CYBER SPACE SAFETY

SMALL HEALTHCARE CYBERSECURITY

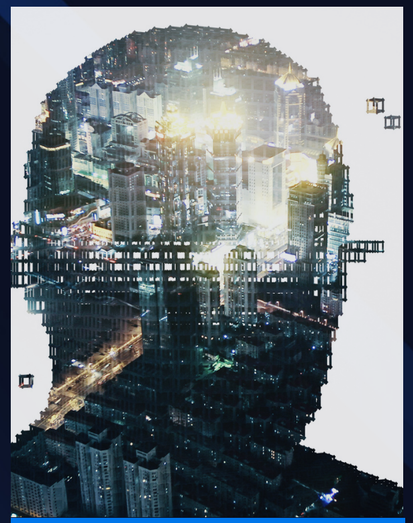
We look to our nearest neighbour (Australia) and their issues with dental clinic cybersecurity to learn and enforce cyber hygiene plans for clinics in developing countries such as Indonesia.

SINGAPORE INTERNATIONAL FOUNDATION

MEET OUR TEAM

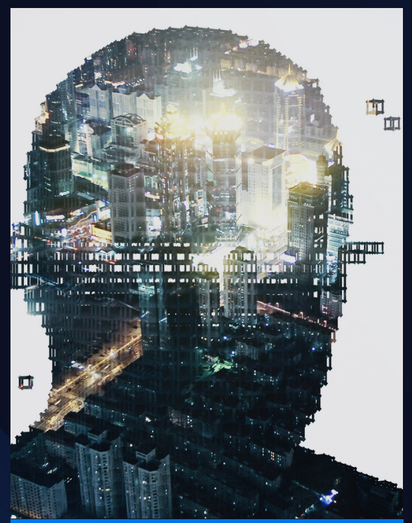
MICHELLE CEACELIA
Group Leader

To learn about cybersecurity, as it is crucial to protect oneself and others from cyber attacks and data breaches, as well as to gain valuable job skills, especially in In today's world.



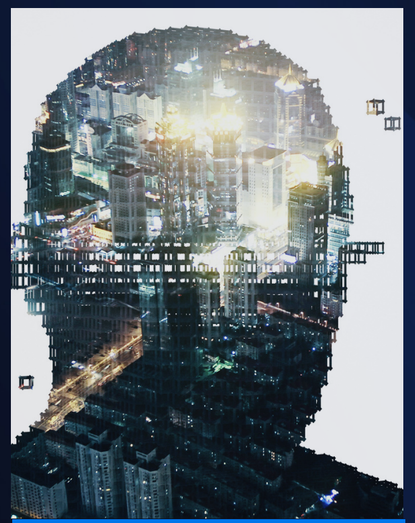
SUTJIPTO BUDIMAN
Group Member

Updated the latest knowledge of cyber security



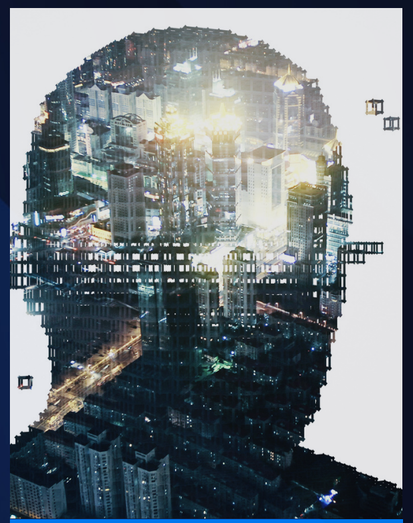
BONAVENTURA HARMAJI
Group Member

Machine Learning in Cyber Defence and Offence



ANUPAM KUMAR GUPTA
Group Member

Incident response and forensic analysis



B. SUTADJI

Group Member

Concern about security in cyber and to update my knowledge.

SAFEGUARDING DIGITAL ASSETS IN DENTAL CLINICS:

ADDRESSING CYBERSECURITY CHALLENGES IN SMALL HEALTHCARE CENTRES

Small healthcare facilities, like dental clinics, are vulnerable to cyberattacks due to their valuable patient data, limited cybersecurity resources, and expertise. These attacks, including ransomware, malware, and phishing, can result in financial and reputational harm and privacy violations. Thus, it's imperative for dental clinics to prioritize cybersecurity and implement effective measures to safeguard their digital assets.

AUS - ATTACK & STATISTICS

A dental clinic in Australia, DENTAL ONE*, recently experienced a data breach, resulting in the theft of 500 GB of customer health data posted on the dark web by a threat actor. To prevent such incidents, businesses should prioritize cybersecurity by updating software regularly, using strong passwords, and training employees to detect and respond to potential threats. In the event of a breach, businesses must act promptly by containing the breach, notifying affected customers, and implementing additional security measures to prevent future incidents. Customers should be advised to monitor their credit reports and bank accounts for suspicious activity. (Source: Firewall Daily Editorial, December 2022)*

Healthcare sector is in the top 3 top of cyberattacks in Australia for the 2021–22 financial year(ACSC, 2022, p. 27).

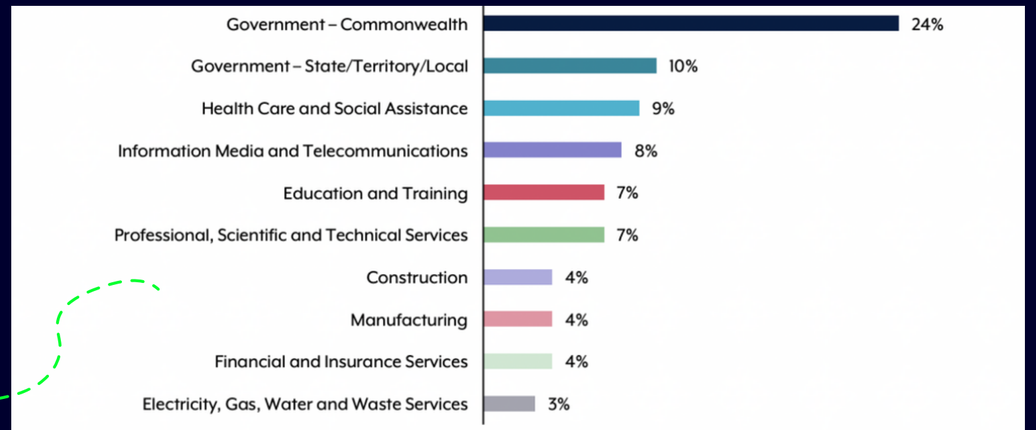
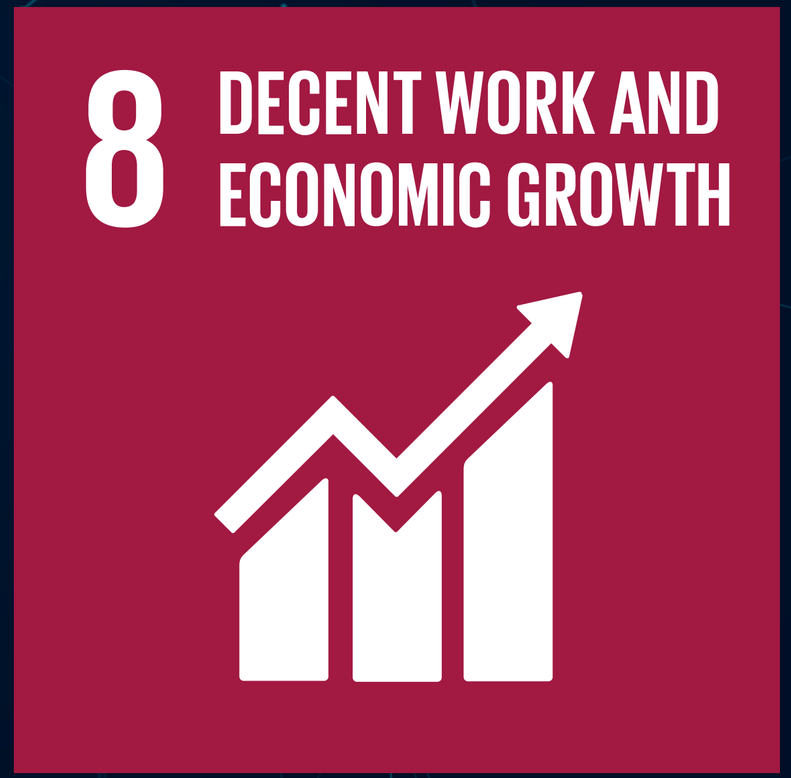


Figure 7: Cyber security incidents to which the ACSC responded in financial year 2021–22, top 10 industry sectors

“ 15% of incidents in the 2021–22 financial year were categorised as C3, up from approximately 6 per cent in the previous financial year” (ACSC, 2022, p. 26).

Catagorazation C1 being the most severe and C6 being the least.

UN SDG GOALS



3. Good Health & Well Being:

- Improved patient care: Digitization of patients records and health information, dental clinics can improve quality and efficiency of patient care. This includes faster access to patient information, easier tracking of patient progress and improved communication among healthcare providers (https://sdgs.un.org/goals).

8. Decent Work & Economic Growth:

- Improved productivity: Digitization of patient records and other administrative tasks, dental clinics can increase productivity and efficiency. This allows dental professionals to focus more on patient care and other high-value activities.
- Enhanced skills and training: Digitizing a dental clinic data system requires dental professionals to learn new technical skills, such as using digital software and tools. This enhances their technical and vocational skills, making them more competitive in the job market and better prepared for future roles.
- Increased economic growth: By improving productivity and efficiency, digitizing a dental clinic data system can contribute to increased economic growth. Creating more job opportunities, including decent jobs and entrepreneurship, which can further contribute to economic growth (https://sdgs.un.org/goals).

5 TECHNOLOGY INFRASTRUCTURE / TOOLS THAT ARE USED IN THE DENTAL CLINIC

- Practice and data management software
- Financial Payment Connection
  (e-wallet, transfer,cash, credit cards)
- Wi-Fi Network
- Local Storage Devices
- Security Software and Firewalls

DENTAL CLINIC

ORGANIZATIONAL CHART

ROLES IN CYBERSECURITY RISK MANAGEMENT

Each stakeholder at the dental clinic has a responsibility to manage cybersecurity risks and protect patient information. Dr. Maria Cilvia, the CTO and owner, oversees the clinic's overall management, including IT, and ensures that cybersecurity policies and procedures are followed. Dr. Fransisca Amy, a dentist, oversees billing and financial control to ensure patient information is protected with the owner. Dental assistants Amilia Lin and Sarah Lee update the clinic's inventory management systems to protect against cyber threats. The receptionist, Emily Davis, collects and stores sensitive patient information that must be safeguarded from cyber threats. Michael Nguyen, the CTSO, manages the clinic's IT infrastructure and ensures cybersecurity policies are implemented, including data encryption, malware protection, and daily backups.

USER ACCESS DECLARATION

S/N	Personnel name	Level in security pyramid	Access to Financials	Edit Stock Quantity	Change Passwords	Edit Price of Doctor Services	Edit of Registration & Schedule
1	Dr. Maria Cilvia (Owner)	Executive/Sec Mgmt	TRUE	TRUE	TRUE	TRUE	TRUE
2	Dr. Fransiska Amy (Partner)	Technical	TRUE	TRUE	FALSE	TRUE	TRUE
3	Amilia Lin, Dentist Asst	Technical	FALSE	TRUE	FALSE	FALSE	FALSE
4	Sarah Lee, Dentist Asst	Technical	FALSE	TRUE	FALSE	FALSE	FALSE
5	Emily Davis, Receptionist	Technical	FALSE	FALSE	FALSE	FALSE	TRUE
6	Michael Nguyen IT Admin	Technical	FALSE	FALSE	TRUE	FALSE	TRUE

ACCESS & CONTROL

S/N	Device	Owner	Registration ID	IPv4	Public/ Private	Password	Anti-Virus
1	IMac 2022 (M1)	Dr Maria Cilvia (treatment room 1) Access to dental assistant Amilia Lin	REG-DOC-MC001 REG-DA-AL003	192.168.1.10	Private	SmileCilvi1*** AmiSmile0815!	McAfee
2	IMac 2022 (M1)	Dr Fransisca Amy (treatment room 2)Access to dental assistant Sarah Lee	REG-DOC-FA002 REG-DA-SL004	192.168.1.11	Private	FransSmle12$ SmilLeee24>>*	McAfee
3	Canon Printer	Control Item	REG-PRINTER-09	192.168.1.30	Private	Nil	Nil
4	ASUS Laptop	Receptionist - Emily Davis (Accessible to IT and Doctors)	REG-REC-ED005	192.168.1.40	Private	RcptSmle01#$	Wndw Dfndr
5	2TB Seagate Hard Drive (Owner)	Dr Maria. C	HDD-MC1001	NIL		MarCil1224^*$	Nil
6	2TB Seagate Hard Drive (Partner)	Dr Fransisca. A	HDD-FA1001	NIL		MyFraiCa10!*	Nil

ACCESS & CONTROL

S/N	Device	Owner	Registration ID	IPv4	Public/ Private	Password	Anti-Virus
7	“SmileStorage” Server (I9 quad-core processor, Nvidia with 2TB CPU storage and 8G RAM)	Control Item	REG-IT-MN006	192.168.1.50	Private	StorSmle0610*	McAfee & Firewall
8	WAPs (Wireless Access Points) Wi-Fi	Wireless Internet access for personal devices and patients (Control Item)	REG-WAP-12	192.168.1.60	Private	D3ntst@Open#	Firewall Std
9	Smart TV (3 - Lounge, Room 1 and 2)	Entertainment	REG-TV1-13 REG-TV2-14 REG-TV3-15	192.168.1.70 192.168.1.71 192.168.1.72	Private	Nil	Nil
10	Internet Router	Internet Access	indihome	Dynamic	Private	D3ntstSml99!^	Firewall
11	XRay (teeth imaging)	Control Item	REG-XRAY-01	192.168.1.20	Private	@DentRay123!	Nil
12	Website	Hosting public ISP Michael Nguyen	Webdentist	125.163.29.10	Public	D3nt1@st@dm	Nil
13	6 personal devices (mobile phones)	Personal owner, partner and employee use	REG-PHONE1-03 REG-PHONE2-04 REG-PHONE3-05 REG-PHONE4-06 REG-PHONE5-07 REG-PHONE6-08	192.168.1.12 192.168.1.13 192.168.1.14 192.168.1.15 192.168.1.16 192.168.1.17	Private		

PORT SCAN & ANALYSIS

S/N	Control Item	Registration ID	Ports scanned	Status of port	Follow-up action required
1	X-ray teeth imaging	REG-XRAY-01	21,22,80,443	All closed	Closed only local connected device through wireless/bluetooth or cable will transfer data. (should be checked weekly basis)
2	WAPS Wifi	REG-WAP-12	21,22,80,443	All closed	All closed, only people with wifi password will be allowed entry. (should be checked weekly basis)
3	"SmileStorage" Server (I9 quad-core processor, Nvidia with 2TB CPU storage and 8G RAM)	REG-IT-MN006	21,22,80,443	All closed	Closed all port, not open to the internet space (if must connect - firewall, intrusion detection, prevention systems, and encryption will be weekly checked/updated)
4	Canon printer	REG-PRINTER-09	21,22,80,443	All closed	Closed only local devices will be able to connect either through bluetooth/cable connection. (should be checked fortnightly basis)

```python
import socket

target = '192.168.1.50' # replace with the IP or hostname of the target machine
ports = [21, 22, 80, 443] # replace with the list of ports to scan

for port in ports:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1) # set the timeout for the connection
    result = sock.connect_ex((target, port)) # attempt to connect to the port
    if result == 0:
        print(f"Port {port} is open")
    else:
        print(f"Port {port} is closed")

    sock.close()
```

```
Port 21 is closed
Port 22 is closed
Port 80 is closed
Port 443 is closed
```

```python
import socket

target = '192.168.1.60' # replace with the IP or hostname of the target machine
ports = [21, 22, 80, 443] # replace with the list of ports to scan

for port in ports:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1) # set the timeout for the connection
    result = sock.connect_ex((target, port)) # attempt to connect to the port
    if result == 0:
        print(f"Port {port} is open")
    else:
        print(f"Port {port} is closed")

    sock.close()
```

```
Port 21 is closed
Port 22 is closed
Port 80 is closed
Port 443 is closed
```

```python
import socket

target = '192.168.1.20' # replace with the IP or hostname of the target machine
ports = [21, 22, 80, 443] # replace with the list of ports to scan

for port in ports:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1) # set the timeout for the connection
    result = sock.connect_ex((target, port)) # attempt to connect to the port
    if result == 0:
        print(f"Port {port} is open")
    else:
        print(f"Port {port} is closed")

    sock.close()
```

```
Port 21 is closed
Port 22 is closed
Port 80 is closed
Port 443 is closed
```

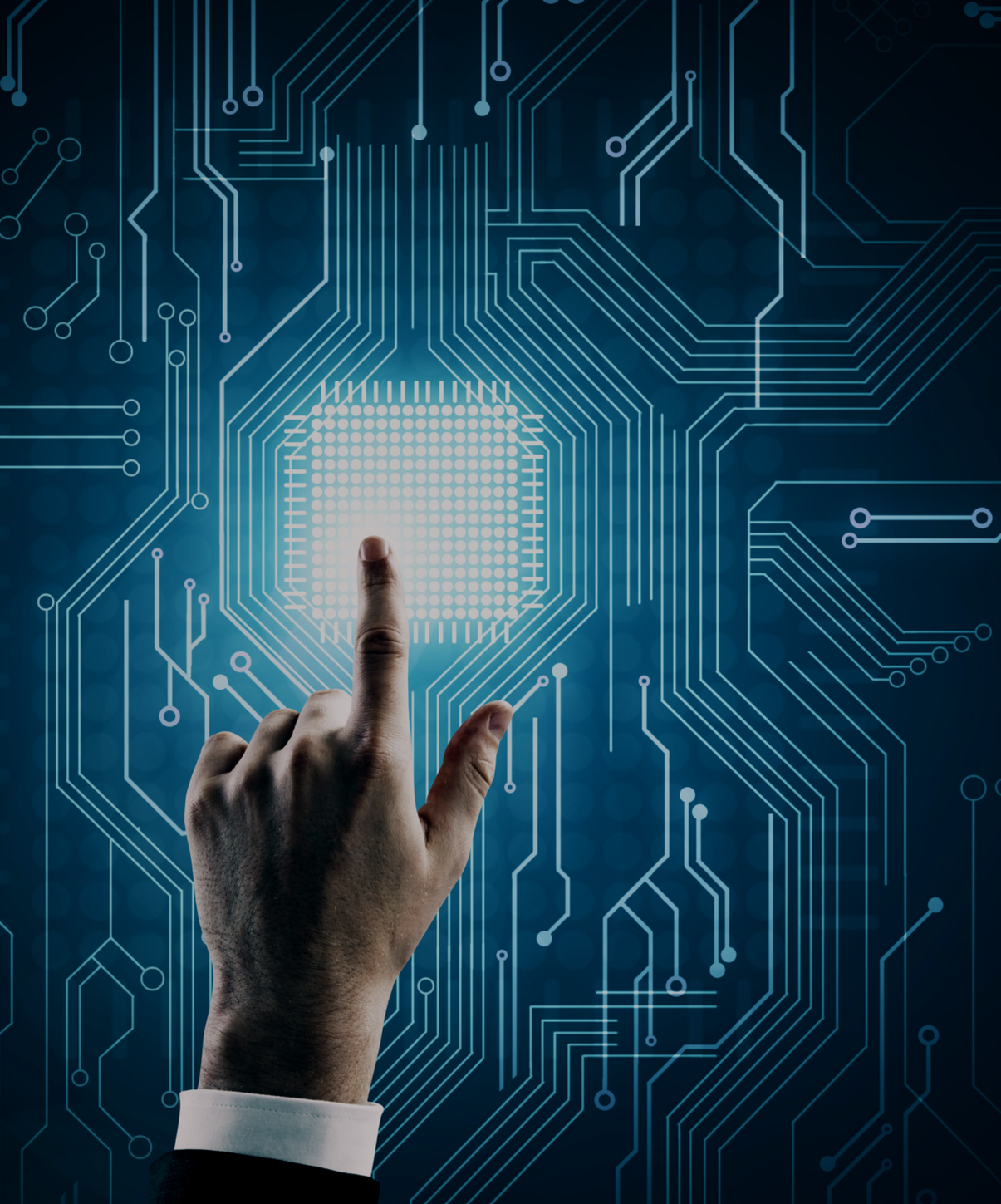
```python
import socket

target = '192.168.1.30' # replace with the IP or hostname of the target machine
ports = [21, 22, 80, 443] # replace with the list of ports to scan

for port in ports:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1) # set the timeout for the connection
    result = sock.connect_ex((target, port)) # attempt to connect to the port
    if result == 0:
        print(f"Port {port} is open")
    else:
        print(f"Port {port} is closed")

    sock.close()
```

```
Port 21 is closed
Port 22 is closed
Port 80 is closed
Port 443 is closed
```



POTENTIAL THREATS & VULNERABILITIES FACING THE CLINIC & PATIENTS

Using a local storage device in a dental clinic can pose several risks, including data loss or damage, physical theft or damage, cybersecurity threats, lack of accessibility, and limited scalability. These risks can result in disruptions in patient care, legal or financial consequences, compromise patient privacy, limit growth opportunities, and impact patient outcomes and satisfaction (SIF-Digilabs, 2023).

POTENTIAL THREATS & VULNERABILITIES

Asset 1: Patient Data	Vulnerability 1: Human error input	Potential threat 1: Incorrect treatment	Risk 1: Reputation
	Vulnerability 2: Weak passwords	Potential threat 2: Unauthorised access, plug-in internal data breach & theft	Risk 2: Patient data loss or misuse
	Vulnerability 3: Inadequate access control	Potential threat 3: Cyber attacks (such as phishing, malware, or ransomware)	Risk 3: Loss of patient trust, legal and financial penalties, reputational damage
Asset 2: Connected Medical Devices	Vulnerability 1: Human error input	Potential threat 1: Incorrect treatment	Risk 1: Data damage
	Vulnerability 2: Inconsistent electricity grid	Potential threat 2: Loss of treatment time	Risk 2: Broken medical device, loss of profit
	Vulnerability 3: Outdated or unsupported operating systems and software that cannot be patched or updated	Potential threat 3: Malware or viruses that infect the device or the network, Physical theft or tampering of the device, Denial of Service (DoS) attacks	Risk 3:Liability risks from using insecure medical devices, Reputational damage to the clinic's reputation

POTENTIAL THREATS & VULNERABILITIES

Asset 3: Wi fi/ Internet Connectivity/ Computers/ Printers	Vulnerability 1: Weak password	Potential threat 1: Spoofing	Risk 1: Data theft online (hacker)
	Vulnerability 2: Local access	Potential threat 2: Plug-in device	Risk 2: Local data theft
	Vulnerability 3: Lack of encryption and secure protocols for Wi-Fi networks	Potential threat 3: Data interception or eavesdropping on Wi-Fi network traffic, Malware or viruses introduced to the network through a compromised device	Risk 3: Losing patient trust, Breaches of patient data and confidential information
Asset 4: Website	Vulnerability 1: Weak coding	Potential threat 1: Defame, malfunction	Risk 1: Reputation, loss of prospect
	Vulnerability 2: Weak hosting infrastructure	Potential threat 2: DDOS	Risk 2: Customer cannot access the website, lost of prospect customer
	Vulnerability 3: Human error	Potential threat 3: Inaccurate information/schedule	Risk 3: Reputation, loss of customer

CYBERSECURITY RISK ASSESSMENT

The IT Administrator will have to conduct a CYBERSECURITY risk assessment every month, have regular data backups, and keep software and security systems up to date to minimize the risk of a cyber attack, ensuring the systems are well protected and running smoothly.

> "NEARLY ALL CYBERSECURITY PROBLEMS ARE DUE TO HUMAN ERROR"
> (SIF-DIGILABS, 2023)

RISK RATINGS:

1 (LEAST) - 5 (SEVERE)

Assets	Risk Probablility	Risk Likelihood	Impact from Risk
1.Patient Data	5, Small clinics do not have large budget for comprehensive safeguards.	4, Higher risk as this is the most valuable information for the hackers.	5, Highest as it might cause financial, reputational, misuse of data and all health data loss.
2.Connected Medical Devices	2,Most devices could not be accessed remotely	3, If medical devices can be accessed, they may have their own software systems that may not be well protected (updates is important, if there are any).	5,Could lead to mistreatment and financial loss
3.Wifi/Internet connectivity and Computers/Printers	5,This is the most convenient way for the hackers to intrude.	5,The advancement in IT is making us increasingly susceptible to loss of data. Smaller clinics are unable to allocate considerable budget for rapid expansion.	4, High impact in terms of liability of website and its access to clinic information, however it can be reduced if defensive systems are in place.
4.Website	3, There are possibility that hackers will try to attack the website	2, The clinic has hired a reputable ISP provider to provide hosting & Website with subscription to have security and IT support.	4, Loss of potential patient due lack of info in case of website hack but the customer can contact through phone

CYBER INCIDENCE RESPONSE

Identify

Training all employee, including owners to recognize the signs of a cyber attack either from internally or externally, such as unusual network activity or suspicious emails.

Contain

If possible, disconnect the affected systems from the network to prevent further damage. This may involve shutting down servers or disconnecting devices from the wifi network.

Assess

Determine the extent of the damage and identify any sensitive data that may have been compromised. This may involve analyzing system logs or conducting a forensic analysis of the affected systems.

Notify

Depending on the severity of the incident, you may need to notify law enforcement, regulatory agencies, or affected patients.

Restore

Once the incident has been contained and the impact has been assessed, work to restore operations as quickly as possible. This may involve restoring from backups or rebuilding affected systems.

Review & Improve

After the incident is resolved, conduct a review the cyber incident response plan and identify areas for improvement. This may involve updating policies and procedures, providing additional training, or implementing additional security measures.

Based from the (NIST CSF Framework, 2014 - Provided by SIF-Digilabs, 2023)

IDEATION - CYBER HYGIENE PLAN

Hardware:

- *Install firewalls to secure the network and block unauthorized access.*
- *Use antivirus software to protect the clinic's computers and network from malware and other cyber threats.*
- *Use secure routers and access points to ensure that only authorized devices can access the network.*
- *Use encryption for all data in transit and at rest to protect it from unauthorized access.*
- *Regularly update all hardware, including computers, servers, routers, and other devices, with the latest security patches and firmware updates.*

Training:

- *Train all employees on the importance of cybersecurity and how to prevent cyber attacks, such as phishing scams, social engineering, and password attacks.*
- *Conduct regular cybersecurity awareness training sessions to ensure that employees are up-to-date with the latest cyber threats and prevention methods.*
- *Develop a cybersecurity policy that outlines the acceptable use of computers, internet, and email for employees.*

Password:

- *Require strong passwords of at minimum 12 characters (Upper, lower case, symbols and numbers) for all devices, accounts, and applications that employees use. Also checking with the password checker safety from the csa.gov.sg or other types of official password checkers.*
- *Enforce password policies, such as requiring password changes every 90 days and disallowing the use of weak passwords.*

Access Control:

- *Limit employee access to sensitive data and systems to only those who require it to perform their job duties.*
- *Implement access controls to ensure that only authorized users can access sensitive data and systems.*
- *Use multi-factor authentication to provide an extra layer of security.*

IDEATION - CYBER HYGIENE PLAN

***Cybersecurity beyond the office*:**

- *Implement secure remote access for employees who need to work from home or other remote locations.*
- *Use VPNs (Virtual Private Networks) to encrypt all data that is transmitted between the clinic's network and remote devices.*

***Data protection*:**

- *Regularly backup all data to prevent data loss in case of a cyber attack.*
- *Use encrypted hard drives and other data storage devices to protect sensitive data at rest.*
- *Store backup data off-site or in the cloud to ensure that it is safe in case of a physical disaster, such as a fire or flood.*

***Worst-case scenario*:**

- *Develop a cyber incident response plan that outlines the steps to take in case of a cyber attack or data breach.*
- *Regularly test the incident response plan to ensure that it is effective and up-to-date.*
- *Work with a cybersecurity expert to develop a plan to recover from a cyber attack and prevent future attacks.*

***Cybersecurity education*:**

- *Conduct regular cybersecurity training sessions for employees to ensure that they are aware of the latest cyber threats and prevention methods.*
- *Keep records of cybersecurity training and assessments to track employee progress and ensure that everyone is up-to-date with the latest cybersecurity practices.*

PERSONAL REFLECTIONS

"I am grateful to have had the opportunity to participate in the Singapore International Foundation's foundational cybersecurity course, which covered a wide range of topics from access and controls to ports, Python, and cyber safety from both external and internal sources. Through the course, I gained knowledge about the NIST framework, CSV SG password detection, ports scanning, and internet distribution from local to WLAN to city-level coverage. I believe that this knowledge is crucial in today's ever-evolving digitized world, and I am eager to extend my understanding further even as a novice in this field.

I would like to express my sincere appreciation to Niki, WanYing, and all the volunteers who generously gave their time and knowledge to facilitate the course. Their dedication to promoting social understanding and community building at an international level is truly commendable, and I feel privileged to have been a part of this meaningful learning experience. I look forward to applying the knowledge gained from this course in my personal and professional endeavors, and I am confident that it will be valuable in navigating the complex landscape of cybersecurity." Michelle Ceacelia

"In the cybersecurity foundation course, I gained a solid understanding of fundamental concepts such as threat analysis, risk management, network security, cryptography, and incident response. The hands-on exercises and simulations provided me with practical skills in implementing security controls to protect against cyber threats. Additionally, the course's emphasis on ethics, professionalism, and social responsibility stood out to me, as it helped me approach security challenges with a comprehensive perspective on their ethical, political, financial, and legal implications. I highly recommend this course to anyone interested in pursuing a career in cybersecurity or looking to improve their knowledge of best practices. It's a crucial first step that provides an excellent foundation for further learning and growth in this exciting field. The course is incredibly valuable, and I found it to be a great experience." Anupam Kumar Gupta

"I plan to take a Cyber Security Course to update my knowledge and stay up-to-date with the latest developments in the field, despite being a Certified Information System Auditor from ISACA. This eight-week course provided me with a solid foundation in red team and blue team functions, risk management, and password rules. I learned how port scanning can ensure that the company or organization's assets are secure and how understanding basic traceroute can provide a deeper understanding of attack possibilities. As a business owner, I cannot participate in the accelerator project due to other commitments, but I highly recommend this course to anyone who wants to enter the field or improve their knowledge of cybersecurity best practices. It's an excellent foundation for further learning and growth in this exciting field." Sutjipto Budiman

"I was motivated to learn about cyber security because, in today's digital world, so many cyber crimes create anxiety in society. I also lack knowledge about cyber security. Thanks to this course, I understood the mindset and ways of working that lead to negligence or cyber-criminal opportunities and their precautions. It gave me basic knowledge on how to trace the source of the problem and how to prevent data theft in the system of our company." Bonaventura Harmaji

"I'm into the cyber world because I can learn a lot and meet new people from all over. But there are also bad people out there who do bad stuff like hacking and cheating. Thankfully, I haven't had my credit card hacked (knock on wood), but I know it's important to be careful. I took this really helpful cyber security course from Digilabs that taught me how to stay safe online. Now, I feel more confident and can help others stay safe too." B.Sutadji

TEAM REFLECTION

As a team, we express gratitude to all members for their dedication in completing the project. Collaborating, leveraging our diverse backgrounds and skills, we accomplished our goals. This learning opportunity enriched our teamwork skills and allowed us to develop a better understanding of each other's strengths and weaknesses. Proud of the successful project completion, we commend the quality of our work and recognize the growth we have achieved as a team. The cybersecurity course provided vital knowledge, facilitating project implementation. Utilizing WhatsApp and Zoom enhanced our communication, and we learned to effectively communicate despite our different time zones. Our leader played a vital role, guiding and leading us to success, ensuring high-quality standards. We recognize and appreciate our leader's efforts and leadership that helped us accomplish our goals. We congratulate all team members for their contribution to the project's success and anticipate continuing our teamwork.

"THE PRICE OF FREEDOM IS ETERNAL VIGILANCE."

THOMAS JEFFERSON

REFERENCES

- Singapore International Foundation (SIF) - Digilabs Weekly Tutorial PPT, 2023
- Annual Cyber Threat Report - Australian Cyber Security Centre (ACSC), June 2023
- Dental One Cyber Attack - Firewall Daily Editorial, December 2022
- United Nations Website - Department of Economic and Social AffairsSustainable Development: The 17 Goals, accessed April 2023