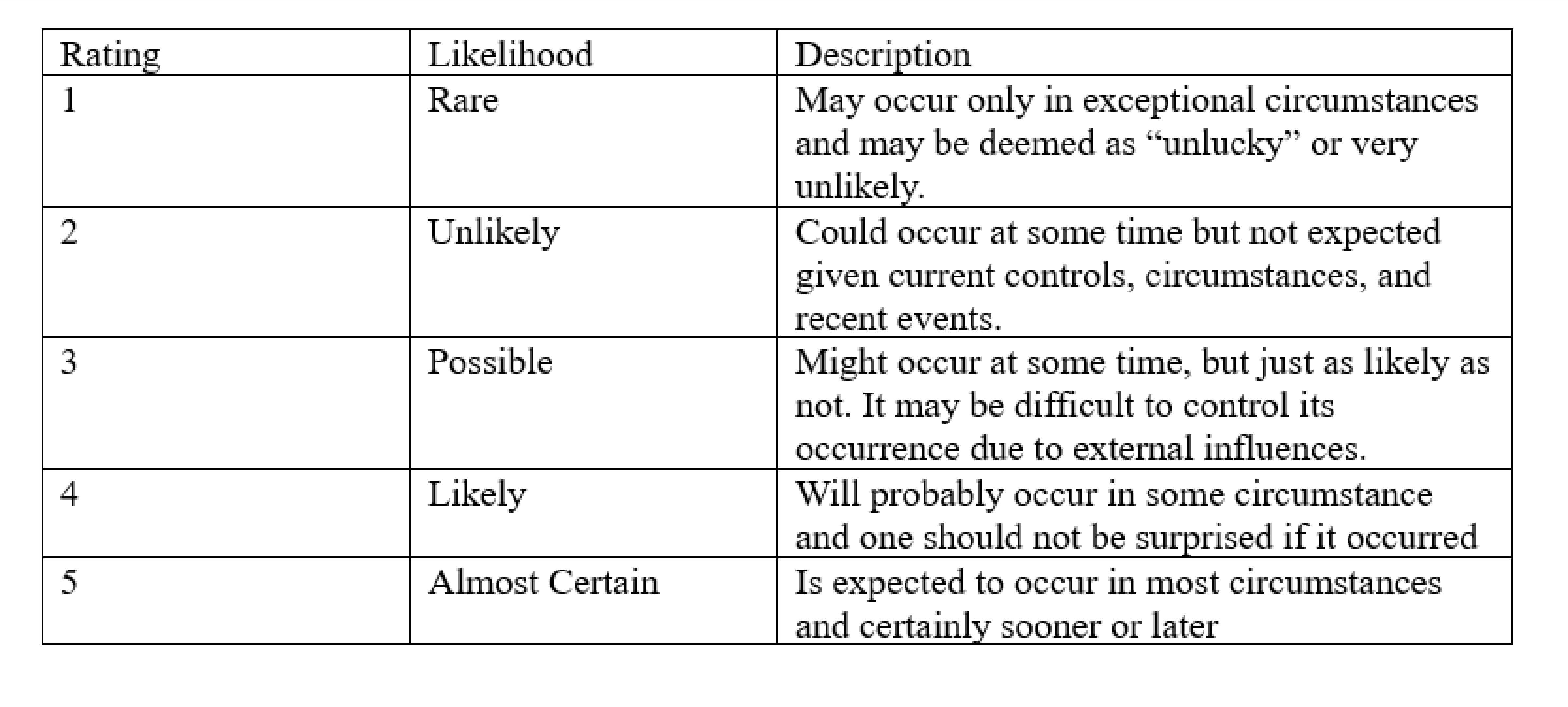
C-8 Strict permission model

C-9 Least privilege access

C-10 Backup and role back system

THREAT EVALUATION

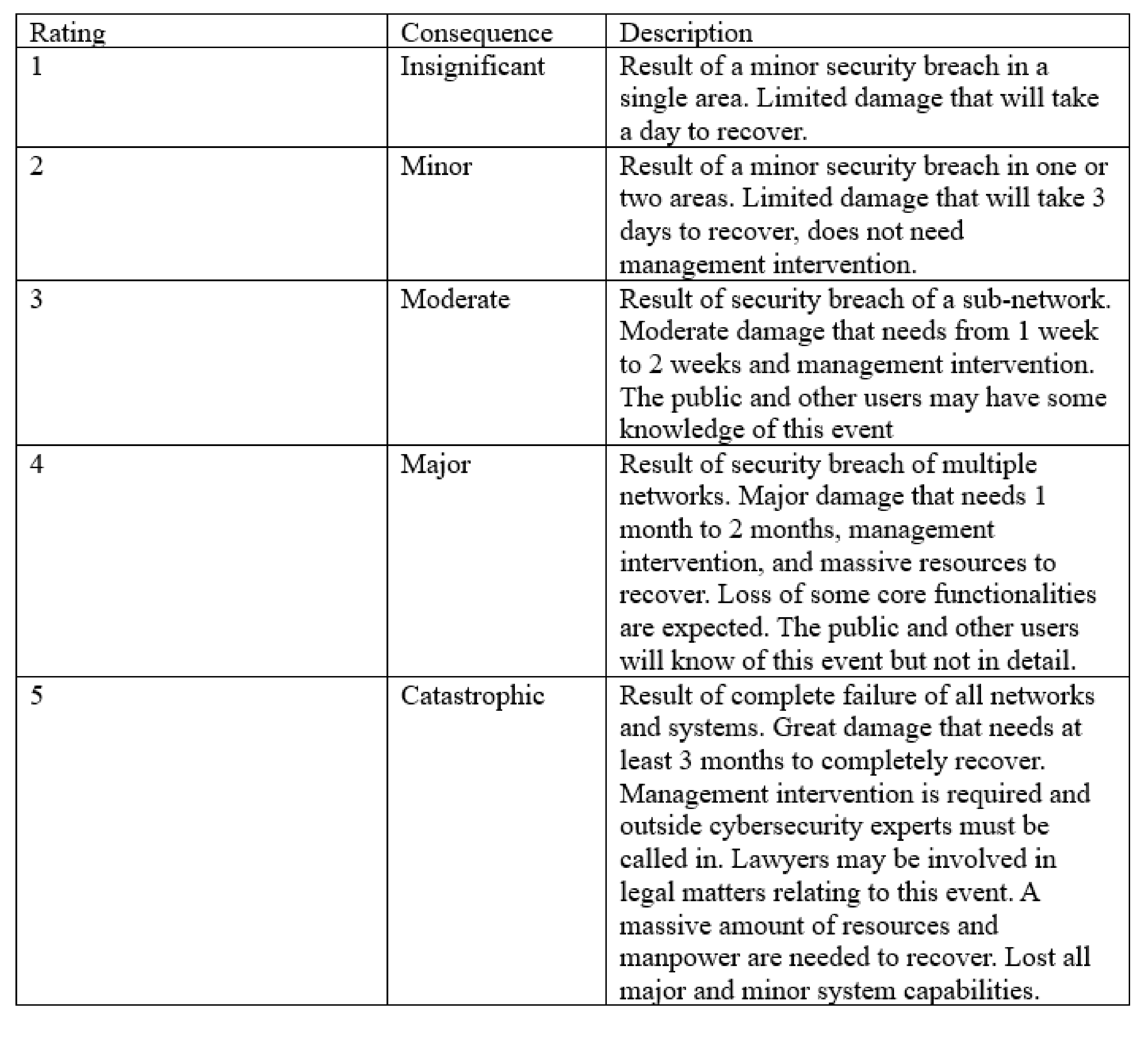
LIKELIHOOD TABLE



Rating	Likelihood	Description
1	Rare	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	Unlikely	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	Possible	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	Likely	Will probably occur in some circumstance and one should not be surprised if it occurred
5	Almost Certain	Is expected to occur in most circumstances and certainly sooner or later

THREAT EVALUATION

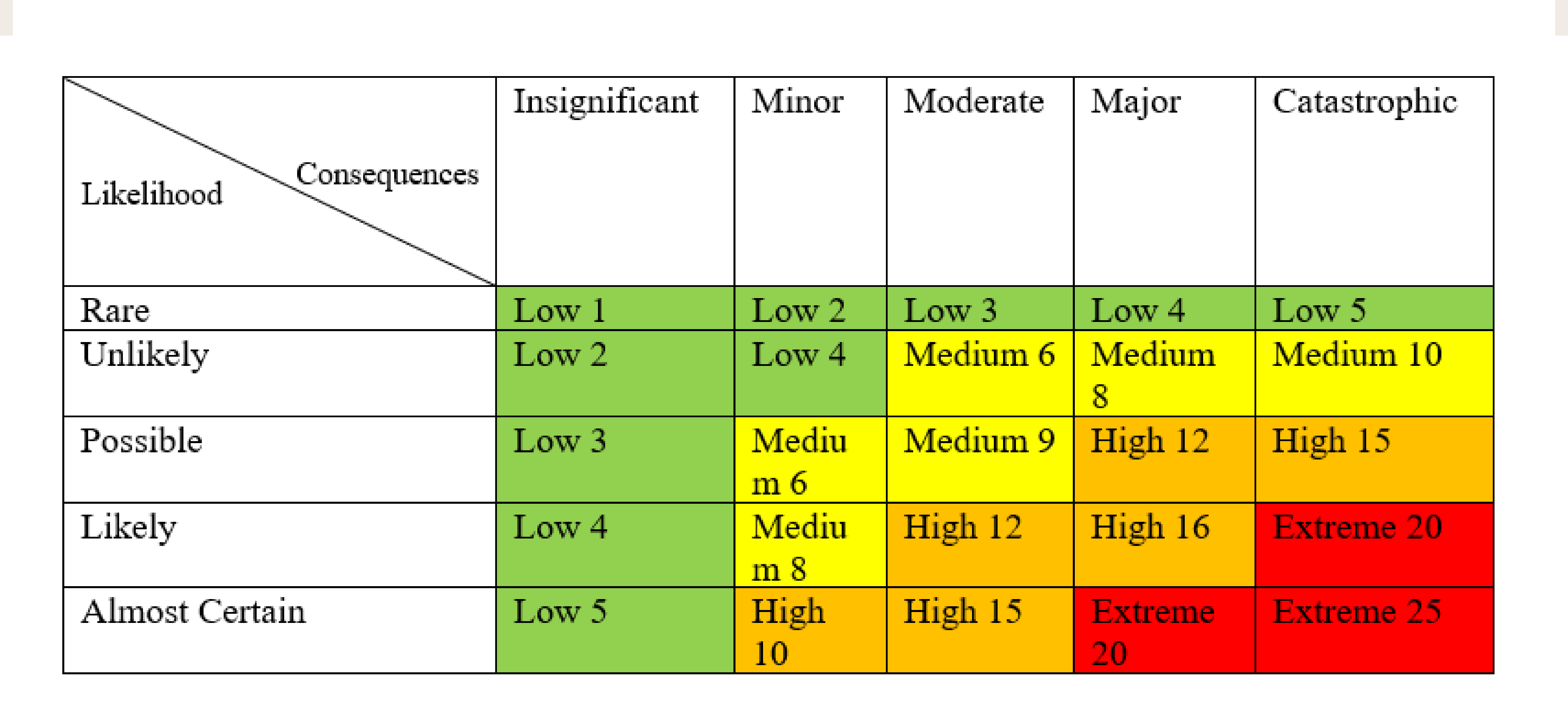
CONSEQUENCES TABLE



Rating	Consequence	Description
1	Insignificant	Result of a minor security breach in a single area. Limited damage that will take a day to recover.
2	Minor	Result of a minor security breach in one or two areas. Limited damage that will take 3 days to recover, does not need management intervention.
3	Moderate	Result of security breach of a sub-network. Moderate damage that needs from 1 week to 2 weeks and management intervention. The public and other users may have some knowledge of this event
4	Major	Result of security breach of multiple networks. Major damage that needs 1 month to 2 months, management intervention, and massive resources to recover. Loss of some core functionalities are expected. The public and other users will know of this event but not in detail.
5	Catastrophic	Result of complete failure of all networks and systems. Great damage that needs at least 3 months to completely recover. Management intervention is required and outside cybersecurity experts must be called in. Lawyers may be involved in legal matters relating to this event. A massive amount of resources and manpower are needed to recover. Lost all major and minor system capabilities.

THREAT EVALUATION

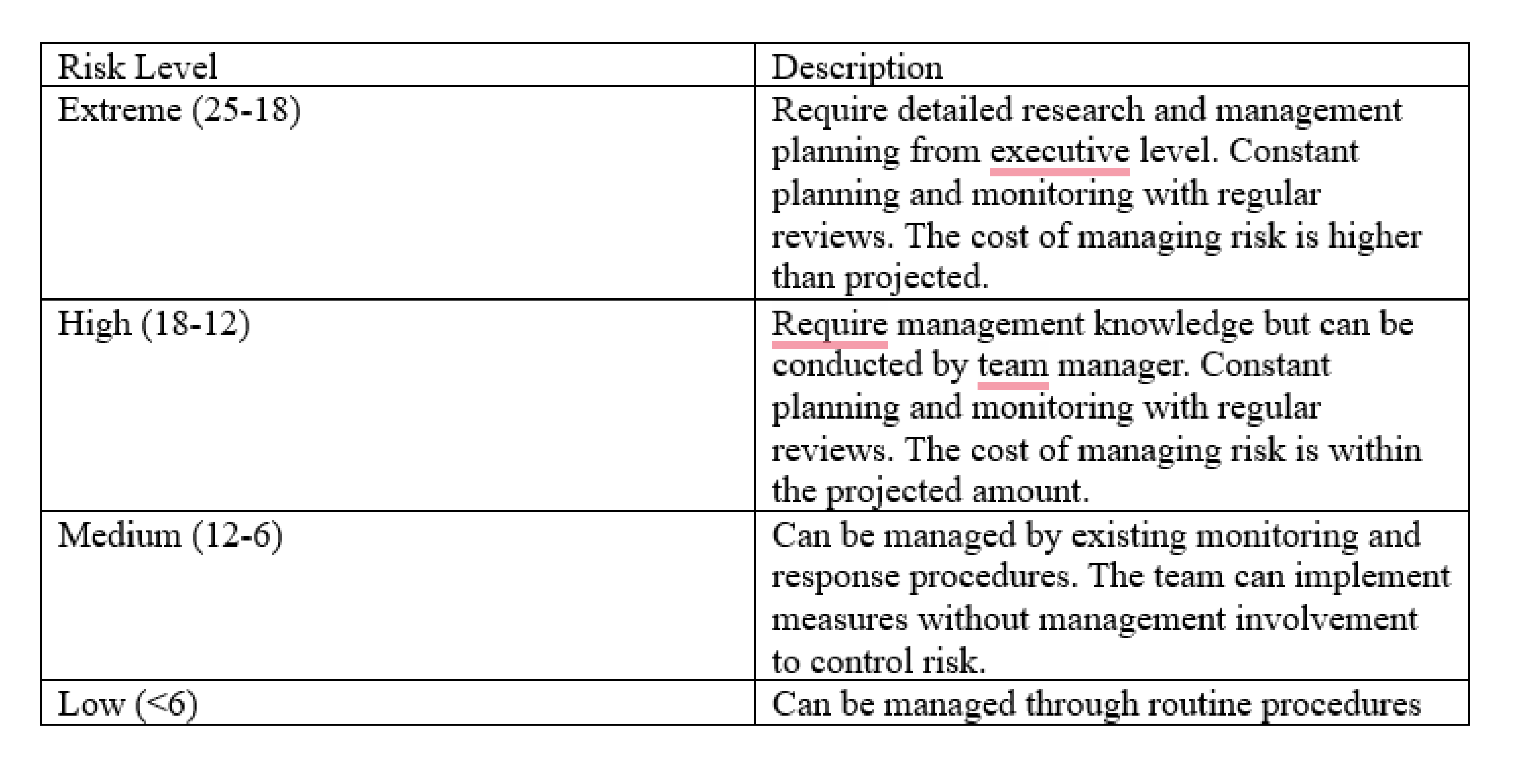
RISK MATRIX



Consequences Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	Low 1	Low 2	Low 3	Low 4	Low 5
Unlikely	Low 2	Low 4	Medium 6	Medium 8	Medium 10
Possible	Low 3	Medium 6	Medium 9	High 12	High 15
Likely	Low 4	Medium 8	High 12	High 16	Extreme 20
Almost Certain	Low 5	High 10	High 15	Extreme 20	Extreme 25

THREAT EVALUATION

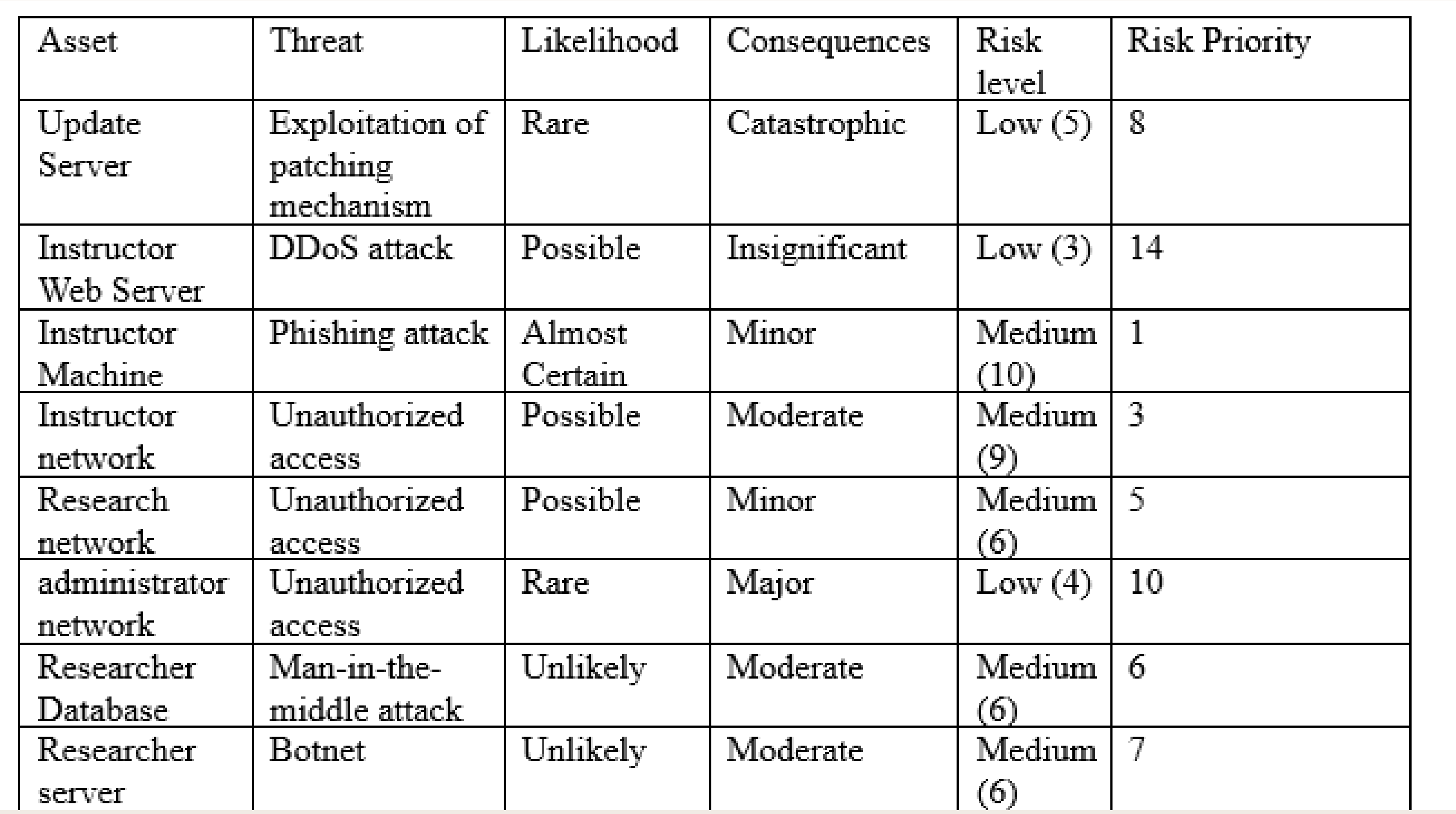
RISK LEVEL TABLE



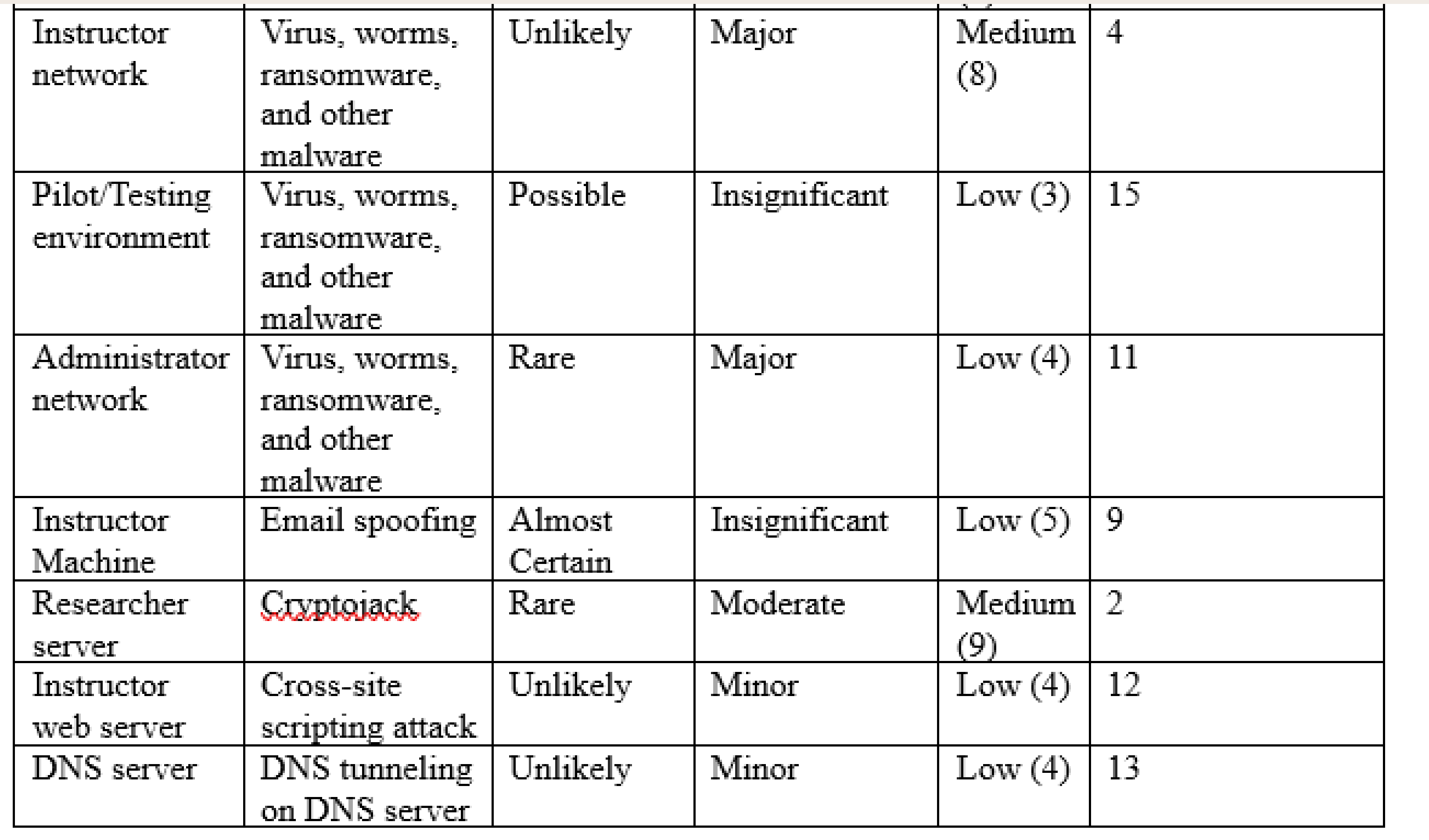
Risk Level	Description
Extreme (25-18)	Require detailed research and management planning from executive level. Constant planning and monitoring with regular reviews. The cost of managing risk is higher than projected.
High (18-12)	Require management knowledge but can be conducted by team manager. Constant planning and monitoring with regular reviews. The cost of managing risk is within the projected amount.
Medium (12-6)	Can be managed by existing monitoring and response procedures. The team can implement measures without management involvement to control risk.
Low (<6)	Can be managed through routine procedures

THREAT EVALUATION

RISK REGISTRY



Asset	Threat	Likelihood	Consequences	Risk level	Risk Priority
Update Server	Exploitation of patching mechanism	Rare	Catastrophic	Low (5)	8
Instructor Web Server	DDoS attack	Possible	Insignificant	Low (3)	14
Instructor Machine	Phishing attack	Almost Certain	Minor	Medium (10)	1
Instructor network	Unauthorized access	Possible	Moderate	Medium (9)	3
Research network	Unauthorized access	Possible	Minor	Medium (6)	5
administrator network	Unauthorized access	Rare	Major	Low (4)	10
Researcher Database	Man-in-the-middle attack	Unlikely	Moderate	Medium (6)	6
Researcher server	Botnet	Unlikely	Moderate	Medium (6)	7



Instructor network	Virus, worms, ransomware, and other malware	Unlikely	Major	Medium (8)	4
Pilot/Testing environment	Virus, worms, ransomware, and other malware	Possible	Insignificant	Low (3)	15
Administrator network	Virus, worms, ransomware, and other malware	Rare	Major	Low (4)	11
Instructor Machine	Email spoofing	Almost Certain	Insignificant	Low (5)	9
Researcher server	Cryptojack	Rare	Moderate	Medium (9)	2
Instructor web server	Cross-site scripting attack	Unlikely	Minor	Low (4)	12
DNS server	DNS tunneling on DNS server	Unlikely	Minor	Low (4)	13

IDENTIFIED VULNERABILITIES AND RISKS

PHYSICAL SECURITY

RESOURCE CONSTRAINT

ADVANDED PERSISTANT THREAT

ZERO-DAY VUNERBILITIES

IDENTIFIED VULNERABILITIES AND RISKS

INSIDER THREAT

OUTSIDE THREAT

FILELESS MALWARE

PHISHING ATTACK

IDENTIFIED VULNERABILITIES AND RISKS

POLICIE
S

UPDATE PROCESS

ACCESS AND PRIVILEGE
CONTROL

COMMUNICATION

RECOMMENDATIONS

MOVE SHARED PRINTER

FINGER-PRINT LOCKS

HIRE MORE PERSONNEL

NO EDUROAM

LIMITED INTERNET

VIRTUAL MACHINE

PHISHING AWARENESS

RECOMMENDATIONS

PROPOSED SECURITY POLICY

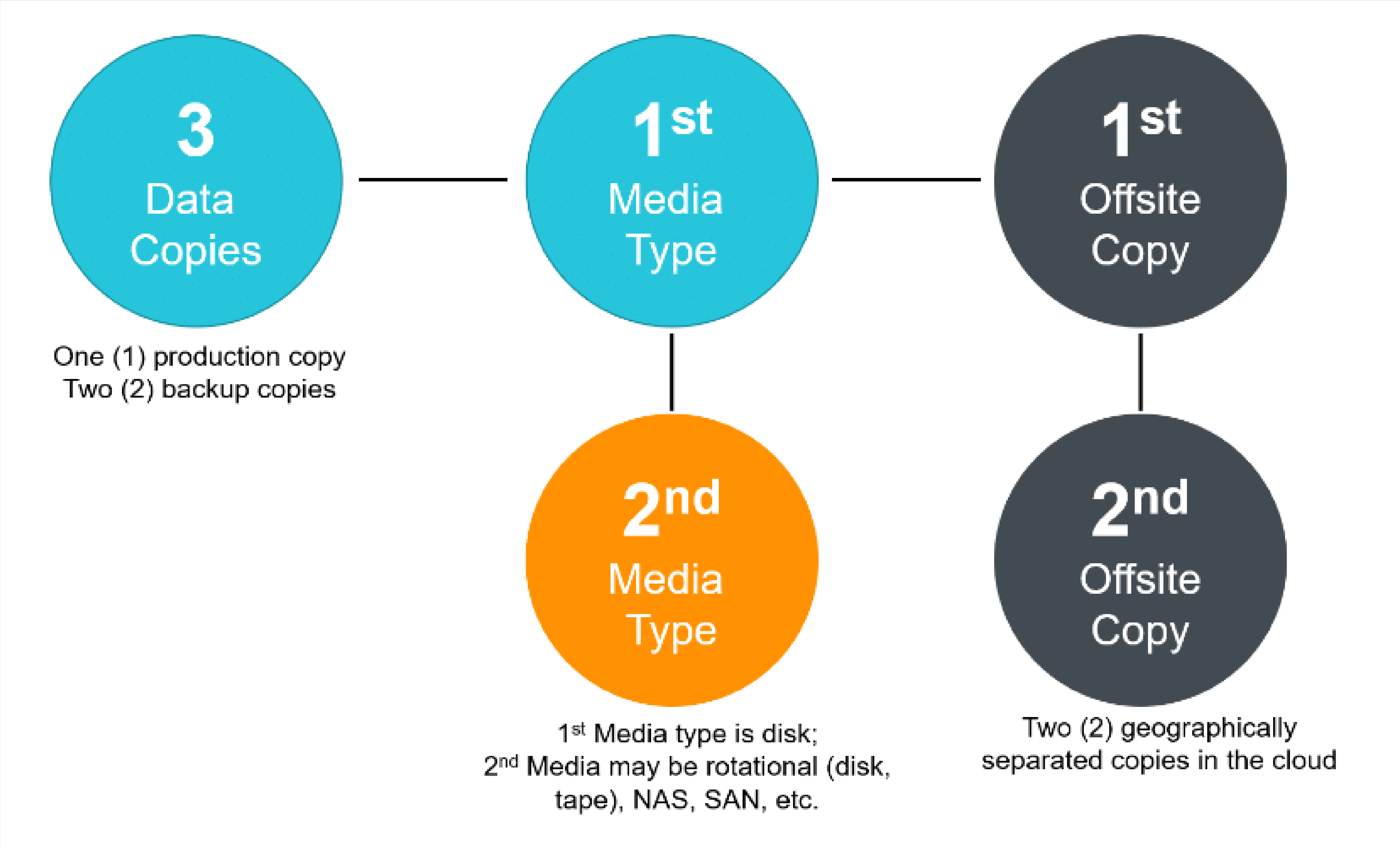
No device connected to the ACS network can connect to Eduroam wifi network

Researcher’s servers and system cannot directly connect to the Internet

All external package such as email attachments, download must first be open in virtual machine before opening in user machine

RECOMMENDATIONS

3-2-2 BACKUP SYSTEM



3 Data Copies

One (1) production copy
Two (2) backup copies

1st Media Type

2nd Media Type

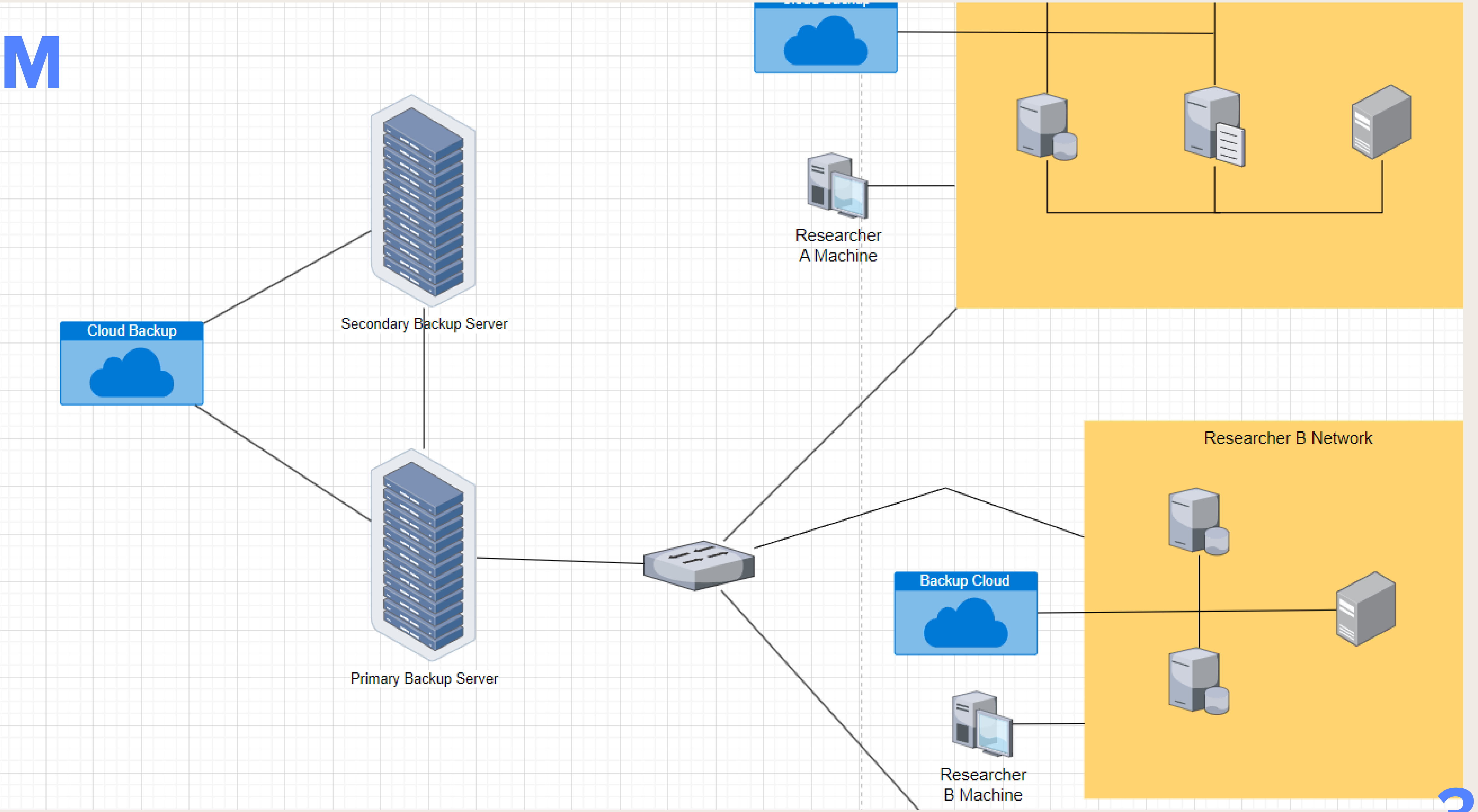
1st Media type is disk;
2nd Media may be rotational (disk, tape), NAS, SAN, etc.

1st Offsite Copy

2nd Offsite Copy

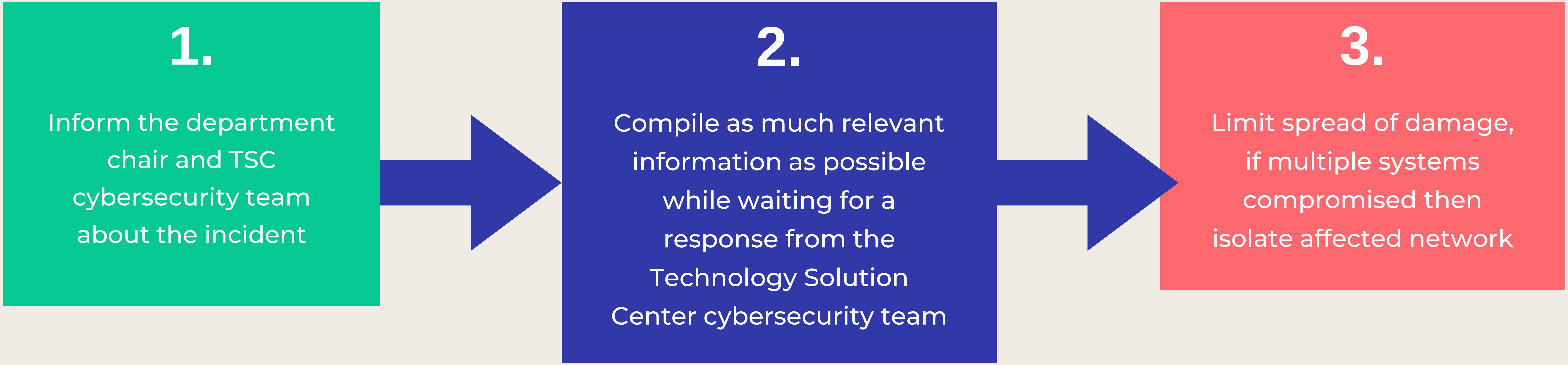
Two (2) geographically separated copies in the cloud

CHANGED HIGH LEVEL NETWORK DIAGRAM



RECOMMENDATIONS

PROPOSED INCIDENT RESPONSE PLAN



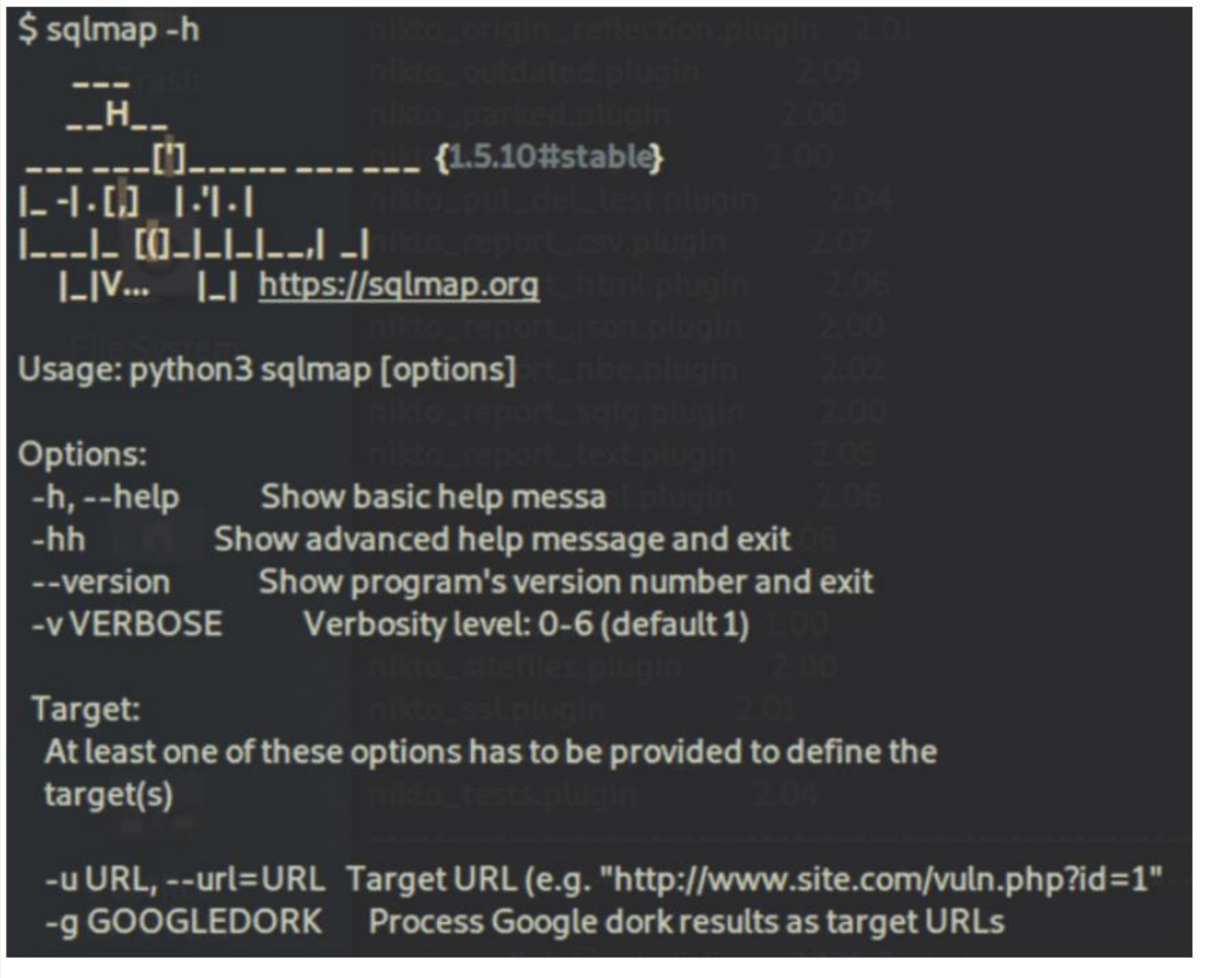
1. Inform the department chair and TSC cybersecurity team about the incident

2. Compile as much relevant information as possible while waiting for a response from the Technology Solution Center cybersecurity team

3. Limit spread of damage, if multiple systems compromised then isolate affected network

RECOMMENDATIONS

PENETRATION TESTING TOOL



```
$ sqlmap -h
    ___
   __H__
 ___ ___[']_____ ___ ___  {1.5.10#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help messa
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1"
    -g GOOGLEDORK       Process Google dork results as target URLs
```

RECOMMENDATIONS

PENETRATION TESTING PLAN

PHASE 1

Test pilot SQLmap on a dummy server in a testing environment

PHASE 2

Implementing SQLmap in a limited capacity to a researcher’s network for 3 months, monitor testing and evaluate effectinvess

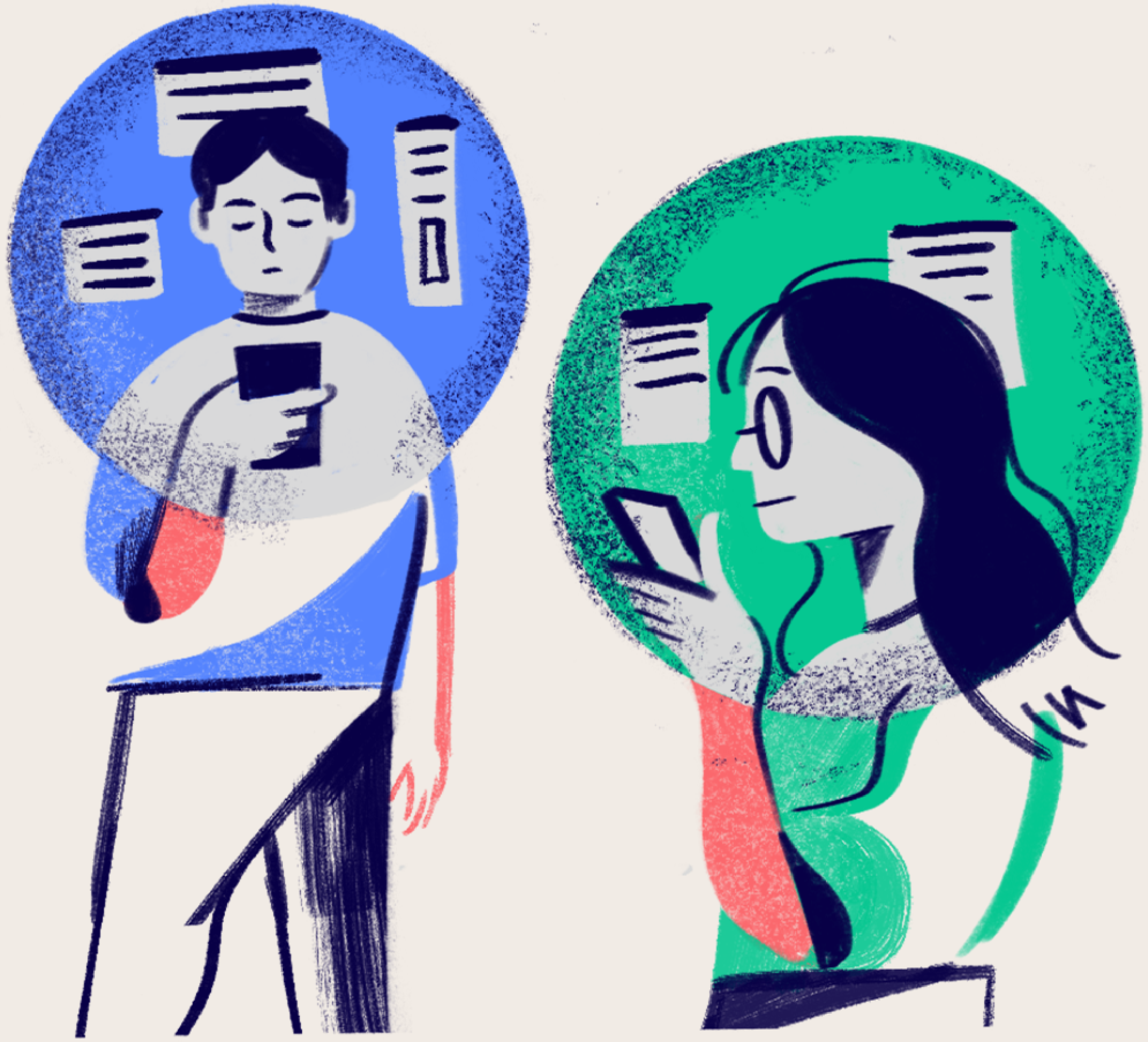
PHASE 3

Expand penetration testing to all researchers’ networks and automate the process

CITATION

- Statista. (2024, March 18). Canada’s number of internet fraud cases from 2014 to 2023. https://www.statista.com/statistics/1456731/internet-fraud-cases-canada/
- Statista. (2024b, March 19). Canada’s number of identity fraud cases from 2014 to 2023. https://www.statista.com/statistics/1457331/identity-fraud-cases-canada/
- Statista. (2024b, March 19). Canada’s predicted cost of Cybercrime from 2017 to 2028. https://www.statista.com/forecasts/1457244/canada-cybercrime-cost-annual
- Jain , S. (2024, February 8). 160 cybersecurity statistics: Updated report 2024. Astra Security Blog. https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Cybersecurity%20statistics%20indicate%20that%20there,cost%20%248%20trillion%20by%202023.
- Security Magazine. (2020, May 24). Hackers attack every 39 seconds. Security Magazine RSS. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
- Check Point Blog. (2022, August 16). Check point research: Education sector experiencing more than double monthly attacks, compared to other industries. https://blog.checkpoint.com/2022/08/09/check-point-research-education-sector-experiencing-more-than-double-monthly-attacks-compared-to-other-industries/
- The University of Winnipeg. (2024, March 25). Cyber attack and service outage. https://www.uwinnipeg.ca/updates/index.html?eid=aa32babed1cb2cfb62dd985e81fd67e1

THANK YOU FOR LISTENING
ANY QUESTIONS? ASK AWAY



PRESENTED BY VI LE, SUPERVISED BY DR. VICTOR BALOGUN