Don't be Caught Unaware: A Ransomware Primer with a Specific Focus on Africa

Joey Jansen van Vuuren, Louise Leenen, Anna-Marie Jansen van Vuuren

Don't be caught unaware: A Ransomware Primer with a specific focus on Africa.

Joey Jansen van Vuuren [1], Louise Leenen [2] and Anna-Marie Jansen van Vuuren[3]

[1&3] Tshwane University of Technology, Pretoria, South Africa
jansenvanvuurenjc@tut.ac.za
Jansenvanvuurena1@tut.ac.za

[2] University of the Western Cape and CAIR, Cape Town, South Africa
lleenen@uwc.co.za

Abstract. Ransomware attacks have become the fastest growing and most serious type of cybercrime. A ransomware attack does not only capture victims' data, but also prevents victims from accessing their own data until a ransom has been paid. The prevention of and recovery from a ransomware attack have become a major concern for governments and organizations. This paper presents guidelines for institutions to secure their systems from ransomware attacks and to put steps in place for recovery if their systems have been attacked. The human is often the weak link in allowing an intrusion into a network. African countries are at even greater risk because their populations are often not sufficiently trained nor aware of cybersecurity risks.

Keywords: Ransomware, Cybersecurity Culture, Cybercrime Combatting Culture.

1 Introduction

Ransomware attacks are currently considered to be one of the most serious cyber threats to businesses and governments, and the severity of their impact is constantly increasing. Ransomware is a type of malware that encrypts a victim's data or steals personal data of the victim, and the attacker then demands a ransom to release the data [1]. IBM Security published a guide to ransomware in 2020 in which they note that as ransomware is evolving, the ransom demands are increasing in value - up to US $80 million have been claimed. Attackers are now also using extortion methods. They may threaten a target if ransom is not paid to escalate the attack, release captured data publicly, or to auction confidential data to the highest bidder [2]. Ransomware can cause irreversible damage to the Operating System (OS) or user files even after its removal. Prevention or early detection of ransomware is important [1].

Our methodology consists of a literature search on ransomware attacks combined with our knowledge in cybersecurity and cybersecurity culture, in order to present a primer for the prevention of or recovery from a ransomware attack.

2 Ransomware

Ransomware is defined as "malware" (malicious software) with the primary aim to extort money from users [3,4]. It is software code that blocks access to a computer system, or gains access to private information [5]. The captured information is encrypted so that authorized users loose access to their own data until a ransom is paid. In summary, ransomware blocks users' access to their own resources and the attacker coerces victims to pay (usually) to regain access to their data files or, in some cases, to prevent the attacker from releasing private information on different platforms on the web.

Attackers gain access to computers by using different techniques such as "Social Engineering" where an authorized user is manipulated to give the attacker access to their systems. This is mostly done via phishing emails where attackers use fake emails, e.g. a supposed emails from a bank, to lure users into providing sensitive information which may include passwords [5]. These emails often encourage users to open malicious attachments, or the email body contains links to malicious websites. As part of their attack, attackers can create a website which contains code capable of exploiting unpatched security vulnerabilities on a site visitor's system [6]. Social media platforms are often used to gather personal information about potential victims. Attackers also use vulnerabilities in a network service or unpatched software. Sometimes the attacker falsely claims that the user system is locked and coerces the victim to pay the ransom.

2.1 Types of Ransomware

The following types of ransomware are frequently employed during attacks:

- **Scareware or hoaxware** is fake ransomware presented on the user interface to demand ransom payments even if there is no threat [7]. The attacker pretends to belong to a technical support team and falsely informs users that their computers have been infected with malware and that they can remove the supposed malware if the victims purchase his "removal" or (fake) antivirus services. After the purchase, the attacker removes his presence. An unsophisticated user may believe his system is protected by an antivirus program. Scareware normally do not damage the files or other information on the system and can usually be halted by killing the process in the computer's memory and in its startup entries.
- **ScreenLocker** or **Locker Ransomware** is software that locks a target's computer interface. The attacker blackmails the victim into paying a ransom [4] to unlock the computer. The attack can also be on the OS level to disable user operations and block the user from accessing the operating system. Normally the attacker displays warnings (ransom note) that the user's system is being attacked. These warnings cover a significant part of the user's screen. In most cases this ransomware can be removed without losing

files or private information by terminating the process and deleting the payload.

- **Crypto Ransomware** deletes important data of the user [8]. The ransomware searches through a victim's computer or network in search of specific data including images, PDFs and text files which may be important to the victim and collects these selected items. Strong cryptography is used to encrypt the relevant files. If the victim fails to comply with the ransom demands, the encrypted data is lost permanently. Some variants such as the Petya-ransomware attacks the Master File Table (MFT) of the file system which makes it very difficult to recover the files without paying the ransom [1].
- **Doxware,** also called "Ransomware with Data Exfiltration", behaves similarly to other types of ransomware by encrypting files and presenting its demands to the victim, but it also steals sensitive files and photos, and sends copies back to whoever controls the malware. The attacker threatens to expose sensitive information on the internet unless the victims pay the ransom amount. The attacker is thus able to make a twofold threat for payment - to return the encrypted files to the victim as well refraining from publishing the victim's sensitive information online [6]. Examples of data exfiltration ransomware are the Maze and the DoppelPaymer ransomware [1].

Most of the above ransomware examples use executable files that are run on the victims' computers. A new phenomenon is **Fileless ransomware** that executes an attack without placing malicious software on a victim's computer. Rather than using executable files, an attacker uses Command Scripts or Remote Desktop Protocol (RDP) connections. Poshcoder mimicks Locker ransomware by using PowerShell scripts on Windows, and SamSam and CryptON attack via RDP connections [1].

Another option is **VM-Based Ransomware** that deploys a Virtual Machine (VM) on the victim's system and hides itself in this virtual machine to avoid detection. It then maps host folders as shared folders into the VM. The folders inside the VM are then encrypted. Ragnar ransomware was the first of this type of ransomware [1].

2.2 A framework for ransomware attacks

Figure 1 captures the process an attacker follows during a ransomware attack. The attacker first has to gain initial access into a target system. This initial access is escalated to take control of a target system by means of infiltrating a higher level of access to file systems. During the exploitation phase, can go ahead and encrypt the data so that he can issue a ransom note.

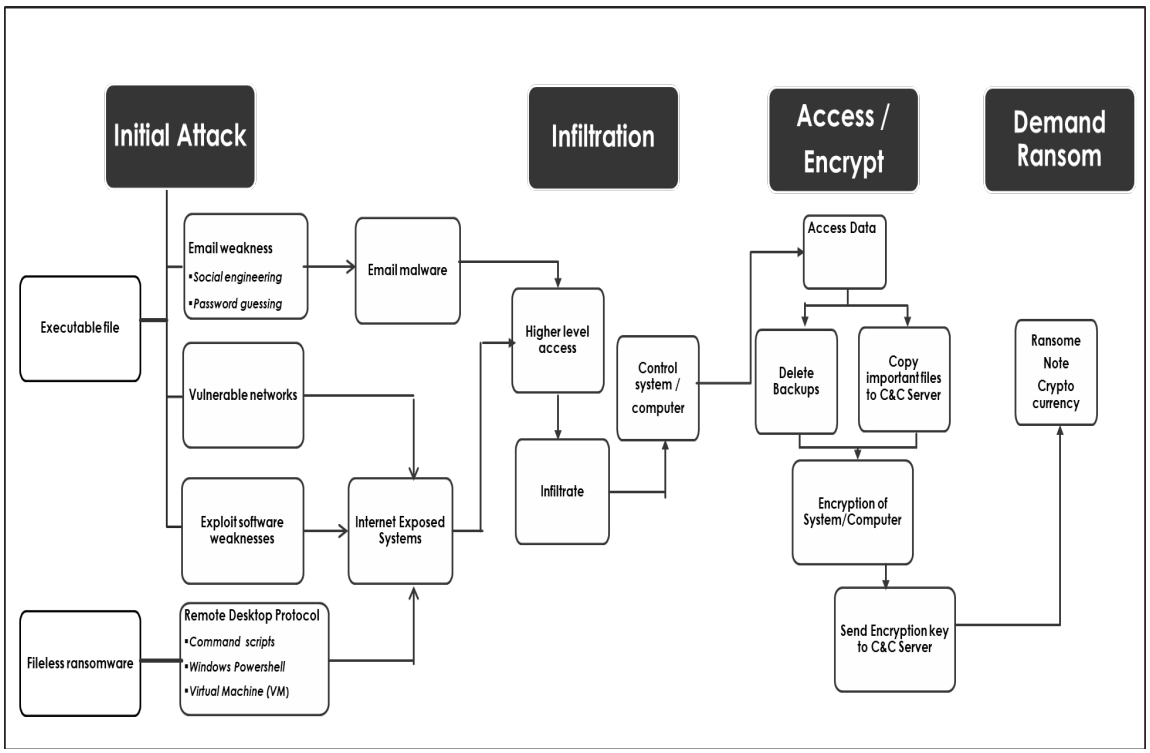

Figure 1 A Ransomware Attack Framework

3 Major International Ransomware Attacks in 2021

Over the past years, ransomware attackers have shifted their targets from individuals to larger corporations due to the possibility of higher ransom profits. By 2020, the increase in ransom payments grew by 300% in the United States, and attacks shifted to exfiltrating company information - the more sensitive, the better [9]. The damages that companies or governments suffer globally due to cybercrime was expected to reach US $6 trillion and for ransomware alone was expected to reach $20 billion by the end of 2021. Ransomware is now the fastest growing and most damaging type of cybercrime. [10]. Most ransomware payments are done in cryptocurrencies, which makes it more difficult to trace the attackers [1].

The Touro College & University System [11] identified the ransomware attacks that had the biggest impact on the USA in 2021. These include attacks on the Colonial Pipeline, Brentagg, Acer, JBS Foods, Aunata, the National BasketBall Association, AXA, CAN, CD Project and KIA Motors. The attackers that demanded the ransom amounts are given in Table 1.

Table 1: Ransomware attackers 2021

Attacker	**Victim**	Ransom
DarkSide gang	The Colonial Pipeline is part of the USA's critical infrastructure systems and supplies gas along the East Coast of the country. The billing system of the Colonial Pipeline was attacked, and this resulted in the company not able to bill its customers. Not having access to this system influenced the supply of gasoline, resulting in gasoline shortages, chaos and panic. Customers panicked and tried to hoard the gasoline and ignored safety precautions. Colonial Pipeline paid the ransom because they were afraid that personal information of customers will be leaked [11].	Attackers demanded more than $4.4 million. The FBI cold-traced the digital wallets and crypto currency. $2.3 million of the paid ransom amount was recovered [12]
	Brentagg is a world leading chemical distribution company with 670 sites and headquarters in Germany. Attackers targeted the North American division by encrypted devices on the company's network and stealing unencrypted files (150GB). An attacker created a private leak for proof of the stolen data [13].	Attackers demanded $7.5 million dollars. Brentagg paid $4.4 million nothing and was recovered [13].
REvil or Sodinokibi hacker group	ACER is a multinational computer manufacturer. Attackers exploited the Microsoft exchange server to get access to Acer's files, and leaked images of sensitive financial documents and spreadsheets. In another attack in 2021, not ransomware-related, ACER's Indian offices were also attacked and 60GB of files were stolen. [14].	Attackers demanded $50 million. Acer counter-offering $10 million, a 20% discount was allowed. It is not known how much ACER paid.
	JBS FOODS is one of the biggest meat processing companies supplying to restaurants and grocery stores in North America. The company was forced to halt cattle-slaughtering operations at 13 of its meat processing plants. Consumers were warned not to do panic buying [15,11].	Attackers demanded $11 million. JBS paid in crypto currency and this was the largest ransomware payment by June 2021 [11].
	QUANTA, the Computer Manufacturer and Apple's business partner, was attacked and the apple product blueprints and other sensitive information were	Attackers demanded $50 million, but the

	stolen. After the firm refused to negotiate with the attackers, they targeted Apple instead [11].	ransom was not paid [11].
	KASEYA, the enterprise technology company, experienced the first instance of a supply chain attack. Kaseya provides IT solutions, a management tool for handling networks and endpoints, compliance systems, service desks, and a professional services automation platform. Because Kaseya managed their customers networks and endpoints, the attack on Kaseya also gave the attackers access to then networks and endpoints of their customers [16]. Companies in 17 countries and more than a thousand businesses were affected by this attack. Some victims, such as Swedish supermarket, Coop, remained closed for business on the day of the attack [17].	Attackers demanded $70 million but no ransom was paid [17] .
Babuk	The National Basketball Association (NBA) was attacked, and the attackers claimed they had stolen 500 GB of data about the Houston Rockets. This included confidential documents, such as financial info and contracts [18].	The ransom amount was probably $85 million but it has not been confirmed [19].
Avaddon	AXA was attacked soon after the company announced important changes to their insurance policy such as halting reimbursement for ransomware payments to many of their clients in France. The attackers gained access to 3 TB of data [20].	The ransom amount is unknown but this attacker group's ransom is normally about $40 million [20].
Evil Corp	The network of CNA, an insurance company, was attacked and the attackers encrypted 15,000 devices, including many computers of employees working remotely and logged in via a VPN. The malware used was Phoenix CryptoLocker.	A ransom amount of $40 million was paid [21].
HelloKitty gang	CDProjekt Red is a popular videogame development firm based in Poland. Attackers accessed source code for Cyberpunk and Witcher 3 games which was in development, and encrypted some devices [22].	The attackers wanted $7 million and sent the ransom note via Twitter. The victim company did not pay ransom because they had backups and was able to restore their

		data. They did not recover completely from the attack and the games that were attacked presented some errors. [22]
DoppelPaymer	KIA MOTORS, a subsidiary of Hyundai, reported a widespread IT and systems outage, but they did not confirm the hack. The system outage affected its Mobile UVO link apps, payment services, phone services, owner portal, and dealerships' internal systems. The attackers claimed they attacked Hyundai Motor America [23].	Attackers demanded $20 million or 800 bitcoins (worth $30 million) [23]. Because KIA did not confirm the hack, it is speculated that they did pay the ransom.

4 Ransomware attacks in Africa

A report released by the International Criminal Police Organization (Interpol) on cybercrime in Africa, identified ransomware as one of the top five prominent threats in Africa [24] (Figure 2). The report further indicated that South Africa is the most hard hit country in Africa with Egypt being second and Tunisia third [24].

South Africa's figure of 52 victims per one million internet users is around 92 times lower than that of the UK, which has 4,783 victims per one million internet users, and about 29 times lower than that of the USA. South Africa is listed as seventh highest in terms of number of attacks in the world, behind France with the Netherlands in the next spot [25].

In a global survey by Sophos, the state of response to ransomware attacks in South Africa showed that about 49% of organisations are paying the requested ransom. The amount of ransom paid is not the total cost, as the cost of recovery can be up to $710,000 (R11.5 million). Insurance policies covered 99% of the costs of the 77% of organisations that had cyber insurance [26]. However, these attacks are becoming even more serious in South Africa due to the Protection of Personal Information (PoPI) Act of 2013 that came into effect on 1 July 2020. Non-compliance with the PoPI Act, for example not securing personal information, can result in a fine of R10 million or a 10 year jail sentence [27]. The PoPI Act also prescribed to companies that they have to alert users or customers when the company falls victim to a cyberattack. Therefore, when the South African retail giant, Dis-Chem, suffered from an incident where a third-party service provider of the company was attacked, it notified its customers of the breach of their personal information.[28] At this moment there is no confirmation if it was a ransomware attack on the service provider, yet the data-breach resulting from this could potentially lead to future attacks.

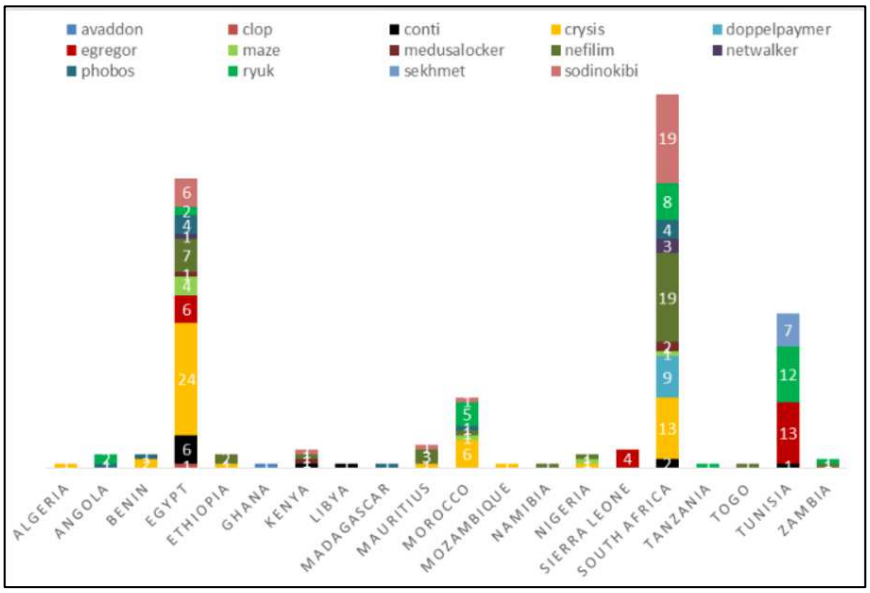

Figure 2: Ransomware Attacks in Africa [24]

4.1 Major ransomware attacks in Africa in 2021 and 2022

Almost all reports of ransomware attacks in Africa contain information of attacks against South African companies or government institutions. Other African countries are also attacked but there is less information available about them. The reports on ransomware attacks in Africa also tend to contain less information than reports on attacks in the USA, UK and Europe. According to a report by Interpol, published in October 2021, African organisations experienced the highest increase in ransomware attacks, at 34%, during the first quarter of 2021, compared to the rest of the world [29] .

Several South African government departments and institutions were attacked during 2021. This country's Department of Justice was attacked in September 2021. All online services, including email and the department's website, became inoperable [30]. Information on the servers was encrypted and became unavailable to employees and the public. Consequently, the department could not issue of letters of authority, render bail services or respond to emails [31]. The department immediately activated a contingency plan, preventing the ransomware from spreading to other government systems. Their systems only returned back to service one month after the attack. According to media reports, no ransom was paid [30]. At about the same time another government institution, the South African National Space Agency (SANSA), also suffered an attack, from a group called "CoomingProject." Although SANSA's network was not affected, data of the agency was found in the public domain [32].

Two months earlier, in July 2021, the "Hello Kitty"-gang attacked Transnet. Transnet is a public entity who reports to the Department of Transport. They manage the port in Durban. This attack on them affected many other African countries, because Durban is used for the shipment of their products, including copper and cobalt mined in Zambia

and the Democratic Republic of Congo [30]. This supply chain attack paralysed the port for more than 10 days, resulting in trucks standing idle while waiting for goods to be released, perishable goods expiring, businesses facing late deliveries and penalties due to delayed goods. Many ships were anchored for days or weeks waiting to offload cargo at the port [33]. These attacks were not all the same; Transnet and the justice department were locked out of their systems but SANSA's data was made public. In none of these cases it was reported that the ransom was paid.

The private sector and financial services have also suffered from these type of attacks. Curo, one of South Africa's best-known asset management firms controlling more than 2 trillion South African Rand in its overall portfolio, was attacked in January 2022. The attackers prevented the company from accessing their data for five days. Fortunately, the attack did not affect highly sensitive customer information, and Curo did not lose control of its financial assets at any stage. Curo's management decided to ignore the attackers and focused on restoring their systems to full functionality [34]

The latest attack was against TransUnion, a company with 3 million consumers and 600000 businesses. The attacker, N4ughtySecTU, allegedly stole 4TB of data that included identity numbers, personal and email addresses, telephone numbers, etc. Even the member database of the governing ANC party was leaked. TransUnion refused to pay the ransom amount of $15 million [25].

One of Egypt's oldest and largest publishing houses was attacked by ransomware in August 2021, and the attack resulted in a loss of access to electronic copies of reference books [35].The Nigerian Guardian reports that about 71 percent of Nigerian organisations were hit by ransomware in 2021 [36].

4.2 Causes of Ransomware attacks in South Africa

A study done by ITWEB and KnowBe4 on 378 South African organizations showed that 34% of the organizations fell victim to ransomware and 48% of the victims experienced a severe impact on their business operations [5]. Kaspersky saw a 24% increase in ransomware attacks in the second quarter of 2021 in South Africa. Sophos found that the average cost to rectify a ransomware attack in South Africa is about ZAR 6,7M ($0.45 Million), and that 24% of businesses that formed part of the survey indicated they were hit by a ransomware attack during the past year. Only 11% of those businesses were able to recover all their data in a reasonable timeframe [5]. The attacks on South African entities were launched by a variety of ransomware including Crysis, Nefilim, Ryuk, Clop and Conti (BUSINESSTECH, 2021). The methodologies of the ransomware intrusions are shown in Figure 3.

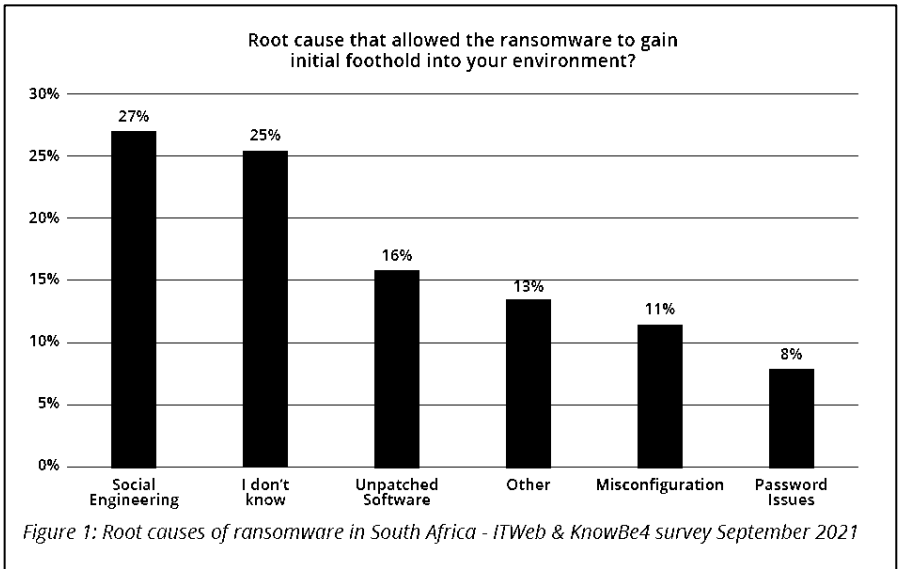

Figure 3: Root causes for ransomware access [5]

5 Preventing a Ransomware Attack

In this section, the authors provide guidelines that can be followed by organizations to prevent ransomware attacks. There are steps for managers to follow, as well as guidelines for employees. Some of the guidelines form part of a general cybersecurity culture to be fostered in any organization.

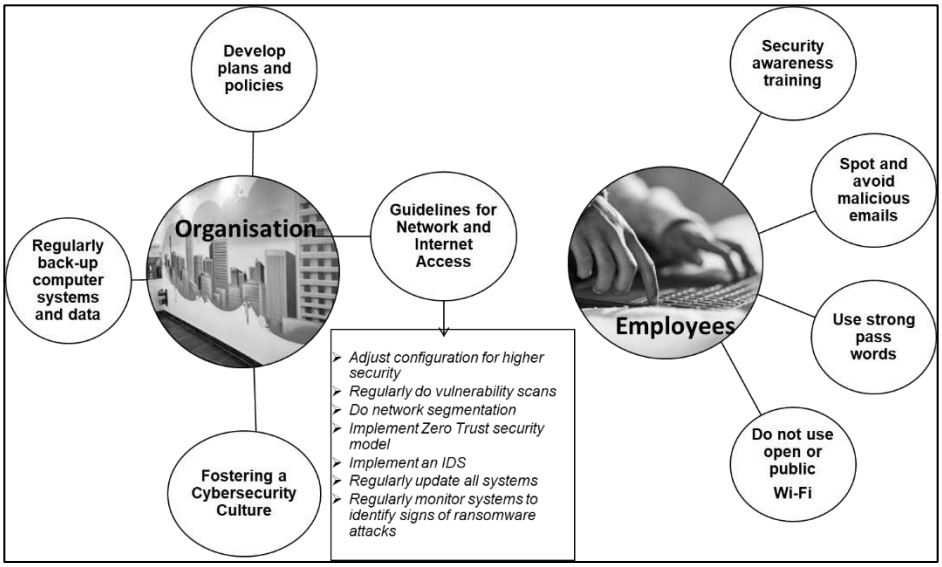

Figure 4: Framework for prevention of ransomware attack

5.1 Steps for Organizations

- **Develop plans and policies**

Every organization should have a Cybersecurity Policy that includes the raising of cybersecurity awareness within the organization [37]. There must be specific guidance for raising ransomware awareness.

A Cyber Incident Response Plan is crucial. This plan depicts steps to be followed by the company's IT security team during a ransomware event. It should include response and notification procedures when attacked, as well as the roles and responsibilities and communications that should be shared, during and after an attack. When designing this plan, remember to include partners, vendors and CSIRTs (Cyber Incident Response Teams) that would need to be notified of an attack. A resilience plan that includes data recovery and addresses, the procedure on what to do if the organization has lost control of critical functions, is also necessary.

- **Fostering a Cybersecurity Culture**

ENISA, the European Union Agency for Network and Information Security, defines the term "Cybersecurity Culture" (CSC) as "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies (ENISA, 2017). ENISA also advises to raise cybersecurity awareness and to implement an information security framework. A Cybersecurity Culture framework was developed by Leenen, Jansen van Vuuren & Jansen van Vuuren [38] where they advised that a CSC

should be integrated in the employee's job, habits and conduct, including all the socio-cultural measures that support technical security methods, for cyber actions to become a natural aspect of the daily activity. Awareness and education are also important pillars of the CSC. The International Telecommunications Union regards the fostering of a cybersecurity culture as a core aspect of maintaining cybersecurity [39]. ENISA provides a very useful guide to advise organizations in creating Cybersecurity Culture programs [40].

- **Regularly back-up computer systems and data**

The most important way to recover from a ransomware attack is to make regular backups of all your important data and to ensure the availability of backups. Backups should be stored offline or in a cloud-based file hosting service with automatic backup processes to prevent attackers from accessing it. A policy should be drafted on the correct procedures for making backups. External storage device must be disconnected and only be connected when backups are being made. If a cloud service is used, it is advised to disconnect from the cloud storage when it is not required for making backups. Routinely test backups for efficacy. In the case of an attack, verify that backups have not been tampered with before rolling back data.

- **Network and Internet Access**

It is important to create Best Practice Guidelines for the use of a Remote Desktop Protocol (RDP) and other remote desktop services. Disable unused RDP Server and Message Block (SMB) ports for both cloud and company usage, and remove or disable outdated versions of SMBs. Secure configuration settings can help to limit an organization's threat surface and close security gaps left from default configurations. Regularly perform vulnerability scans of the network and especially for internet facing devices [41]. Devices must be properly configured, security features must be enabled, and vulnerable plugins as well as file extensions must be disabled. Filter network traffic to stop incoming and outgoing communications with known malicious IP addresses [42]. Do network segmentation to allow only certain users onto the network, and implement a Zero Trust Security model to protect the most critical applications and data [42].

- **Implement an IDS**

An Intrusion Detection System (IDS) identifies malware activity by comparing network traffic logs to signatures that detect known malicious activity. A good IDS updates signatures often and will send alerts if it detects potential malicious activity.

- **Regularly update all systems**

Ensure that all the organization's operating systems, applications, and software are updated regularly and turn on auto updates for security patches including updates on the firmware and systems. Prioritize the patching of critical vulnerabilities on systems, and vulnerabilities on Internet-facing servers including software that processes Internet data, such as web browsers, browser plugins, and document readers [42]. A Privileged

Access Management (PAM) solution can be implemented where used and changed passwords can be verified. [5].

- **User device and account management**

All user devices must have antivirus and anti-malware solutions with up-to-date signatures installed. Limit user and privileged accounts through "account use"-policies, user account control, and privileged account management. Employ multi-factor authentication for all services, logins, particularly for web mail, virtual private networks (VPNs), and accounts that access critical systems. Adopt solutions that will force an immediate review of the account escalation attempts and implement applications that allow block listing. Enable strong spam filters to reduce the risk of phishing emails being distributed to employees [42]. Use deceptions such as the creation of fake file repositories (honeypots) that look like legitimate repositories which hackers can target. These deception systems can alert the company that there is suspicious behavior on the network. In this process the hacker activity can be identified and the company can act in time [43,5].

- **Regular monitoring of systems to identify signs of ransomware attacks**

Use behavioural analysis to monitor networks systems for anomalous traffic flows and patterns [5]. Look for anomalous file system activity, such as numerous of failed file modifications (due to the ransomware attempting to access those files). Investigate if the computer or system suddenly gets slower, or if there is an increase in CPU and hard disk activity for no apparent reason. This can be due to the ransomware searching for files, encrypting files, and removing data files. Sudden unavailability of some of these files could be due to the encryption, deleting, renaming or relocation of files. There can also be suspicious network communications that is caused by interaction between the ransomware and the attackers' command and control server [43].

- **Cyber insurance policy**

Consider getting a Cyber insurance policy and check whether the policy covers ransomware losses. As described above, with ransomware attacks increasing this could be a viable way to prevent huge losses.

5.2 Employees

- **Security awareness training**

Security awareness training is an important factor of a cybersecure culture. Training must cover hacking and phishing techniques, and in general, make employees aware of Social Engineering attacks to extract information from individuals.

- **Emails**

  Employees must be able to spot and avoid malicious emails – this is a key factor to stop ransomware attacks. Employees must remain vigilant and check the source of any email before downloading an attachment.

- **Passwords**

Employees must be encouraged to use strong passwords that should not be reused across multiple accounts or stored where others can get access to it. Employees should not use information generally available on social networks, such as their birthdays or family members' names, to create passwords.

- **Open or public Wi-Fi**

Employees must be discouraged to use open or public Wi-Fi or networks because hackers can easily infiltrate these networks.

6 Recovery After a Ransomware Attack

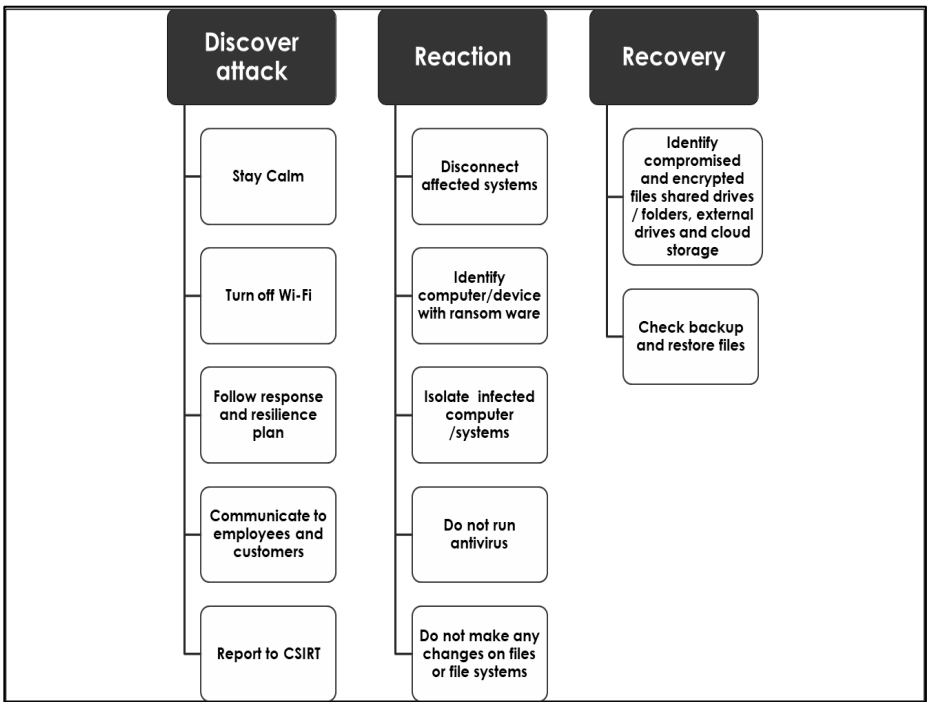

Figure 5: Recovery after Ransomware attack

What should one do if you fall victim to such an attack? Here are some suggested guidelines an individual or an organization should follow:

- Stay calm. Stick to the response and resilience plans and do not make any rash decisions. Contact the organization's CSIRT or sector CSIRT at the earliest opportunity.

- Identify and disconnect all affected systems from any network or isolate them and unplug storage devices such as USB or external hard drives. Do not erase any information or make any changes on your file systems. Do not run the antivirus programs. Check the file properties of the infected or encrypted files to identify on which computer the ransomware is installed.
- Turn off any wireless capabilities such as Wi-Fi or Bluetooth.
- Determine the size of the attack including the number of files that is compromised or encrypted on the shared drives or folders, cloud storage or external hard drives. Check which files were backed up and what needs to be restored.
- Encourage open and honest communication, internally to the company and users, as well as externally to vendors and clients. Issue a public statement that explains what had happened, the information available on the attack and your plan to recover the files. Notify law enforcement and regulatory bodies of the attack [5].

7 Conclusion

This paper considers the growing threat of ransomware internationally, with a specific focus on Africa. Ransomware has become the cybercrime with the biggest impact on governments and businesses. The authors presents a primer for institutions to strengthen their cybersecurity measures against ransom ware attacks. It is often human error that leads to ransomware attackers gaining a first entry into a system, and thus cybersecurity training and awareness become crucial. African companies are particularly vulnerable against ransomware because cybersecurity awareness tends to be lower in African countries, compared to the rest of the globe.

References

1. McIntosh T, Kayes A, Chen Y-PP, Ng A, Watters P, (2021). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys (CSUR) 54 (9):1-36. (2021)
2. IBM Security, The definitive guide to ransomware: Readiness, response, and remediation. IBM Security. https://www.ibm.com/downloads/cas/EV6NAQR4. last accessed Februar,y 12 2020.
3. Barak I, How Does Ransomware Work? https://www.cybereason.com/blog/how-does-ransomware-work#:~:text=Ransomware%20is%20a%20type%20of,ransom%20payment%20to%20restore%20access. last accessed September, 25 2017.
4. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the gordian knot: A look under the hood of ransomware attacks. In: International conference on detection of intrusions and malware, and vulnerability assessment, DIMVA 2015, Milan, Italy, 2015. Springer, pp 3-24

5. Van der Walt C, Collard A, Grimes R. A., Pillay K, Defending Against Ransomware - An Advisory by the South African Cybersecurity Hub. www.orangecyberdefense.com/za/contact/. last accessed May,10 2021.
6. SecureMac, What is Doxware? https://www.securemac.com/blog/what-is-doxware. last accessed January, 15 2020.
7. Brewer R, (2016). Ransomware attacks: detection, prevention and cure. Network Security 2016 (9):5-9. (2016)
8. COMODO, Ransomware Attacks 2021. https://enterprise.comodo.com/blog/recent-ransomware-attacks/. last accessed October, 4 2022.
9. Harvard Business Review, Ransomware Attacks Are Spiking. Is Your Company Prepared? https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared. last accessed January, 15 2021.
10. Morgan S, Cybercrime to cost the world $10.5 trillion Annual by 2025. Cybercrime Magazine. (2020)
11. The Touro College & University System, The 10 Biggest Ransomware Attacks of 2021. https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php. last accessed November 25 2021.
12. Macias A, Wilkie C, U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom. CNBC. https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html. last accessed October, 10 2021.
13. Din A, Chemical Distributor Brenntag Says What Data Was Stolen During the Ransomware Attack. HEIMDAL. https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/. last accessed September, 15 2021.
14. Greig J, Acer confirms second cyberattack in 2021 after ransomware incident in March. ZDNET. https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/. last accessed November, 5 2021.
15. Morrison S, Ransomware attack hits another massive, crucial industry: Meat. Vox. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers. last accessed September, 15 2021.
16. Osborne C, Updated Kaseya ransomware attack FAQ: What we know now. ZDNET. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/. last accessed October, 20 2021.
17. Tung L, Kaseya ransomware attack: 1,500 companies affected, company confirms. ZDNET. https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/. last accessed September, 9 2021.
18. Mehrotra K, NBA's Houston Rockets Face Cyber-Attack by Ransomware Group. Bloomberg. https://www.bloomberg.com/news/articles/2021-04-14/nba-s-houston-rockets-face-cyber-attack-by-ransomware-group. last accessed September, 15 2021.
19. Goud N, https://www.cybersecurity-insiders.com/babuk-ransomware-attack-on-nba-houston-rockets/. https://www.cybersecurity-insiders.com/babuk-ransomware-attack-on-nba-houston-rockets/. last accessed January, 28 2021.

20. Ikeda S, Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France. CPO Magazine, Rezonen Pte. Ltd. https://www.cpomagazine.com/cyber-security/ransomware-attack-reported-at-insurance-giant-axa-one-week-after-it-changes-cyber-insurance-policies-in-france/. last accessed November, 15 2021.
21. Mehrotra K, Turton W, CNA Financial Paid $40 Million in Ransom After March Cyberattack. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack. last accessed September, 15 2021.
22. Keane S, Gonzalez O, Cyberpunk 2077 developer CD Projekt hit by ransomware attack, source code leaked. Cnet. https://www.cnet.com/tech/computing/cyberpunk-2077-developer-cd-projekt-hit-by-ransomware-attack-source-code-leaked/. last accessed September, 15 2021.
23. Hope A, Kia Motors America Suffers a $20 Million Suspected DoppelPaymer Ransomware Attack. CPO Magazine, Rezonen Pte. Ltd. https://www.cpomagazine.com/cyber-security/kia-motors-america-suffers-a-20-million-suspected-doppelpaymer-ransomware-attack/#:~:text=Automaker%20Kia%20Motors%20America%20%28KMA%29%20suffered%20a. last accessed November, 15 2021.
24. BUSINESSTECH, South Africa under cyber attack: Interpol reveals top threats in South Africa. https://businesstech.co.za/news/it-services/531990/south-africa-under-cyber-attack-interpol-reveals-top-threats-in-south-africa/. 2021.
25. Myles I, Cybercriminals love South Africa -Study. MyBroadband. https://mybroadband.co.za/news/security/443090-cybercriminals-love-south-africa-study.html. last accessed May, 9 2022.
26. Myles I, South African companies getting nailed by ransomware — and they are paying up. MyBroadband. https://mybroadband.co.za/news/security/443728-south-african-companies-getting-nailed-by-ransomware-and-they-are-paying-up.html?msclkid=da174ab7d07511ecadd77ffe4139712e. last accessed May, 9 2022.
27. Money Expert South Africa, What-is-the-POPI-Act-a-simple-summary. https://www.moneyexpert.co.za/broadband/what-is-the-popi-act-a-simple-summary/. last accessed May, 9 2022.
28. Moyo A, Dis-Chem prescription service outage after cyber attack. ITWeb. https://www.itweb.co.za/content/8OKdWqDXNezqbznQ last accessed May,11 2022.
29. ITWeb, Hornetsecurity global ransomware survey reveals the ‘stinging' truth. https://www.itweb.co.za/content/kLgB17e8QnNv59N4. last accessed May,10 2022.
30. Thomas I, The State of Ransomware Attacks in Africa. Ironscales. https://ironscales.com/blog/the-state-of-ransomware-attacks-in-africa. last accessed February, 9 2022.
31. Moyo A, Justice department battles to contain ransomware attack. ITWeb https://www.itweb.co.za/content/DZQ58vVPOB1MzXy2. last accessed October, 9 2021.

32. Moyo A, SA's govt entities under attack as space agency hit by data breach. ITWeb https://www.itweb.co.za/content/6GxRKMYJy1bqb3Wj. last accessed October, 9 2021.
33. ITWeb, Lessons from Transnet: Is your business prepared for a ransomware attack. https://www.itweb.co.za/content/GxwQDq1ZJQLvlPVo. last accessed September, 29 2021.
34. Soteria, Ransomware attack hits financial services firm Curo. http://soteriacloud.co.za/news/financial-services-ransomware-attack-ransomware/. last accessed February, 9 2022.
35. H-Tayea, Ransomware Virus Hits One of Egypt's Largest Publishing Houses. SEE-egy. https://see.news/ransomware-virus-hits-one-of-egypts-largest-pub/. last accessed May,10 2021.
36. Guardian Nigeria, Ransomware hits 71% of Nigerian organisations https://guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/. last accessed May,10 2022.
37. Government Technology, 7 Steps to Help Prevent & Limit the Impact of Ransomware. https://www.govtech.com/security/7-steps-to-help-prevent--limit-the-impact-of-ransomware.html. last accessed Agust, 15 2020.
38. Leenen L, Jansen van Vuuren J, Jansen van Vuuren A-M. Cybersecurity and Cybercrime Combatting Culture for African Police Services. In: IFIP International Conference on Human Choice and Computers, 2020. Springer, pp 248-261
39. ITU, International Telecommunications Union Corporate Annual Report 2008. International Telecommunications Union. https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf. last accessed November, 8 2008.
40. ENISA, Cyber Security Culture in Organisations. European Agency for Network and Information Security (ENISA), (2017)
41. Piper D, (2021). Cybersecurity and infrastructure security agency releases guidance regarding ransomware. Internet Law 25 (1). (2021)
42. CISA, Protecting sensitive and personal information from ransomware-caused data breaches. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf. last accessed January,10 2021.
43. Melnick J, How to Detect Ransomware. https://blog.netwrix.com/2020/09/03/how-to-detect-ransomware/. last accessed January, 28 2020.