Risk Assessment for Malware Attacks in Small Businesses

Tabisa Ncubukezi
Information Technology Department, Faculty of Informatics and Design
Cape Peninsula University of Technology, Cape Town, South Africa

Ncubukezit@cput.ac.za

Abstract: The presence of severe malware attacks in business systems compromise devices, data, information, and network hygiene. The increased usage of cyberspace as a convenient tool exposed all organisations to various malware attacks. The malware attacks have become one of the most common threats in all sectors. These attacks often find their way into systems where poor or inadequate security measures are implemented and leaving institution's resources vulnerable, and compromised. Data used in this work was collected using purposive sampling from the selected small businesses that used cyberspace for business transactions. A questionnaire distributed to the participants was mounted on Google Forms. To analyse the collected data, this work performed the risk assessment of the malware attacks and used the risk management processes to determine the risk impact and risk probability. Risk management processes were used to analyse and interpret different risks associated with malware attacks and also ranked them from low, medium, and high. The work also revealed the different forms of common malware attacks, business assets affected, and main causes of malware attacks, risk value, risk likelihood and the risk impact. The extent of security measures implemented on different levels contributes to the overall state of the organisational resources. The study also shared the recommendations and accounted for the conclusion.

Keywords: Cybersecurity Risks, Cyber Threats, Malware Attacks, Risk Assessment, Risk Causes, Risk Probability, Risk Impact, Small Businesses

1. Introduction

The increased use of the network has equally increased the existence of the malware attacks. These attacks present malicious software that spreads on computer systems with the aim of corrupting and deleting stored information and files. At times, malware attacks result to sudden system crashes (Kumhar, Kewat, & Kumar, 2022). Mostly, networked and standalone computers can be affected by a range of malware attacks due to the unannounced destructive behaviour that usually alter and highjack computer operations (Kirwan & Power, 2012). There are quite a number of malware attacks ranging from viruses, Trojan, spyware, adware, and dialler (Singh, Singh, & Joseph, 2008). Collectively, the pervasive malware attacks intrude into the business systems to gain unauthorised access for the purpose of stealing, deleting, and corrupting data or devices (Shukla et al., 2022). Malware also installs new programs and disrupt business operations (Aslam et al., 2023, Ibrahim, 2022). Even though malware can mostly penetrate through the networked systems, sometimes it can also be internally generated through the stand alone device due to employee actions (Brewer, 2016; Yuan & Wu, 2021).

For example, ignorant activities and actions caused illiterate personnel on the systems can pose as an entry point for malware attacks. In addition, minimal enforcement of the cybersecurity rules and guidelines which included adherence to the rules influences the personnel decision making process (Ncubukezi, 2022). An uninformed decision-making by network users become a loophole in business sector (Fortuin, 2021). Poor adherence to cybersecurity policies and guidelines can lead network users or employees of the business organisation to access convenient websites with an intention to explore free available software from illegitimate sources (Ncubukezi & Mwansa, 2021). Sometimes, people download information from the website with beautiful user interface. This action can grant an opportunity for criminals to deploy their advanced strategies to gain unauthorised access into the business system with private and sensitive data (Ncubukezi, 2022).

Literature indicates that malware attacks have been the main strategy used to penetrate small businesses, leaving them highly vulnerable (Osborn, 2015). Malware attacks have increases due to the sudden Covid19 pandemic which caught many unprepared businesses. Thus, the small business sector has become the primary target for cybercriminals (Ncubukezi, 2021). The deployment of the malware attacks pose a risk within the small business sector. These risk range from dented business reputation, loss of customer trust, decreased revenues as well as delayed business growth (Ncubukezi, 2023).

This study performs risk assessment for malware attacks in the business space. To achieve this, the study:

- Determines the common malware attacks that small business sector experiences
- Use risk management processes to determine the risk impact and risk probability
- Performs qualitative and quantitative risk assessment to analyse and rank malware risks

The rest of this research paper is arranged as follows. Section 2 presents different malware attacks followed by and malware risks. Section 3 presents malware risk assessment, the results and lastly, the study concludes with the main highlights.

2. Malware Attacks

Malware attacks also known as the malicious attacks are a form of cyberattacks that penetrates the system through unauthorised access (Talukder & Talukder, 2020). The malware attacks usually freeze or lock the devices, or sometimes steal, delete information to disrupt the activities performed on the system (Ncubukezi, 2022). Most deadly cyber threats and attacks including malware attacks occurred during the Covid-19 global pandemic. With the increased use of the cyberspace, small businesses become vulnerable to the common malware threats ranging from viruses, Trojan horse, key loggers, spyware, rootkits, adware, worms, bots, ransomware and mobile malware (Ngo et al., 2020). Standalone computers and networked computers become the main agents and entry points for malware attacks (Brewer, 2016).

Malware attacks can gain unauthorised access through planned or unplanned actions. Within the small business sector, people use the external drives on standalone devices to share files and folders on the stand alone computers (Dearman & Pierce, 2008). On the contrary, employees carelessly access unknown websites on the networked systems or ignorantly click on links to download software while processing business transactions (Ncubukezi, 2022). Moreover, the disruptive pop up messages disturbs network users. Malware attacks have been a big problem in the small business sector. As a result, all the actions and activities performed on the unsecured business system yield to risks relating to loss, stealing and deletion of the information that could cost millions to recover. The following section presents risks associated with malware attacks.

2.1 Risks Associated with Malware Attacks

Among other institutions, the small business sector has become victims of the planned and unplanned actions of the network users (legitimate and cybercriminals) (Minnaar, 2014). For example, legitimate users usually use the different external hard drives that could potentially harm the entire business. These actions become insider generated. On the contrary, informed or uninformed users would access the network through unsecured network interfaces to accidentally install the infected installation package of the illegitimate program available on the site to trick uninformed users (Ncubukezi, 2023). Some users become the channel of the malware attacks owing to quick and easy access to the free and infected software packages on the Internet. The criminals on the network use and deploy malware on the business systems and devices (Millaire, Sathe & Thielen, 2015). The less skilled people who access less protected web pages become extremely dangerous for the business and are difficult to mitigate. As a result, ignorant users download and install software from unverified sources (Kobis, 2021). The risks of malware attacks affect the network level, systems and applications, personnel and related sensitive and private information. As results some organisations become victims of malware attacks that are linked to the ransomware. The attacks generally impact all institutions negatively, as their primary aim is to gain unauthorised access to valuable and sensitive information and systems to corrupt and damage the operations.

2.2 Impact of Malware Attacks

The global Covid19 era and beyond revealed a significant increase of cyber related risks and attacks which directly impacts the operations of the businesses. Moreover, the impact these severe and replicable attacks affect overall business continuity and client trust. Even though cybersecurity should be prioritised by all institutions, there are still organisations that do not pay much attention on the safety and security of information which exposes different levels of the businesses (Ncubukezi, 2023). This becomes an entry point for a range attacks, gaining unauthorised access to unsecured networked devices as well as standalone devices. Business resources become vulnerable to a diverse range of attacks including disruptive and persuasive malware attacks which results to major loss or theft of private and sensitive information (Bello & Maurushat, 2020). In addition, malware results in data leakage (Alexei & Alexei, 2021). At times, the attackers would be after corruption or deletion of data as well as the identity theft (Chopra, Marwaha, & Sharma, 2022).

Some services get interrupted as results of the denial of service leading to freezing of certain business divisions. The unexpected restriction negatively impacts the small business sectors as they also lose their reputation due to the delayed delivery of services. Less secured businesses become victims of the malware attacks due to minimal on no training offered to the system users or the authorised third parties that equally have access to the system (Sharif et al., 2016). In such cases, proper awareness education and training becomes crucial. The

awareness training as a strategy improves privacy and safety of all the elements of the business. When system users are well oriented, the practice gets implemented smoothly to minimise and reduce all malware risks. This practice improves the lifespan of all the business departments, systems and resources.

The amount of cybersecurity risks associated with diverse malware attacks requires some assessment. It is therefore necessary to perform qualitative and quantitative malware risk assessment for the small business sector. The application of the malware risk assessment is presented below.

3. Research Method

The rise on the usage of the networked environments has increased several attacks in different institutions and organisations, including malware attacks. This work performed the risk assessment for malware attacks in small businesses. This section presents the research method used to carry out the study.

Sampling and participant selection criteria: To achieve the main aim, this research used purposive sampling to collected data from the sample of fifteen (15) small businesses. These businesses use cyberspace for their business operations and daily business activities. The study selected businesses generate annual turnover of less than three hundred thousand R300 000 per annum.

Data collection: Businesses were contacted via emails and those that responded were sent a link of the qualitative questionnaire mounted in Google Forms to collect data.

Application of risk assessment: The collected data was then analysed using the risk assessment approach. This work performed the qualitative and quantitative risk assessment of the malware attacks. The risk assessment process is used to identify the major hazards of the collected risks to determine the likelihood and the impact of the malware risk. The selected approach is explained and applied on section 3.2.

Ethical considerations: This work followed the university ethical clearance process to protect the research participants and the researcher. This process demonstrates that the researcher adhered to the ethical standards.

3.1 Determination of Malware Risks

A total of ten (10) malware risks were identified as shown on table 1. The common types of malware attacks experienced by the small business sector ranges from viruses, worms, bot, mobile malware, ransomware, adware, rootkits, key loggers, rootkits and Trojan horse. These attacks are shown on Figure 1. The attacks pose a risk to the business sector and the risks can be categorised according to their impact.

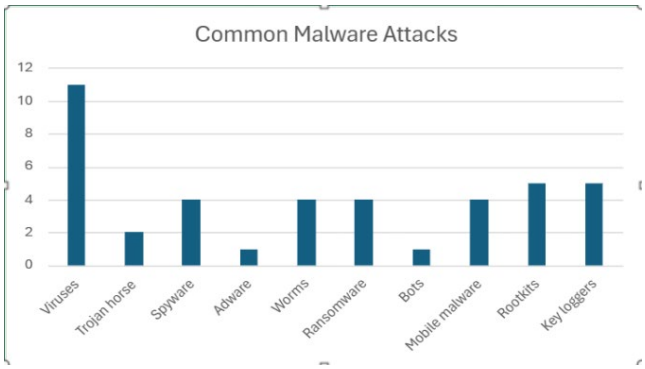

Figure 1: Common Malware attacks

3.2 Application of Risk Assessment

The study performed the malware risk identification by classifying the common malware risks in order to identify the source of the risk. Each risk is allocated a unique reference and a risk code used for the risk matrix and which gets stored on the risk registry (Nasir, Naderi & Momeni, 2020). Identifying malware risks promotes understanding of the nature of the possible risks yielding either a positive or negative impact. This process assists to determine potential risks and is performed before conducting a qualitative and quantitative risk assessment to develop the risk register to analyse, prioritise and monitor risks. Table 1 shows the risk number, risk, given risk code and the corresponding risk cause. Table 1 shows the ranking of the malware related experiences.

Table 1: Ranking of the malware risks

Risk #	Risk	Risk code	Cause
1	Outdated antivirus and antispyware	OAnti	Easiest gateway for cybercriminals, loss of data caused by software failures and no software compatibility
2	Unauthorised access to software	UAccSof	Poor guideline compliance, malware, criminals, employee ignorance
3	Use of USB	UUSB	Criminals, inside attempts, lack of guidelines
4	Viruses, worms, and Trojan	Mal	Malfunctioning of the network, data loss, financial loss
5	Accidental installation of unsecured applications	AccInst	Phishing, malware
6	Denial of service and network downtime	DoS	Prolonged network performance when opening files or accessing websites, unavailable websites, or unable to access any website.
7	Hardware and software failure	HSwaFai	Old hardware equipment and obsolete software, phishing
8	Stolen typed information	Klg	Recording of typed information
9	Disrupted services	Wrm	Spreading of the malware on the network
10	Excess operations	Bt	Repetitive automated services

3.3 Malware Risk Assessment

To determine the risk matrix, this work employed the qualitative and quantitative risk techniques to describe the likelihood of malware attacks and their impact in small businesses. The qualitative risk assessment of the malware attacks uses the risk probability and impact. The risk assessment is based on the basic measure that determines the risk probability and the consequence assessment using the following elements: scale, probability, time, cost and scope. The scale presents the risk rating for the risk probabilities, time of occurrence, amount caused by the risk and its impact. For example, if the likelihood of the risk occurrence is high, it is very high for every risk. Similarly, if the risk occurs more frequently, then the risk is also very high. So, every possibility of risk is assigned costs and the frequency at which the risk occurs to determine the rating of the risk impact. Table 3 presents the risk probability and impact assessment applied.

Table 2: Risk probability and impact assessment (Ncubukezi, 2023)

Scale	Probability	Time	Cost	Scope
Very high	>75%	>4 months	900K – 1M	Severe Impact
High	55-74%	1-3 months	500K-899K	Major impact on business functions
Medium	30-54%	2-4 weeks	300K-499K	Impact on the key business areas
Low	11-29%	1-2 weeks	100K-299K	Low impact on business operations
Very low	1-10%	6 days	0K-99K	Minor impact on business operations

After developing a common measure for risk probability and impact assessment, the following section unpacks the use of the risk impact technique as applied on malware risks.

3.4 Use of the Risk Impact Technique

The impact analysis is essential to produce a recovery plan focusing on identifying the potential cyberrisks and their probability of occurrence. The impact analysis describes a particular cyberrisk cause, threat occurrence and severity of the impact on the business system, providing information on how each cyberrisk can be treated (Radanliev et al., 2018). In the business system, a cyberattack can temporarily interrupt the business service, resulting in a single point of failure or an entire business system failure. Thus, estimating the impact of potential cyber threats on assets is essential.

Table 4 shows the impact values, the impact ratings, their description and the related cost. The impact values range from 0.1 for a negligible rating to 1.0 for a high rating. The impact ratings range from 1 for a minor impact to 5 for a high impact. The ratings determine the impact of the risks according to their severity. The lower the impact value, the safer the business and the higher the impact value, the more it can become dangerous to the business. Each impact rating has a descriptive statement that explains the consequence and the related cost of the impact to the budget.

Table 3: Definitions of impact values

Impact value	Impact rating	Rating	Description	Cost
0.1	Negligible	1	Threats have no harm	Does not affect budget
0.3	Minor	2	Threats are acceptable	< 15% more on budget
0.5	Moderate	3	Threats exist which can expose the business to risks	16-25% more on the budget
0.7	Major	4	The threat exists and needs remedial actions	26-35% more on the budget
1.0	Severe	5	Urgent threat to the organisation exists	>36% more on the budget

The following section clarifies the risk likelihood values in order to evaluate the probability and impact analysis.

3.5 Probability Estimation Technique

When conducting the probability and impact analysis, the risk likelihood values are essential for presenting the cyber risk matrix. The probability of the risks is presented concerning the risk likelihood rating, with the quantitative likelihood rating values and their description. Table 5 shows the risk likelihood ranging from rare, unlikely to happen, moderate likelihood of occurring and certain to happen. All these qualitative likelihood values are assigned the quantitative values, which are the ratings from 1 to 5 and the likelihood score from 3% to 100%. In addition, the table also shows the description of the likelihood rating and its criteria concerning the negative effect on the business system, which exposes the systems, information, assets and personnel. Therefore, the description shows the level of vulnerability of the business.

Table 4: Risk probability values (Ncubukezi, 2023)

Qualitative values	Quantitative values		Description and the criteria
Likelihood	Rating	Score	
Rare	1	3%	Vulnerability is not a concern.
			Security controls are implemented
Unlikely to happen	2	4-20%	Vulnerability could have **limited effects** on the business
			The effectiveness of the measures could be improved
Moderate chance	3	21-50%	Vulnerability might cause **minor financial loss**
			Relevant security controls are partially implemented but somewhat effective.
Likely to happen	4	51-79%	Vulnerability could severely affect the business system's operation
			Relevant security controls are planned but not effectively implemented
Certain to happen	5	80-100%	Vulnerability is exploitable, resulting in **multiple effects** on the business system
			No security measure could be identified.

After clearly describing the risk impact and likelihood, the researcher conducted the risk probability and impact analysis.

3.6 Risk Consequence and Scoring

Table 6 shows the qualitative values, quantitative values and the risk consequence. The qualitative risk likelihood values are rare, unlikely to happen, moderate chance of occurring, more than likely to happen to certain to happen. The quantitative values have the risk rating and the score. The rating is between 1 and 5 and the corresponding risk score is from 3% to 100%. The risk consequence has values from 1 to 5, where its values carry a risk description which is negligible, minor, moderate, major and severe.

Table 5: Risk likelihood, rating, score and the risk consequences

Qualitative values	Quantitative values		Risk consequence	
Likelihood	**Rating**	**Score**	**Value**	**Description**
Rare	1	3%	1	Negligible
Unlikely to happen	2	4-20%	2	Minor
Moderate	3	21-50%	3	Moderate
Likely to happen	4	51-79%	4	Major
Certain to happen	5	80-100%	5	Severe

Table 7 shows the risk scoring and the criteria used to calculate the final risk rating based on the risk consequence multiplied by the risk probability. When the output of the risk consequence and the probability amounts to a range of 1 to 5, the risk scoring becomes 1 and the final risk rating becomes minor. At the same time, if the risk consequence and probability falls into the 6 to 10 range, then the scoring is 2 and the final scoring becomes low. So, for every risk consequence multiplied by the probability, there is a corresponding risk score and final risk rating as shown in Table 7.

Table 6: Risk scoring (Ncubukezi, 2023)

Consequence*Probability	Risk scoring	Risk rating
1-5	1	Negligible
6-10	2	Minor
11-15	3	Moderate
16-20	4	Major

3.7 Malware Risk Values

Table 8 presents risks posed by malware attacks on the business system based on the risk probability and the risk impact as defined in Table 5 and Table 6 in order to calculate the final malware risk score. The criteria to determine the final risk score is defined in Table 7. According to the description, the lower risk consequence and likelihood presents lower risk scoring and lower risk rating. The higher consequence and likelihood range and the risk score pose a higher risk rating. These descriptions determine the urgency to address the risk.

Table 7: Malware risk probability, impact and value

Risk category	Risk item	Probability	Impact	Risk value	Risk score
Malware Risks	Unauthorised access	**3**	**4**	**12**	**Moderate**
	Stolen typed information	**4**	**4**	**16**	**Major**
	Disrupted services	**4**	**4**	**16**	**Major**
	Excess operations	**4**	**4**	**16**	**Major**
	Outdated antivirus and antispyware	**4**	**3**	**12**	**Moderate**

Risk category	Risk item	Probability	Impact	Risk value	Risk score
	Malware (viruses, worms, Trojan)	4	4	16	Major
	Accidental installation of unsecured applications	4	4	16	Major
	Denial of service and network downtime	3	3	9	Minor
	Hardware and software failure	2	2	4	Negligible
	Use of USB	4	3	12	Moderate

The following section presents the summary of the malware attacks

3.8 Summary of the Malware Attacks

This study highlighted various malware attacks, affected business assets, risk cause, risk impact and the risk likelihood that different business sectors experience. As presented and shown on Table 9, there are different forms of malware yield to various risks. These attacks affect different assets of the business system such as the network, devices, websites, emails, systems and the range of application used for daily business operations. Malware attacks pose a danger to business assets (people and resources), and its operations.

Table 8: Description of collected cyber risks

	Malware	Affected Asset	Risk cause	Risk likelihood	Risk impact
Malware Attacks	• Viruses • Trojan horse • Spyware • Adware • Worms • Ransomware • Bots • Mobile malware • Rootkits • Key loggers	• Network • Networked or standalone devices • Websites • Emails • Systems • Applications	• Human errors • Unsecured networked systems • Lack of cybersecurity policies, rules, procedures and guidelines • Poor enforcement and adherence of guidelines • Improper security architecture	• Malfunctioning of all device (servers, computers, systems, applications and other devices) • Unexpected system and network failure • Limited or no access to resources • Compromised system and information security, privacy and safety lead to data breaches	• Identity and private information theft. • Deletion, theft and corruption of data. • Denial of service • Fraud – freeze access until payment is made • Captures private information • Loss of reputation • Disruption of services and processes

Recommendations: Business institutions should prioritise the safety and security of their resources at large. The increased use of the cyberspace requires businesses to improve and maintain their security measures. Businesses should strengthen and equip their human resources in order to enforce the relevant rules, policies, guidelines and procedures when working on the business systems. This will promote the use of secure systems and improved interaction on the system. Highly secured systems bring trust to the clients.

4. Conclusion

This study presented the malware attacks and their risk likelihood and impact in businesses. The work showed that the malicious software harms the business systems in many ways. These include the locked devices without the user knowledge, unusable files, applications or other systems. When malware attacks gain unauthorised access into the systems, the software steals information, delete private or encrypted data as well as damage systems or devices on the network. In addition, the software deployed by cybercriminals disrupts and damage the business services, devices and systems. The criminals use different strategies to deploy the malicious software in the business network. At times, malware can be internally-generated.

The risks caused by the malicious software in businesses results to slow computers, unusual installed programs, and disruptive pop up messages, device or system failures, and interrupted operations. These actions result into loss, theft or deletion of private and sensitive data that would require remedial actions that costs money. In future, artificial intelligence can be used to simulate and predict the risk likelihood and the risk impact of the malware attacks in businesses. Different tools can also be used to analyse the attacks.

References

Alexei, L.A. and Alexei, A., 2021. Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, 10(3): 129–133.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), pp.1333.

Bello, A. and Maurushat, A., 2020. Technical and behavioural training and awareness solutions for mitigating ransomware attacks. In *Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science Online Conference 2020, (3) 9,* pp. 164-176. Springer International Publishing.

Brewer, R., 2016. Ransomware attacks: detection, prevention and cure. *Network security*, *2016*(9), pp.5-9.

Chopra, S., Marwaha, H. and Sharma, A., 2022, April. Cyber-Attacks Identification and Measures for Prevention. In *International Conference on Cybersecurity and Cybercrime*, 9, pp. 83-90.

Dearman, D. and Pierce, J.S., 2008, April. It's on my other computer! computing with multiple devices. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems,* pp. 767-776.

Fortuin, A., 2021. *The effects of mobile cloud accounting on the operations of small, medium and micro-enterprises in selected Cape Town markets* (Doctoral dissertation, Cape Peninsula University of Technology).

Ibrahim, H., 2022. A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), pp.50-68.

Kobis, P. 2021. Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions*, 1, pp. 61–76.

Kumhar, D., Kewat, A. and Kumar, A., 2022. Internet Security: Threats and Its Preventive Measures. In *Advances in VLSI, Communication, and Signal Processing: Select Proceedings of VCAS 2021*, pp. 753-766. Singapore: Springer Nature Singapore.

Millaire, P., Sathe, A. and Thielen, P. 2015. What All cyber criminals know: Small & midsize businesses with little or no cybersecurity are ideal targets. Available: https://www.chubb.com/my-en/articles/smes-with-little-or-no-cybersecurity-are-ideal-targets.aspx. [Accessed: 18th December 2023].

Minnaar, A., 2014. 'Crackers', cyberattacks and cybersecurity vulnerabilities: the difficulties in combatting the'new'cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*, *27*(sed-2), pp.127-144.

Nasir, A., Naderi, M.A. and Momeni, S.M. 2020. 'Risk management of information technology projects using Bayesian networks.' *Practical IT*, 1(5), pp. 01–10.

Ncubukezi, T. 2021. *An exploration of the malware impact on the end devices*. Conference Proceedings: CPUT Postgraduate Conference: pp.70.

Ncubukezi, T. and Mwansa, L., 2021. Best practices used by businesses to maintain good cyber hygiene during Covid19 pandemic. *Journal of Internet Technology and Secured Transactions*, *9*(1), pp. 714-721.

Ncubukezi, T., 2023. *Design development and evaluation of the cybersecurity risk tool: a case of small and medium-sized enterprises in South Africa* (Doctoral dissertation, Cape Peninsula University of Technology).

Ncubukezit, T., 2022, March. Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. In *International Conference on Cyber Warfare and Security*, 17(1), pp. 395-403.

Ngo, F.T., Agarwal, A., Govindu, R. and MacDonald, C., 2020. Malicious software threats. *The Palgrave handbook of international cybercrime and cyberdeviance*, pp.793-813.

Radanliev, P., De Roure, D.C., Nicolescu, R., Huth, M., Montalvo, R.M., Cannady, S. and Burnap, P., 2018. Future developments in cyber risk assessment for the internet of things. *Computers in industry*, *102*, pp.14-22.

Sharif, M., Bhagavatula, S., Bauer, L. and Reiter, M.K., 2016, October. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 acm sigsac conference on computer and communications security*, pp. 1528-1540.

Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.

Singh, A., Singh, B. and Joseph, H., 2008. Malware analysis. In *Vulnerability Analysis and Defense for the Internet* (pp. 169-211). Boston, MA: Springer US.

Talukder, S. and Talukder, Z., 2020. A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *12*.

Yuan, S. and Wu, X., 2021. Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, *104*, p.102221.