Determination of the end Device risk Likelihood Using the Bayesian Network Tools

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

Ncubukezit@cput.ac.za

Abstract: All institutions use end devices for information processing which includes sending and receiving on the network. This process helps them to improve their business production as well as perform daily activities at a faster rate. However, the increased usage of end devices by both employees and criminals raises concerns and exposes businesses to a range of cyber risks. End devices can sometimes be used as agents and weapons to expose internal business operations. The vulnerability of the end devices to cyber threats and attacks compromises business data, its safety, and security. This paper determines the risk likelihood of the end devices using the Bayesian network tools. To achieve this, the study illustrates the connections of the end device variables to simulate the risk likelihood and its impact. The analysis and interpretation of the simulation are performed using decision tree analysis (DTA), scenario analysis, and sensitivity analysis techniques (Tornado graphs, conditional probability tables (CPT), and value of information configuration (VOI)). The relationship of the variables is demonstrated on the AgenaRisk package. Results revealed variables that influence the risk probability and its impact. End device risks can be caused by insiders and cybercriminals. The risks associated with end devices are influenced by the level of security implementation on different levels. The impact of the cyber risks was also accounted for and the concluding remarks were also made.

Keywords: AgenaRisk, Bayesian Network, Cybersecurity, Decision Tree Analysis, End Devices, Risk Assessment, Risk Likelihood, Sensitivity Analysis

1. Introduction

For communication purposes, the network is made up of different levels which include devices. The devices can be positioned as the end nodes, interconnections, and peripherals that form part of the business systems. Devices connected to the Internet or acting as stand-alone may be the main entry points that victims use to commit cybercrimes. Cybercrimes can either be caused by intentional cybercriminals or ignorant employees (Ncubukezi, 2022a). All business institutions are operated by both computer-literate and illiterate employees and are sometimes referred to as insiders. Employees as insiders who are end users can be the weakest link causing risks to the organisation (Alohali, et al., 2018). With the increased demand to connect to cyberspace, most people and businesses use various end devices: smartphones, mobile devices, tablets, laptops, and computers (Imgraben, Engelbrecht, & Choo, 2014). Some organisations practice Bring Your Own Device (BYOD) as a policy that allows insiders to use their own devices such as external hard drives, laptops, and smartphones among others to access and exchange information (Ferdousi, 2022). The priviledge of employees using their own devices sometimes results in devices that get stolen, intruded upon, or information lost. Sometimes, employees perform certain activities on the Internet to attract criminals into the systems (McGuire & Dowling, 2013). Criminals are opportunists that are continually searching for the lucrative benefit and use any available and open interfaces on the network to gain unauthorised access (Ncubukezi, Mwansa, and Rocaries, 2020b).

End devices are one of the main resources that promote activities by both legitimate users and criminals in the business space (Ncubukezi, 2022b). The increased use of end devices introduces ways that compromise privacy, safety, and security in all organisations, requiring mitigation strategies and increased awareness (Mzileni & Ncubukezi, 2022). The literature shows that there is minimal understanding of users' safety practices on end devices in homes and business sectors (Tabassum, Kosinski & Lipford 2019). Employees ignorantly want to use their home devices at work, establish unsecured connections, pose a risk, and compromise computer and information security (Ncubukezi, 2022a).

Cyberattackers understand and pay close attention to the end devices as they become their primary targets for deploying malware attacks (Rusi & Lehto, 2017). Criminals steal information of good value and money by infiltrating end devices (Mosteanu, 2020). Likewise, these devices may not be connected to the business network but serve as standalone computers where employees share and exchange information. Regardless of the connection to the network, the end devices generally pose a risk because some end devices do not use proper security measures owing to the access of BYOD. In many different institutions, the culture of BYOD and lack of strong security on end devices can result in a range of cyber security risks such as highjacked unauthorized access

to the resources, loss, breach, and leakage of a data breach, regular phishing or malware attacks, poor handling of data (Bhadouria, A.S.; Ferdousi, 2022; Shukla et al., 2022).

Some end devices could experience power supply failure or a single point of failure where a device can crash or malfunction due to poor practice of device safety and regular protection of the devices (Ncubukezi, 2022b; Hong, 2017). Some could even display error messages that could freeze the device or automatically shut down owing to corrupt software or faulty hardware (Ncubukezi, Mwansa & Rocaries, 2020b). These risks related to the devices could cost the companies and requires the use of artificially intelligent systems to help organisations to make better security decisions and improve the security of the resources and data handling to reduce risks (Ncubukezi, Mwansa & Rocaries, 2020a).

After analyzing the relevant and available literature, this study determined the risk likelihood of the end devices using the Bayesian network tools. To achieve the main goal, the paper:

- Used scenario analysis and decision tree analysis to understand end device risks
- Illustrated and simulated end device risk likelihood and the impact using the Bayesian network
- Performed sensitivity analysis using Tornado graphs, conditional probability tables (CPT), and value of information configuration (VOI)

The rest of the paper is organized as follows: The method used to carry out the study is presented in the following section, followed by the sensitivity analysis results with discussions, and the conclusion of the study is accounted for.

1.1 Possible risks associated with end devices

End devices generally form part of the network infrastructure. These devices on the network can range from mobile devices, laptops, desktops, servers, phones, and printers and can be used for transmission for either the source or the destination. For data transmission, these devices get allocated a unique number that identifies them with a network address (Ncubukezi, Mwansa & Rocaries, 2020b). So, these devices can operate stand-alone or in a networked environment which exposes them to a wide range of risks. Table 1 shows the risk exposure of end devices, the form of attack, related security principles, the risk likelihood, and the risk impact. End devices are exposed to a variety of risks such as device loss, theft or robbery, damage due to third-party involvement, malware, denial of service or phishing as well as unauthorised access to both the facilities where resources are stored and the actual devices. These risks are initiated by employees or criminals in the form of actions performed by ignorant employees. At times, the insiders make poor decisions, computer illiterate on poorly configured devices due to a lack of policy enforcement and poor management (Ncubukezi, Mwansa & Rocaries, 2021). All these sources of device attacks challenge security principles such as confidentiality, integrity, and the availability of stored information on the devices (Mzileni & Ncubukezi, 2022).

According to Table 1, end devices are most likely to have software and hardware failure, misplacing old equipment, affected by constant network downtime, malware, phishing, or the denial of service as well as the negative activities performed by legitimate system users (Wheelus & Zhu, 2020). The impact of the end device risk probability affects the devices and information stored, organisations at large, and the current and potential clients (Ncubukezi, 2022b).

Table 1 which illustrates factors that contribute to the risk likelihood of the end devices is presented below.

Table 1: Risk of end devices (Ncubukezi, 2022b)

END DEVICES				
Risk exposure	**Form of attack**	**Related security principle**	**Risk likelihood**	**Risk Impact**
• Theft, loss or robbery • Third-party involvement • Network related (Malware attack or denial of service) • Unauthorised access to devices	• Human actions • Ignorance - poor decision-making • Lack of employee skills • No device encryption • Lack of device management	• Availability • Confidentiality • Integrity	• Hardware & software failure • Old equipment • Network downtime and denial of service Human factors • Network related events	• Poor production & business growth • Fraudulent acts • Lack of clients and their trust • Loss of intellectual property • Poor economic growth • Loss or stolen information and devices • Network related (denial of service, malware) • Delayed delivery of the services and economic growth • Hardware failure, slow or unusable device

1.2 Related works

There has been an increase in the use of information and communication technologies (ICT) for Internet and information processing which leaves institutions vulnerable to a diverse range of risks. The exposure of the different components of the business sectors to risks necessitates the determination of the risk likelihood using computers and other intelligent systems such as the Bayesian Network (BN). For example, a study conducted by Ncubukezi (2023) determined the risk probability of human-related actions within the business small sector to determine the risk probability. The study simulated the risk probability and impact based on the human factor variables (dependent and independent), and their relationships resulting in data leakage. On a cloud-based model, other authors used multilevel BN to assess the risk likelihood of gas transmission stations and present different flows (Gao et al., 2022). This study also used the BN to determine the risk likelihood on the end devices used for information exchange.

Even though institutions use IoT devices such as different gadgets, machines, sensors, and other hardware devices for information exchange, this study focuses on the end devices such as computers, printers, smartphones, and laptops. Devices can pose risks on different levels. For example, a more detailed scenario for IoT devices which is not part of the scope of this study is presented in the study conducted by Muñoz, Fernández-Gago, and López-Villa (2022). Their work described the risks and attacks on the protocol level. In addition, the use of hardware and software certifications of the end devices to improve security is also not part of the scope of the study but a study conducted by Munoz and Mafia (2014) has thoroughly presented and combined the model. These two studies complement this study in the sense that one work reveals the weaknesses of IoT devices at the protocol level and the other study proposes a certification solution using secure elements for establishing the pseudo-hardware certification system. This work uses different techniques with BN tools to determine the risk likelihood of the end devices.

The following section presents the method used to carry out the study.

2. Methodology

The Covid-19 global pandemic revealed an increase in cyber-attacks on all levels resulting in a range of risks within different business sectors. This study focuses on end device exploitation to determine the risk likelihood using the risk analysis methods and the Bayesian network. Risk analysis techniques such as scenario analysis and decision tree analysis (DTA) simulate the end device case and demonstrates the possibilities of the risk probability. They also provide an assessment of the likelihood that project decisions affect risk measures.

On the contrary, Bayesian Network tools are demonstrated using the AgenaRisk platform which illustrates the variables used and their relationships resulting in the risk likelihood and its impact. Sensitivity analysis was used to determine the risk probability of the end devices using the Tornado graphs, conditional probability tables (CPT), and value of information configuration (VOI). Sensitivity analysis is a quantitative technique that helps to determine variables that have a greater impact on risk (Cox, 2008). Variables estimate risks with potential impact and determine the changes in objectives and uncertainties that are correlated, along with the effect of each element on the objectives. It also communicates data and outcomes, understanding the link between the input and output variables while identifying sensitive variables (Wang & Neil, 2021; Khodakarami, & Abdi, 2014). It then helps to make assumptions that allow decision-making and examines the amount of risk in given scenarios. Only scenarios with the greatest risk are taken into account in the sensitivity analysis. The study also developed a different Bayesian model (BM) as part of the graphical probabilistic model that used the Bayesian inference analysis. The simulated model illustrates the risk likelihood and the risk impact of end devices. The use of these Bayesian network techniques determines the risk likelihood.

As cyber risks increased, they need a system with artificial intelligence capabilities that perform better than the human mind in predicting risks (Ncubukezi, Mwansa & Rocaries, 2020a). This work used the Bayesian Network as a model on the AgenaRisk package to predict the risk likelihood of the end devices. The BN helps to develop the probabilistic model by demonstrating and presenting different nodes with random variables to influence conditional probability for other dependent variables (Ramesh et al., 2003). BN in this study determines end device risk probability based on the prior indicators (networked or stand-alone), device protection levels, risk impact, and risk likelihood. The interface of the AgenaRisk package is shown in Figure 1 demonstrates different scenario cases of phishing attacks.

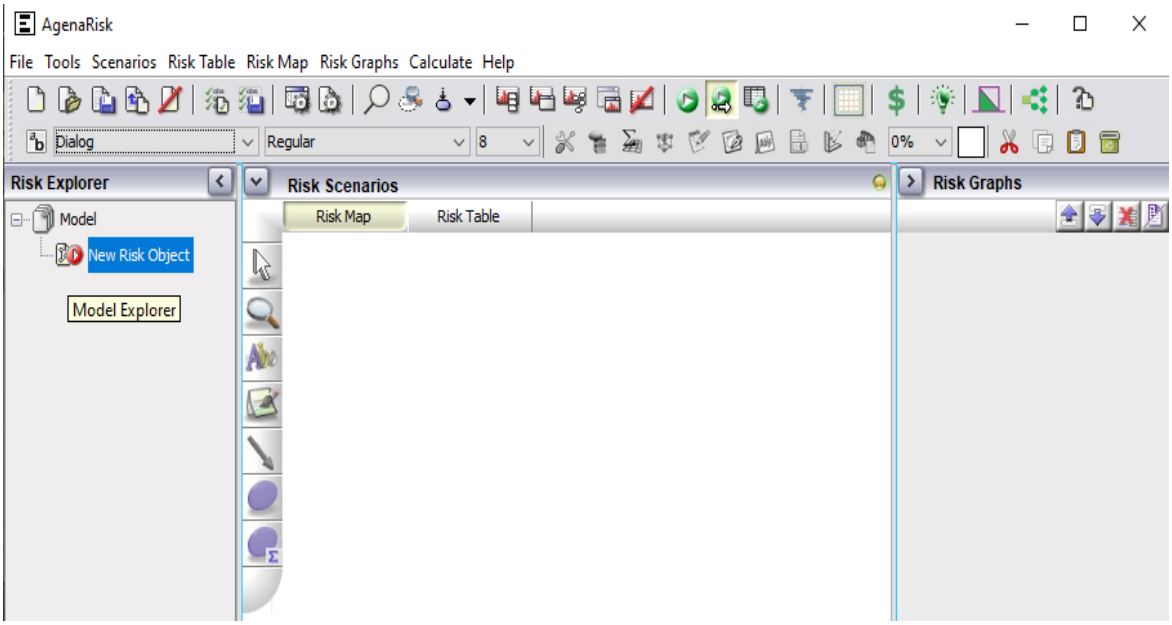

Figure 1: AgenaRisk interface

Ethical considerations: To conduct this work, the researcher received the ethical clearance that grants permission for the research to be conducted. The simulation of the end device scenario is presented below.

3. Simulation

This work presents the scenario of the end devices by using the decision tree analysis shown in Figure 2. The analysis describes how the end devices become vulnerable to risks. Two sources of risks experienced by the access level devices are mentioned.

3.1 Scenario and Decision Tree Analysis (DTA)

Devices are primarily used to penetrate and access business services. In the business sector, there are both networking devices (routers, switches, hubs), while the end devices can be smartphones, notebooks, laptops, and desktops. If these devices are connected to the network they become vulnerable to a range of cyber threats and attacks, which result in different risks to businesses (Ncubukezi, Mwansa and Rocaries, 2021). Figure 2 shows the cybercriminal and insider-related actions used to exploit the end devices. Within business institutions, the risk relating to the end devices can be caused by both the cyber criminals and insiders (employees) that take advantage. Cybercriminals as attackers gain unauthorised access to networked devices by using a piece of code to cause and trigger unintended behavior on the device. This process hijacks authorized users' actions by deploying a code that manipulates the device (Ncubukezi, 2022b).

With unsafe storage and handling of the end devices, cybercriminals also use opportunities to steal the devices and the information stored on the devices. On the other hand, criminals sometimes deploy software code to guess and steal passwords so that they may gain unauthorised access to business systems. These actions are performed by gaining unauthorised access through the network and result in poor and malfunctioning network performance in the form of denial of service or malware. Cybercriminals also hijack the network so that it may not be available and can further hijack user privileges (Ncubukezi, 2022a).

On the contrary, employees ignorantly perform activities that leave the business system vulnerable. Some employees could lose the device, which could land in the criminals' hands or they can be criminals by stealing the devices. Sometimes, the employees use unsecured memory sticks for information exchange. Those memory sticks could have malware that triggers device exploitation. In addition, using the Internet could result in device exploitation because employees could ignorantly download software from unknown sources. This scenario describes how the end devices can be exposed to risks. These activities are shown in Figure 2.

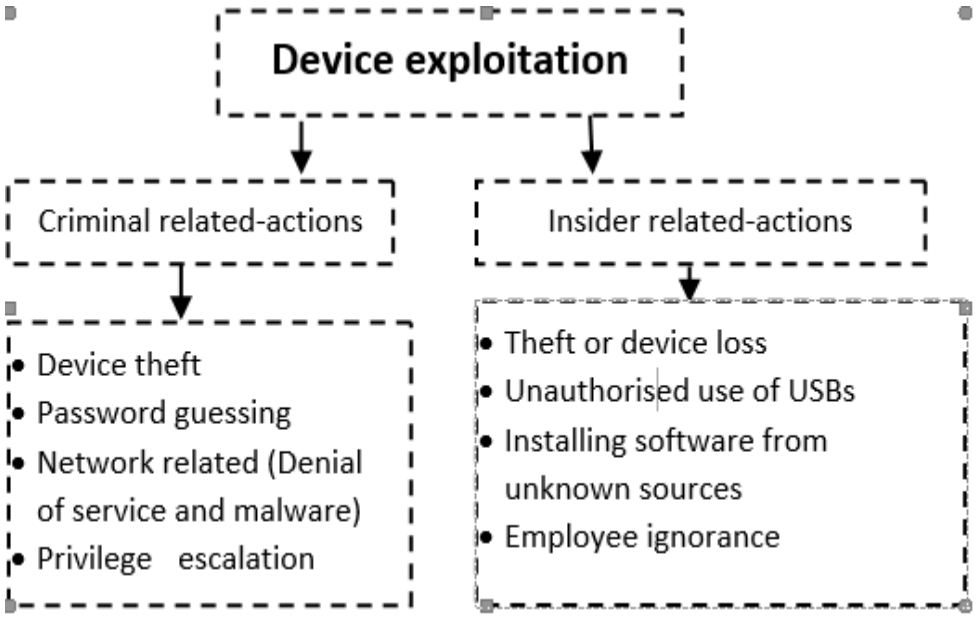

Figure 2: End Device exploitation

This study also used the Bayesian network tools with the AgenaRisk package to determine the potential cybersecurity risk probabilities and their impacts in the business space. BM is part of the graphical probabilistic models that use the Bayesian inference analysis (van de Schoot, et al., 2021). The BN analysis demonstrates the end devices' risk likelihood using sensitivity analysis techniques. The application of the BN is presented below.

3.2 Bayesian Network Model setting

The main variables of the end device scenarios are the prior indicators of the receiving end devices, the device protection level, and the posterior indicators, which influence the risk likelihood and impact. As used on the different models, the prior indicators are the end devices that could be either portable or fixed and connected to the network or act as standalone devices. The device's protection level is influenced by implementing security measures such as updated software (application and operating systems), device encryption, physical protection, and hardware security. In addition, complete device protection is also influenced by the nature of a device (networked or standalone). The level of device protection affects the posterior indicators to determine the risk likelihood as well as the impact. The higher the device protection, the lower the impact, even though the risk likelihood would be influenced by the device protection, portable or fixed device, which could be networked or standalone. This section demonstrates the sensitive analysis of the devices which result in different cyber risks. Sensitivity analysis challenges the reliability, difference, and significance of the assumptions to address the 'what if' analysis. In addition, sensitivity analysis is the quantitative technique for determining variables that have a greater impact on risk (Cox, 2008). Different end device scenarios are simulated and presented below.

3.3 End device risk likelihood simulation

The simulations of the end device scenario are based on different possible conditions. According to the figures, end-device simulations range from 1 to 7. The influencers of these scenarios are the state of an end device (fixed or portable), networked or stand-alone, and device protection level (software, device encryption, physical protection, and security of the hardware). These prior indicators influence and determines the risk likelihood and the risk impact of the device per scenario. These different scenarios are presented below.

Simulation 1: Figure 3 illustrates fixed and standalone devices with 84% high device-protection level based on 100% outdated software updates and 100% lack of hardware security. The device is in a secured physical environment with a 78% high level of encryption. Based on the overall device protection, this scenario had a medium-risk likelihood with 57% of the risk impact.

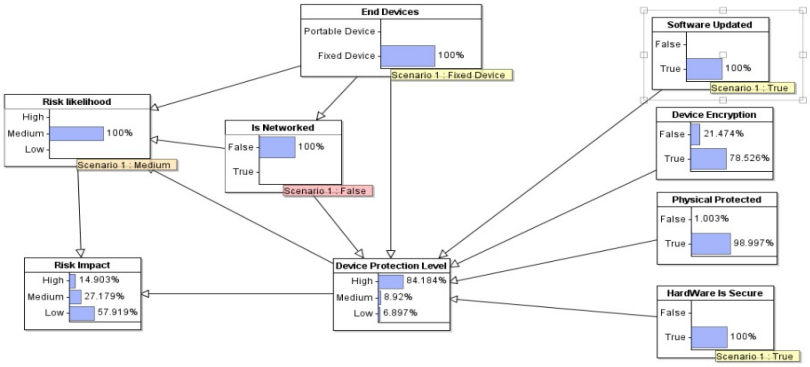

Figure 3: Fixed standalone end devices with high protection level

Simulation 2: Presents fixed standalone end devices with low hardware and software protection. Figure 4 illustrates networked fixed-end devices with a 41% low device-protection level. This scenario has no software updates, 80% high device encryption, 99% physical safety, and 100% hardware security. Inconsistent device protection influences medium risk likelihood and 36% medium risk impact.

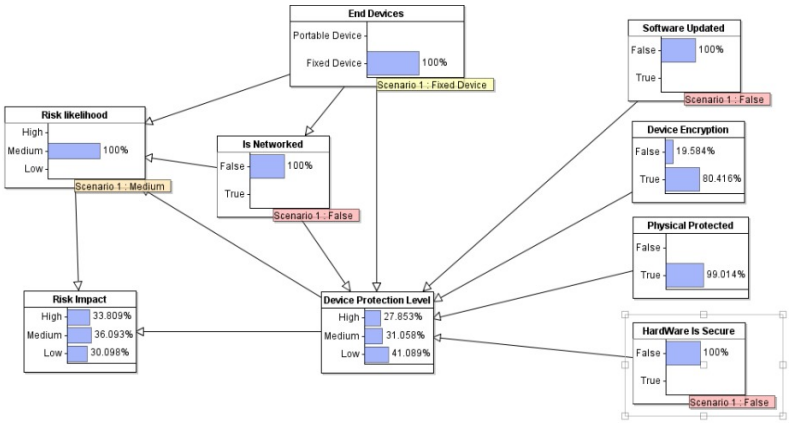

Figure 4: Fixed standalone end devices with low protection level

Simulation 3: Figure 5 presents portable networked end devices with high device protection levels owing to the physical space, hardware, and device encryption. The software becomes the only low influential factor for risk level. The range of the high mediating factors influences the device security's overall level, determining the risk likelihood and impact.

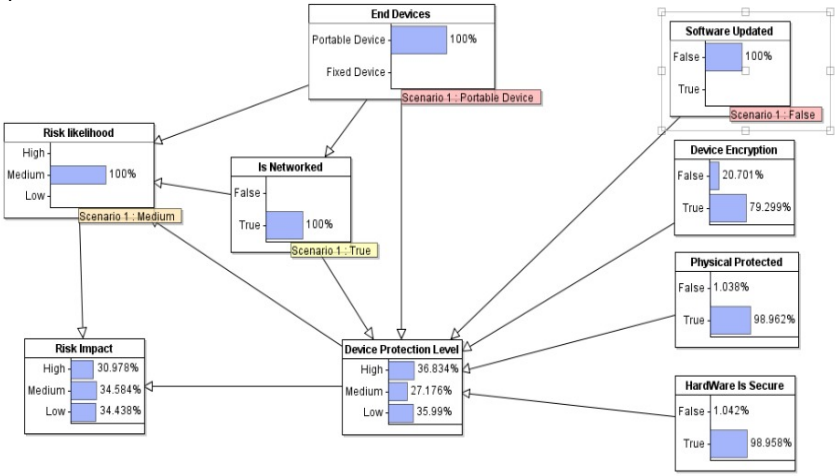

Figure 5: Portable networked end devices with high device protection

Simulation 4: On Figure 6 demonstrates a networked portable end device with a 57% low protection level owing to no hardware and software updates, 98% dominating physical protection, and 79% device encryption. The dominating 57% low device protection level has a medium-risk probability and 42% high-risk impact.

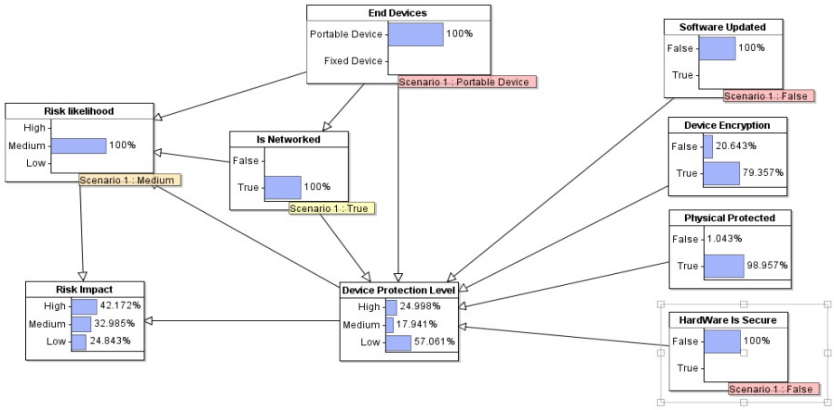

Figure 6: Portable networked end devices with low hardware and software security

Simulation 5: Figure 7 presents a networked portable end device scenario with medium-risk likelihood and 34% medium-risk impact. The 36% of device protection has influenced the results. In this scenario, the software is not regularly updated, only 79% of device encryption, 98% of physical safety of the buildings, and 98% of hardware security.

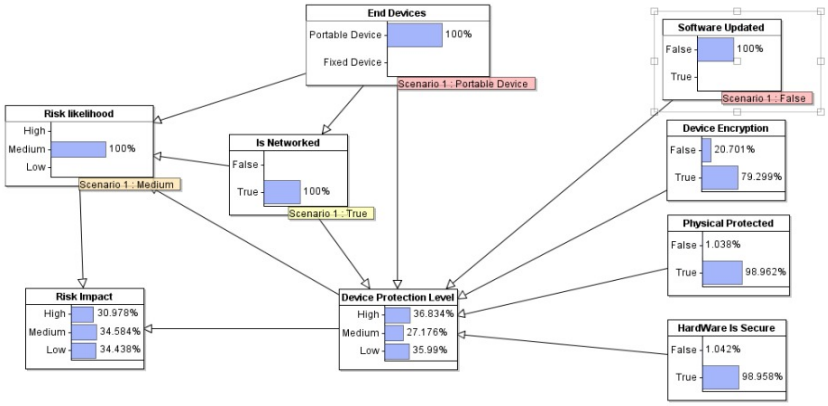

Figure 7: Portable networked end devices with low software protection

Simulation 6: Figure 8 shows the portable standalone end devices with an 84% protection level resulted in an 83% low-risk likelihood and a 75% low-risk impact. Safety measures are 99% software updates, 99% hardware, and 80% physical security, resulting in 84% device protection.

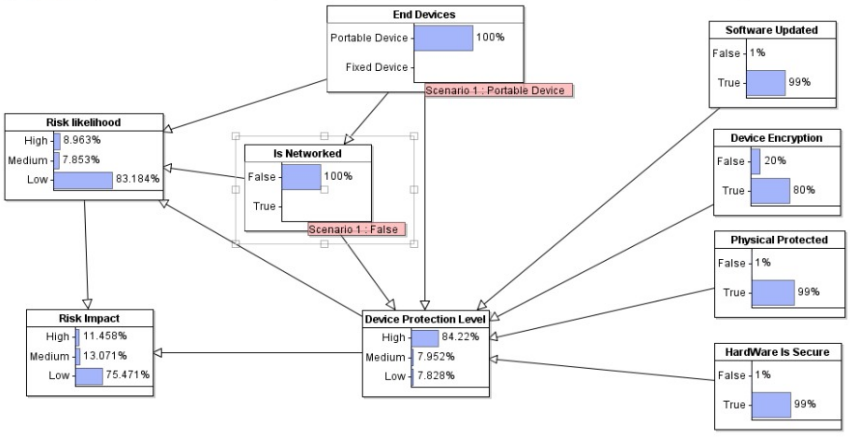

Figure 8: Portable standalone end devices with high device protection

Simulation 7: Figure 9 shows a 100% low device protection level due to 96% software updates, 22% device encryption, 98% physical protection, and 97% hardware protection. All the variables, in this case, contribute to the overall cyber risk likelihood and impact medium-risk likelihood results and 5% low-risk impact for a portable networked device.

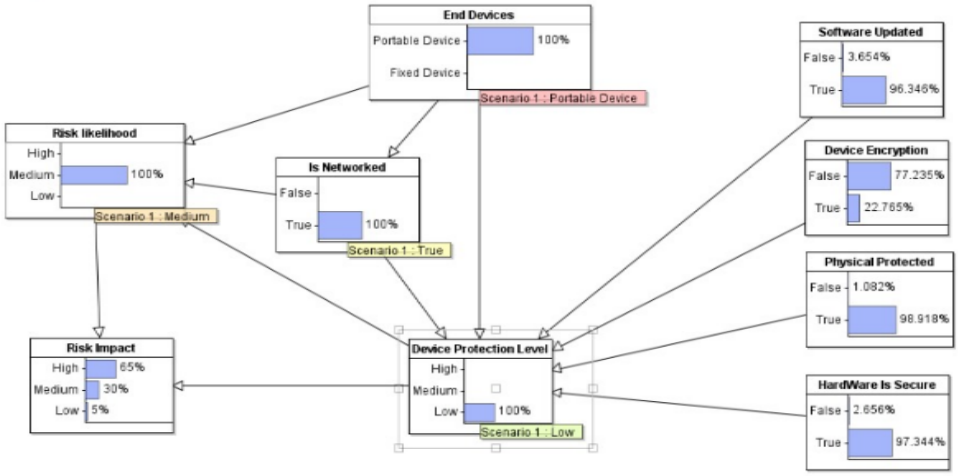

Figure 9: Portable networked end devices with low device protection level

4. Sensitivity Analysis Results

This part of the work presents the end device results based on the sensitivity analysis and the prediction of the risk probability using the Bayesian Network. This study used the AgenaRisk to conduct an extensive sensitivity analysis of the end device scenarios to check the sensitivity of the answers against the technique and its related parameters. The study is a hypothetical analysed sensitivity of the AgenaRisk package in isolation, in that if numerous interrelated parameters relate to the answer, then the researcher only considers the effect of one parameter at a time. For the tool's effectiveness, the researcher determined the technique's sensitivity to the Conditional Probability Tables (CPT). The sensitivity analysis communicates data and outcomes, understanding the link between the input and output variables while identifying sensitive variables. It then helps to make assumptions that allow decision-making and examines the amount of risk in given scenarios. The tornado graphs are generated based on the study's scenario analysis. Below are the CPT results followed by the Tornado graphs and the value of information configuration.

4.1 Conditional Probability Tables

The conditional probability tables (CPT) represent the probabilistic dependence of the parameters in BN models. The table shows results based on the observation outcomes which are generated based on the available prior knowledge. This section presents the conditional probability table for the end devices, which determined the sensitivity outcome based on the threat level that results in a data breach. CPT has the threat level ranked high, medium, and low, while the data breach has two Boolean states, which are true and false. Figure 10 shows the CPT for end devices with a false data breach when the threat level is high (0.007), medium (0.347), and low (0.646). The data breach is true when the threat level is high (0.631), medium (0.311), and low (0.058).

		Threat Level		
		High	Medium	Low
Data breach	False	0.007	0.347	0.646
	True	0.631	0.311	0.058

Figure 10: CPT for end devices

4.2 Tornado graphs

Tornado graphs present a chart that demonstrates the sensitivity based on given deciding variables. Each variable can have a different range of values which directly affects the impact and the risk likelihood. As a graphical representation of the sensitivity analysis, the tornado graph illustrates the sensitivity of the dependent and independent variables. On the AgenaRisk platform, the graph is generated by clicking on the Tornado chart button. The graph also presented different scenarios for sensitivity analysis. So this study presented three Tornado graphs for different rankings of the threat levels, which are high, medium, and low, and two Boolean values (true and false) for the data breach. The Tornado technique examined the sensitivity analysis for the end device-related risks. Figure 11 shows the Tornado graph for a false (0.007) data breach and (0.631) threat level.

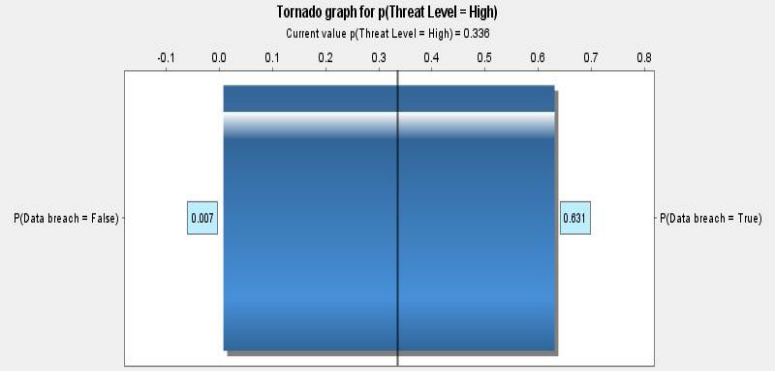

Figure 11: Tornado graph for false data breaches and high threats level

Figure 12 shows the Tornado graph for a true (0.311) data breach and (0.347) medium threat level.

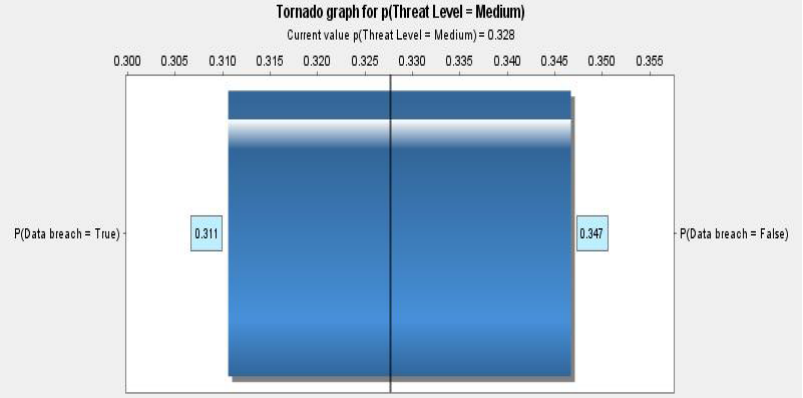

Figure 12: Tornado graph for true data breach and medium threats level

Figure 13 shows the Tornado graph for a true (0.058) data breach and (0648) low threat level.

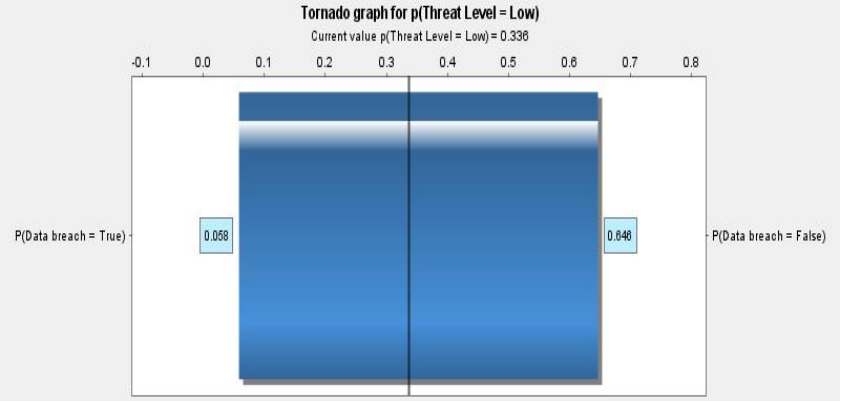

Figure 13: Tornado graph for true data breach and low threats level

4.3 Value of information configuration

The study used VOI as the sensitivity analytical method for decision-making based on the quantified available information to clarify difficult issues and reduce any risk uncertainties. In addition, VOI determines the sensitivity of the observations to improve decision-making. As used in the study, the value of information (VOI) configuration presents the amount that businesses or management could pay for required information that will help them to make decisions. This method is used to obtain more information that relates to the end device risk scenario that is used with the AgenaRisk package. The method reduces uncertainties prior decision-making stage. So, this work presented the decision nodes used in the scenario, the total time to build the risk scenarios in seconds, the expected maximum value (EMV), the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI) for each configuration. Figure 14 shows the configuration for the devices and technical systems with the probability of risk as a decision node, the level of protection of the device as an uncertainty node, and the impact of risk as a utility node. This scenario took 122 minutes to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI).

VOI Configuration	
Decision Node	Risk likelihood [M7]
Uncertainty Nodes	Device Protection Level [M1]
Utility Node	Risk Impact [M8]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 122 ms

Expected Maximum Value (Utility|Decision) – EMV

Expected Value Given Perfect Information – EV|PI

Expected Value of (Partially) Perfect Information – EV(P)PI

Figure 14: Configuration information for end devices

As shown in Figure 15, the devices' EMV is 0.759 with two different malware conditions, EV|PI of 0.728 and EV(P)PI of -0.031. In addition, the device protection has three rankings of low, medium, and high, while the risk likelihood is ranked low, medium, and high.

EMV				0.759
Device Protection Level [M1]			EV|PI	0.728
			EV(P)PI	-0.031
Click to show/hide details				
		Risk likelihood		
		High	Medium	Low
Device Protection Level	High	0.65	0.68	**0.767**
	Medium	0.553	0.563	**0.683**
	Low	0.283	**0.3**	0.23

EV|PI = 0.859 * 0.767 + 0.071 * 0.683 + 0.07 * 0.3 = 0.728

EV(P)PI = 0.728 - 0.759 = -0.031

Figure 15: End devices' EMV

4.4 Discussions

This work determined the risk likelihood and the impact of the end devices with different capabilities. The end device simulation case scenario revealed different outcomes of the risk probability and impact, which are influenced by the prior indicators. Observations and the use of available data such as the prior indicators were used to determine sensitivity analysis using CPT, Tornado graphs, and VOI. CPT determined the end device risk likelihood based on the events of the different variables that result in a risk. In addition, CPT helped to determine the future events of the risks relating to the end devices. The input data was generated and computed to determine the risk outcome (Alkhairy et al., 2020). The results of using the Tornado graphs demonstrated the risk impact and the likelihood of the end devices based on the available prior indicators to determine the level

of the risk likelihood and extent of the risk impact. The results of the VOI showed the sensitivity analysis which could help to identify potential risks relating to the end devices. Organizations and other institutions can use the VOI outcomes to use advanced tools which can reduce costs relating to the end risks (Zabeo et al., 2019).

The analytical techniques used in the study revealed that the safety and security of the end devices depend on the different implementations of the security measures. These measures are linked to the physical hardware of the device, network connection, and software installed. The diverse contributing factors showed the varying probability of the risk related to the end devices. The minimal implementation of device protection security measures exposed the transmitting end devices to a range of cyber threats (Ncubukezi, Mwansa & Rocaries, 2020b).

Even though some end devices may be fixed and not connected to the network, the device's protection level continues to influence the risk level and its impact. The physical security of the devices may not reduce the risk probability of the device if the hardware, software, and encryption are ignored. The guarantee of the end devices should be applied at all levels (hardware, physical, software, and encryption) (Ncubukezi & Mwansa, 2021). If the device's security is prioritised for the hardware, software, physical, and encryption level, the level of risk to the device will be low, resulting in a low-risk impact. For good hygiene of the devices, a wide range of security controls, remedies, and measures should be used at different levels. For example, implementing firewalls, and intrusion detection systems (IDS) would be beneficial to securing and protecting the business's assets (Rawindaran et al., 2021).

Ncubukezi, Mwansa, and Rocaries (2020b) emphasize using adequate security measures to promote good cyber hygiene. With the high rate of risk uncertainties, it would be beneficial for the small business sector to deploy protective measures at all levels of end devices. Poor management of the institutional infrastructure including the end devices becomes the primary target of cyber attackers and results in most institutions losing their private and sensitive information. In addition, during the process of transmission, attackers also gain unauthorised access to the data that is transmitted. Furthermore, networking devices also become the victims that releasing confidential data (Lamba et al., 2017).

Recommendations: Several authors suggest the following safety practices that promote guide hygiene for end devices. Even though institutions differ, organisations need to take precautions and safety measures to improve the security of the devices, and the information stored on the devices. Ncubukezi (2022a), Ncubukezi and Mwansa (2021), Ncubukezi, Mwansa, and Rocaries (2020b) Williams, Chaturvedi, and Chakravarthy (2020), Sung et al., (2018) suggest the following recommendations to reduce the probability of risk on end devices.

- Perform regular system and software updates
- Use of the firewall to proactively filter traffic
- Use of antivirus, and antispyware software to protect the devices and the system
- Use of device encryption in case of the lost device
- Ensure devices are always on secure and locked storage
- Use multi-factor authentication to improve access to the device and its systems
- Perform regular software and hardware updates to reduce device downtime and failure
- Periodically back up data to avoid the single point of failure
- Ensure endpoint protection by securing the devices

5. Conclusion

This study determined the risk likelihood of the end devices using different analytical methods to predict the risk likelihood and their impact. As the end devices operate on the access level of every network, they become vulnerable to different risks. The sources of criminal and insider-related risks were accounted for. The work described the end device scenario which was interpreted using the decision tree analysis – which showed the possible risks devices are vulnerable to. In addition, BN tools were used to analyse sensitivity analysis of the end device risk. These tools include the VOI, CPT, and Tornado graphs. VOI showed the EMV of the device. CPT revealed the threat level on devices. Tornado graphs showed the threat levels for different threat rankings that results in the ultimate data breach.

The paper achieved the usage of the Bayesian network to illustrate the risk likelihood of the end device variables using the dependent and independent variables. The prior indicators used were the software updates,

encryption, physical security, and safety of the hardware determined the level of the risk probability and the risk impact. The outcomes produced different results which revealed low, medium, and high risks of the devices. The study benefits all institutions and people who use the devices to transmit data on the network to proactively take measures that protect and secure devices. In addition, management would come up with policies that will address and promote device security.

Acknowledgments

I would like to thank National Research Foundation (NRF) Black Academics Advancement Programme (BAAP) Grant for the time to conduct the study and financially supporting this work.

References

Alkhairy, I., Low-Choy, S., Murray, J., Wang, J. and Pettitt, A., 2020. Quantifying conditional probability tables in Bayesian networks: Bayesian regression for scenario-based encoding of elicited expert assessments on feral pig habitat. *Journal of Applied Statistics*, 47(10), pp.1848-1884.

Alohali, M., Clarke, N., Li, F. and Furnell, S., 2018. Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security*.

Bhadouria, A.S., Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches.

Cox, A. 2008. What's wrong with risk matrices? *Risk Analysis: An International Journal*, *28*(2), pp.497–512.

Ferdousi, B., 2022. Cyber security risks of bringing your own device (BYOD) practice in the workplace and strategies to address the risks. *International Journal of Science Academic Research.* 3(10), pp.4554-4558.

Gao, P., Li, W., Sun, Y. and Liu, S., 2022. Risk assessment for gas transmission station based on cloud model-based multilevel Bayesian network from the perspective of multi-flow intersecting theory. *Process Safety and Environmental Protection*, *159*, pp.887-898.

Hong, H.J., 2017. From cloud computing to fog computing: unleash the power of edge and end devices. In 2017 IEEE *International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 331-334). IEEE.

Imgraben, J., Engelbrecht, A. and Choo, K.K.R. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, 33(12), pp. 1347–1360.

Khodakarami, V. and Abdi, A., 2014. Project cost risk analysis: A Bayesian networks approach for modeling dependencies between cost items. *International Journal of Project Management*, *32*(7), pp.1233-1245.

Lamba, A., Singh, S., Balvinder, S., Dutta, N. and Rela, S., 2017. Analyzing and fixing cyber security threats for supply chain management. *In International Journal For Technological Research In Engineer*ing, 4(5).

McGuire, M. and Dowling, S., 2013. Cybercrime: A review of the evidence. Summary of key findings and implications. *Home Office Research report*, 75, pp.1-35.

Mosteanu, N.R., 2020. Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. *Quality-Access to Success*, *21*(175).

Munoz, A. and Mafia, A., 2014. Software and hardware certification techniques in a combined certification model. In *2014 11th International Conference on Security and Cryptography (SECRYPT)* (pp. 1-6). IEEE.

Muñoz, A., Fernández-Gago, C. and López-Villa, R., 2022. A Test Environment for Wireless Hacking in Domestic IoT Scenarios. *Mobile Networks and Applications*, pp.1-10.

Mzileni, I., Ncubukezi, T., 2022. Impact of information security threats on small businesses during the Covid-19 pandemic. In *European Conference on Cyber Warfare and Securit*y, 21(1), pp. 401-410.

Ncubukezi, T. and Mwansa, L., 2021. Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid-19 Pandemic. *Journal of Internet Technology and Secured Transactions*, 9(1), pp.714-721.

Ncubukezi, T., 2022a. Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. Conference Proceedings: *International Conference on Cyber Warfare and Security,* 17(1), pp. 395–403.

Ncubukezi, T., 2022b. *Design development and evaluation of the cybersecurity risk tool: a case of small and medium-sized enterprises in South Africa.* (Doctoral Thesis, Cape Peninsula University of Technology, unpublished).

Ncubukezi, T., 2023. Risk Likelihood of Planned and Unplanned Cyber-Attacks in Small Business Sectors: A Cybersecurity Concern. In *International Conference on Cyber Warfare and Security* (pp. 279-XV). Academic Conferences International Limited.

Ncubukezi, T., Mwansa, L. and Rocaries, F., 2020a. A Proposed: Integration of the Monte Carlo model and the Bayes network to Propose Cyber Security Risk Assessment Tool for Small and Medium Enterprises in South Africa. *International Journal of Computer Science and Information Security*, 3(18), pp.152-155.

Ncubukezi, T., Mwansa, L. and Rocaries, F., 2020b. A review of the current cyber hygiene in small and medium-sized businesses. Conference Proceedings: *International Conference for Internet Technology and Secured Transactions (ICITST*), 15, pp. 1–6, IEEE.

Ncubukezi, T., Mwansa, L. and Rocaries, F., 2021. Analysis and impact of the cybercrimes in the Western Cape small and medium-sized businesses. *Conference Proceedings: International Conference on Cyber Warfare and Security*, 16, pp. 425–235.

Ramesh, R., Mannan, M.A., Poo, A.N. and Keerthi, S.S., 2003. Thermal error measurement and modelling in machine tools. Part II. Hybrid Bayesian Network—support vector machine model. *International Journal of Machine Tools and Manufacture*, *43*(4), pp.405-419.

Rawindaran, N., Jayal, A., Prakash, E. and Hewage, C., 2021. Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet*, *13*(8), p.186.

Rusi and Lehto, 2017, T. and Lehto, M. 2017. Cyber threats megatrends in cyberspace. Conference proceedings: *International Conference on Management Leadership and Governance.* Academic Conferences and Publishing Limited, 5, pp.323.

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.

Sung, W.J., Ahn, H.G., Kim, J.B. and Choi, S.G., 2018. Protecting end-device from replay attack on LoRaWAN. In 2018 20th *International Conference on Advanced Communication Technology (ICACT*) (pp.167-171).

Tabassum, M., Kosinski, T. and Lipford, H.R. 2019. I don't own the data: End-user perceptions of smart home device data practices and risks. *Conference proceedings: Symposium on Usable Privacy and Security (SOUPS)*, 15, pp.435–450.

van de Schoot, R., Depaoli, S., King, R., Kramer, B., Märtens, K., Tadesse, M.G., Vannucci, M., Gelman, A., Veen, D., Willemsen, J. and Yau, C., 2021. Bayesian statistics and modeling. *Nature Reviews Methods Primers*, *1*(1), pp.1-26.

Wang, J. and Neil, M., 2021. A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples. *arXiv preprint arXiv:2106.00471*.

Wheelus, C. and Zhu, X., 2020. IoT network security: Threats, risks, and a data-driven defense framework. IoT, 1(2), pp.259-285.

Williams, C.M., Chaturvedi, R. and Chakravarthy, K., 2020. Cybersecurity risks in a pandemic. *Journal of medical Internet research*, *22*(9), p.e23692.

Zabeo, A., Keisler, J.M., Hristozov, D., Marcomini, A. and Linkov, I., 2019. Value of information analysis for assessing risks and benefits of nanotechnology innovation. *Environmental Sciences Europe*, *31*(1), pp.1-8.