MITRE ATT&CK-driven Cyber Risk Assessment

Mohamed G Ahmed
ma5875m@greenwich.ac.uk
School of Computing and Mathematical Sciences,
University of Greenwich
United Kingdom

Sakshyam Panda*
s.panda@greenwich.ac.uk
School of Computing and Mathematical Sciences,
University of Greenwich
United Kingdom

Christos Xenakis
xenakis@unipi.gr
Department of Digital Systems,
University of Piraeus, Greece

Emmanouil Panaousis
e.panaousis@greenwich.ac.uk
School of Computing and Mathematical Sciences,
University of Greenwich
United Kingdom

ABSTRACT

Assessing the risk posed by Advanced Cyber Threats (APTs) is challenging without understanding the methods and tactics adversaries use to attack an organisation. The MITRE ATT&CK provides information on the motivation, capabilities, interests and tactics, techniques and procedures (TTPs) used by threat actors. In this paper, we leverage these characteristics of threat actors to support informed cyber risk characterisation and assessment. In particular, we utilise the MITRE repository of known adversarial TTPs along with attack graphs to determine the attack probability as well as the likelihood of success of an attack. We further identify attack paths with the highest likelihood of success considering the techniques and procedures of a threat actor. The assessment is supported by a case study of a health care organisation to identify the level of risk against two adversary groups– Lazarus and menuPass.

CCS CONCEPTS

• **Security and privacy**; • **Mathematics of computing** → **Mathematical analysis**; • **Theory of computation** → *Probabilistic computation*;

KEYWORDS

Cyber risk assessment, MITRE ATT&CK, Attack graph, Threat modelling.

ACM Reference Format:
Mohamed G Ahmed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis. 2022. MITRE ATT&CK-driven Cyber Risk Assessment. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3538969.3544420

1 INTRODUCTION

Digitisation, inter-connectivity and smart technologies have escalated the severity and regularity of cybercrime. Surveys highlight that despite increased awareness of cybersecurity, organisations are reluctant to take relevant measures to mitigate cyber risks [11, 14]. The impact of inadequate cybersecurity is estimated to cost USD 945 billion globally in 2020 [35]. Despite the increasing relevance of cybersecurity to the economy, the availability of data on cyber risks remains confined. The lack of data establishes significant challenges for research, risk management and cybersecurity.

Adversaries often use sophisticated and changing tactics, techniques and procedures (TTPs) to exploit known weaknesses and identify zero-day vulnerabilities making it challenging to assess and predict the extent of cyber threats. To address this challenge, organisations have started sharing threat intelligence to have a fair view of the range of threats, threat actors and their behaviours. The shared adversarial knowledge bases are used by cybersecurity professionals globally to analyse, understand and enhance defensive strategies. This paper introduces a cybersecurity risk assessment methodology that utilises the MITRE ATT&CK knowledge base, the NIST SP 800-30 Rev.1[1] guidelines for risk assessment and attack graphs to support risk characterisation and assessment. MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics, techniques and procedures based on real-world observations [23]. The ATT&CK knowledge base is used to develop specific threat models and methodologies, both in the private and government sector, as well as by the cybersecurity product and service community.

Existing work on cyber risk management has covered specific aspects such as cyber security culture, awareness and training [28, 38], the impact and mitigation of cyber-attacks [7, 25, 33] and the cyber risk management process [5, 32]. Organisations must implement effective cyber risk management practices aligned with their business objectives through protection [4, 6, 24, 29, 36], mitigation [7, 16, 28] and insurance [5, 26, 30] to contain the cyber risk and exposure. Risk management is a continuous process that must acknowledge the changing internal and external environment of the organisation. Using a systematic and rigorous approach, this paper analyses existing risk assessment methodologies and proposes an exhaustive risk assessment approach building upon the concepts of the

[1] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

ARES 2022, August 23–26, 2022, Vienna, Austria
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3544420

vulnerability-centric approach, asset/impact-centric approach and, in particular, the threat-centric approach. We identify weaknesses a threat actor can exploit that increase the success probability of an attack and map those weaknesses to various TTPs. The impact is determined in terms of a hindrance to business objectives. Leveraging the MITRE ATT&CK knowledge base together with attack graphs, this paper aims to investigate the following questions:

- How knowledge about adversaries can improve cyber risk assessment and preparedness?
- Other than technical vulnerabilities, which other parameters contribute towards the realisation of a threat?

The remainder of the paper is structured as follows. Section 2 discusses relevant work and positions our contribution. Section 3 presents the proposed methodology, including the concepts, parameters and risk assessment formulation. Next, Section 4 layout the simulation scenarios under investigation and presents the results. Finally, Section 5 concludes the paper.

2 RELATED WORK

This section presents relevant work related to cybersecurity risk assessment with a focus on two aspects: the framework used for risk assessment and the approaches implemented to conduct the assessment. We begin by analysing risk assessment approaches to understand the existing practices and highlight the advantages and gaps. Frameworks used are either globally recognised risk assessment frameworks such as ISO 27005, COBIT 5, NIST SP 800-30 or frameworks proposed by the scholars as their work. The approaches for risk assessment can be categorised into (i) Subjective approach where professional experience and knowledge of the scholars and/or the organisation under assessment is used to collect the required information for the risk assessment process; (ii) Asset/Impact-centric approach uses critical assets and the impact that might occur if these assets are compromised; (iii) Asset/Vulnerability-centric approach uses vulnerabilities identified within critical assets; and (iv) Threat/adversary-centric approach is built on threats analysis and threat actors' behavioural aspects.

Subjective approach. Lim and Suparman [21] used NIST SP 800-30 along with a subjective approach called Review Document, Interview Key Personnel, Inspect Security Control, Observes Personnel Behaviour and Test Security Control (RIIOT) to collect the required information for the risk assessment within the Indonesian cloud providers environment. Setiawan et al. [34] used a similar approach by integrating the techniques from NIST SP 800-30, ISO 27000 series with interviews, questionnaires and observations for information security risk management and risk treatment. On the other hand, Supriyadi and Hardani [37] used COBIT 5 with NIST SP 800-30 to assess risk on critical application systems. The authors used a subjective approach based on questionnaires and observations to identify threats, threat types, threat actors, possible threat events and a list of affected assets. Using interviews and questionnaires for risk assessment is a common practice. A limitation of such an approach in risk assessment is that the process is restrained by the assessor's knowledge and experience, which could lead to a false sense of security.

Asset/Impact-centric approach. Alwi and Ariffin [2] used an asset/impact-centric approach with ISO 27005 to identify and evaluate mission-critical assets, consequences of compromise, vulnerabilities, threats related to vulnerabilities and countermeasures to protect these assets to support the Malaysian Aeronautical Information Management System. Although the authors emphasised the importance of mission-critical assets to business objectives, their approach lacked insights on the type of threats or threat actors that might target these assets and how they affected the evaluation. Harry and Gallagher [13] proposed an approach to effectively measure the impact of malicious events on complex systems. However, determining the overall risk is a challenge as the approach does not consider the likelihood of occurrence of an event. To overcome this challenge, [28, 33] focused on determining the likelihood of occurrence of a threat to identify the overall expected impact on an organisation. In this paper, we adopt a similar approach to determine the likelihood of occurrence of an attack to support the risk assessment. Kure and Islam [19] utilised ISO 31000, NIST SP 800-30 and NERC CIP guidelines[2] to classify assets and weight them using KPI score based on confidentiality, integrity, availability and reliability. The authors used a subjective approach to identify possible vulnerabilities and threats. Our model extends this approach by considering lateral as well as vertical movement of an attack. Furthermore, vulnerabilities are measured in terms of impact rather than the easiness of exploitation. Finally, factors like the attackers' capability and motivation are also taken into consideration.

Asset/Vulnerability-centric approach. Using the CVSS metrics, George and Thampi [9] proposed a risk assessment model for IoT edge devices. Relevant vulnerabilities are identified using vulnerability scanners such as Shodan, Retina IoT Scanner, IoT Sploit, and Kaspersky IoT and attack graphs are used to calculate the easiness of attack based on the vulnerability values in each attack path from the edge device to the target device. Aksu et al. [1] used a similar approach where assets value and impact are calculated based on the effects of confidentiality, integrity and availability. Although the authors presented a numeric estimation of threats, they used a subjective approach to estimate these numeric values without using any data from threat intelligence sources available. Russo et al. [31] introduced a web-based software platform to automate cyber risk assessment using NIST SP 800-30 Rev.1 framework in a vulnerability-based approach. In contrast, our methodology extends the analysis by considering threat information to evaluate the threat and understand the threat actors' behaviour.

Threat/Adversary-centric approach. Katsumata et al. [17] proposed a risk management methodology for the acquisition and development of mission critical systems. Utilising the concepts of NIST SP800-30, the authors proposed the cyber security risk management framework from a system development life cycle standpoint. Kure and Islam [20] introduced a risk assessment approach for critical infrastructure based on Cyber Threat Intelligence (CTI) leveraging the concepts of ISO 27005 and NIST SP 800-30. [22] and [18] used a similar approach to identify security metrics describing threats and their countermeasures. Haji et al. [12] proposed a risk management module that uses threat modelling to identify threats using NIST SP 800-30 and OWASP threat scenarios. Our

[2] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

methodology extends this practice by identifying and including relevant threat metrics to strengthen the characterisation and assessment of risks. Ben et al. [3] used a quantitative approach to evaluate the motivation, capabilities and opportunity of attackers to calculate the risk associated with specific threats. While [15] and [8] proposed a threat-centric approach for risk management based on the cyber kill chain. Figueira et al. [8], in particular, used machine learning to identify the frequency of threat occurrence. Although these studies suggest a threat-centric risk assessment approach, unlike our approach, attributes of threat actors such as motivation, capabilities and TTPs were not applied to evaluate the level of threat posed to an organisation by a threat actor.

To model cyber security threats, Golushko and Zhukov [10] utilised the MITRE ATT&CK knowledge base. As this approach does not include the vulnerability levels, level of exposure, available controls and relevance of threat to an organisation, identifying relevant threats and the measures to mitigate them effectively is a challenge. A holistic approach to risk assessment would be to integrate threat knowledge with risk assessment, as adopted in our approach. Although a considerable effort is placed on cyber risk assessment, existing work still lacks a demonstration of a comprehensive risk assessment approach that utilises behavioural metrics of threat actors. In particular, the reviewed methods did not consider one or more risk assessment factors such as threats, vulnerabilities, assets, impact, and business objectives. In addition, the aforementioned work lacks a comprehensive approach to using the MITRE ATT&CK framework in the risk assessment process.

3 MITRE-DRIVEN RISK ASSESSMENT MODEL

In this section, we define the core components of our methodology, which allows us to identify, assess and communicate the cyber risk for an organisation. Our methodology is built upon a four-step process – based on the NIST SP 800-30 Rev.1, a widely accepted risk assessment framework – as follows:

3.1 Step 1: Organisational Modelling

This step establishes the context of the organisation such as the identification of business objectives, business processes, network architecture, data types and user types, in which risk is to be assessed. These characteristics are unique for an organisation, recording them in a structured form is essential for an acceptable risk assessment process. This step includes:

- *Identifying business objectives.* Business objectives are the reference on which impact is measured. Any event that negatively affects business objectives is considered a risk to the organisation.
- *Identifying and classifying assets.* Information, data and communication must be identified and classified based on their sensitivity and the level of impact. Business processes are classified according to their criticality to business objectives. Data types are categorised according to their criticality to business processes and the level of impact on confidentiality, integrity and availability of information. ICT systems must be classified according to the business processes they are utilised in and the data types they use and process.
- *Identify users and users' access level to information assets.* Different users require different access permission to information assets. Identifying user types and the data and systems they have authorised access to is essential, as users are commonly targeted by threat actors to gain initial access.

3.2 Step 2: Threat Modelling

Threats are events caused by actors (known as threat actors) with malicious intent leading to adverse situations for an entity. Threat actors, to achieve their objectives, use different tactics, techniques and procedures (TTPs) to exploit the weakness of a system or network. In our model, the gain of an adversary is defined by the used tactic, whereas the techniques and procedures define the probability of success of an attack. An adversary could implement several techniques against a weakness where each implementation could lead to a different impact. We define such implementations as the implementation variants of a threat. A threat can have multiple variants for a target. For instance, PowerShell could be used to execute commands on a local machine as well as on a remote machine.

A Weakness can be a technical vulnerability or poorly configured control or legitimate services which could be exploited by adversaries. We classify weaknesses into two categories based on how they supplement the execution of a technique.

i. Preconditional weakness: A weakness that must exist for a technique to be implemented on the target. For example, when windows PowerShell is not installed, none of the techniques that exploit weaknesses of the windows power shell can be implemented on that system.
ii. Enabling weakness: A weakness that increases the success probability of a technique on the target. These weaknesses are instrumental in aiding adversaries to advance through a system or network.

Once the weaknesses and attack probabilities are defined, the next metric is Opportunity which represents the success probability of an implemented technique by a threat actor. We assume that the success probability of any technique depends on the environment under attack and the gain from the attack. We define gain as the outcome of a threat variant (eg., user accounts, access to a specific system) and are derived from the overarching tactic of the technique used by the threat variant, while, Preconditional gain is the gain from previous steps. For example, if a threat actor wants to run a discovery technique on a specific system, the gain "execution" should have been achieved earlier on that system. This approach represents the dependency of the discovery technique on the successful implementation of the execution technique.

We identify a set of enablers in an environment that can support a technique. We define two categories of enables: i) Binary enablers (eg., a service is enabled or disabled) with a contribution of zero or one to the technique; ii) Variable enablers (eg., audit frequency or access control level) with a contribution $\in [0, 1]$. Regardless of the type, the sum of contributions from all the enablers for a technique is one. Enabling weaknesses that contribute to the success of a specific threat variant are grouped into one or more weaknesses. Each weakness in the group has a contribution value that represents how it contributes to the success of that variant compared to other weaknesses in the group. The overall contribution of all weaknesses

Preferences	**Simulation-1**	**Simulation-2**	**Simulation-3**	**Simulation-4**
Scenario	Scenario-1a	Scenario-1b	Scenario-2a	Scenario-2b
Group	menuPass	Lazarus	menuPass	Lazarus
Goal	Data Exfiltration	Service Destruction	Data Exfiltration	Service Destruction
Target	DT0001	PR0002	DT0001	PR0002
Initial access	ASS018	ASS003	ASS018	ASS003

Table 1: Simulation choice

P_y	Permission P is a precondition for attack variant Y
G_y	Enabling weakness group G of attack variant Y
$w_i \in G_y$	w_i is an enabling weakness in weakness group G_y
Cw_i	Contribution value of w_i in group G_y
Ew_i	Environmental value of w_i
PW_y	Preconditional weakness of attack variant Y
pw_i	Environmental value of w_i
PG_y	Preconditional gain of attack variant Y
pg_i	Gain value
PV_y	Preconditions value of attack variant Y
VO_y	Opportunity of attack variant Y

Table 2: List of Symbols

in a weakness group is capped at 80%. The remaining 20% is called residual opportunity and is assumed by default for each threat variant. This means that if all enabling weaknesses are mitigated on any given system, the model still assumes 20% opportunity for the relevant threat variant on that system. This assumption is made to reflect the residual risk after all mitigation relevant to the specific threat is implemented and to compensate for any workaround that might be done by an attacker to overcome an implemented control. This assumption also acknowledges that full protection is never attainable. Gains obtained from defence evasion techniques can change the environmental properties by overriding some controls (i.e. adding weaknesses that did not exist earlier or bypassing an existing control), this process is called controls override. Any weaknesses added due to control override have a contribution value equal to the contribution value of the weakness in its group multiplied by the opportunity of the technique which triggered the control override.

From the adversarial profiles presented in MITRE ATT&CK framework, three main attributes of an adversarial group i.e., Industries of Interest (II) (eg., healthcare, government) and Regions of Interest (RI) (eg., UK, Germany) are used to express the level of interest a threat actor might have in any given organisation. We express this interest as the Likelihood of Occurrence (LO) of a threat. Further, we assume that LO can never be zero. A minimum of 20% of attack probability is assumed even for threat actors who have never attacked an organisation from a specific region or industry. This assumption is based on the consideration that attackers are opportunists [27]. The remaining 80% is determined based on the industry and region of interest for a specific threat actor. For example, if an organisation is operating from a region of interest to the threat actor then we assume that $RI = 0.4$. Thus, we express $RO = II + RI + 0.2$

Next, we use attack graphs to identify all possible attack paths from initial access to the end goal. Ens goals are objectives with a direct impact on the business objectives and are identified according to the known intentions of the threat actor. The end goals are considered to be: i) Data exfiltration, ii) Data destruction, iii) Data manipulation, iv) Service destruction and v) Resource hijacking. Attack graphs are used to illustrate how threat actors escalate their tactics locally on a compromised system through *vertical escalation* and how they laterally move through the network to other systems through *horizontal escalation*. Each node in the attack graph represents a tactic achieved on a specific system, while inward arrows represent the opportunity for the used technique. The accumulative opportunity, which is the success probability of an attack path, is calculated on each node given that y represents the threat implementation variant. Table 2 presents the parameters used in the model.

The following formulas are used on each node along every attack path from the initial access to the end goal. The path with the highest VO in achieving the end goal gain is selected as the critical attack path. The Ease of Exploitation (EoE) equals the opportunity of the variant that is used to achieve the end goal gained in the critical attack path.

$$G_y = \sum_{i}^{n} Ew_i \cdot Cw_i + 0.2 \tag{1}$$

$$PW_y = min(pw_i) \tag{2}$$

$$PG_y = min(pgi) \tag{3}$$

$$PV_y = min(P_y, PW_y, PG_y) \tag{4}$$

$$VO_y = PV_y \cdot G_y \tag{5}$$

$$EoE = max(VO_y) \tag{6}$$

3.3 Impact Assessment

Cyber-attacks, by definition, compromise IT systems by compromising either business processes dependent on these systems or the confidentiality, integrity and/or availability of data stored and shared on these systems, or both. The magnitude of impact is measured as a result of adding the impact of compromise for each business objective. We define four categories of impact for each business objective: (i) Compromise to Human Welfare (CHW); (ii) Image/Reputation Damage (IRD); (iii) Direct Financial Losses (DFL); and (iv) Legal Fines (LF). The Impact Average value (IAV) is calculated as the average of the impact to all four categories of business objectives.

$$IAV = (CHW + IRD + DFL + LF)/4 \tag{7}$$

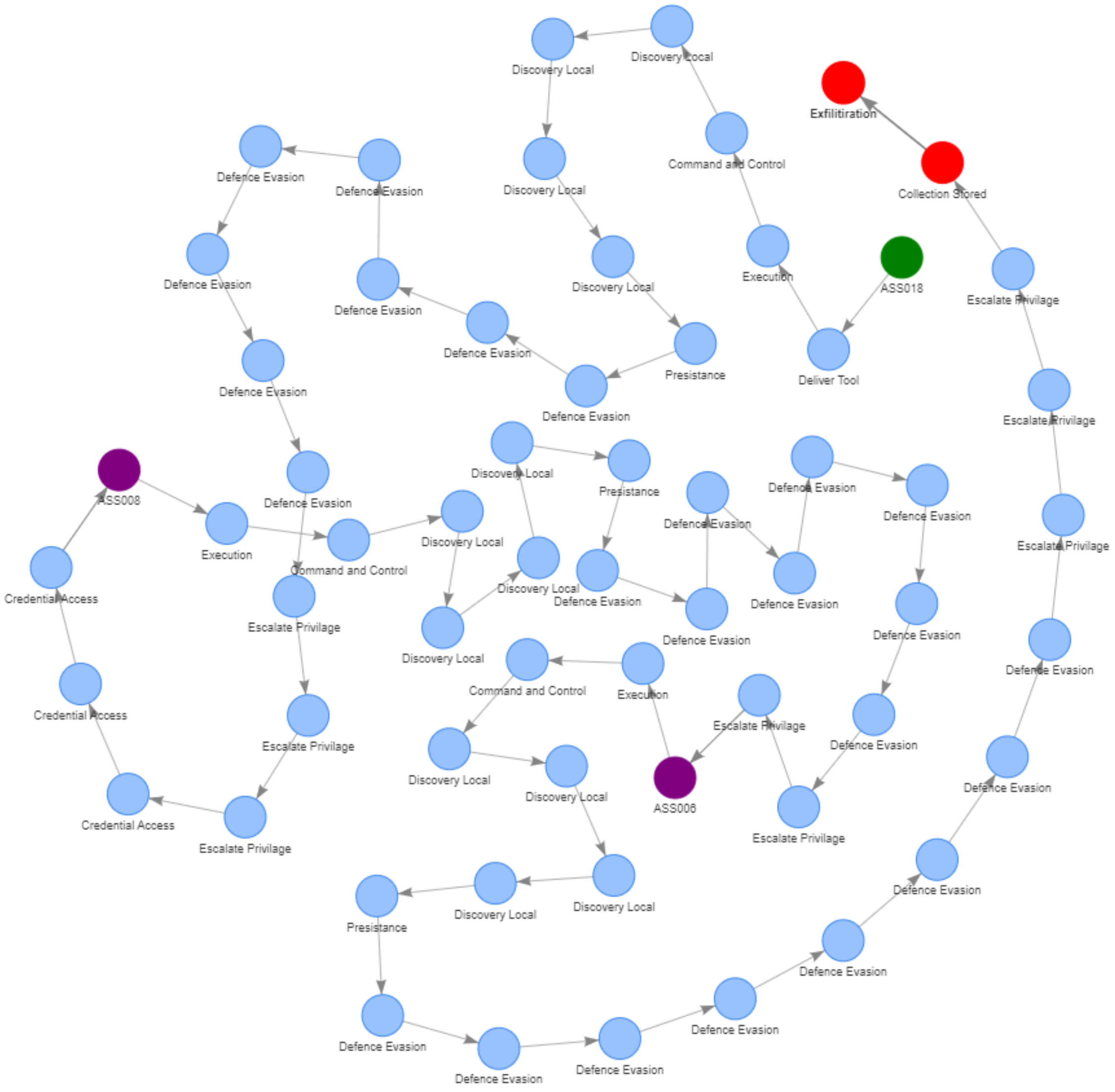

Figure 1: Critical attack route for Simulation-1

Next, the business processes are mapped to business objectives. A Process Critically Factor (PCF) is defined to express the criticality of a business process to each business objective. Similarly, data types are mapped to business objectives with a Confidentiality Factor (CF), Integrity Factor (IF) and Availability Factor (AF). To represent the dependency level of each business objective on the confidentiality, integrity and availability of each data type. According to the specified end goal, the Impact of Compromise (IoC) is determined as:

$$IoC = \kappa \cdot IAV \tag{8}$$

where $\kappa \in \{PCF, CF, IF, AF\}$. The Magnitude of Impact (MoI) of all business objectives on the organisation is the average of IoC.

$$MoI = \sum IoC/4 \tag{9}$$

The overall risk from an adversary group (Ai) on a target j can be expressed as:

$$Risk_{Aij} = LO_{ij} \cdot MoL_{ij} \cdot EoE_{ij} \tag{10}$$

4 SIMULATIONS AND RESULTS

In this section, we validate our model using a case study of a healthcare organisation operating in the United Kingdom and two adversary groups (from the MITRE ATT&CK framework) targeting the organisation. Figure 5 (in the appendix) presents a network topology sample detailing the critical assets and their connectivity. We define two scenarios, each with a different security level for the healthcare organisation. This is done by assuming that a subset of the mitigation controls is implemented within the organisation. Based on the percentage of controls implemented, we define two scenarios: (i) Scenario-1: 30 to 40 per cent of recommended

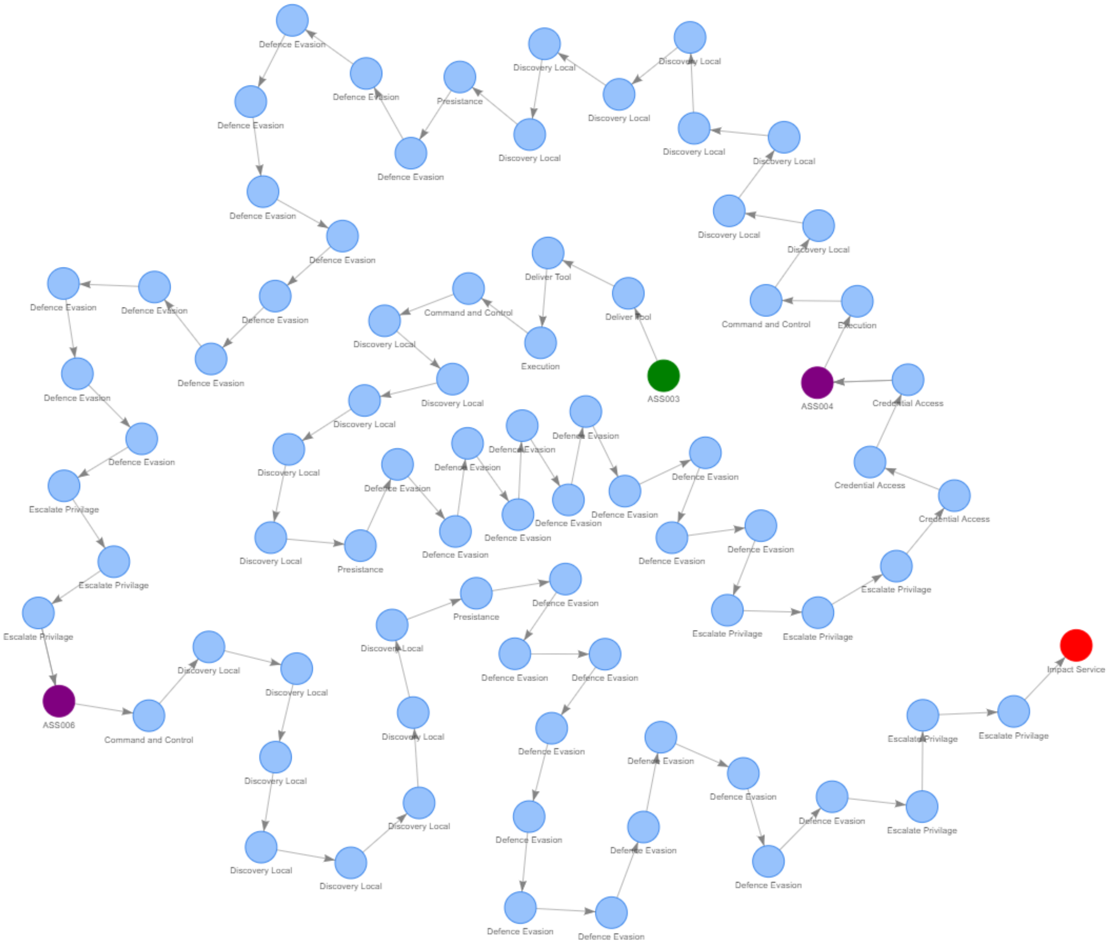

Figure 2: Critical attack route for Simulation-2

controls are implemented; and (ii) Scenario-2: 70 to 80 per cent of recommended controls are implemented. For each scenario, a set of simulations were performed to determine the risk exposure against the adversary group, Lazarus (G0032) and menuPass (G0040). The Lazarus group with 68 identified attack techniques has shown interest in organisations in the UK but has not particularly targeted the healthcare sector. On the other hand, the menuPass group with 39 identified attack techniques has targeted the healthcare sector in the UK.

Medical care services (PR0002) and Medical records (DT0001) being the most valuable assets of healthcare, we consider them as the target in our simulations. Table 4 (in Appendix) presents the list of artefacts and associated codes used in this paper. Table 1 highlights the choices for the simulations. The results show that the highest risk of 58% was accounted for in the menuPass group in Simulation-1. Although the Lazarus group uses almost double the techniques that menuPass uses, they present a lower risk of 44% for the same scenario. The menuPass group achieved exfiltration of the medical records with ease of exploitation $EoE = 72\%$ and a likelihood of occurrence $LO = 100\%$ as they operate in the same region and industry as the target organisation. On the other hand, the Lazarus group can disrupt the services with $EoE = 90\%$ but since their industries of interest do not include healthcare, there is a reduced LO of 60%. The magnitude of impact (MoI) for exfiltrating medical records and interrupting medical care services is 81% and 80% against each adversary group, respectively.

In Scenario-2, the risk levels were lower than those in Scenario-1. The risk was 28% and 39% from the menuPass group and Lazarus group, respectively. The EoE for menuPass dropped to half compared the Scenario-1, while EoE for Lazarus remained similar. These results reflect the difference in the implemented control level between the two scenarios, as well as emphasise the capabilities of the two adversary groups. This is evident from the significant drop in EoE obtained in Simulation-3 for menuPass when compared to Lazarus who experienced only a 10% drop-in EoE. The other reason for the drop in EoE is the level of sophistication required to achieve the goals. Data exfiltration requires access to the machine, as well as requires access to the target data, preparation of data and connection to an exfiltration destination (e.g., a C2 server).

Figures 1, 2 and 3 and 4 present the most critical attack route to the target for the defined simulations. The simulation also shows that in both scenarios both adversary groups achieved their goal

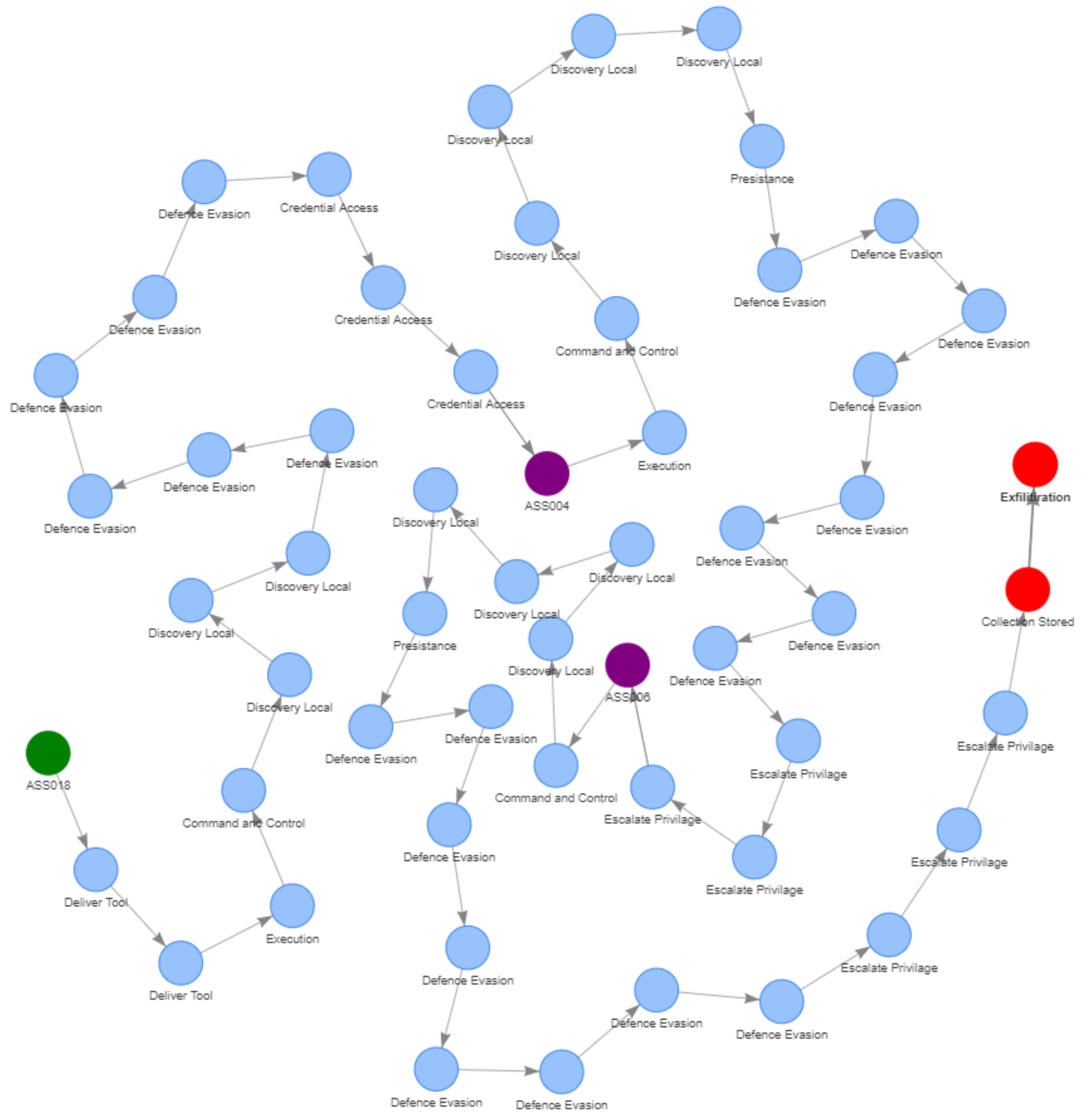

Figure 3: Critical attack route for Simulation-3

Simulation	Adversary Group	Attack Path	EoE	LO	MoI	Risk Level
Simulation-1	menuPass	ASS018⟶ASS008⟶ASS006	72.0%	100%	80.0%	58%
Simulation-2	Lazarus	ASS003⟶ASS004⟶ASS006	90.0%	60.0%	81.0%	44%
Simulation-3	menuPass	ASS018⟶ASS004⟶ASS006	35.0%	100%	80.0%	28%
Simulation-4	Lazarus	ASS003⟶ASS012⟶ASS006	80.0%	60.0%	81.0%	39%

Table 3: Simulation results

by exploiting the medical care database server which stores the medical records and is critical for the medical care business process. Despite the initial access node, both adversary groups collected the IT Administrator account from the intermediate nodes ASS004, ASS008 and ASS012 as in both scenarios these servers cache the IT administrator account which allows remote access to all systems in the network. The account can be used to move laterally to ASS006 (the medical database server) and from there both adversary groups can dump the local admin credentials allowing them full access to the stored data.

The above-mentioned simulation shows that the percentage of controls implemented does not influence the level of risk a threat actor can pose to an organisation. Although the risk decreased in the second scenario compared to that in the first scenario, the

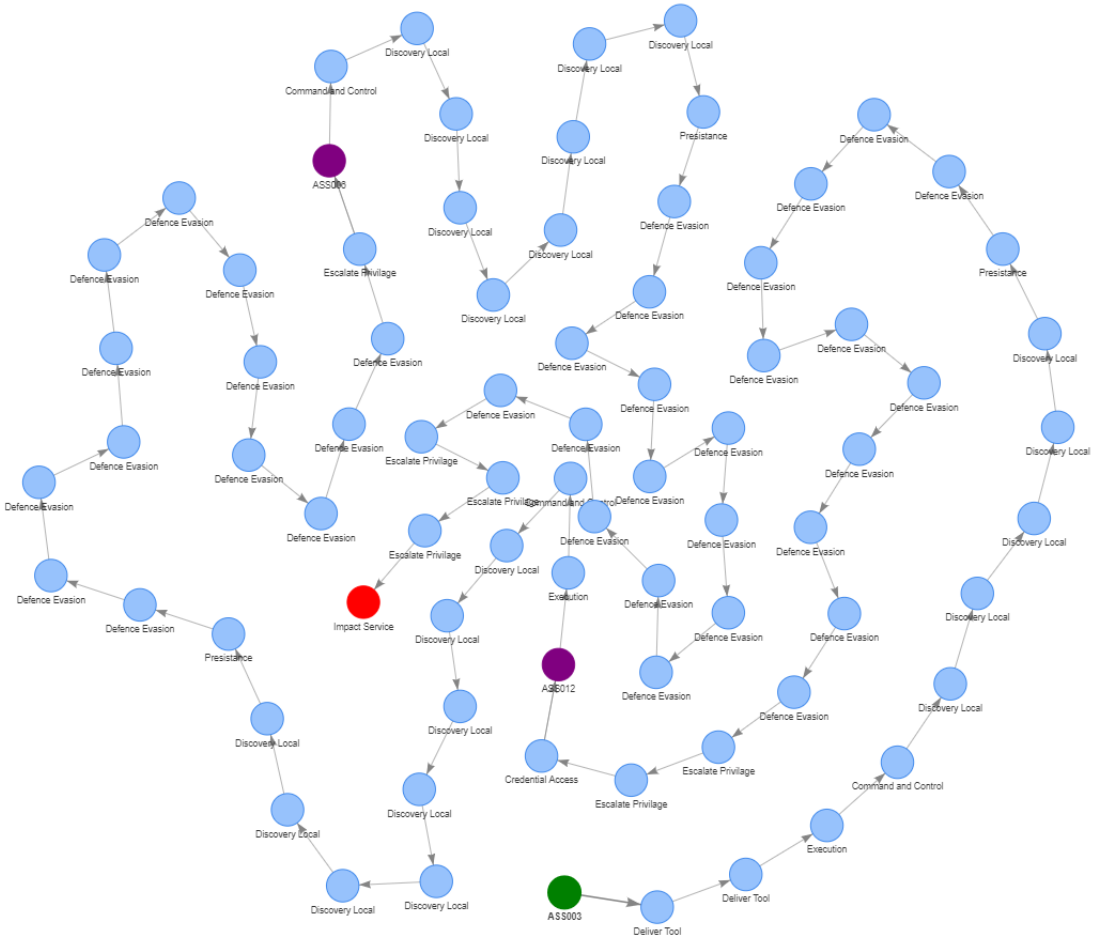

Figure 4: Critical attack route for Simulation-4

change in risk is not proportionate to the percentage of controls in each scenario. The reason being different assets might have a different level of impact on the organisation and different threat actors might have different levels of interest in the organisation. Furthermore, the level of ease of exploitation, the sophistication level and the capabilities of the threat actor define the possible opportunity level and the attack success rate.

5 CONCLUSION

In this paper, we presented a hybrid cyber risk assessment methodology that utilises concepts from the available risk assessment approaches. The proposed methodology leveraged the threat actor characteristics from the MITRE ATT&CK knowledge base together with attack graphs to support informed risk characterisation and assessment. First, we identified business-critical objectives and threats that might affect them. We next identified specific threat metrics and environmental parameters to model the threat and assess the impact. We simulated various threat scenarios for a hypothetical healthcare organisation in the UK and identified the most probable attack path, level of risk, ease of exploitation and the magnitude of impact posed by an adversary group. This study highlighted that by considering threat information in the risk assessment process, organisations can better assess their risks leading to decisive cyber security strategies.

This work is our first step towards designing a comprehensive and robust cyber risk assessment framework that not only considers risk management concepts but also cyber threat information. Given the scope and applicability of this work, there are numerous directions that which this research could be extended. For us, the most significant contribution would be to integrate organisation-specific threat information (collected through honeypots [4, 29]) and how this assessment would support better cyber risk management through self-protection (implementing controls) and cyber insurance.

ACKNOWLEDGMENTS

This research has been funded by the European Commission (Horizon 2020 Programme), and particularly by the projects SECONDO (Grant Agreement no. 823997) and CyberSec4Europe (Grant Agreement no. 830929).

REFERENCES

[1] M Ugur Aksu, M Hadi Dilek, E İslam Tatlı, Kemal Bicakci, H Ibrahim Dirik, M Umut Demirezen, and Tayfun Aykır. 2017. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–8.

[2] Alfian Alwi and Khairul Akram Zainol Ariffin. 2018. Information Security Risk Assessment for the Malaysian Aeronautical Information Management System. In *2018 Cyber Resilience Conference (CRC)*. IEEE, 1–4.

[3] Lotfi ben Othmane, Harold Weffers, and Martijn Klabbers. 2013. Using attacker capabilities and motivations in estimating security risk. In *Workshop on risk perception in it security and privacy, Newcastle, UK*.

[4] Nadia Boumkheld, Sakshyam Panda, Stefan Rass, and Emmanouil Panaousis. 2019. Honeypot type selection games for smart grid networks. In *International Conference on Decision and Game Theory for Security*. Springer, 85–96.

[5] Aristeidis Farao, Sakshyam Panda, Sofia Anna Menesidou, Entso Veliou, et al. 2020. SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In *International Conference on Trust and Privacy in Digital Business*. Springer, 65–74.

[6] Aristeidis Farao, Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. 2021. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. *Sensors* 21, 8 (2021), 2686.

[7] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. 2016. Decision support approaches for cyber security investment. *Decision support systems* 86 (2016), 13–23.

[8] Pedro Tubío Figueira, Cristina López Bravo, and José Luis Rivas López. 2020. Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security* 88 (2020), 101609.

[9] Gemini George and Sabu M Thampi. 2019. Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive and Mobile Computing* 59 (2019), 101068.

[10] Anna P Golushko and Vadim G Zhukov. 2020. Application of Advanced Persistent Threat ActorsTechniques aor Evaluating Defensive Countermeasures. In *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 312–317.

[11] GOV.UK Department of Digital, Culture, Media and Sport. 2020. Cyber security breaches survey 2020. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020. Accessed: 12-01-2022.

[12] Sami Haji, Qing Tan, and Rebeca Soler Costa. 2019. A hybrid model for information security risk assessment. *Int. j. adv. trends comput. sci. eng.* ART-2019-111611 (2019).

[13] Charles T Harry and Nancy Gallagher. 2019. *An Effects-Centric Approach to Assessing Cybersecurity Risk*. JSTOR.

[14] Hiscox. 2021. Hiscox cyber readiness report 2021. https://www.hiscox.co.uk/cyberreadiness. Accessed: 12-01-2022.

[15] Romuald Hoffmann, Jarosław Napiórkowski, Tomasz Protasowicki, and Jerzy Stanik. 2020. Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing* 44 (2020), 655–662.

[16] Ioannis Kalderemidis, Aristeidis Farao, Panagiotis Bountakas, Sakshyam Panda, and Christos Xenakis. 2022. GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In *The 17th International Conference on Availability, Reliability and Security*.

[17] Peter Katsumata, Judy Hemenway, and Wes Gavins. 2010. Cybersecurity risk management. In *2010-MILCOM 2010 Military Communications Conference*. IEEE, 890–895.

[18] Tobias Kiesling, Matias Krempel, Josef Niederl, and Jürgen Ziegler. 2016. A model-based approach for aviation cyber security risk assessment. In *2016 11th international conference on availability, reliability and security (ARES)*. IEEE, 517–525.

[19] H Kure and Shareeful Islam. 2019. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems* 4, 4 (2019), 332–340.

[20] Halima Kure and Shareeful Islam. 2019. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *JUCS-Journal of Universal Computer Science* 25 (2019), 1478.

[21] Charles Lim and Alex Suparman. 2012. Risk analysis and comparative study of the different cloud computing providers in Indonesia. In *2012 International Conference on Cloud Computing and Social Networking (ICCCSN)*. IEEE, 1–5.

[22] Richard P Lippmann and James F Riordan. 2016. Threat-based risk assessment for enterprise networks. *Lincoln Lab. J* 22, 1 (2016), 33–45.

[23] MITRE. [n.d.]. MITRE ATT&CK. https://attack.mitre.org/. Accessed: 14-07-2021.

[24] Antonio Muñoz, Aristeidis Farao, Jordy Ryan Casas Correia, and Christos Xenakis. 2020. ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM). In *European Symposium on Research in Computer Security*. Springer, 147–165.

[25] Scott Musman, Mike Tanner, Aaron Temin, Evan Elsaesser, and Lewis Loren. 2011. Computing the impact of cyber attacks on complex missions. In *2011 IEEE International Systems Conference*. IEEE, 46–51.

[26] Sakshyam Panda, Aristeidis Farao, Emmanouil Panaousis, and Christos Xenakis. 2019. *Cyber-Insurance: Past, Present and Future*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1624-1

[27] S Panda, I Oliver, and S Holtmanns. 2018. Behavioural modelling of attackers choices. In *Asian Control Conference*. 119–126.

[28] Sakshyam Panda, Emmanouil Panaousis, George Loukas, and Christos Laoudias. 2020. Optimizing investments in cyber hygiene for protecting healthcare users. In *From Lambda Calculus to Cybersecurity Through Program Analysis*. Springer, 268–291.

[29] Sakshyam Panda, Stefan Rass, Sotiris Moschoyiannis, Kaitai Liang, George Loukas, and Emmanouil Panaousis. 2021. HoneyCar: A Framework to Configure Honeypot Vulnerabilities on the Internet of Vehicles. *arXiv preprint arXiv:2111.02364* (2021).

[30] Sakshyam Panda, Daniel W Woods, Aron Laszka, Andrew Fielder, and Emmanouil Panaousis. 2019. Post-incident audits on cyber insurance discounts. *Computers & Security* 87 (2019), 101593.

[31] Pietro Russo, Alberto Caponi, Marco Leuti, and Giuseppe Bianchi. 2019. A web platform for integrated vulnerability assessment and cyber risk management. *Information* 10, 7 (2019), 242.

[32] Alberto Sardi, Alessandro Rizzi, Enrico Sorano, and Anna Guerrieri. 2020. Cyber risk in health facilities: A systematic literature review. *Sustainability* 12, 17 (2020), 7002.

[33] Emma Scott, Sakshyam Panda, George Loukas, and Emmanouil Panaousis. 2022. Optimising User Security Recommendations for AI-powered Smart-homes. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE.

[34] Hermawan Setiawan, Fandi Aditya Putra, and Anggi Rifa Pradana. 2017. Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. In *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, 251–256.

[35] Zhanna Malekos Smith, Eugenia Lostri, and James A. Lewis. 2020. The hidden costs of cybercrime. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf. Accessed: 12-01-2022.

[36] George Suciu, Cristiana-Ioana Istrate, Alexandru Vulpe, Mari-Anais Sachian, Marius Vochin, Aristeidis Farao, and Christos Xenakis. 2019. Attribute-based access control for secure and resilient smart grids. In *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*. 67–73.

[37] Yose Supriyadi and Charla Wara Hardani. 2018. Information system risk scenario using COBIT 5 for Risk and NIST SP 800-30 Rev. 1 A case study. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*. IEEE, 287–291.

[38] Ashleigh Wiley, Agata McCormac, and Dragana Calic. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security* 88 (2020), 101640.

A APPENDIX

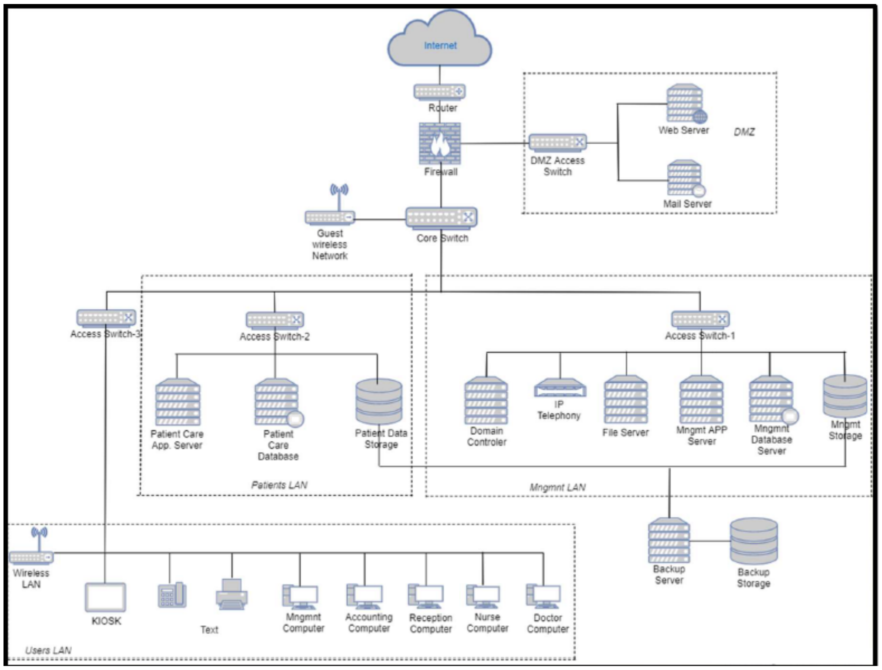

Figure 5: Sample network topology of the healthcare organisation.

Code	Business Processes	Code	Device Name	Type
PR0001	Management	ASS001	IDPS	IDPS
PR0002	Medical care	ASS002	Border Firewall	Firewall
PR0003	Nursing	ASS003	Web Server	Windows Server
PR0004	Patient flow	ASS004	Mail Server	Windows Server
PR0005	Admission	ASS005	Patient Care App Server	Windows Server
PR0006	Supply chain management	ASS006	Search and Development Server	Windows Server
PR0007	Search & Development	ASS007	Pharmacy Server	Windows Server
PR0008	Human Resources	ASS008	Domain Controller 1	Windows Server
PR0009	Pharmacy	ASS009	Domain Controller 2	Windows Server
PR0010	Finance	ASS010	File Server	Windows Server
PR0011	Marketing	ASS011	Backup Server	Windows Server
	Business Objective	ASS012	Management App Server	Windows Server
OB0001	Patient safety	ASS013	Management Database	Windows Server
OB0002	Customer service	ASS014	Management Computer	Windows Server
OB0003	Regulatory compliance	ASS015	Management Computer	Windows PC
OB0004	Continuous improvement	ASS016	Accounting Computer	Windows PC
	Data Type	ASS017	Nurse Computer	Windows PC
DT0001	Medical records	ASS018	Reception Computer	Windows PC
DT0002	PII-patients	ASS019	Doctor Computer	Windows PC
DT0003	Management data	ASS020	IT Administrator Computer	Windows PC
DT0004	R&D data	ASS021	Procurement Computer	Windows PC
DT0005	HR data	ASS022	Marketing Computer	Windows PC
DT0006	Financial records	ASS023	Search and Development Computer	Windows PC
DT0007	Public information	ASS024	HR Computer	Windows PC

Table 4: Business processes, Business objectives, Data types and Assets for the usecase.