

INNOVATION & RESEARCH ASSIGNMENT 1

15 January 2026 15:12

STUDENT NAME: SAAIMA AFSAR

STUDENT ID NUMBER: 2427066

MODULE: CHANGEMAKERS: Creativity & Value Creation

MODULE CODE: ACCA5033

LECTURAR: Dr Osman Elgawi

ASSIGNMENT TITLE: ASSIGNMENT 1: Innovation & Research

E-PORTFOLIO LINK TO MY CYBER SECURITY PROJECT:

INTRODUCTION

Sunday, January 25, 2026 3:36 PM

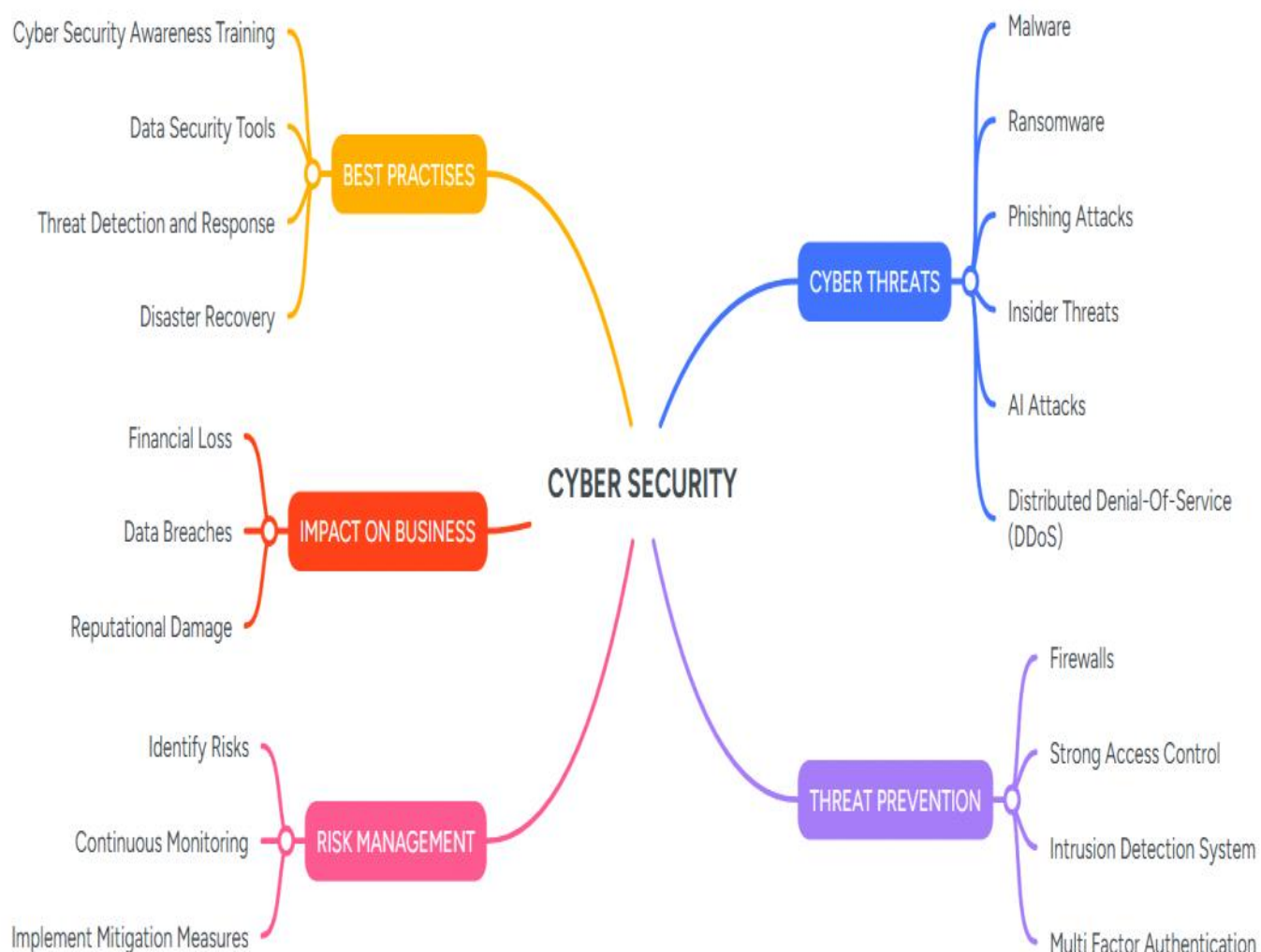
For the Changemakers: Creativity & Value Creation Module, the assignment involves creating a project. I generated an idea related to my specific area of study, from this idea I created a Mind Map, I then documented an Aim and several Objectives from the Mind Map. I identified appropriate research philosophy and search tools, I then selected specific research databases to identify research related to my chosen project area. I documented strategies to enhance Validity, Reliability, Generalizability and Ethical Considerations related to my project. I also discussed the relevant data collection methods required for my project, and from this information I designed a pilot data collection appropriate for my chosen project. I then outlined some different types of quantitative and qualitative analysis. From this information I created a poster for my project, followed by references to support my information.

TASK1: IDEATION & MIND MAP

Tuesday, January 20, 2026 7:30 PM

Cyber Security:

I selected Cyber Security for my chosen project, Cyber security has become a very critical concern that needs the attention of researchers [1]. Cyber Security is very important for the protection of cyber threats, the attacks are increasing rapidly [2], and are constantly causing disruption to organizations, by unauthorized access, data leaks, financial loss and damage to businesses. The potential attacks and impacts of those attacks need to be investigated to develop an effective cyber security infrastructure [3]. Cyber Security protects privacy, it plays a vital role in risk mitigation and safeguarding sensitive information. Cyber Security offers a range of methods, such as, data encryption, network security and regular security updates, as well as the art of maintaining information confidentiality, integrity, and availability [4]. It also establishes strong cyber security policies and procedures.



TASK 2: AIM & OBJECTIVES AND RESEARCH AREA

Tuesday, January 20, 2026 7:58 PM

AIM: Cyber Security:

The aim of cyber security is to protect systems, networks and data from unauthorized access and cyber threats. Cyber security's main aim is the "CIA triad":

Confidentiality: This ensures data can only be accessed by authorised users.

Integrity: Maintains data accuracy, preventing any changes.

Availability: Is when systems and data are available when required.

OBJECTIVES:

1) Cyber threats:

Cyber threats are malicious attacks that cause damage and disrupt systems. The types of cyber-attacks are: Malware, Ransomware, Phishing attacks, Insider threats, AI attacks, Distributed denial-of-service (DDoS) and many more. These attacks are carried out by hackers and cyber criminals who want to exploit the system for financial gain or to cause disruption. Organizations aim to gather and share real-life cyber threat information and then turn it into threat intelligence for preventing attacks[5], by placing security measures.

2) Threat Prevention:

Threat prevention prevents attacks from entering the system, by using high security measures, such as, Firewalls, Strong Access Control, Intrusion Detection Systems and Multi-Factor Authentication. The users want their data to be highly secured and the internet is a public network [6], all these measures provide controls that block malicious activity and unauthorised access across systems and networks. The aim is to block all malicious threats from entering the systems.

3) Risk Management:

Risk management identifies, analyses and evaluates risks to reduce the likelihood and potential impact of each risk. It mitigates measures to prevent, control and continuously monitors and reviews security measures. An accurate prediction of risk can help organizations to determine the suitable controls in a proactive manner to manage the risk [7]. This will assist organizations to protect their systems and data by recognizing and responding to threats immediately.

4) Impact on Organisations:

Organisations suffer a great extent by financial loss through cyber-attacks, such as, Ransomware. These attacks include theft of funds, intellectual property and payment card details. Other impacts are Data breaches and Reputational damage to businesses, also increase in security vulnerabilities and hacking attacks are causing the loss of human trust [8]. Failure to protect customer data will result in customer loss, and also severe penalties from authorities.

A breach in one company will cause disruption to the supply chain and affect the partners and operations across the ecosystem, this will result in reputational damage to the organisation.

5) Best Practices:

Applying best practices in organisations help build businesses. One of the important measures to increase the degree of security is by awareness training [9]. These trainings educate and train staff to identify and prevent attacks from occurring. Threat detection and response plan will encourage staff to record and monitor all threats, and also review and update the plan after each incident. Data security tools are another form of security measures, these tools offer 24/7 continuous monitoring, they are known as, Firewall, SIEM and SOAR. Zero Trust Policy will also be beneficial to organizations, by never trusting and always verifying users and devices, these tools will prevent breaches across networks.

Pragmatism:

Pragmatism research philosophy protects the cyber security system by dealing with threats and vulnerabilities in a realistic, sensible and actionable manner. It works on solving practical problems and operates decisions that are based on "What will work best", to find solutions to research problems.

Positivism:

Positivism analyses security incidents, network traffic and system vulnerabilities. It uses quantitative methods to log analysis, survey data and establish security laws or frameworks.

Critical realism (CR):

Critical realism investigates not only the "What", but also the "Why and How" that creates vulnerabilities. The goal of CR is to analyse the "dark side" to understand the security mechanisms, then to be able to create, evaluate and change them to improve security.

Google Scholar:

Google scholar is a free broad search engine, it contains articles, reports journals, and books, it is tailored to search queries for cyber security. There is an advanced search feature that filters searches by author, journal and date of publication. Users can search using high impact journals, such as IEEE to search for cyber security related research.

IEEE Xplore Digital Library:

IEEE Xplore Digital Library is a powerful resource to access cyber security research published by IEEE. It contains, articles, conferences, magazines, journals, books and standard documents. It is freely available for users and researchers to obtain high quality literature for cyber security within the IEEE Xplore database.

ACM Digital Library:

ACM Digital Library offers free open-access area to its content. It offers journals, conference proceedings and books for security and privacy for cyber security research. The platform allows searching for specific topics, authors and users can filter by date to find research on threats and defences. It has an in-depth research to support researches in the cyber security field.

TASK3: RESEARCH STRATEGIES

Tuesday, January 20, 2026 9:28 PM

Validity:

Enhancing the validity of cyber security is to ensure security measures are effective, accurate and reduce risks, by implementing frameworks that detect vulnerabilities and take action against them. Poorly executed security measures result in poor cyber security [10]. Therefore, a response plan should be regularly tested and updated, security controls should be monitored, to see the effectiveness of the plan to prevent real attacks from occurring. Staff should have regular trainings to educate them on recognizing threats, and identifying tactics, and protecting organisations with high security measures.

Reliability:

Enhancing the reliability in cyber security requires continuous improvement, by minimizing human error and quick recovery from incidents. This can be achieved by multiple security controls, if one fails, others are in place to mitigate the threat. Another form of security measure is enforcing strong multi-factor authentication for all users, also implementing zero trust policy, ensuring verification of all users and devices before access is granted. An incident response plan should be created and documented. Continuous monitoring, threat information collecting, and collaboration with key parties are essential for a quick and efficient response [11]. By implementing all these strategies, organizations can remain functional even when subjected to cyber-attacks and system failures.

Generalisability:

Strategies to enhance generalisability in cyber security is to strictly verify every user and device, regardless of location before allowing access. Human errors, negligence, lack of awareness, insufficient training, increase the risk of successful cyberattacks [12]. Frameworks should be implemented, like NIST cyber security framework (CSF) and ISO 27001 to manage risks and continuous monitoring against threats, ensuring security measures are effective across the system.

Ethical Considerations:

Ethical considerations in cyber security is handling sensitive data with confidentiality, by protecting data from unauthorized access. Managing insider threats, addressing risks from unauthorized access who may misuse their position, this results in considerable personal and organisational damage [13]. Accountability should be taken for data breaches, ensuring regulations like GDPR are taken seriously, by implementing security measures and using security tools to manage threats.

Research strategies and data collection methods for cyber security involves surveys and questionnaires. This involves collecting publicly available data to identify behaviour from professionals and users, also to collect data on human factors and monitor security awareness. Interviews and focusing on groups is a qualitative method to explore ideas and motivate each other to understand and recognize the attacks and prevention methods, by using tools, such as Firewalls, security configurations and logs. Each method has its unique strengths and used in combination will give insights into security challenges. Data should be used to identify problems, improve the security

measures, and make smarter business decisions by implementing automation tools, such as, SIEM for 24/7 monitoring of the system.

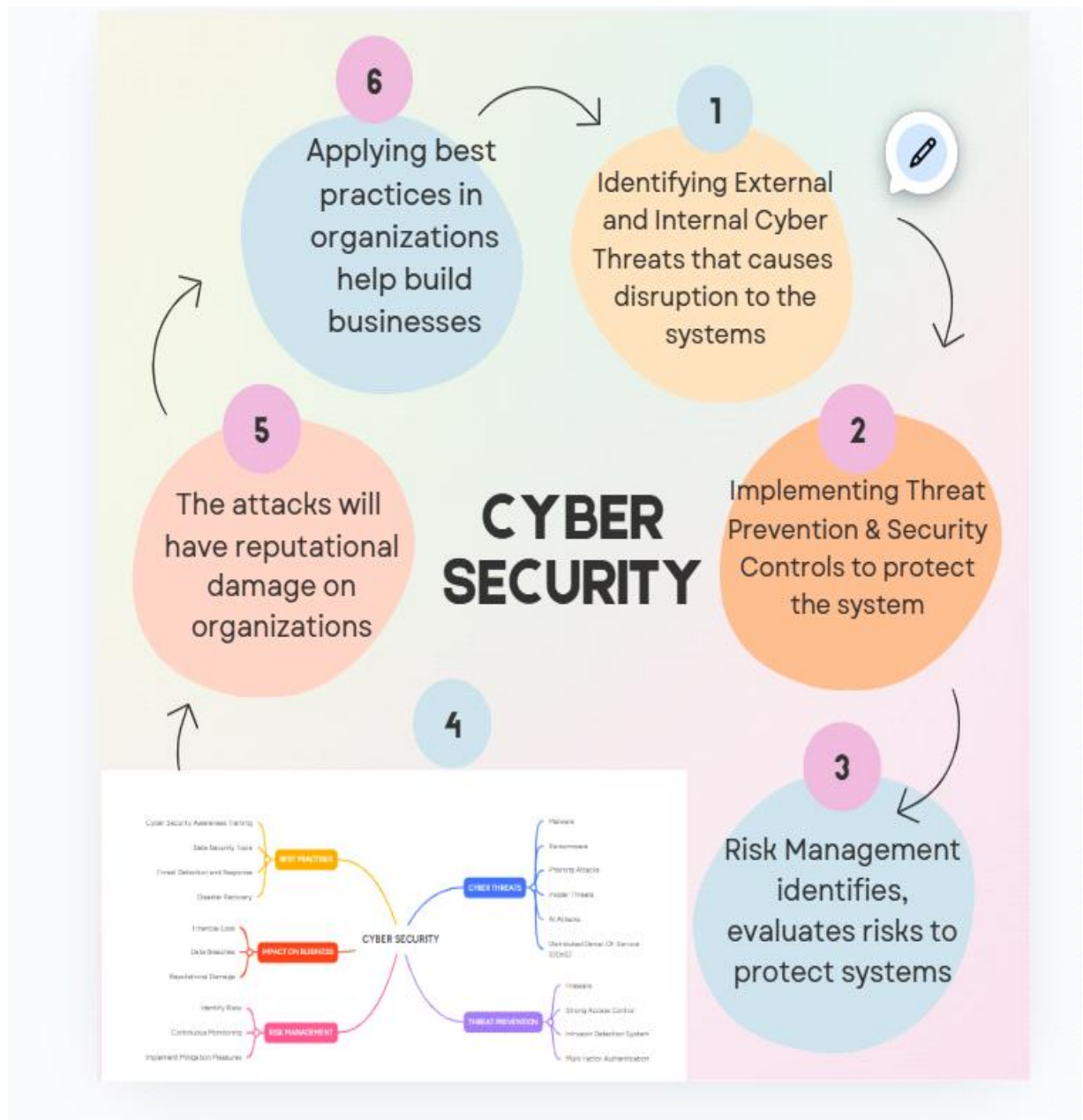
Clear goals should be set when designing a pilot data collection method. Appropriate tools should be selected that are required for cyber security. Automated tools, such as, SIEM & SOAR will offer continuous monitoring, early signs of unauthorized access and malicious attacks should be detected and reported. The findings should be logged by collecting all necessary information for the research, this will minimize privacy risks, especially when dealing with personal, sensitive information. For this the implementation of encryption and strict access control is required. Errors should be removed, any duplicates erased, all invalid entries should be deleted from the collected data.

Quantitative analysis focuses on numerical data, it calculates the financial impact of the threats. It measures the effectiveness of the security controls, by comparing it to the reduction in risks, it calculates the risk scores by using hard data. Quantitative analysis is used for a more deeper analysis for higher threats, it measures variables and theories, such as, surveys and experiments.

Qualitative analysis identifies risks and threats on the probability scale of the impact on the likelihood of the risk occurring, (e g, low, medium, high, critical). Qualitative analysis is used for a quick assessment, it focuses on non-numerical data, such as interviews and observations.

APPENDICES: CYBER SECURITY POSTER

Tuesday, January 20, 2026 9:28 PM



REFERENCES:

Tuesday, January 27, 2026 10:13 PM

- [1] Admass, W.S., Munaye, Y.Y. and Diro, A.A., 2024. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, p.100031.
- [2] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo and J. Shin, "Analysing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach," in *IEEE Access*, vol. 10, pp. 65044-65054, 2022
- [3] N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," in *IEEE Access*, vol. 12, pp. 18147-18167, 2024
- [4] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," in *IEEE Access*, vol. 10, pp. 93104-93139, 2022
- [5] N. Sun et al., "Cyber Threat Intelligence Mining for Proactive Cybersecurity Défense: A Survey and New Perspectives," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748-1774, third quarter 2023
- [6] UI Nabi, A., Ahmed, M., & Abro, A. (2022). An Overview of Firewall Types, Technologies, and Functionalities. *International Journal of Computing and Related Technologies*, 3(No 1), 10-16.
- [7] Kure, H.I., Islam, S., Ghazanfar, M. *et al.* Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Comput & Applic* 34, 493–514 (2022).
- [8] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo and J. Shin, "Analysing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach," in *IEEE Access*, vol. 10, pp. 65044-65054, 2022
- [9] B. Alkhazi, M. Alshaikh, S. Alkhezi and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," in *IEEE Access*, vol. 10, pp. 132132-132143, 2022
- [10] M. N. Y. Marican, S. A. Razak, A. Selamat and S. H. Othman, "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review," in *IEEE Access*, vol. 11, pp. 5442-5452, 2023
- [11] Jha, R.K., 2023. Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. *Recent Research Reviews Journal*, 2(2), pp.215-241
- [12] Aljumaiah, O., Jiang, W., Addula, S.R. and Almaiah, M.A., 2025. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J. Cyber Secur. Risk Audit*, 2025(2), pp.12-26.
- [13] S. Rauf, M. Muneer, K. Suseenthiran, T. Weerasinghe and F. Rashid, "Can LLM-Embeddings Detect Phishing URLs?," 2025 *IEEE 50th Conference on Local Computer Networks (LCN)*, Sydney, Australia, 2025