



Assignment Title: **Security Policy and Management**

Module Title: **ACCC5003 Network Operating Systems and Security**

Lecturer: **Terry Walcott**

Student Number: **1815743**

Student: **Anghel Sandra-Stefania**

## Abstract

The main objective of this report is to present a security analysis based on a low-level hacking incident suffered by Republic of Snowdenia County Council.

The report includes a short description of information security evolution and highlights the confidentiality, integrity and available security principles. It describes the Address Resolution Protocol poisoning, password cracking and wireless network attacks' detection and prevention methods.

In the end, the report presents a proposed data protection audit and a list of recommendations in order to increase security for Republic of Snowdenia County Council.

## Contents

|                                                              |    |
|--------------------------------------------------------------|----|
| Abstract.....                                                | 2  |
| List of figures .....                                        | 3  |
| List of tables.....                                          | 3  |
| Information Security Context.....                            | 1  |
| The CIA Triad.....                                           | 3  |
| Confidentiality.....                                         | 3  |
| Integrity .....                                              | 4  |
| Availability .....                                           | 5  |
| Intrusion detection and prevention .....                     | 8  |
| Address Resolution Protocol (ARP) poisoning (spoofing) ..... | 8  |
| Password cracking .....                                      | 9  |
| Wireless access .....                                        | 10 |
| General Data Protection Regulation compliance audit .....    | 10 |
| Conclusion .....                                             | 12 |
| Recommendations .....                                        | 13 |
| Bibliography .....                                           | 14 |

## List of figures

|                                            |    |
|--------------------------------------------|----|
| Figure 1: The Enigma code machine [1]..... | 1  |
| Figure 2: ARPANET Program Plan [1] .....   | 2  |
| Figure 3: The CIA Triad.....               | 3  |
| Figure 4: Loss of confidentiality .....    | 4  |
| Figure 5: Loss of integrity .....          | 5  |
| Figure 6: Loss of availability .....       | 6  |
| Figure 7: ARP poisoning diagram.....       | 8  |
| Figure 8: GDPR audit template .....        | 11 |

## List of tables

|                                                         |   |
|---------------------------------------------------------|---|
| Table 1: General security policies and procedures.....  | 7 |
| Table 2: Server security policies and procedures .....  | 7 |
| Table 3: Network security policies and procedures ..... | 7 |

# Information Security Context

Security, in the context of computers, appeared in 1930s, when first machine Enigma was broken. During the World War II, messages were decrypted using mainframe computers, in order to anticipate the enemies' actions. The term *security* referred to *computer security* at that moment [1].



Figure 1: The Enigma code machine [1]

Later, in 1960s, threats like easy access to sensitive data (including military locations or theft of physical equipment) became a complex security issue and it was addressed by the Department of Defense's Advanced Research Projects Agency which developed ARPANET Program Plan. ARPANET focused on covering aspects as networking and resource sharing based on military needs. ARPANET became the main tool used for sharing Defense Department information [1].

## ARPANET Program Plan

June 3, 1968

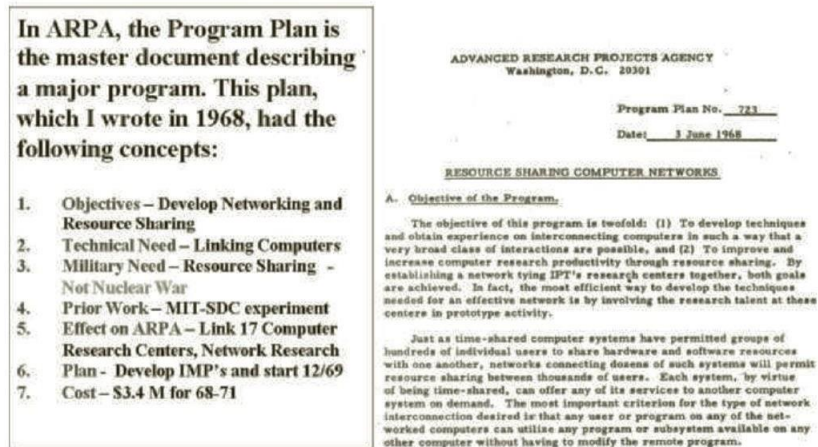


Figure 2: ARPANET Program Plan [1]

The sense of security was expanded over the next decade and the definition of network security emerged. Robert M. Metcalfe, one of the creators of Ethernet, exposed possible threats as authorization, authentication and passwords' vulnerabilities. RAND Corporation published in 1970 a report (RAND Report R-609), released again later by ARPA. The report is a reference point of information security history and includes physical locations and hardware security, data security, authentication, authorizations and access policies [1].

Nowadays, as there are millions of computers connected to Internet, security requires a special attention and becomes a challenge. The number of cyberattacks has increased and organizations need to address security in every aspect, from physical, network, and communication security to information security [1].

As a simple definition, security means protection against any possible attack or threat and it includes multiple levels (people – only authorized employees have access to a company's building, hardware, software) [1].

## The CIA Triad

National Institute of Standards and Technology (NIST) had defined a model called CIA Triad, which describe the main characteristics and policies needed to ensure information security. The model's name represents an abbreviation for *confidentiality*, *integrity* and *availability* [2].

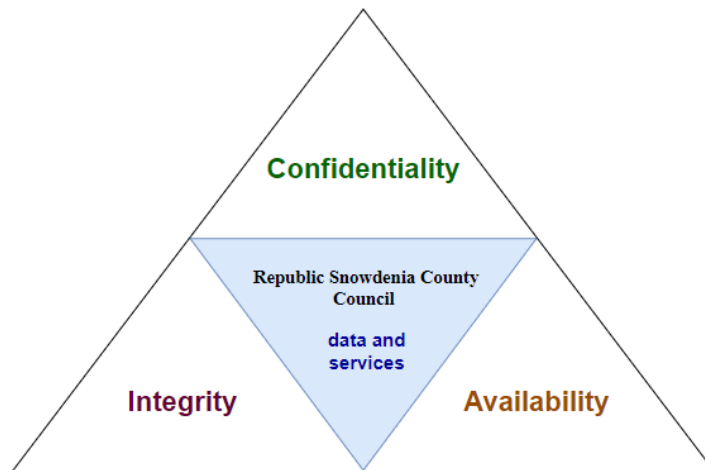


Figure 3: The CIA Triad

### Confidentiality

An information is considered confidential when unauthorized users or systems cannot access it. Confidentiality, in the context of information security, describes how sensitive or secret data is protected. For example, a confidentiality breach results into an exposure of the Republic of Snowdenia County Council's budget plan. General Data Protection Regulation (GDPR) compliance is compromised by revealing other private information such as employees or residents' personal details [3].

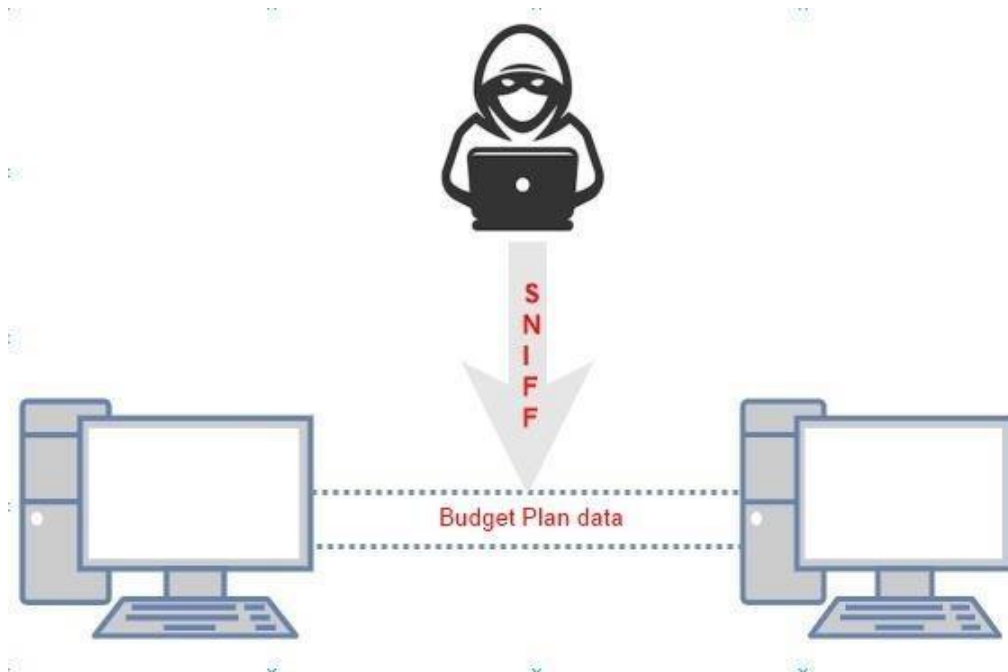


Figure 4: Loss of confidentiality

## Integrity

An information has integrity when it is not corrupt. Integrity, in the context of information security, refers to the ability of keeping data in the original state without being changed or destroyed. Integrity is very relevant because it can affect decision-making. For example, Republic of Snowdenia County Council decides to build a schools' renovation project. The board received auction offers from a variety of building construction experts and they need to choose one to implement the project. If the integrity is not met and the letters are corrupted, then the final decision will not be eloquent and based on real offers and the project is affected [3].

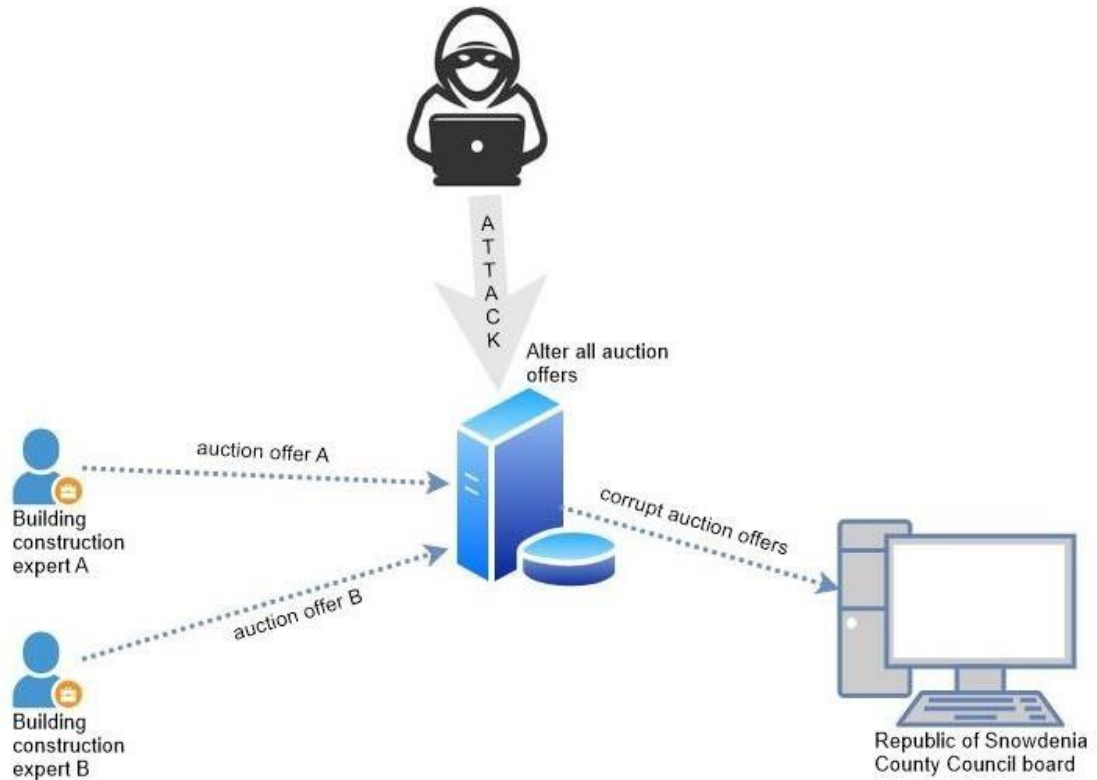


Figure 5: Loss of integrity

## Availability

Nowadays, information can be stored in any storage device (USB flash drive, hard drive, memory card etc.), systems (databases) or Cloud. Availability refers to the ability of accessing the information at any time. For example, Republic Snowdenia County Council keeps the employees records in a database system. The accountant must generate the payslips and then process the salary payments for the employees. If the database is down for technical reasons caused by a possible cyberattack, the accountant cannot perform his task, the employees are affected, and the availability of information is not met [3].

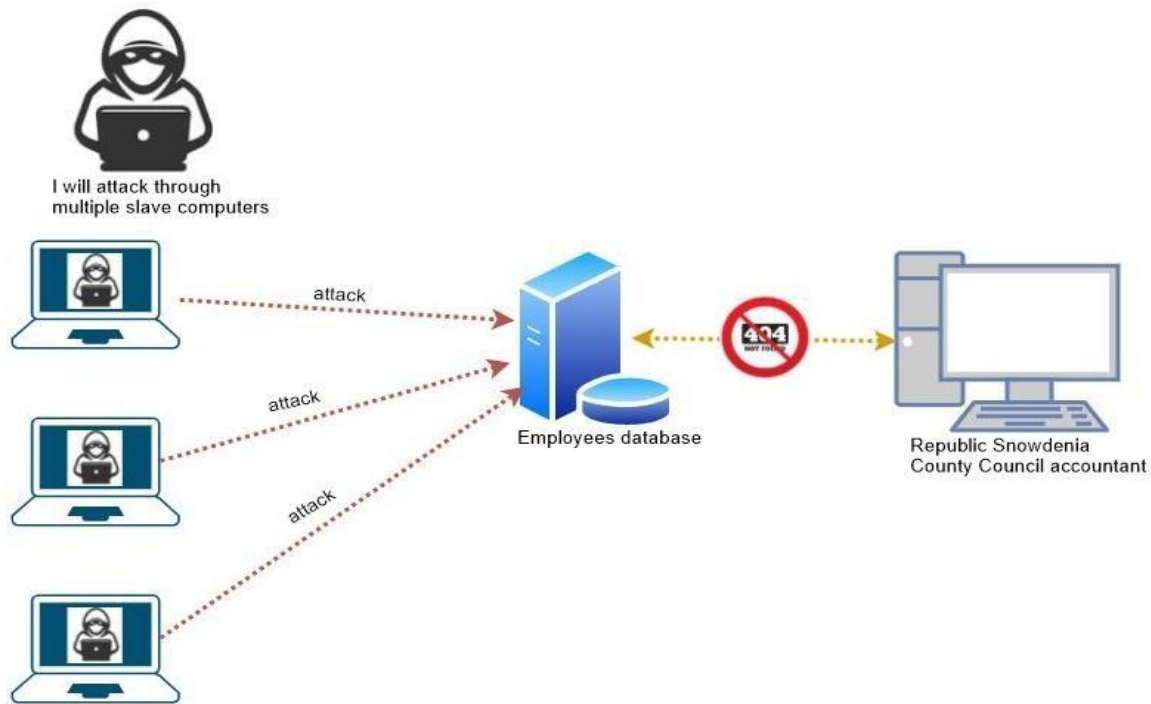


Figure 6: Loss of availability

In association with the three security pitfalls presented, National Institute of Standards and Technology developed a set of security policies and procedures categorized as following [4]:

➤ General

| Policy                | Description                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Acceptable encryption | The organization must use standardized encryption algorithms for passwords, files etc.                                                 |
| Clean desk            | Employees must maintain a clean desk without exposing sensitive/confidential documents. It must be store in lockers.                   |
| Password protection   | Passwords must respect at least the minimum-security requirements defined by NIST [5]. Employees must change the passwords frequently. |

|                        |                                                                                                                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disaster recovery plan | The organization must define a backup plan and a recovery process plan in case of any disaster. Storing critical data on employee's device would represent a major problem if the device was stolen or damaged by a disaster that occurred in the organization's building. |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Table 1: General security policies and procedures

➤ Server security

| Policy                        | Description                                                                                                                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database credentials          | Database credentials must be strong and stored into secure storage. Each user that can access the database must have its own credentials. Configuration files, used by systems to connect to the database, must not expose the credentials in plain text. |
| Software installation         | Employees must not install third-party software without the approval of the administrators. The organization must have a list of trusted software.                                                                                                        |
| Technology equipment disposal | The organization must decide how to destroy the equipment that may contains sensitive/confidential data (USB flash drives, CD-ROMs etc.).                                                                                                                 |

Table 2: Server security policies and procedures

➤ Network security

| Policy                     | Description                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote access              | The organization must allow remote access to employees' devices by using secured VPNs and each device should have a multi factor authentication mechanism implemented.                                                    |
| Router and switch security | The organization must ensure at least minimum-security configurations for routers and switches [6].                                                                                                                       |
| Wireless communication     | Employees must not connect devices to wireless networks without proper VPNs.<br><br>Employees must not connect personal devices to organization network, and they must not store organization's data on personal devices. |

Table 3: Network security policies and procedures

## Intrusion detection and prevention

Republic of Snowdenia County Council suffered a hacking incident resulting in the release of their private data on a public website. Criminals could use these data in order to perform illegal activities. The attack compromised two of the basic information security requirements – confidentiality (critical data released in public) and integrity (criminals can use data for illegal activities).

The council's aim is to create a defense mechanism that combat at least the following three attacks: *ARP poisoning* (known as Man-in-the-Middle), *password cracking* and *wireless access* for employees that are working from home.

### Address Resolution Protocol (ARP) poisoning (spoofing)

ARP poisoning attack represents an interception of communication between devices connected to a network [7].

#### ARP poisoning scenario

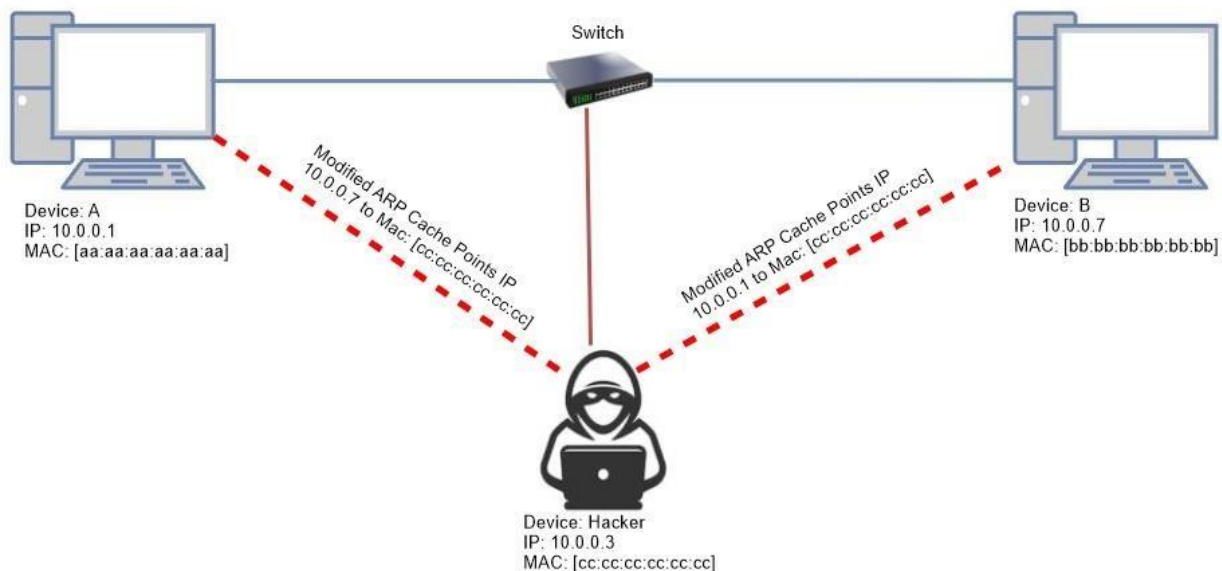


Figure 7: ARP poisoning diagram

### ARP poisoning detection

The easiest way to detect an ARP poisoning attack is by checking ARP table using command **arp -a** into a command window run as administrator. If there are multiple IP addresses with the same MAC address, then an attack is happening [7].

### ARP poisoning prevention

Republic Snowdenia County Council's administrator could prevent the ARP poisoning attack by using [7]:

- Virtual Private Network (VPN) – devices are connecting to the network using encrypted tunnels
- Static ARP – configure devices to listen to static IP addresses
- Packet filtering – use filtering solutions to detect if a packet's information is corrupted

## Password cracking

Password cracking can produce a major security breach, especially when the password's owner is an administrator. In this way, the hacker can have access to the entire system and can perform any action. A hacker can discover a password by convincing the user to expose the password over the phone, obtaining it from computer's files or using specific tools (Brutus, John the Ripper, Cain & Abel, ophcrack) [7].

### Password cracking prevention

Republic Snowdenia County Council must enforce a strong password policy. All employees must respect at least the minimum requirements defined by NIST [5]. The passwords must be changes frequently (at least every three months) and the system passwords (servers, databases passwords) must not be stored in files without encryption.

## Wireless access

A wireless attack relates to packages sniffing (capturing of information at transfer moment). One of the most known wireless attack is *evil twinning* where the attacker creates a fake wireless network, which looks like a legit one. Once connected to this network, the user is redirected to phishing sites where he/she enters credentials or sensitive data [7].

### Wireless network attack prevention

The organization can prevent this attack as following [8]:

- Encrypt data – connection settings must be encrypted
- Use strong credentials for wireless networks and avoid default passwords
- Use monitoring software able to detect unauthorized access points or unexpected activities

## General Data Protection Regulation compliance audit

Security Audit refers to an evaluation of the Republic Snowdenia County Council organization security practices and it can be categorized based on approaches (black/white/grey box audit) or based on methodology (penetration testing, compliance audit etc.) [9] [10]. As data protection violation could result in critical regulation's penalties, a General Data Protection Regulation (GDPR) compliance audit is performed using the following template:

**GDPR compliace audit template - Republic Snowdenia County Council**

| Category                     | Question                                              | Answer |
|------------------------------|-------------------------------------------------------|--------|
| Personal data                | Are you processing personal/sensitive data?           |        |
|                              | Is personal data of children collected and processed? |        |
| Lawful grounds for processig | How is consent collected?                             |        |
|                              | Can subjects withdraw their consent?                  |        |

|                               |                                                                                                                                                             |  |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Transparency requirements     | Is the data subject notified of processing?                                                                                                                 |  |
|                               | Is data collected direct from the subject and is the required information given to them?                                                                    |  |
| Integrity and confidentiality | Are appropriate security measures used to protect the data?                                                                                                 |  |
|                               | are there procedures in place for archiving and destruction of data?                                                                                        |  |
| Data security                 | Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?                            |  |
|                               | Is there a documented process for resolving security related complaints and issues?                                                                         |  |
|                               | Is there a designed individual who is responsible for driving remediation plans for security gaps?                                                          |  |
|                               | Are industry standard encryption algorithms and technologies employed for transferring, storing and receiving individuals' sensitive personal informations? |  |
|                               | Are steps taken to pseudonymise personal data where possible?                                                                                               |  |

Figure 8: GDPR audit template

The GDPR template proposed in figure 8 includes a basic set of questions that will contribute to a better understanding of the Republic Snowdenia County Council's compliance with data protection legislation.

Security testing strategy is defined following Open Web Application Security Project rules. OWASP refers to a set of security recommendations that includes [11]:

- Injection

Republic Snowdenia County Council will be tested against SQL injection attacks. If a formular input does not have UI validations and the SQL commands responsible for retrieving data from the database do not use SQL parameters, then data is easily expose by sending a fake condition like *select \* from employees where name = 'form input' or 1= 1*.

- Broken Authentication

Testing the authentication system includes the usage of a list of credentials (username/password) and a script that tries to login into the system. If any of these randomly generated combinations works then authentication system has a breach.

- Sensitive Data Exposure

This type of attack can be easily performed by stealing the sensitive information from the cache. A tester tries to check if any sensitive data (username and password or a specific for a customer to

access his profile) is stored in cache.

- Broken Access Control

A tester tries to bypass the authentication and authorization by changing the URL. For example, if the URL <http://republicsnowdenia.org/budgets> returns a list of budgets and it can be accessed without being authenticated or without having the required permissions then access control security rule is not satisfied.

## Conclusion

In conclusion, security plays a critical role in every organization and a strong security strategy is required in order to avoid disasters caused by breaches and cyberattacks. Over the years the number of attacks has increased, and security become a challenge. A good strategy includes a proper analysis and ensuring information security at any level from network, application, server security to general security and training. Furthermore, the importance of considering security at an earlier stage of development introduced the concept of “shift left” [12] security.

## Recommendations

Based on the previous evaluation, the following list represents the recommendations for developing a strong security plan for Republic Snowdenia County Council:

- Use Active Directory Domain Services in order to have a better management of employees' accounts, security policies, installed software etc.
- Increase network security by using VPNs especially as there are employees that are working from home and their devices are connected to different unsecured networks.
- Define a password security strategy by enforcing strong passwords and frequently changes requirements
- Improve access security by adding a multi factor authentication mechanism
- Define group policies access rules to avoid critical documents being accessed by unauthorized users (even if they are employees)
- Secure database by creating different credentials per authorized user
- Secure database or servers' ports and not expose them to public access
- Offer security training to employees:
  - Employees must have knowledge about email phishing red flags [13]
  - Employees must not install third-party software without administrators' approval
  - Employees must not expose their credentials over the phone or in person to anyone even if that person pretends is working on support and may need the credentials for troubleshooting
  - Unknown person must not have access into council's building even if that person pretends is from delivery
  - Employees must immediately report any security incident

## Bibliography

- [1] W. Michael and H. Mattord, Principles of Information Security, Sixth Edition, Boston: Cengage Learning, 2018.
- [2] National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations - Special Publication 800-53," NIST, 2013.
- [3] U. Nayak and H. Umesh, The InfoSec handbook - An introduction to Information Security, Apress, 2014.
- [4] National Institute of Standards and Technology, "Guide to Information Technology Security Services - Special Publication 800-35," NIST, Gaithersburg, 2013.
- [5] National Institute of Standards and Technology, "Digital Identity Guidelines - Authentication and Lifecycle Management - Special Publication 800-63B," NIST, 2017.
- [6] National Institute of Standards and Technology, "Guide for Security-Focused Configuration Management of Information Systems - Special Publication 800-128," NIST, 2011.
- [7] K. Beaver, Hacking for dummies, 6th Edition, Hoboken, NJ: John Wiley & Sons, Inc., 2018.
- [8] S. Alex, D. Boodoo and G. Johansen, Assuring Security by Penetration Testing, 4th Edition, Packt Publishing, 2018.
- [9] A. Watkins and C. S, IT Governance - An International Guide to Data Security and ISO27001/ISO27002, 7th Edition, Kogan Page, 2019.
- [10] A. Denley, M. Foulsham and H. B, GDPR: How To Achieve and Maintain Compliance, New York: Routledge, 2018.
- [11] OWASP, OWASP Testing Guide v4, OWASP, 2019.
- [12] Google Cloud, "DevOps tech: Shifting left on security," Google Cloud, 16 11 2020. [Online]. Available: <https://cloud.google.com/solutions/devops/devops-tech-shifting-left-on-security>.
- [13] Microsoft, "How to protect against phishing attacks," Microsoft, 1 11 2020. [Online]. Available: <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing>.