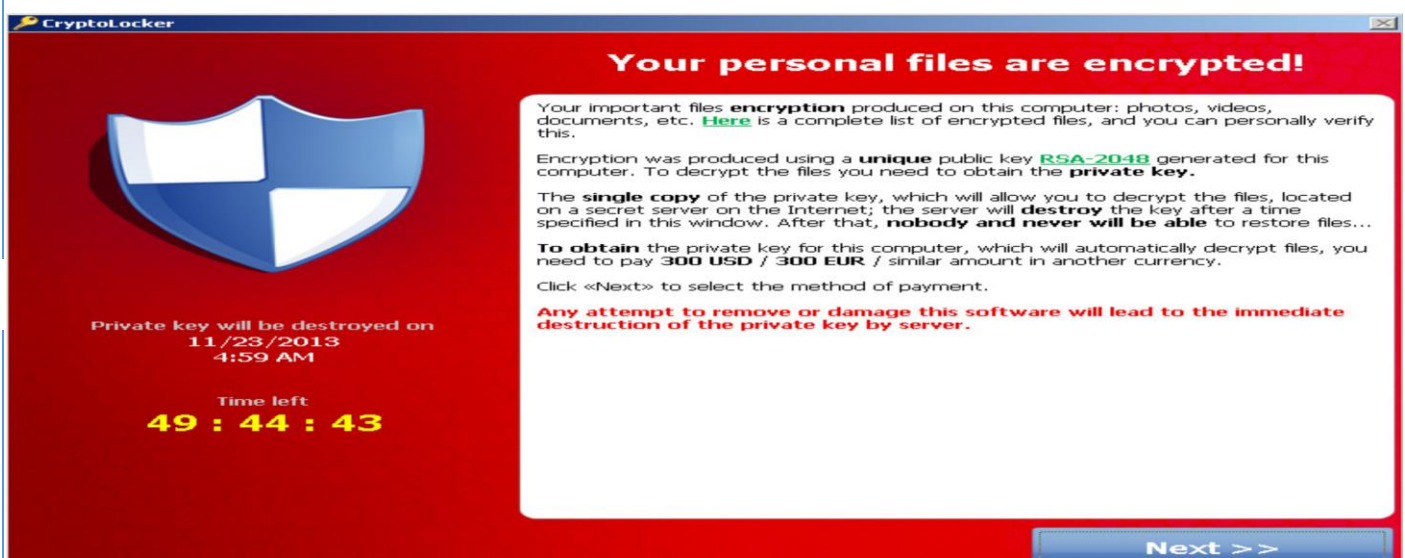


Data Centric Protection against Ransomware Attacks at the Office of the Auditor General



Olebile DINGALO

STUDENT ID: 1614568 Botho University

Table of Contents

Abstract	3
Abbreviations.....	4
Chapter 1	5
1. Introduction	5
1.1. Background Study and Problem Identification.....	8
Chapter 2.....	11
2. Review of Literature	11
2.1. Recent Security Trends	11
2.2. Data Centric Security (DCS)	13
2.3. Ransomware	18
2.3.1. Contextual Basics	18
2.3.2. Ransomware Propagation.....	24
2.3.3. The reality of ransomware	27
2.4. Data Centric approach to Ransomware	28
2.4.1. Data discovery	34
2.4.2. Data classification	34
2.4.3. Deploying Defences	35
2.5. Proposed Model to Data Centric Protection at the Office of the Auditor General.....	39
2.5.1. Identification of Critical Assets and their Protection.....	39
2.5.1.2. Security Philosophy and Mind-set	40
2.5.1.3. Deploy Protection.....	41
2.5.1.4. Monitoring and Detection.....	42
2.6. Conclusion of literature review	42
Chapter 3.....	46
3. Methodology	46
3.1. Introduction	46
3.2. Data Collection Techniques.....	48
3.2.1. Questionnaire Design	49
3.2.2. Interview	49
3.2.3. Data Collection Methods.....	50
3.3. Research Questions.....	50
3.4. Sampling.....	52
Chapter 4.....	55

4. Presentation of Results and Data Analysis.....	55
4.1. Survey Response	55
4.1.1. Management.....	55
4.1.2. Auditors.....	56
4.1.3. DIT and IT Support Management	56
4.2. Survey Results	57
4.2.1. The role of DIT concerning security at OAG	57
4.2.2. The role of the DIT attaché (Chief Systems Analyst) at the OAG	58
4.2.3. Ransomware a viable threat in Botswana	59
4.2.4. Current Defences against Ransomware.....	61
4.2.5. Sufficiency of current security strategy in light of OAG's unique workflows...	63
4.2.5.1. Identification of Critical Asset, Processes and their Protection	63
4.2.5.2. Threat Intelligence	65
4.2.5.3. Incident and Disaster Management	68
4.2.5.4. Monitoring and Detection.....	68
Chapter 5.....	70
5. Discussion	70
5.1.1. The role of DIT concerning security at OAG	70
5.1.2. The role of the DIT attaché (Chief Systems Analyst) at the OAG	70
5.1.3. Ransomware a viable threat in Botswana	71
5.1.4. Sufficiency of current security strategy in light of OAG's unique workflows...	72
5.1.5. Data Centric Protection as an approach to defence at OAG	74
Chapter 6.....	77
6. Conclusion.....	77
7. References.....	78
Annexure 1.....	85
Annexure 2.....	90
Annexure 3.....	93
Annexure 4.....	96

Abstract

In attempting to answer the question of whether the Office of the Auditor General is doing enough to protect the sensitive data in its possession, I start off by stating the current information security trends. The trends highlight an upward rise in data breaches despite the numerous traditional approaches to secure data and network resources like firewalls, antiviruses, anti-malware gateways etc. In validation a study is performed at the Office of the Auditor General. Analysis of the survey data brings to light the current state of affairs that exhibits a random or ad-hoc approach to information security. It also reveals that traditional defences can be useful in protecting information assets against ransomware despite their shortcomings. The weaknesses of such methods is discussed thus emphasising the need for new innovative approaches to data security

An unconventional approach is gradually gaining popularity as an alternative. This approach is known as Data Centric Security. It is a structured approach to enacting security by emphasising data protection as the ultimate objective. Consequently that entails being knowledgeable at all times of your data, how it is transmitted, the destination of that data, and securing it throughout its different forms/states and locations.

Lastly this approach is advanced as an additional control to augment the traditional defences. It is advocated that such approach will give relative assurance that most (if not all) attack vectors are covered when instituting defences.

Abbreviations

OAG	-	Office of the Auditor General
DIT	-	Department of Information Technology
GDN	-	Government Data Network
ITRC	-	Identity Theft Resource Center
ICT	-	Information Communication Technology
DCS	-	Data Centric Security
OECD	-	Organisation for Economic Co-operation & Development
CSA	-	Chief Systems Analyst

Chapter 1

1. Introduction

The cyber world has developed exponentially in the past decades. Over the years computers have become interconnected allowing people, societies, companies and governments to access information in remote areas and also to communicate almost instantaneously across the globe. In effect there has been advanced automation and interconnection of most of the functions and services of the society (Kuusisto and Kuusisto, 2015). This has brought progress and ease to many facets of life like heightened global business, intensified access to health facilities and entertainment to mention a few. It is ostensible that the digitalization and networking of the functions and structures of the social order affords a lot of usefulness.

However the benefits chauffeured in by this globalisation has also seen the introduction of new vulnerabilities and threats. That is to say the new age of global connectivity brought in by interconnections and networks has introduced numerous possibilities as well as an ever changing assortment of vulnerabilities. According to Yu et al. (2014) there has been swift advances in information communication technology and the Internet. This has meant the realisation of great potential and value due to ubiquitous networks and society. But such implementations often result in encroachments on privately owned data like malicious distribution and unauthorized usage (Yu et al., 2014)

Nonetheless, entities now find themselves completely dependent on vulnerable systems for storage and transfer of information. It is thus not astounding that entities are continually exploring new and innovative ways aimed at mitigating possible exploits on networked systems. Information Security, as it is commonly known, evolves as fast as the capabilities of computing. According to Kuusisto and Kuusisto (2015), the cyber world information has become vulnerable to numerous security threats and thus security has come to be a major issue. The fact that the cyber world is continuously evolving means that there is ever increasing complexity and challenges to actors in the cyber world (Kuusisto and Kuusisto, 2015).

The most recent CryptoLocker Ransomware attack of 2017, termed "WannaCryptor/ WannaCry" fully demonstrates the above sentiments. This type of malware/malicious code contaminates a computer by swiftly encrypting data or locking the appliance. Despite the many precautions taken by entities across the globe, in the name of Information Security, the world was still crippled by this malicious code. CNN reported 150 countries and 300000 computers to have been hit in just 3 days (CNNMoney, 2017). Operations in hospitals, airports, banks, universities and many facilities across the globe were brought to an abrupt halt. Some entities in Botswana, including some in Government, were hit by this outbreak, although the Office of the Auditor General within the Government of Botswana was not targeted in this attack. However, the question remains, was it by sheer luck or by the office's own device that the attack was evaded.

It is the purpose of this paper to explore the following questions:

- Is the risk of Ransomware real in Botswana and specifically for the Office of the Auditor General?
- Is the Office of the Auditor General doing enough to protect its data? In so doing the current preparations taken by the office will be assessed.
- Can Data Centric Security be used as an option to protecting Office of the Auditor General data?

1.1. Background Study and Problem Identification

The office of the Auditor General (OAG) of Botswana was established under section 124 of the constitution as a Supreme Audit Institution (SAI) charged with the responsibility of auditing the accounts of all Ministries and extra Ministerial Departments. In pursuing her mandate, the Auditor General is entitled to access any record within the audited Ministry as she sees appropriate. In fact the Public Audit Act entitles any duly appointed auditor of the OAG to have access to all public accounting books, records, reports and other documents. The auditor may require any public officer to give them necessary information or explanation as they see appropriate to carry out their assignment/audit. Such information may not be in the public domain (sensitive in nature and thus not suitable for public consumption) and hence any threat to expose it puts the Auditor General in bad light to say the least. The damage is even more amplified where the data collected is in relation to security institutions (some of which the OAG does have access to).

By nature the OAG is likely to draw attention/interest from a wide range of societies given the probable information within the custody of the office.

Therefore like any enterprise of its calibre, the OAG is not safe from the security ills that are presently ravaging the global community. For instance the recent, alleged hacking of US elections by Russian hackers is well documented and demonstrates that even the most established and reputable entities are at risk. Cybercriminals are continuously exploring and discovering new and innovative ways to breach the most sensitive and

complex of networks globally. We have also seen the world brought down to its knees by ransomware, commonly known as WannaCryptor/ WannaCry in the past year. This type of attack essentially involves locking a victim's data, usually through encryption, and threatening to publish it if a ransom is not paid.

The OAG was not a victim to the attack however some elements of the Government of Botswana were hard hit and had to completely halt all services. This only illustrates how close to home the attack was. It is imperative that the office should thus be in a position to demonstrate to the audited entities as well as the executive (state) that they have pre-emptively taken measures to secure confidentiality of information in their possession if they are to continue to enjoy this privileged access.

Furthermore as a requirement of the profession, auditors are obligated to avail the basis of their audit report and demonstrate that it is indeed based on relevant and reliable evidence. International Standards on Auditing, to which the OAG prescribes to, specifically advocates that the auditor must document and retain all relevant audit evidence obtained, audit procedures performed on all audit data and conclusions the auditors reached. This denotes to availability and integrity of data collected and subsequent analysis thereof.

Put differently, the auditor is required by law to collect, store and retain information that will assist him/her in making conclusions on their subject matter. This information must be relevant and reliable in that it must be

appropriate and adequate to support their conclusions. The information should be readily available when called for (sometimes in a court of law).

Coupled with the anticipated confidentiality, as discussed above, the three traits (required of the auditor) spell out the CIA triad - the essence of security.

CIA is at the heart of Information Security and it is widely accepted that all that relates to information security transmits to these services (Qadir and Quadri, 2016). The CIA triad is an acronym symbolising Confidentiality, Integrity and Availability. Confidentiality designates the attribute/ quality of information to be protected from unauthorized access. Integrity is the state of information to be accurate and consistent/ dependable. While availability relates to the ability to access information when it is justly needed.

Preparation along these three services gives relative assurance against threats to the security of a system. Threats to information security may include attempts to deny service, disclosure, deception and disruption. This is essentially what the attack WANNACRY crypto ransomware sought to do.

The OAG like other arms of Government operates within one common network, affectionately known as the Government Data Network (GDN), which is managed by the Department of Information Technology (DIT). The DIT is charged with providing the IT infrastructure as well as the security strategies and policies across government. The fact that other departments within Government suffered injury from this attack suggests that the OAG could have easily been a victim. It is thus of supreme importance that the OAG appraise the susceptibility of its data to modern attacks - ransomware.

Chapter 2

2. Review of Literature

2.1. Recent Security Trends

In the recent years security breaches have been steadily on the rise.

According to a report by Identity Theft Resource Center (ITRC) attacks have occurred across industries like Banking, Business, Educational, Government, Military, Medical or Healthcare. As at 2017 data breaches were on the rise with the latest stats amounting to 1579 incidents across industries. This was a 44.7 % rise from the previous year. According to them a cumulative total of 1,076,994,867 records have been exposed since 2005 (ITRC, 2018).

Cheng, et al (2017) illustrates the magnitude of data breaches in the recent years in the table below.

TABLE 1 Massive Enterprise Data Leak Incidents in Recent Years (Data Source Is from the Dataset of World's Biggest Data Breaches ¹⁵)						
Organization	Records	Breach Date	Type	Source	Industry	Estimated Cost
Anthem insurance	78 million	January 2015	Identify theft	Malicious outsider	Healthcare	\$100 million
Yahoo	500 million	December 2014	Account access	State sponsored ¹	Business	\$350 million
Home depot	109 million	September 2014	Financial access	Malicious outsider	Business	\$28 million
JPMorgan chase	83 million	August 2014	Identify theft	Malicious outsider	Financial	\$13 billion
Benesse	49 million	July 2014	Identify theft	Malicious insider	Education	\$138 million
Korea credit bureau	104 million	January 2014	Identify theft	Malicious insider	Financial	\$100 million
Target	110 million	November 2013	Financial access	Malicious outsider	Business	\$252 million
Adobe System	152 Million	September 2013	Financial access	Malicious outsider	Business	\$714 Million

¹ Announced by U.S. Department of Justice.¹⁶

Figure 1 – Recent Data Breaches (Cheng, Liu and Yao, 2017)

The illustration also exhibits the financial loss caused by individual breaches.

These generally run in millions of dollars. The authors go on to make assertion

that breaches in data security can be initiated from an internal source or external source.

Internal security breaches on one hand may include human error or malicious motivated data leaks. One such incident includes the leaking of personal data of over half a million blood donors at the Australian Red Cross Blood Service in October 2016. The incident was linked to accidental or human error (the Guardian, 2016). Internal disclosure of confidential data with malicious intent was demonstrated by the Cablegate leaks of 2010. In this breach classified cables of consulates, embassies, and diplomatic missions around the world were duplicated onto an external hard drive and availed to Wikileaks (TIME.com, 2010).

External data leaks on the other hand are perpetrated by an entity outside/not in the employ of the target enterprise. The recent Verizon Yahoo deal illustrates the damage that can be caused by a leak. In this leak Yahoo suffered two breaches in the years 2013 and 2014, as announced by Yahoo in 2016. Eventually the breaches were cause for a reduction of \$350 million in the acquisition price of Yahoo (TechCrunch, 2017).

In another resource, according to a 2017 data breach instigation report by Verizon, in addition to above industry sectors other industries targeted include Accommodation and Food Services, Insurance, Manufacturing, Public Administration and Retail (Verizon Enterprise Solutions, 2018). The report suggests that the top three causes of breaches are hacking, malware and social engineering and these have been on the rise for the past years.

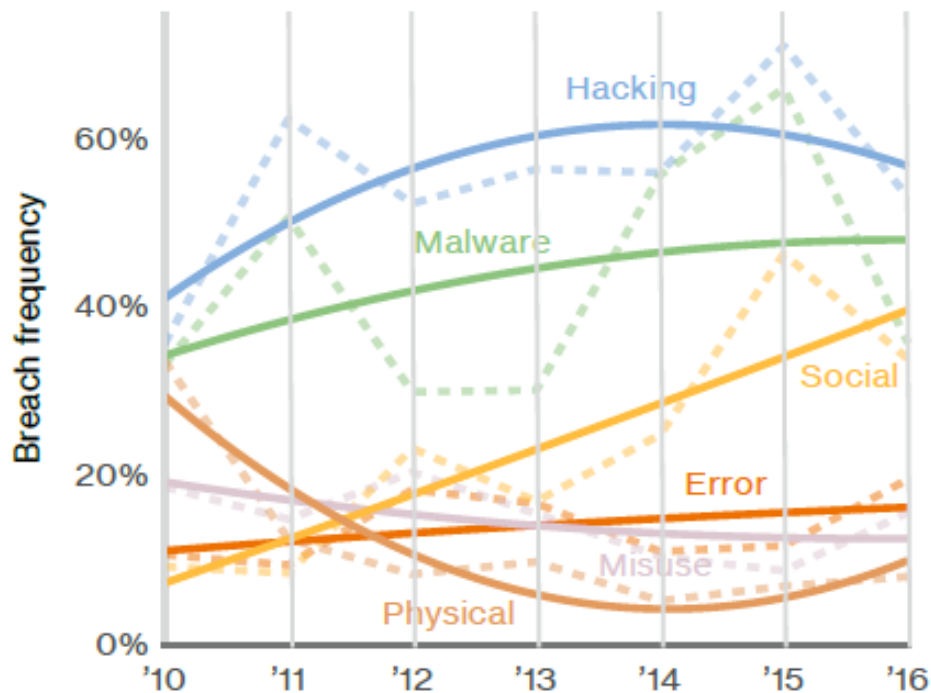


Figure 2 - Percentage of breaches per threat action category over time (Verizon Enterprise Solutions, 2018)

The deduction derived from the above review signifies there is a general upward rise in the number of security breaches in the recent preceding years. These attacks generally cut across industries as no industry is spared the humiliation. Another important point to note is that attacks come in different forms like malware, hacking, social engineering, error etc. They can also be internally or externally instituted. Malware is one of the top forms of attack used in the recent years and continues to grow in popularity.

2.2. Data Centric Security (DCS)

It is clear from the above that security controls are circumvented daily as depicted by many reports. This is notwithstanding the many tried and tested

defences that companies employ to guard against attacks. As a result a new approach to information security termed Data Centric Security is gaining attractiveness amongst many enterprises. The motivation behind this transition is that traditional security defences, like firewalls, access controls and antivirus software etc. are seldom effective against modern innovative attacks.

Brian Mullins writes that, as traditional security approaches are rendered ineffectual, entities are now moving to security models that emphasis data protection as the supreme objective (Mullins, 2016). There is increased need for data-centric security model due to the number of data breaches. Data breaches are indication of the ability of threat actors to circumvent network-level defences. Despite the increased spending in security (in excess of \$86.4 billion worldwide) the number of breaches are not reducing but are rather headed in the opposite direction (Vijayan, 2017).

According to the above author the upward trend is aggravated by the explosion in data at numerous enterprises. As companies collect more and more data from almost all spheres of life, big data and cloud computing are the norm of the day. This coupled with the way data is transferred/shared and distributed among company sites/locations (as well as with company partners/suppliers) means that traditional infrastructure/network restrictions are no longer present.

It is also common for users to access data anytime and from anywhere using portable devices like laptops, smartphones etc. The dawn of bring your own

device (BYOD) has exacerbated the situation further as some devices are unsecure and sometimes malware infested.

The risk is not only in the many ways that distributed data can be accessed but also includes unauthorised use and abuse by insiders. As seen in the previous chapter some attacks can be instigated from within an organisation. This developments thus have the effect of rendering traditional controls ineffective.

Perhaps similar to the above, Oltsik (2015) contributes to the discussion on the reason why traditional approaches are increasingly becoming ineffective against modern sophisticated attacks as follows:

- Traditional approaches focus on networks and endpoints

Conventionally defensive approaches entail technologies like firewalls, antivirus software and anti - malware gateway deployed on networks and hosts. Although they are effective at blocking obvious (recognised) malicious code and detecting uncharacteristic activity, these defences can be bypassed by disguised traffic or activity as normal or authorised.

- Tendency to proliferate data everywhere across the enterprises/organisation

During normal use of data there is inclination to replicate data among destinations, processes and applications. For example employees may copy data for sharing amongst themselves or the developers may copy production data during testing process in order to mimic the

actual live environment. Whatsoever the reason for multiple copies across an enterprise, attackers take advantage of this by finding vulnerable copies of this data.

- Unawareness of where data resides by those charged with implementing security controls

Similar or as an extension to the above the proliferation of delicate data across an enterprise makes it difficult for those charged with the responsibility to institute defences to identify data depositories that need to be protected. In actuality at any given time, security officers may not be aware of where copies of their data is, accessible by who, and whether it's being used for what is intended.

- Most controls are ineffective against internal attacks

Defences are typically deployed to the internal network and hosts from external attacks. A duly authorised member of staff has access to sensitive data through allocated network resources. Animosity may crop up from time to time resulting in a disgruntled employee maliciously acting against his company. Furthermore an employee does not have to be disgruntled to act against his company. Internal members of staff may introduce malware because they wish to disguise or hide unlawful/unauthorised activity by deleting or encrypting data.

Other literature state that in the past, defences like firewalls and IDS offered physical insulation from attackers. Such parameters do not exist anymore as

we find more and more users connecting through mobile devices and public internet (Mullins, 2016).

These issues are thus influential in why Data Centric Security is continually looking attractive. This approach refers to an architecture where the primary focus is data and all efforts are aimed at maintaining data as a permanent asset across dynamic and altering environments e.g. applications. The idea is to protect data wherever it exist i.e. everywhere where it is used, viewed and saved. This is a shift from infrastructure to data-level control (Vijayan, 2017). It is defined as “the enabling and enforcement of data-specific security policies” (Chen, 2012). This encompasses a state where security is provided at the data level by enabling the data to self-describe, self-defend and self-protect throughout its lifecycle – essentially controls that travel with the data rather than being enforced at application level. In this regard the data owner is exclusively responsible for implementing and managing privacy levels and security controls unrelatedly to the application/infrastructure/environment or service provider (Shelke and Sasankar, 2016). Hence for an enterprise seeking to put in practice data centric security model, it will enact measures for regulating underlying access to the data. Consequently that entails being knowledgeable at all times of the destination of data in transit, securing it while in transit. Monitoring and review of user access rights is also vital.

2.3. Ransomware

2.3.1. Contextual Basics

As stated above it is the objective of this study to explore the application of Data Centric Security as a measure against ransomware attacks beyond and above traditional security in protecting data. To address this, first we must understand what ransomware is and how it works.

Ransomware is a malicious code or malware variant designed to quickly lock a computer system or encrypt the data within the computer system once it enters it (Monika, Zavarisky and Lindskog, 2016). The concept of malware has been around for a long time. The most basic form of malware, termed "Creeper" was first seen some 47 years ago in 1971. This period was during the advent of ARPANET, a predecessor to modern day Internet. Creeper replicated itself amongst connected machines and printed the words "I'm the Creeper. Catch me if you can!" on the infected machine (SecureMac, 2017). Although this malicious software was for amusement purposes, it was ground breaking in demonstrating that with networked computing an attack can be launched against a remotely located victim by an anonymous assailant.

Essentially malware, which is shortened term for malicious software, refers to any software written with malicious intent as the motive. It disrupts processes and may collect sensitive data on computer systems. Malware comprises of a variety of unsolicited software like viruses, worms, Trojan

horses, spyware, or adware etc. To gain access to a computer it can assume the form of executable code, scripts, or other programs (En.wikipedia.org, n.d).

Many types of viruses, worms and other self-replicating programs have been seen since this first form of attack propagated on computers (the “Creeper” outbreak). A report by the Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy in 2008 estimated a whopping 59 million users that had been affected by spyware or other types of malware like adware in the United States only. In the preceding 20 years to 2008, malware has evolved from occasional “exploits” to a global multi-million dollar criminal industry (OECD Secretariat, 2008). It is asserted that cyber threats are increasing dramatically with the passing of every year in recent times and the most notable threat is malicious software. Significant malicious software include viruses, Trojans, worms, adware and pornware (Dr GHARIBI, 2011). With these form of malware we now see malicious software now including programs that not only spread by replicating themselves but also mislead users to their true intent. Some are able to gather confidential information about an organisation or individual without their knowledge subsequently sending it to another party without the consent of the owner.

Conceivably the malware most similar to modern day ransomware was first seen in 1989. This malicious software known as “PC Cyborg” (AIDS

Trojan) displayed a message stating that the user's license had expired and payment was required to unlock it (Kansagra, Kumhar and Jha, 2015). Although the malware was ultimately unsuccessful the emergence of the AIDS Trojan established the ransomware threat. The outbreak failed despite occurring at a time when the public was unprepared mainly due to the fact that personal computers were not so pervasive at the time and the internet was not widely used. Also encryption technology was not as advanced at the time and international payments to anonymous recipients were not an easy feat at the time (Savage, Coogan and Lau, 2015).

The next wave of crypto ransomware emerged in the mid-2000s. Trojan.Gpcoder occurred in 2005 followed by Trojan.Cryzip in 2006. The latter used custom-encryption techniques which were frail and easy to overcome. This earlier failures spurred attackers forward causing new versions of this threat (Savage, Coogan and Lau, 2015). The Trojan.Cryzip deleted original copies of data files after archiving them into password protected files. However as luck would have it the passwords could be found in the code of the Trojan itself making it easy to recover the files.

The years that followed saw cybercriminals using bogus antivirus software to introduce code into victim's machines. Once installed the program looked and behaved like genuine security software in appearance and functionality. The result was that the program returned a huge amount of issues. To remove the fake issues the user had to pay a certain fee. This

type of attack proved to be unprofitable as most users choose to ignore the prompts. To address this flaw cybercriminals developed other means to make the desire to act stronger. This shipped in the modern day locker ransomware and crypto ransomware (Savage, Coogan and Lau, 2015). The locker ransomware also referred to as computer locker involves preventing access to the computer by locking the user interface. Usually the locked computer only allows the user to interact with the ransomware thus facilitating the payment of the ransom. These are relatively easy to deal with compared to crypto ransomware as they characteristically deny access to the computer interface, generally leaving the data and core system unaffected. Crypto ransomware (Data locker) characteristically has two functions - encrypting documents or files and locking the computer thus averting ordinary use (Kansagra, Kumhar and Jha, 2015). Hence the files on each drive locally installed, mapped, removable or not are itemised and specific files are encrypted (Saiyed, 2016). However according to Savage, et al (2015), to prevent users from accessing their files the cyber-criminal does not necessarily have to use encryption but the common line of attack usually involves encryption.

The earlier forms of attack involved Encryption of target machine or data. Put in the simplest terms, this is where a message is encoded, using cryptography, into a layout that is not legible or understandable to anyone intercepting or eavesdropping on the communication. Cryptography is the process of applying advanced mathematical

principles on data during storing or transmitting of the data. In the PC Cyborg attack Symmetric Cryptography was used to lock out users from their systems. With this type of cryptography only one secret key is used for both encrypting and decrypting information. It is the simplest form of encryption technique and it is fairly easy to decipher (SSL2BUY Wiki - Get Solution for SSL Certificate Queries, n.d.).

Modern day ransomware has increased drastically in sophistication and involves new attack vectors while applying advanced encryption algorithms. There now exist a substantial range of variants of ransomware including CryptoLocker and CryptoWall and there is no sign of abating mainly due to the ineffectiveness of traditional protection like antivirus (Kotov and Rajpal, 2015). Advanced encryption algorithms, such as the different types of Asymmetrical Encryption, are popular with this modern trend and are particularly difficult to decrypt without the key. Compared to symmetrical, asymmetrical encryption, is considered to be more secure since the key size is much more than the former (Tripathi and Agrawal, 2014). Also known as public key cryptography, it is an improvement on the earlier version Symmetric Cryptography since it boosts resistance to decoding by using two keys. One key is for encrypting a plain text, and is known as the public key, while another known as the secret/private key is used for decrypting the cipher text. View the illustration below by SSL2BUY Wiki for clarity.

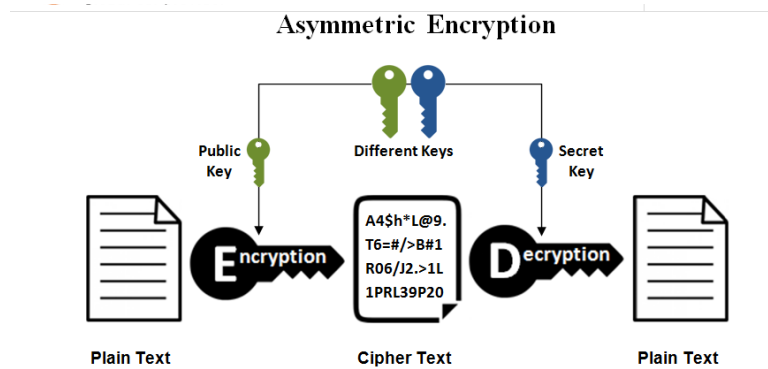


Figure 3 – Asymmetric Encryption (SSL2BUY Wiki - Get Solution for SSL Certificate Queries, n.d.).

With asymmetrical encryption a public key is freely available to the message sender who encrypts the message with this key. On delivery of the message the receiver decrypts it with his/her private key. These pair of keys are related and hence any person who has the public key can encode a message intended for a specific receiver, the one with the secret key. Equivalently attackers utilise this technology to encrypt the victim's data, without the latter's knowledge or consent, and keep the private key secret to be disclosed only on payment of a ransom. Note below a typical ransom note.

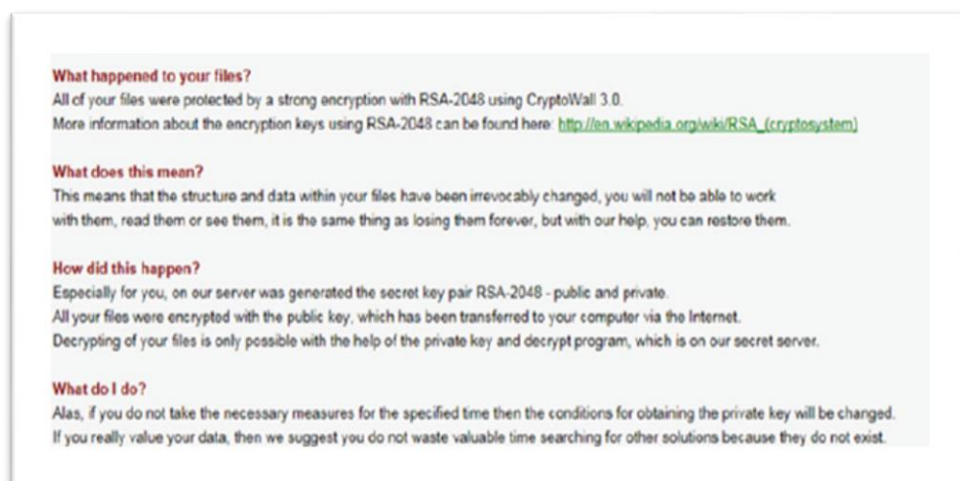


Figure 4 - Typical CryptoLocker ransom note (Saiyed, 2016)

It is apparent from the above review that cybercriminals have taken to using technology that was initially meant for something else to perpetrate criminal acts. Cryptography was originally meant for security purposes. It plays an essential role in securing communication between many parties. It is described as an art, dating back to the roman times, for writing secretly to hide information (Maqsood et al., 2017). Over the years the two widely accepted types of cryptography have been exploited to encrypt information that belongs to another entity without their consent. This broadly accepted types of cryptography are Symmetric and Asymmetric (Mikhail et al., 2014).

It is important to note that modern day ransomware is different from traditional malware in that the main focus is not to circumvent confidentiality but rather to make the victims resources and services (data and computer systems) unavailable. According to Kotov and Rajpal (2015), ransomware does not steal a victim's information but rather makes it impossible to access the information. This relatively easy to produce malware unlike traditional malware does not attempt to remain stealthy by evading detection and stealing sensitive information (Kotov and Rajpal, 2015).

2.3.2. Ransomware Propagation

Over the years cybercriminals have adopted many approaches for the proliferation of ransomware. The list is quiet vast and continues to grow as attackers continue to explore new vulnerabilities. Historically these

criminals have exploited emails and social engineering techniques, downloaders, malvertisement, traffic distribution system (TDS) - the list is long. Savage et al, (2015) depicts the common threats as follows.



Figure 5 – Routes for ransomware to arrive on a computer (Savage, Coogan and Lau, 2015)

Traditionally, email spam using social-engineering themes has been the preferred method for spreading all types of malware including ransomware (Savage, Coogan and Lau, 2015). Multiple infected computers called botnets are used to send the spam. Mauch (2015) also writes that ransomware and its many variants are usually transmitted through infected email attachments or links in malicious emails. Executable zip files masquerading as document files like pdf are attached

to these emails or a link leading to a site hosting an exploit kit. In this regard social engineering themes like mail delivery notification, utility bills, job applications, purchase orders or invoices, police traffic offense notifications etc. are used to trick users into installing the ransomware.

Downloaders are another tactic that cyber-criminals have adopted for perpetrating attacks on unaware victims. These are computer programs installed on computers that serve the purpose of downloading other software. They facilitate the download of peer files and they do not in themselves, as standalones, have the complete content of what the user is downloading. Hence in an attack the downloader would download secondary malware onto the target machine (Savage, Coogan and Lau, 2015).

Similarly in recent years, there has been a trend of attracting users by posting malicious advertisements (malvertisements) onto legitimate websites. Following such a link redirects the user to a compromised site. Likewise ransomware attackers have resolved to procure redirected web traffic from vendors of Traffic Distribution Service (TDS). TDS are systems that redirect users to content that best suits their likings based on their demography or characteristics e.g. location, language, gender and device used etc. It is a legitimate means of making money on the Internet and involves directing traffic to cash in on referrals. The aim is to lead unknowing users to specific sites. Moreover TDS are useful to cybercriminals as they permit them to determine traffic type and the type of extortion

techniques to deploy thus allowing them to maximize gains when directing users to certain malicious sites (Goncharov, 2011).

2.3.3. The reality of ransomware

Regardless of the methodology used, what is clear is that ransomware has become the malware of choice for many cybercriminals. A 2016 report by Deloitte states that there has been an upward surge in the number of infections as well as variants of the malware. There is no sign of slowing down in this trends with a reported figure of 4000 attacks per day in 2016. This represents 300% rise over the 1000 cases per day in 2015.

Currently there are hundreds of ransomware variants in circulation (Archie, Turner and Boynton, 2017). Also the sophistication with which ransomware has changed is indicative of how lucrative culprits perceive the trade to be. For instance many ransomware variants are available for purchase online and they offer strong encryption algorithms that cannot be deciphered.

The creators of ransomware would not be spending so much time and effort if there was no money to be made. The report above states that more than \$325 million was extorted in 2015 from the United State alone (Deloitte Development LLC, 2016). Richard Curtiss writes that ransomware is more prevalent than people realize. This is because most organizations would rather pay the ransom and avoid dealing with the publicity of being victims (Curtiss, 2016). Deloitte also writes that financial gain is the

prime motivation and pay-outs can only succeed in encouraging more criminals (Deloitte Development LLC, 2016).

Another reason why culprits perceive ransomware as appealing is that it offers a risk-free means of extorting money. Kotov, et al (2016) likens this trade to online black markets. Perpetrators are continually finding ways to receive payments while maintaining anonymity by enlisting traffic anonymizers and anonymous currencies. TOR and Bitcoins are examples of these. TOR is an open network and software that conceals the identity and online activity of users from surveillance and traffic analysis. While Bitcoin is a digital currency, widely used worldwide, that allows peer to peer direct transacting with no middle man. Hence they cannot be traced.

It is no wonder that ransomware attacks are on the rise. The reality is that no one is safe. One Computer Security Officer writes that organisations need to evolve to keep up with the quickly changing ransomware landscape. This entails robust business continuity and disaster recovery plans (BCP\DRP). If a business has not updated its BCP\DRP in a while then it should invest in a Bitcoin account (Carder, 2017).

2.4. Data Centric approach to Ransomware

As suggested to, in the previous sections, ransomware typically inhibits access to data. Ransomware is thus a threat to availability of data. The objective of the typical ransomware is not to steal information and breach

privacy. Deloitte equates ransomware as holding your data hostage (Deloitte Development LLC, 2016). Curtiss (2016) writes the risk to confidentiality is not affected by ransomware nor does ransomware require the selling of information in order to profit. Saiyed, C. (2016) also writes that culprits do not attempt to extract and sell data but rather encrypt data at rest. It is thus plausible that any attempt to protect one's data from ransomware should focus on maintaining availability. However there has been reports of ransomware that threatens to publish user files. An article by Constantin (2015) reports of a novel ransomware termed Chimera that claims to have the capability to publish files on the internet unless the ransom is paid. According to him the reliability of this threats has not been verified but the prospect is quiet daunting. In another commentary in the Mailonline publication user of android systems are warned of a new ransomware called LeakerLocker that threatens to disclose images, messages and browsing history of users. The report states that the software is being propagated through fake apps on Google Play Store. Once it infects the user's system the malware claims to have backed-up their data to the cloud and while it also encrypts the local data. Failure to pay would result in publishing of the backed-up data (Collins, 2017). Other publications also warn of a shift in the digital extortion trade where perpetrators are showing more aggression by threatening to leak data rather than just hold it for ransom. Although perpetrators have not made good on their threats the risk to

confidentiality cannot be ignored. It is real and requires significant consideration in any attempt to defend against ransomware.

As a defence against ransomware, the FBI recommends extensive business continuity planning that includes a comprehensive system of backups and security incident response. These attempts are aimed at securing availability of data even in the midst of attacks. Other literature also recommends regular backup of servers and client computers, installing up to date patches and plug-ins, using sound anti-virus software and adopting a policy of scanning inbound emails for threats (Symantec, 2016). In a similar article by Sherman the author adds end user education, blocking end users from installing files, limiting the spread of malware by restricting user access to mapped devices and installing and configuring host intrusion prevention (IDS/IPS) (Sherman, 2015).

It is undeniable that these solutions are effective in mitigating the ransomware threat. However some of these defences inherently have weaknesses that cyber-criminals seek to take advantage of. For example loss of data due to time lag between the backup files and production data. An enterprise may be more willing to opt for paying where a substantial amount of data is generated between backup schedules. Also backups may not be effective against malware where a machine has been compromised. Viruses and Trojan horses can delete both the original data and backup especially where the backup can be accessed from the device being protected (Antoniou, 2014).

Where backups are stored within the same premises of origin there is high risk of destruction by the same ruse that may affect the original data. To mitigate these most enterprises may deploy offsite storage. However these may be costly and may result in substantial time lag. Lastly where laptops are utilised ubiquitously new challenges are introduced to the business backup model. For instance the unconventional business hours and the mobility of the device means the backup schedule may be missed as well as exposed to unprotected networks (Antoniou, 2014).

Staff training is another defence that is highly recommended for the fight against ransomware. This is based on the premise that the user is the weakest link in any security strategy. As noted above the majority of ransomware propagation exploits emails and social engineering techniques, downloaders and malvertisement. These methods take advantage of the user's unfamiliarity with risk. Furthermore as indicated in the literature review above, voluminous security breaches were due to human interaction with computer systems. The 2015 Data Breach Investigation Report by Verizon `states that it takes only 82 seconds for phishing attempt to get its first click after being sent (Verizon, 2015). Hence the importance of user security awareness at all levels of the organization cannot be overstated. This can be done through continuous education programs. These are effective at informing users about the latest security best practices as well as changing the general attitude/culture towards security. However aggrieved personnel may still propagate malware

internally. Hence it is important to put in place monitoring and audit of all activity.

Other defences include maintaining a current patch level for operating systems and applications, using Host Intrusion Prevention, and content scanning of mail servers. However these solutions are reliant on weaknesses that have been identified and patched, and code or activity that is recognised or previously termed malicious. In other words they are only good at stopping something they have seen before. Ransomware attacks are tailored and unique every time they are propagated (Orlando, 2016). Oltsik (2015) states that although they are effective at blocking obvious (recognised) malicious code and detecting uncharacteristic activity, these defences can be bypassed by disguising traffic or activity as normal or authorised use. Hence for this methods to work a lot of work has to be done in the background to keep up with current developments in the cyber-security landscape. Even then the task is not easy as we continue to witness new and improved ways to deliver ransomware tailored for bypassing this defences. For example the actual code of the ransomware is usually encrypted itself and consequently the scanners cannot open them to view the code. Furthermore in the recent past we have witnessed an overabundance of tools and delivery systems for facilitating malware development, being sold in the dark web (obscured collection of websites) (Espinosa, 2016).

As noted previously the primary objective of any initiative against ransomware is to protect the data and ensure its availability. However the risk to confidentiality cannot be overlooked as depicted by the new threats introduced above. It thus follows that the right data security intelligence tool needs to be deployed for identifying the right security model/mix that provides a comprehensive approach to risk management and value for money (effective, efficient and economical in proportion to the threat). The Institute of Risk Management (IRM) recommends that the principles for effective risk management are that the activity should be proportionate to the risk, aligned to other activities, comprehensively address risk and must be dynamic and responsive to change (IRM, 2018).

It is ostensible from the review above that companies need to know where to focus their efforts in the fight against this new threats. An effective approach is to deploy a data centric model that will highlight the areas where emphasis needs to occur as well as consider the business process models. That is to say security is viewed as an activity that takes into consideration the intrinsic value¹ and business context² of the data. A detailed approach to implementing data centric security (DCS) is offered in the write up by Oltsik (2015). According to him an entity must have tools for Data discovery, Data classification, End-to-end visibility, and Data security analytics for risk management. Similar to the above a SANS Institute article quotes the director of the institution, John Pescatore, as

¹ This indicates the value placed on the data by the entity

² Refers to how the business elects to use its data.

noting that DCS is more than just data encryption and masking but rather involves initiatives for data discovery, data classification, access control, authentication, user and usage monitoring, and auditing (SANS Institute, 2015).

2.4.1. Data discovery

This is the discovery of where an organisation's sensitive data is. The process helps the entity comprehend and fully understand the location, volume, context and risk associated with all its data - including unstructured and remotely located data e.g. data on the cloud. The insights gained from the exercise will help the entity define patterns and trends in data that will guide subsequent activity like categorising it and prioritising effort to protect it (O'Leary, Ferreira and Grahn, 2016).

2.4.2. Data classification

Having discovered all the data under its ownership the entity proceeds to separate, categorize and divide the data into predefined clusters in accordance to data set requirements for the realisation of business objectives. In other words the data categorizing is based upon drivers signifying the business context (M. Ferrell, 2008). This drives towards a prescriptive characterization of how, when and by whom the data is sanctioned to be used in light of the business context.

The segregation also includes the association or linking of data that are prone to similar risk. (O'Leary, Ferreira and Grahn, 2016). The value of data plays an important part in terms of which data is likely to attract attention as compared to less valuable data. The classifications in turn inform the entity on where to prioritize effort with regards to protection. Data that is sensitive will call for extra security controls and oversight as opposed to less sensitive data (Oltsik, 2015).

Data tagging and watermarking may be utilised for rapid identification at a later time. The tagging echoes the security categorisation and any other information associated with the data. By thus tagging, the resources that transmit, process and store the data are accordingly associated with the risk allocated to the data class. Consequently the controls for mitigating the risk are applied to the resource.

2.4.3. Deploying Defences

In addition to data discovery and classification, a lot of literature have differing interpretations of the unique steps involved in the data centric security approach. In my view these are essentially differing attitudes towards implementing controls³ in light of the preceding steps (the risk identification and analysis processes above – Data Discovery and Classification). Collectively stated they involve steps for the creation of policy and deployment of mitigating controls like access control, authentication, encryption, user and usage monitoring, and auditing

³ security mechanisms

etc. To put things in perspective these are controls fine-tuned to suit/address the business context and the intrinsic value of the data (as defined by the business owner of data in the preceding steps). The approach is contrary to the traditional protection that limits access to IT resources (focus on users and roles).

With data centric approach controls beyond the traditional protection are added around the data resource e.g. limiting access to just viewing and not copying (M. Ferrell, 2008). Nonetheless this should not be viewed as controls that are added as an afterthought or after the perimeter security has been established. Security should rather be designed and built from the data out to the perimeter (Bilger et al., 2006). Figure 6 illustrates the typical; approach. However in light of the authoritative nature in which security (in terms of firewalls, intrusion detection systems etc.) is bestowed on all government departments from DIT⁴, the inverse will have to be adopted. In such cases Bilger et al. (2006) advocates for not discarding traditional security architectures but rather modifying them in light of the fundamental data within the protected resources.

⁴ The Department of Information Technology (DIT) as the entity in charge of IT Governance, managing the government data network and data centre for most of government entities.

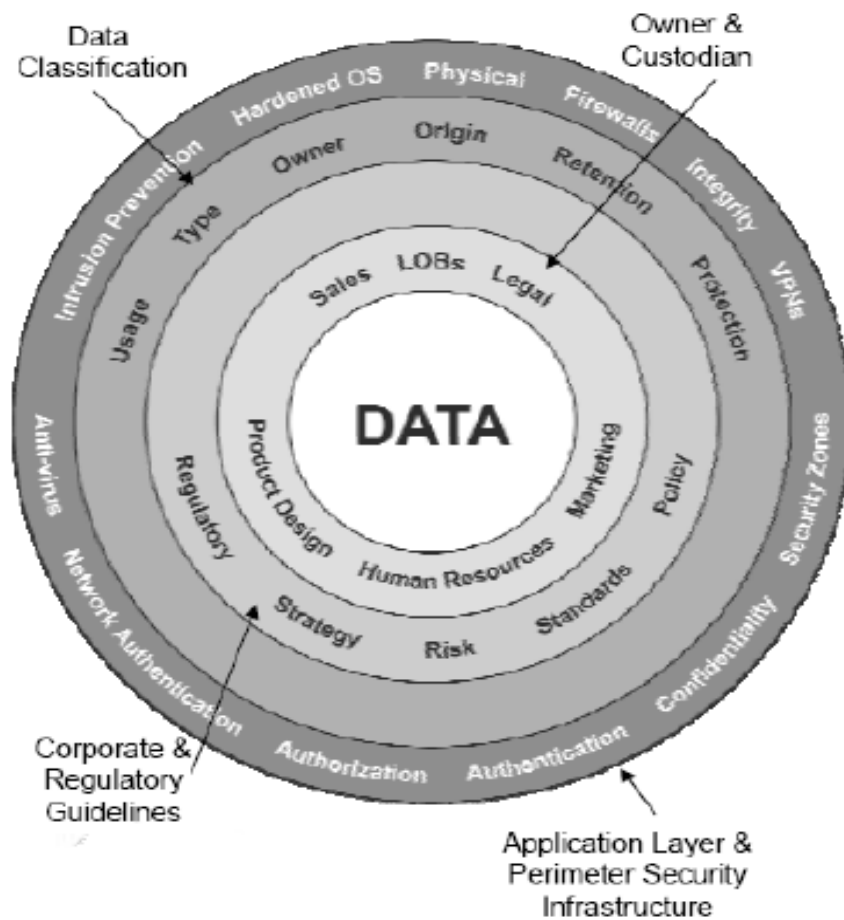


Figure 6 – IBM's Data-Centric Security Model (DCSM) as presented by (Bilger, O'Conner, Schunter, Swimmer and Zunic)

In the data centric approach and as illustrated in figure 6 a data owner or custodian is responsible for the definition of data classifications including requirements for data usage, lifetime and protection. This is done in consultation of regulation, strategy and standards etc. Consequently the security measures as illustrated in the last layer are put in place to address the requirements that have been defined.

Another literature by Booz Allen Hamilton (2015) describes the data centric approach as a process that involves an organisational risk assessment, leading to the design of a cyber-solution blueprint, and the deployment data de-identification solutions. According to them the blueprinting comprises of the process for mapping people, process, & technology. This is where the roles required are defined as well as specifying process and workflow requirements. Technology for data protection while enabling the requirements are identified e.g. encryption and tokenization. The author proposes specific approaches to documenting the processes/ workflow requirements like RACI charts as well as the analysis of the technology alongside the capability and people skills necessary for the deployment.

The blueprinting is followed by deployment of data de-identification solutions. According to them this is the process of neutralizing data theft by making the data categorically valueless to an attacker. This can be done by encryption and tokenization. Encryption has already been described above as the process of encoding a message or data to make it literally incomprehensible to an unauthorised individual.

Tokenization involves the substituting of protected data with unrelated and non-sensitive equivalent known as a token. The token has no meaning or value to the one eavesdropping. Review figure 7 for examples of encryption and tokenization, where FPE and SST denotes encryption and tokenization respectively.

Name	SS#	Credit Card#	Street Address	Customer ID
James Potter	385-12-1199	37123 456789 01001	1279 Farland Avenue	G8199143
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348
Brent Warner	604-41-6687	4929 4358 7398 4379	1984 Middleville Road	G8888767
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273

Name	SS#	Credit Card#	Street Address	Customer ID
Kwfdv Cqvzqk	161-82-1292	37123 786354 51001	2890 Ykzbpoi Clpppn	S7202483
Veks Iounrfo	200-79-7127	5587 0856 7634 0139	406 Cmxto Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 9209 2367 2829	1498 Zejojtbbx pqkag	G8265029
Eskfw Gzhqlv	178-17-8353	4929 4333 0934 4379	8261 Saicbmeayqw Yotv	G3951257
Jsfk Tbluhm	525-25-2125	4556 2545 6223 1830	8412 Wbbhalhs Ueyzg	B662594

Figure 7 - Format-Preserving Encryption (FPE), and HPE Secure Stateless Tokenization (SST) by Booz Allen Hamilton

2.5. Proposed Model to Data Centric Protection at the Office of the Auditor General

It is clear from the multitudes of literature that the approaches to data centric protection vary from one establishment to the other. In light of the above literature, the approach that I propose for the purpose of implementing a data centric approach at the Office of the Auditor General is presented as follows. It is meant to access if the OAG is doing enough to protect its data in terms of the current challenges⁵ faced given its information assets. The approach will attempt to ascertain if the office has previously taken note of the threats to the security of their data and accordingly mitigated them.

2.5.1. Identification of Critical Assets and their Protection

⁵ It might not be possible to identify all possible challenges to data security however the focal point is ransomware attacks in light of the recent outbreak of which the Government of Botswana was affected.

The first proposed step is to identify information assets of the OAG.

These are then prioritized in terms of their criticality to the mission of the organisation. Subsequent protection should thus commensurate with the criticality of these assets.

2.5.1.1. Threat Intelligence

SANS Institute describes threat intelligence as a process for determining the threats to an entity based on existing data points and how the data relates to the entity (SANS Institute, 2016). Adequate protection will not exist without sufficient comprehension of the threats to the audit industry or supreme audit trade. Analytical inquiry meant to uncover the threat setting of the OAG is central to adequate protection.

Inquisitive thought on rivals to the enterprise, their motivation and technologies they use will guide future security initiatives.

2.5.1.2. Security Philosophy and Mind-set

As indicated above the principles for effective risk management are that the activity should be proportionate to the risk. Where the threat is perceived to be high it will normally necessitate high expenditure on mitigating controls. Such expenditure is controlled by management of the entity. There is need to have management buy in for effective security strategy. ISO 27001 states that executive management involvement is vital for the success of any security program. The security culture should cascade from the top downwards. Those lowly placed are likely to take security issues seriously if their management

demonstrates dedication and participation. Management may demonstrate their security culture through policies and standard working procedures which in turn reveal ideal ethics and conduct.

2.5.1.3. Deploy Protection

2.5.1.3.1. Process and Technology Provisions

This entails the appraising of existing processes and technology with the view of enhancing them to ensure relative assurance of protection in light of the identified risks. This may entail process reengineering to reflect ideal secure processing or data handling. New procedures may be introduced to address a certain risk e.g. steps for ensuring core platforms and technology are upgraded/patched as advocated for with ransomware risks.

2.5.1.3.2. Incident and Disaster Management

In the event of an attack a well thought out and tested response plan may be the difference that keeps the entity operating as a going concern. The OAG should have in place incident identification and response plans for active crisis handling. These should take on board all the relevant stakeholders or departments and prescribe an up to date contingency plan.

2.5.1.4. Monitoring and Detection

A thorough self-assessment of the security programs we have implemented is important to ascertain their effectiveness against threats. This will entail not only compliance to policy or standards but will also determine the entity's ability to stay abreast of new developments/security events. Of course methodology must be in place to advance awareness of those affected by security events, the user. This may necessitate timely and regular training programs for the users.

2.6. Conclusion of literature review

In conclusion it can be deduced from the various literature that the common factor and undoubtedly the most crucial process to data centric protection is the accomplishment of a full/comprehensive understanding of the data requirements and the processes involved in the use of that data in an entity. The entity's data flows and business needs from the data are derived from the dedicated enquiry and identification of enterprise needs from data. Furthermore there should be detailed documenting of the how and where the data can be compromised. The derived knowledge will allow a complete view and attempt at defining mitigating controls.

The data is the focal point in this regard thus highlighting the need to protect data throughout its entire lifecycle⁶. It is quite clear from the literature review that security approaches that focus on the perimeter security have attempted to lock out cyber criminals from accessing the network. This is reported to be less than effective as evidenced by the numerous security breaches. However this does not mean these approaches should be abandoned. It is advocated that additional protection should be incorporated alongside these technologies. However the question is, where the risk to data is identified as ransomware, can data centric approach offer better/improved protection. It is acknowledged that data centric approach will not guard against the possibility of a breach of the network. The drive therefore is the safe guard of data in the midst of a break-in/penetration of the network defences.

Like other malware, ransomware has to be inserted in a system to cause harm – a situation where the network security has failed.

It is testified that the purpose of ransomware is to target availability of data more than any other element of the CIA triad e.g. confidentiality.

However new reports have indicated a new upsurge of ransomware that claim to be capable of disclosing data over the internet. This makes the data centric approaches relevant against ransomware.

Also it is envisioned that a formal approach at data discovery and classification will afford the entity a controlled, structured and

⁶ Encompassing the process stage at which data is captured, throughout its movement across the enterprise

balanced look at all that needs to be protected hence opportunity to implement controls where there is real value. Contrastingly with traditional methods there is temptation to deploy defences with the hope that they will protect all that is contained without consideration of all the forms and locations of data. To reiterate this, it is acknowledged that the current recommended defences against ransomware like backups are effective. Nonetheless a backup will not serve much purpose if it does not include all the stores and movement of data. Other defences include maintaining a current patch level. These may not be effective if the exercise excludes other data stores e.g. workstations.

Also it is widely accepted that users are the leading most vulnerable point of penetration of any security enterprise. Any data security strategy that does not consider the human aspect will not be successful. Security controls can be unintentionally or deliberately circumvented by human contact with applications/systems. Thus timely and continuous education of users at all levels of the organization is essential. This is even more so since it is reported that many attacks lure users by using social engineering tactics through emails, downloaders and advertising.

Lastly, ransomware is here to stay as symbolized by the significant rise in the number of variants and outbreaks. The ease with which ransomware variants are developed as well as the ease to receive payments while maintaining anonymity, can only contribute to

increase in cases. The reality is that no one is safe. Organisations need to evolve to keep up with the quickly changing ransomware landscape. This means exploring new unconventional approaches to security like data centric security.

Chapter 3

3. Methodology

3.1. Introduction

This section expresses the approach adopted in carrying out the dissertation. Both questionnaires and interviews will be used to compile the data from all levels of the office involved in the core business or auditing. It is important to note however that participation is not limited to only core business but also the support staff charged with supporting the enabling environment, infrastructure and applications also known as IT Support Unit.

The Office of the Auditor General comprises of essentially two main functions, namely support and the auditors (which I have termed core business above). Support is headed by one executive manager called the Corporate Services Manager. Under this manager comprises of the units for Administration (charged with human resource, facilities and transport management), Accounts (financial accounting and management) and IT Support. The latter is responsible for advising management on issues of IT Governance, strategic growth and IT security/risk management. The unit is resourced with members from the mother entity DIT. It is thus habitual for IT Support to call on DIT for escalation of certain issues as well as support beyond their control like issues of policy and infrastructure growth e.g. expansion initiatives or development of new systems.

The other function, core business, is made up of auditors and there are currently at least three types of auditors. First is the financial auditors which are further classified into those that audit Central Government, Local Government and Parastatal entities. All of the above have their own Executive Manager. Their main responsibility as financial auditors is to perform the regulatory audit/statutory audit whose main objective is to report on truth and fairness of financial statements of government entities and their agents.

Second, after the financial auditors, we have the Performance auditors whose task is mainly the review of development projects across government. They share executive leadership with the parastatal auditors. Last but not least we have the Information Technology Auditors. In the advent of widespread and pervasive automation of systems across government there is need to review IT risks and controls. Basically IT Auditors test the application and performance of controls to assess how well they work in mitigating Identified risks.

In addition to the above functions the OAG has two standalone functions reporting directly to the Auditor General (AG) and which are very important to the pursuance of the mandate of the OAG. They are perhaps the control and monitoring tools with which the AG keeps abreast of performance and quality of the office. They are respectively the Performance Improvement Coordinator and Quality Assurance manned by two individuals.

3.2. Data Collection Techniques

To achieve the objective of the study, representation from all the identified groupings is pursued. At least three members from each unit in core business/auditors was sought. These are mainly members at operational level tasked with performing procedures. Auditors, otherwise known as the data collectors, are the first contact with data at the client/auditee. Their handling of data is important to the entity's exposure to risk.

In addition management of each unit is included as the ultimate signatory/authority signing off on work performed. Ideally they are in position to offer insight on what constitutes impeccable performance and record of work done. For example in the case of the auditors who are expected to document work done as well as support their findings with appropriate evidence, a member from the executive management must ultimately review (after two stages of review) the work done and decide on whether it is adequate and meets the standards required of it. Thus they make decisions on what data should exist and in what form. The Executive Management is also responsible for instituting guidelines on issues like classification of data as well as how it should be handled. IT Governance is also their responsibility. In this regard IT Governance entails, but not limited to, the delivery of value to the organisation and mitigation of IT risks. Hence they drive the strategic alignment of IT with the business, and embedding of accountability into the organisation so as to mitigate IT risks.

Lastly representation from IT Support as well as their management is required. The operational staff should give an insight on the mechanisms implemented if any and overall success in mitigating risks or keeping threats aloof. Their management who is ideally the definitive advisor to the office on IT issues including security is vital to the study.

3.2.1. Questionnaire Design

Specific questionnaires will be designed in order to collect appropriate/relevant data from the above representations. For the auditors the questionnaires will cover their awareness of any measures instituted for the purpose of protecting data and any related training imparted to them.

3.2.2. Interview

Given the small number of management, interviews are preferred over questionnaires. The reason is that this form of enquiry is likely to obtain the most response given the busy schedule of the respondents. Also with interviews follow up enquiry is possible hence enabling thorough exploration of possible responses. Depending on whether core business management or support management the line of questioning differed. For auditors, an indication of the overall work done in terms of regulation is sought. This includes issues of classification and sharing of data among

security levels. Their expectation from the auditors (data collectors) in terms of what should be on file will be enquired on.

With regards to support management the security strategies adopted for the protection of data is explored. Their performance monitoring tools as well as key performance indicators will be investigated. Issues like problem and incident management will also be enquired on.

Lastly the DIT as the entity in charge of IT Governance, managing the government data network and data centre for most of government entities, will be interviewed.

3.2.3. Data Collection Methods

The human resource unit maintains an establishment list of the entire Office. This is essentially a staff list detailing all members of staff, their levels and departments. All filled up positions as well as vacant posts will be identified. Those on acting appointment for vacant positions will also be identified and accordingly included in the study.

3.3. Research Questions

As noted, in order to obtain relevant response from all types of respondents (with different properties), differing enquiry specific to the level or area of operation, will be carried out. In no chronological order, the different lines of enquiry are meant to address the following areas.

- Whether ransomware is a viable threat

- In Botswana Government?
- In the Office of the Auditor General?
- The statistics of the attack (how hard were we hit)
- Current Defences against ransomware
 - What defences are in place against ransomware attacks in Botswana Government?
 - In light of the recent ransomware attack within government what steps has the OAG taken to secure its assets?
- Sufficiency of the resultant security strategy given the OAG's unique environment.

In attempt to substantiate the OAG's unique environment relative to the current security strategy the following questions need to be addressed:

- Threat intelligence at the OAG
 - What steps were taken to identify threats and (or) risks to the OAG's mission?
 - Are cyber threats considered a plausible threat to the OAG?
 - Security Philosophy and Mind-set of the OAG – what is the OAG's attitude towards cyber threats?
- Does the resultant security strategy include:
 - An incident detection and disaster management plan?
 - Procedures for timely upgrading and patching of core platforms and technology?

- Has OAG identified, prioritized, and secured mission critical assets?
- In the view of stakeholders (management and end users) are these assets adequately protected?
- Is client or audit data a mission critical asset?
- Does the work flow and handling of data take into consideration the security (confidentiality and availability) of data?
 - Are there policy and procedures in place to ensure audit data is secure during:
 - Collection (input),
 - processing (analysing/audit testing or audit procedures)
 - transmission (in transit)
 - Storage
- Are there documented as standard operating procedures?
- What initiatives have been taken to apprise staff of policy/procedures?
- Are there measures in place to advance awareness of security events/trends and accordingly respond to them (area watching/monitoring)?

3.4. Sampling

Stratified or proportional random sampling will be done for operational staff carrying out the audits (auditors). This method of sampling involves dividing

the population into smaller groups known as strata. The strata comprises of members of the same/similar attributes. A random sample is then selected from each of the strata. This method is preferred as it will facilitate the inclusion of all types of representation.

In the case of the OAG there are at least three levels involved in an audit at any given time. First is the auditor assigned to data collection of the area/component (of the audit) allocated to him/her. They perform audit procedures (interrogatory work) and compile their working papers (typically a summary of work done along with supporting evidence).

In the interest of quality (and to comply with audit standards – ISA 220) the working papers or data collected is presented to the next level on the hierarchy, who performs review of work performed and signs off on it. This continues likewise to the next level and ultimately reaches the executive manager responsible for the audit area. A typical team will comprise of the auditors, team leader and section head.

As stated above, a response total of at least three members is sought from each unit: Parastatal, Performance, Local Government, Central Government and IT Audit. This will make five (5) first-line auditors, five (5) reviews (team leaders) and five (5) second reviewers (section heads).

No sampling will be done for top management. That is to say all the top management positions that are currently filled will be interviewed. These are inclusive of managers in charge of audits as well as support. In total three executive managers in charge of audit (Parastatal/Performance, Central

Government and Local Government Audit) as well as the Deputy Auditor General (in charge of IT Audit), Corporate Service Manager, Performance Improvement Coordinator and Quality Assurance Manager. This amounted to a total of seven (7) managers.

Lastly a representative will be sought from the DIT. This should be an official with authority and well-informed about the DIT's security strategy across government departments. Any formal agreements between DIT and other government departments will be pursued and inquired on to verify the extent to which DIT is involved in the provision and management of security.

Chapter 4

4. Presentation of Results and Data Analysis

This chapter presents the results of the data collection exercise as well as the analysis of the data that was collected. At least three main groups were identified for the purpose of this study, namely Management, Auditors and IT Support. In addition, the DIT was interviewed as the government component mandated to provide IT governance and security across government.

The auditors were further classified into five groups being Central Government Financial Audit, Local Government Financial Audit, Parastatal Financial Audit, IT Audit and Performance Audit.

4.1. Survey Response

4.1.1. Management

The first line of inquiry was directed at Management. Interviews were carried out for this class as per Annexure 1. As stated above these were members of staff with the authority to pronounce policy and standard working procedures. Also they are accountable for prescribing guidelines on data classification and desired behaviours. A total of six (6) individuals was projected as at the time of planning the survey. This represented the number of divisional managers for the auditor divisions above and support managers. A total of only three (3) members could be interviewed giving a response rate

of 83%. This was owed to the fact that one member had recently retired from office and their positions had not been filled.

4.1.2. Auditors

Three members from each of the sub groups of auditors was issued a questionnaire making a total of fifteen (15) copies. These are mainly members at operational level tasked with performing procedures. Auditors, otherwise known as the data collectors, are the first contact with data at the client/auditee. Their handling of data is important to the entity's exposure to risk. A copy of the questionnaire issued to the auditors can be found in Annexure 2. A response rate of 86.67% (thirteen out fifteen) was attained.

4.1.3. DIT and IT Support Management

The Chief Systems Analyst being the manager in charge of ICT at the OAG was interviewed (Annexure 3). This is the individual tasked with coordination and implementation of DIT initiatives within the entity. He advises management on ICT investments and ensures adequate alignment to the corporate strategy. The device of an ICT strategy covering IT security is within his mandate.

In addition, a telephonic interview was carried out with a representative of the DIT. The individual was well placed to apprise the study on the security initiatives that the department has adopted in light of the ransomware outbreaks in 2017. The questions are as in Annexure 4

4.2. Survey Results

The results of the survey are presented in the following section.

4.2.1. The role of DIT concerning security at OAG

First and foremost it was important to establish the relationship between the OAG and DIT. This was meant to clarify responsibilities and jurisdiction of the latter with regards to security.

- i. First the DIT was asked if there are any Service Level Agreements or Memorandum of Agreements between them and other government entities.

To this the representative of DIT responded that currently there are no formal agreements with other government departments. However he added that there is currently an ongoing project termed GDNProject (Government Data Network Project) which is tasked with evaluating strategy, governance and policy issues. Part of the deliverables are to adopt procedures for managing agreements with their clients.

- ii. In the absence of such formal contract the DIT was asked what their role is regarding security in government.

In a nutshell the DIT has the responsibility of maintaining a Data Centre for most of government entities. In extension they have to provide and manage the Government Data Network. As such DIT is responsible for the security strategy and framework for security across government.

- iii. The instruments in place to verify performance or delivery on their obligation were enquired on.

Nothing is in place currently. However as mentioned above a project is in progress where such issues will be scrutinized and addressed.

4.2.2. The role of the DIT attaché (Chief Systems Analyst) at the OAG

As indicated in the write up above there is a designation called Chief Systems Analyst, staffed by an attaché from DIT, in every Ministry. It was thus necessary to put things in perspective as to what their role is at the Ministry, relative to the role played by the DIT.

- i. What is the role of the Chief Systems Analyst (CSA) at the OAG?

The role of the CSA is to advice management (OAG) on IT governance issues, assist management secure their IT infrastructure and information assets. This means they are tasked with recommending IT strategy that is aligned or will support the enterprise strategy. In addition they are in place to liaise with DIT for the project management of development projects.

- ii. What is the role of the Chief Systems Analyst In relation to the DIT?

The CSA is a representative of DIT within the Ministry and is required to advance the implementation of DIT strategy and policy. They are typically the eyes for DIT in terms of area watching. This entails they are to actively report and escalate any issues regarding security. Likewise the DIT expects them to

implement any security initiatives and contingency response recommended by DIT.

4.2.3. Ransomware a viable threat in Botswana

According to unsubstantiated reports the 2017 ransomware outbreak, termed WannaCrypt, found its way within the Botswana Government. The next line of questions are meant at verifying the allegations as well quantify the extent to which we were affected. Subsequently, it is enquired as to whether future risk still exist.

- i. DIT was asked if any of the government entities were affected.

A few systems were affected by the outbreak.

- ii. The representative was asked to rate the extent to which we were affected in terms of the impact on computer resources/services.

Mainly the affected were able to recover relatively quickly (1 day) from backups. The damage suffered was mainly system downtime and data loss (relatively recent data not backup). Furthermore it must be noted that one of the DIT's impromptu steps to arrest the situation, was to discontinue the internet across government. This meant that a lot more systems were affected and service was interrupted.

- iii. DIT was asked to substantiate their claims with statistics or a report?

Although a formal report was not prepared with regards to specifically this attack, the DIT would be reluctant to share it externally. This is mainly for security resolutions and also the reputational damage that is like to come with exposure of such information. The statistics however do exist but for the same reason they cannot be availed.

- iv. Their opinion, as to whether ransomware is currently a significant threat to government was pursued.

The DIT responded that they do feel that ransomware is a threat given the current trends in cyber world. The rate at which new version are developed means that a lot of work has to be done on a daily basis to keep up. DIT however has deployed anti-malware software to help curb the risk.

According to the CSA, the ransomware threat is real. Even with the current measures in place, the possibility of this malware evolving into a new unfamiliar form is real.

- v. In your assessment what was the root cause?

According to the DIT the reason why the malware found its way into our network was because the users are not sensitised to avoid opening links and attachments from unknown sources. Also it has come to DIT's realisation that users are in the habit of downloading files from questionable websites, especially those that are not work related. In addition besides the existing policies and procedures, some IT officers still fail to comply with mitigating

mediations like ensuring only system administrators have administrator privileges and updating/patching their systems regularly. For example it was noted during the outbreak that some hosts within the GDN were still running on Windows 2000 which was not supported by Microsoft anymore.

The OAG Chief Systems Analyst indicated that in the case of the OAG, none of the systems/computers were affected. This was mainly due to the fact that most of the systems were running Windows 10 (which according to Microsoft was not targeted by the attack). In addition the office was fortunate enough to have all systems running on earlier versions of windows with updated anti-malware software (Symantec). As such it would seem those that were not as fortunate to have these in place suffered from the attack.

- vi. Typically, how does ransomware attempt to enter your enterprise?

Both the DIT and the CSA felt that users are the weakest link in the security strategies adopted by government. As mentioned above there needs to be exhaustive trainings to sensitise users on how to behave when using the internet and other channels of communication like emails. Social media and social engineering tactics have also opened up the playing field to culprits looking to find access to our systems.

4.2.4. Current Defences against Ransomware

The following questions were directed to DIT and CSA as the entities responsible for implementing and deploying security mechanisms. The objective was to appreciate what defence the DIT and the OAG have instituted against ransomware.

- i. What are we doing as DIT to mitigate the risk against future attacks?

As a procedure every host is required to be installed with anti-malware software, Symantec to be precise. This should be updated timely. Also upgrading and patching of all software is recommended. However the DIT may not have influence on applications at their client as they are only hosting their databases on certain instances.

In agreement the CSA confirmed that Symantec is installed in all machines and definition updates are pushed timeously. With regards to applications used at OAG which are entirely supported by OAG IT unit (no hosting at DIT) upgrades and patching are usually decided on an individual basis based on the cost-benefits (some upgrades are costly).

- ii. How confident are you that your current defences are proficient in detecting and stopping ransomware attempts?

According to DIT these defences would be adequate if they were implemented appropriately. The CSA emphasised this assertion by stating that during the ransomware attack, Symantec was able to halt some attempts as noted by the reports from the software.

- iii. From the following, what other security interventions do you presently employ to fight ransomware? Data backup and recovery, User awareness, Email and web gateways, maintaining current Operating systems and software with latest patches, Incident detection and disaster management plan.

The two respondents responded that beyond the defences mentioned above (which include maintaining current upgrades and patches) they also employ

data backup and recovery. User awareness thru training is also an initiative that is recommended. However it has not picked up as anticipated. Currently users are informed of threats via email.

In addition IT officers have been instructed to limit administrator rights to privileged users only or IT support. This policy is however not always enforced.

- iv. In your opinion what is the biggest lesson(s) from the ransomware surge of the recent couple of years?

According to DIT there is need to document policies and monitor compliance to these policies at the outstations. Although it is assumed that direct supervision by Ministry management is carried out the supervisors are usually not versed with technical issues nor the policies. Lastly the need for user awareness of security issues is critical to the fight against such threats.

4.2.5. Sufficiency of current security strategy in light of OAG's unique workflows

4.2.5.1. Identification of Critical Asset, Processes and their Protection

As noted in the numerous literature, adequate protection is reliant on complete comprehension of an entity's unique processes and workflows. In addition the data generated along with where it exist, how it is used and by whom. The following questions were designed to identify the steps taken by OAG to identify and protect their important assets.

- i. In light of the OAG mission has the office identified the most critical information assets?

Four out of five of the members of management disclosed that they are not aware of any exercise to identify information assets. The last interviewee indicated that they vaguely remember an exercise for classifying information that was carried out some years back. This was during the tenure of one Research and Development officer that has since left the office. To their knowledge this resulted in a draft policy indicating how information should be handled within the office. All members however indicated that if they had to single out any information asset it would have to be audit data. It is essentially what the mandate of the OAG is about – to collect data on auditees and report on that data.

As regards auditors, eight (8) responders elected audit data as the most mission critical information asset, while four (4) felt research and development is crucial to OAG's mandate and one (1) choose human resource information. Training materials was chosen by six (6) individuals.

- ii. Where are they stored and how are they transmitted?

All management respondents admitted that data exist in many forms and in numerous locations. They as management are not always aware of where this data is. Primarily the bulk of the data is in the auditor's hands presumably on their laptops. Every auditor has been issued a laptop to facilitate mobility as they visit clients.

According to the auditors 12 choose networked laptops and Teammate server. Six (6) also choose electronic media. Manual files were selected by 7 individuals. Ten of the auditors selected all the options of transmitting data

i.e. Exchange of Storage Media (e.g. USB flash drives), Emails, Computer networks and Hardcopy Sharing (Physical sharing of printed files/copies).

Only three did not select the latter i.e. hardcopy sharing but select the rest.

- iii. What exercise was taken to evaluate the value and impact of this data to the OAG mission?

No activity is on record that suggests this.

- iv. Has priority been given to the protection of this assets over other information assets?

No activity is on record that suggests this.

- v. The auditors were asked if they are aware of any policy for classifying data.

They all responded that they were not aware of any policy.

- vi. Lastly their opinion (auditors) on whether data protection is prioritized in order of criticality to OAG mission was inquired.

The auditors were in agreement that there is no prioritising security in terms of criticality of data.

4.2.5.2. Threat Intelligence

In order to corroborate if the current security strategies are adequate, given the OAG's unique workflows and processes, it was important to comprehend the OAG's threat landscape and what activity has been carried out to detect the risks.

It became clear early in the interviews that no separate strategy exist to augment the initiatives recommended by DIT. According to the response by the CSA the OAG

relies on what the DIT has in place. It also became obvious that no exercise had been carried out to comprehend the threats to the mission of the OAG.

- i. However when asked if the OAG have any rivals/ adversaries all responses were in the affirmative.

YES

- ii. When asked if they think the adversaries where internal or external they were divided as follows

5 External only

6 External and Internal

2 Internal only

- iii. What motivates this adversaries?

Twelve (12) said to steal and (or) sell information, while no one felt rivals are motivated by service disruption. One added that adversaries are motivated by need to publish information in the media.

- iv. If motivation is information what information are they interested in obtaining from the office?

All auditors answered audit evidence as the response.

- v. What strategies and technologies are they using?

5 Physical access to premises (unauthorised entry)

13 Hacking

0 Malware

2 Unauthorised copying of data by employees

- vi. To your knowledge what steps has the office taken in anticipation of attempts on information assets?

13 Physical security measures

8 Antivirus/Antimalware software

- vii. In your opinion is data protected throughout its life cycle, i.e. from the time it is captured/obtained, through transmission (including being carried on laptops at client premises) to the time it is archived?

3 Yes

8 No

Reasons:

- *Laptops are at the risk of being stolen.*
- *Laptops can be used on unsecure networks.*

- viii. As the CSA are these information assets adequately protected given the workflows and procedures at the OAG e.g. is data protected throughout its life cycle?

In part it is protected. We a tool called Teammate which facilitates the collection, storage and sharing of audit workings papers. Data saved on the server is backed up while data on laptops at the site of audit is no backed up.

- ix. Do you consider yourself to be knowledgeable at all times about:

a. Where sensitive data copies are?

No. It is assumed that all audit data is sensitive. As a result it is presumed that this data is proliferated in many locations including laptops, storage media like flash drives and printouts.

b. Who has access to this data?

No. Only the auditors have control over who they share the data with.

c. What users are doing with the data?

No. Auditors have carte blanche what information they collect as well as how they utilise it.

x. As the OAG CSA how confident are you that your current defences are proficient in detecting and stopping ransomware attempts?

Current defences are adequate if they are correctly applied and as long as malware definitions can keep up with new versions.

4.2.5.3. Incident and Disaster Management

In addition to the defences alluded to above it is important to establish an inter-departmental incident identification and response plan for active crisis handling. This involves putting in place cyberattack contingency planning to respond actively and promptly to crisis.

On initial review it was noted that no preparations towards this line of defence was instituted at the OAG. This was substantiated by the auditors' response that they were not aware of plans for crisis handling, nor did they know what the standard procedures are in the event of crisis.

4.2.5.4. Monitoring and Detection

This line of enquiry is aimed at establishing if measures are in place to improve institutional detection and responsiveness to security events. This entails all activity carried out to update the enterprise and apprise user on new security trends/events.

On inquiry with management it became clear that no formal arrangement has been instituted by management to apprise itself about security trends. It is assumed that the CSA and his team are carrying out this exercise. However the seven (7) auditors felt that measures were in place to notify them of new threats. According to them, email is the medium of communication used for this purpose. In the follow up question do you feel that you are sufficiently notified and made aware of cyber risks, all seven answered yes.

All auditors answered yes to the question whether they felt ransomware is a significant threat to the OAG.

Chapter 5

5. Discussion

5.1.1. The role of DIT concerning security at OAG

The role between the DIT and OAG are that of are that of service provider and client. Nevertheless the relationship is not managed by any formal agreements. The responsibilities between the two to the other remain vague and unenforceable. Nothing is in place current to enumerate what constitutes delivery on each other's obligations.

However an informal description designates DIT's responsibilities to the OAG and other government entities as a service provider of a Data Centre and the computer network that comes with it, called the Government Data Network. By extension the DIT has had to secure these IT services. Hence the security strategy and framework is also DIT's dominion. In assessment of the above, it is my feeling that the DIT is not obligated to assess the OAG's unique environment in terms of security needs and accordingly plan for it. The whole of Government is treated as a whole and even shares one network.

5.1.2. The role of the DIT attaché (Chief Systems Analyst) at the OAG

As recognition that the arrangement with DIT does not negate the need for an IT expert at the clients, the DIT has come up with an arrangement of attaching IT Officers (also CSA) at each and every Ministry. Their primary responsibilities is to

advice Ministry management on IT governance issues, assist management secure their IT infrastructure and information assets. This means they are tasked with recommending IT strategy that will support the enterprise strategy. In addition they are in place to liaise with DIT for the project management of development projects. In carrying out these responsibilities the CSA is guided by the policies and procedures of the mother enterprise DIT whom they apprise regularly on what is happening onsite.

Being experts on IT issues and with a working relationship with DIT it would seem these individuals are in better placed to notify the DIT of the service needs of their unique entities. The OAG's unique environment may require a distinguished approach as compared to other entities and the CSA should advice on these and ensure OAG assets are secured.

5.1.3. Ransomware a viable threat in Botswana

The study could not quantify statistically the extent to which ransomware attack of the previous year affected the government enterprise. An unsubstantiated account by the DIT's own personnel labelled the damage as on a few systems. What is clear however from the survey is that the ransomware did indeed infiltrate the Government Data Network. It is also clear from the discussions and questionnaires that predominantly ransomware is perceived to be a threat in Botswana. By extension the OAG is believed to be at risk of this type of attack even though it suffered no damage from the outbreak.

However it has been demonstrated that it was indeed the OAG's adherence to security policy/defences that prevented the outbreak within the OAG. Unlike other entities the OAG was able to maintain an up to date antimalware software and

patch level for their operating systems. Also as at the time of attack the office was fortunate to have recently upgraded most of their laptops to windows 10 which was immune to the attack.

This success story suggests to the DIT that adherence to the current defence strategy can be useful against malware. However in light of the ever changing landscape where security software developers are always playing catch-up with new versions of malware there is agreement that the risk is real even for OAG.

The users have been identified as the primary point of entry for such attacks. This is in line with most of the literature as presented earlier. By their own admission the survey responders highlighted the need for training of users and advancement of security awareness. This is perceived to be lagging behind as depicted in the responses.

According to OAG management no arrangements are in place for continuous training on security events. By the DIT and CSA's own admission security awareness is through emails and only in the midst of an attack. It my position that prior notification and awareness is more effective than a response strategy to minimise damage.

5.1.4. Sufficiency of current security strategy in light of OAG's unique workflows

It can be deduced from the survey that the OAG's unique processes and work flows, where information is propagated in numerous locations and shared sometimes through movable media, makes it even more prone to an attack. Seventy six percent (76%) of the responders reported that data is shared⁷ through storage media (e.g. USB flash drives), emails, computer networks and hardcopy sharing (physical sharing of printed files/copies). Ninety two percent (12 out of 13) of the

⁷ Note that sharing is essential to facilitate review of work as is prescribed by audit standards

auditors testified to the use of networked laptops and Teammate server. This is despite the fact that these laptops are exposed to malware infection as they connect to unsafe networks at the clients. In the event that a new ransomware finds its way into the OAG systems, it would spread uncontrollable given the workflows at OAG.

According to the response by the CSA, the OAG relies comprehensively on what the DIT has in place in terms of security strategy. It must be noted that this is the same strategy that the DIT has not documented, suggesting an ad-hoc approach to defence. It is apparent that no separate strategy exist to augment the initiatives recommended by DIT within the OAG. By the OAG's own admission thru management and the auditors the OAG is at the risk of adversaries (both external and internal) looking to access or share audit information unlawfully. Ninety six percent of the responders felt that financial gain⁸ is the main motivation behind this risk.

Further to the above a whopping sixty one percent of the responders felt that data was not protected throughout its life cycle. The reasons forwarded were that physically laptops are at the risk of being stolen and also they can be used on unsecure networks. Although it was suggested that the OAG has invested substantially in physical security, within the OAG buildings, it is perceived that laptops are easily accessible when outside the premises. Exposure may include an adversary looking to introduce malware on the laptop or obtain access onto the network (e.g. an unlocked laptop at a workstation). The CSA also alluded to the fact that data is propagated across many locations within the OAG IT resources. Wherever data exists on the server a failback strategy is in place where data is

⁸ A motivation commonly seen in ransomware attacks

routinely backed up daily. However the currency⁹ of data on the server is questionable given that a lot of data collection happens on client sites and on laptops which are synchronised later - activity that might take days (or the period of the audit visit).

It is thus ostensible that the OAG is exposed to unique circumstances that require a more detailed approach to security than a generalised solution that seems to have been adopted by default (no formal exercise carried out to identify threats and accordingly plan for them by the DIT).

5.1.5. Data Centric Protection as an approach to defence at OAG

It is recommended by this paper that data centric approach to OAG security is suitable in light of the unique challenges. This approach adopts a structured methodology to defining what needs to be protected and where protection needs to be instituted. Not only that, the complete understanding of the asset to be protected accords the enterprise opportunity to customise defences to the unique nature of the asset. The OAG by nature has an exceptional environment that also attracts attention. Some attention is from culprits looking to make quick financial gains thus exposing the OAG to probes and attacks including ransomware.

In implementing Data Centric protection the OAG should ideally identify their mission critical information assets. According to this survey the magnitudes recognize audit data as the most critical asset. The where and how this asset is transmitted should be noted. In the case of the OAG the fact that no exercise was taken to evaluate the value of this assets and where they are propagated means that a

⁹ Currency in terms of how up-to-date (quality of being generally accepted as reliable and in use)

great deal of data exist beyond the locations focal to the defences instituted by DIT (traditional approach). Likewise had there been an exercise to evaluate their value, the need to augment the DIT's strategy with their own (OAG) would have arose. The result effect is an approach with no threat intelligence of the OAG.

As noted in the literature, implementation of a data centric approach does not mean discarding of the traditional defences. They can be useful in curbing threats as was seen in the ransomware outbreak last year. As seen in the survey a great deal of work by the DIT involves technology fundamentals. The DIT has policy for ensuring that core platforms and technology are upgraded and patched. This is primarily the reason behind the success story.

The objective of data centric approach is to augment. In addition to the DIT's strategy the OAG should institute controls that will allow it to shield data in all the unique forms and locations. This may entail instituting additional controls to deal with the vulnerabilities of legacy technology. By nature there is likelihood of one system being incompatible with new technology, resulting in the decision not to upgrade. There should be controls to mitigate the risk, like for example removing it from the network.

Additionally protection by inaugurating robust incident and disaster management response plans may be done. By nature and as already alluded to, the OAG is exposed to malware infections as auditor carry out their daily duty of auditing. Should one computer get infected by a malware strand that has not been protected against, then the whole office is likely to suffer damage once the computer is reconnects back onto the OAG network. The need to establish standard procedures for quickly responding to outbreaks is crucial and may be the

only remedy keeping malware from spreading ubiquitously and ultimately the office being held at ransom.

Last but not least, a data centric approach is most likely to reveal the resource needs required to protect the assets. The technical infrastructure and expertise required should be highlighted by a successful attempt. Even more importantly the user needs are brought to the forefront. This will result in the realisation that continuous user development is crucial. As already indicated user training is perceived to be a major contributor to security. The OAG cannot leave it to the prerogative of the DIT in light of the risks they recognise. Institutional detection and responsiveness should be put in place to progress awareness of security trends.

Chapter 6

6. Conclusion

Traditional approaches are effective and can be effective against ransomware attacks. This was evidenced by the success story at the OAG during the outbreak of 2017. However, traditional defences like the one that was instrumental in arresting the outbreak (anti-malware software) are depended on a lot of work behind the scene to keep up to date with the ever changing ransomware attack vectors. By nature ransomware evolves on a daily basis as seen in the literature and as demonstrated by the respondents to the survey. Anti-malware software developers are continually chasing an ever changing finish line. The bottom line is there is money to be made and attackers are not showing any sign of slowing down.

It is thus important that this defences are augmented by other defences. The Data Centric Approach to security can be influential in ensuring that all attack vectors are considered and obstructed. The scenario presented by the OAG offered an even more defined need to instil additional protection. The unique process flows require a detailed understanding of the risk vectors. Inherently the role of the auditors requires a lot of travel and visiting of clients. This exposes the laptops they are equipped with to malware as the exchange and share data between themselves and the client's personnel. Anti-malware software may not be updating with malware definition files while at the client resulting in infection and loss of valuable data that may at that time exist only in the auditor's laptop.

7. References

- i. Qadir, S. and Quadri, S. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, 07(03), pp.185-194.
- ii. Kuusisto, T. and Kuusisto, R. (2015). Cyber World as a Social System. *Intelligent Systems, Control and Automation: Science and Engineering*, pp.31-43.
- iii. Yu, F., Chang, C., Khan, M., Cao, T. and Ivanovic, M. (2014). Recent Advances in Information Security. *The Scientific World Journal*, 2014, pp.1-4.
- iv. Disis, J. (2017). Ransomware attack: Who's been hit. [online] CNNMoney. Available at: <http://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html> [Accessed 9 Apr. 2018].
- v. Identity Theft Resource Center. (2018). Identity Theft Resource Center. [online] Available at: <https://www.idtheftcenter.org/Data-Breaches/data-breaches> [Accessed 8 Apr. 2018].
- vi. Cheng, L., Liu, F. and Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), p.e1211.
- vii. Verizon Enterprise Solutions. (2018). Data Breach Digest: Cybercrime Case Studies. [online] Available at: <http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/> [Accessed 14 Apr. 2018].
- viii. Oltsik, J. (2015). Data---centric Security: A New Information Security Perimeter. The Enterprise Strategy Group, Inc..
- ix. Davey, M. (2016). Red Cross Blood Service data breach: personal details of 550,000 blood donors leaked. [online] the Guardian. Available at: <https://www.theguardian.com/australia-news/2016/oct/28/personal-details->

of-550000-red-cross-blood-donors-leaked-in-data-breach [Accessed 1 Apr. 2018].

- x. TIME.com. (2010). Top 10 Leaks - TIME. [online] Available at: http://content.time.com/time/specials/packages/article/0,28804,2006558_2006562_2033508,00.html [Accessed 14 Apr. 2018].
- xi. TechCrunch. (2017). After data breaches, Verizon knocks \$350M off Yahoo sale, now valued at \$4.48B. [online] Available at: <https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/> [Accessed 2 Apr. 2018].
- xii. Vijayan, J. (2017). Is data-centric security worth the implementation challenge?. [online] SearchCloudSecurity. Available at: <https://searchcloudsecurity.techtarget.com/feature/Is-data-centric-security-worth-the-implementation-challenge> [Accessed 9 Apr. 2018].
- xiii. Mullins, B. (2016). All Trends Lead to Data-Centric Security. [online] Digital Guardian. Available at: <https://digitalguardian.com/blog/all-trends-lead-data-centric-security> [Accessed 7 Apr. 2018].
- xiv. Chen, Y. (2012). Architecture for Data-Centric Security. Ph.D. Princeton University.
- xv. Shelke, P. (Prof.) and Sasankar, A. (Dr.) (2016). Data Centric Security Approach: A way to Cloud Computing Security & Privacy. IOSR Journal of Computer Engineering (IOSR-JCE), [online] pp.PP 10-14.
- xvi. SANS Institute. (2015). Data-Centric Security Needed to Protect Big Data Implementations: Results of the 2015 SANS Big Data Survey Released. [online] Prnewswire.com. Available at: <https://www.prnewswire.com/news-releases/data-centric-security-needed-to-protect-big-data-implementations->

results-of-the-2015-sans-big-data-survey-released-300097955.html [Accessed 16 Apr. 2018].

- xvii. Monika, Zavorsky, P. and Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. *Procedia Computer Science*, 94, pp.465-472.
- xviii. SecureMac, I. (2017). A Brief History of Malware - SecureMac. [online] SecureMac. Available at: <https://www.securemac.com/checklist/a-brief-history-of-malware> [Accessed 26 Mar. 2018].
- xix. En.wikipedia.org. (n.d.). Malware. [online] Available at: <https://en.wikipedia.org/wiki/Malware> [Accessed 26 Mar. 2018].
- xx. Kansagra, D., Kumhar, M. and Jha, D. (2015). Ransomware: A Threat to Cyber security. *csjournalss*, 7(1), pp.224-227.
- xxi. SSL2BUY Wiki - Get Solution for SSL Certificate Queries. (n.d.). Symmetric vs. Asymmetric Encryption – What are differences?. [online] Available at: <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences> [Accessed 26 Mar. 2018].
- xxii. Kotov, V. and Rajpal, M. (2015). Understanding Crypto-Ransomware In-Depth Analysis of the Most Popular Malware Families. Bromium, Inc.
- xxiii. Saiyed, C. (2016). CryptoLocker. *ISSA Journal - Developing And Connecting Cybersecurity Leaders Globally*.
- xxiv. Savage, K., Coogan, P. and Lau, H. (2015). The evolution of ransomware. Symantec - SECURITY RESPONSE (Version 1.0 – August 6, 2015).
- xxv. Maqsood, F., Ahmed, M., Mumtaz, M. and Ali, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. *International Journal of Advanced Computer Science and Applications*, 8(6).

- xxvi. M. Mikhail, Y. Abouelseoud, and G. Elkobrosy, "Extension and Application of El-Gamal Encryption Scheme," 2014.
- xxvii. R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," *Int. J. Adv. Found. Res. Comput.*, vol. 1, no. 6, pp. 68–76, 2014.
- xxviii. Mauch, B. (2015). CryptoLocker and CryptoWall: The Threat of Ransomware. TOPICS - BCLMA Biennial 2015 Conference.
- xxix. Goncharov, M. (2011). Traffic Direction Systems as Malware Distribution Tools. Trend Micro Research Paper.
- xxx. Curtiss, R. (2016). If Ransomware Is the Question, Then Information Risk Management Is the Answer - The Compliance and Ethics Blog. [online] The Compliance and Ethics Blog. Available at: <http://complianceandethics.org/ransomware-information-risk-management/> [Accessed 12 May 2018].
- xxxi. Archie, J., Turner, S. and Boynton, M. (2017). Ransomware Attacks: When Is Notification Required? | Lexology. [online] Lexology.com. Available at: <https://www.lexology.com/library/detail.aspx?g=3e9f388a-06b6-46a8-a93c-e480f514db53> [Accessed 1 May 2018].
- xxxii. Deloitte Development LLC (2016). Ransomware - Holding Your Data Hostage. Serial: W-TS-EN-16-00734. Deloitte Threat Intelligence and Analytics.
- xxxiii. Carder, J. (2017). The reality of ransomware. [online] CSO Online. Available at: <https://www.csoonline.com/article/3219709/ransomware/the-reality-of-ransomware.html> [Accessed 10 May 2018].
- xxxiv. Symantec (2016). Internet Security Threat Report, Symantec Corporation, volume 21.

- xxxv. Sherman, M. (2015). Ransomware Do's and Don'ts: Protecting critical data. Available at: <https://www.symantec.com/connect/blogs/ransomwaredos-and-donts-protecting-critical-data>
- xxxvi. Antoniou, P. (2014). Weaknesses of Backup Systems and How to Overcome Them | Fresh Business Thinking. [online] Fresh Business Thinking. Available at: <http://www.freshbusinessthinking.com/weaknesses-of-backup-systems-and-how-to-overcome-them/> [Accessed 12 May 2018].
- xxxvii. Orlando, S. (2016). Why your antivirus software can't stop ransomware - Futurity. [online] Futurity. Available at: <https://www.futurity.org/ransomware-computer-files-1198242-2/> [Accessed 1 Jun. 2018].
- xxxviii. Espinosa, N. and Espinosa, V. (2016). How Anti-virus Software Fails Against Ransomware Attacks. [online] SmartFile. Available at: <https://www.smartfile.com/blog/how-anti-virus-software-fails-against-ransomware/> [Accessed 1 Jun. 2018].
- xxxix. O'Leary, D., Ferreira, J. and Grahn, A. (2016). 10 Keys to Data-Centric Security. [online] FOCUS Forsythe. Available at: <http://focus.forsythe.com/articles/512/10-Keys-to-Data-Centric-Security> [Accessed 5 Jun. 2018].
- xl. Ferrell, M. (2008). A New View and Guidelines for Data Centric Security. Master of Science. JAMES MADISON UNIVERSITY.
- xli. Constantin, L. (2015). New ransomware program threatens to publish user files. [online] Computerworld. Available at: <https://www.computerworld.com/article/3002120/security/new-ransomware-program-threatens-to-publish-user-files.html> [Accessed 7 Jun. 2018].
- xlii. Collins, T. (2017). LeakerLocker ransomware threatens to share your private data. [online] Mail Online. Available at:

<http://www.dailymail.co.uk/sciencetech/article-4689932/LeakerLocker-ransomware-threatens-share-data.html> [Accessed 9 Jun. 2018].

- xliii. Bilger, M., O'Connor, L., Schunter, M., Swimmer, M. and Zunic, N. (2006). Data-centric security. Enabling business objectives to drive security. IBM.
- xliv. Institute of Risk Management (2018). A Risk Practitioners Guide to ISO 31000: 2018, International Organization for Standardization
- xlvi. International Auditing and Assurance Standards Board (IAASB) International Standard on Auditing (2009) - (ISA) 220, "Quality Control for an Audit of Financial Statements" published by the International Federation of Accountants (IFAC)

Interview Questions for Executive Management

The internet of things has brought to life a dynamic environment that is increasingly interconnected, integrated, and interdependent. However with this new developments the risk landscape has changed tremendously. Company assets are now open to exploitation by global adversaries. The recent ransomware attacks are indication of how cybercriminals are continually looking for ways to cash in on vulnerabilities of organisational information assets. The following questions are aimed at assessing your organisation's preparedness and ability to respond to new challenges.

1. Identification of Critical Asset and their Protection

Identify, prioritize, and secure mission critical assets

- a) In light of the OAG mission has the office identified the most critical information assets?

.....

.....

.....

.....

- b) Where are they stored and how are they transmitted?

.....

.....

.....

.....

- c) What exercise was taken to evaluate their value and impact to the OAG mission?

.....

.....

.....

.....

.....

- d) Has priority been given to the protection of this assets over other information assets?

.....

.....

.....

.....

.....

2. Threat Intelligence

Comprehend the threats to audit industry and your trade

e) Does the office have any rivals/ adversaries/ antagonists?

.....
.....
.....
.....
.....

f) What are their motivations?

.....
.....
.....
.....

g) What information are they interested in obtaining from the office?

.....
.....
.....
.....

h) What strategies and technologies are they using?

.....
.....
.....
.....

i) What steps has the office taken in anticipation of attempts on information assets?

.....
.....
.....
.....

j) Have your strategy and controls accordingly adopted these measures?

.....
.....
.....
.....
.....

3. Incident and Disaster Management

Establish an inter-departmental incident identification and response plan for active crisis handling

- k) Has Management commenced cyberattack contingency planning?

.....
.....
.....
.....

- l) Is an inter-departmental structure in place to process and respond to incidents?

.....
.....
.....
.....

- m) Is the contingency plan accordingly updated to include ongoing business changes and evolving threats?

.....
.....
.....
.....
.....

4. Process and Technology Fundamentals

Appraise and enhance effectiveness of existing processes and technologies

- n) What steps are in place to ensure core platforms and technology are upgraded and patched in a timely manner?

.....
.....
.....
.....
.....

- o) Are there change management procedures for adopting new technology and ensuring they meet the appropriate security?

.....
.....
.....
.....

- p) How are vulnerabilities with your legacy technology managed?

.....

.....

.....

.....

5. Monitoring and Detection

Improve institutional detection and responsiveness to security events

- q) Are there measures in place to advance awareness of both internal and external security events and activities?

.....

.....

.....

.....

- r) Is there any analytics of trends, correlations and patterns of security events?

.....

.....

.....

.....

- s) Does the decision to take action take into consideration the above analysis

.....

.....

.....

.....

.....

- t) How do you ensure there is timely and efficient response action?

.....

.....

.....

.....

6. Security Philosophy and Mind-set

Institute ethics and conduct that is commensurate to effective security culture

- u) Is Management involved and dedicated to addressing cyber threats at the Office of the Auditor General?

.....

.....

.....

.....

v) What (regular) steps are carried out to ensure improved awareness and sensitivity to cyber risks?

.....
.....
.....
.....

w) Has there been any process re-engineering to reflect assessed risks to the office?

.....
.....
.....
.....
.....

Interview Questions for Auditors (End Users)

The internet of things has brought to life a dynamic environment that is increasingly interconnected, integrated, and interdependent. However with this new developments the risk landscape has changed tremendously. Company assets are now open to exploitation by global adversaries. The recent ransomware attacks are indication of how cybercriminals are continually looking for ways to cash in on vulnerabilities of organisational information assets. The following questions are aimed at assessing your organisation's preparedness and ability to respond to new challenges.

1. Identification of Critical Asset and their Protection

Identify, prioritize, and secure mission critical assets

- a) In light of the OAG mission what are the most critical information assets?
 - ☐ Research & Development
 - ☐ Training Materials
 - ☐ Human Resource Information
 - ☐ Audit Data (evidence)
 - ☐ Other (specify).....
- b) Where are they stored? (select all that apply)
 - ☐ Computer Hard Disk e.g. Stand-alone laptops
 - ☐ Networked laptops (hosts)
 - ☐ Teammate server(application storage component)
 - ☐ Manual Files
 - ☐ Electronic Media e.g. CD-RW/DVD-RW, External Drives or tapes
 - ☐ Cloud Based Storage
 - ☐ Other (specify).....
- c) How are they transmitted?
 - ☐ Exchange of Storage Media (e.g. USB flash drives)
 - ☐ Emails
 - ☐ Computer networks
 - ☐ Hardcopy Sharing (Physical sharing of printed files/copies)
 - ☐ Other (specify).....
- d) Are you aware of any policy for classifying data?
 - ☐ Yes
 - ☐ No
- e) Is data protection prioritized in order of criticality to OAG mission?
 - ☐ Yes
 - ☐ No

2. Threat Intelligence

Comprehend the threats to audit industry and your trade

f) In your opinion does the OAG have any rivals/ adversaries?

- ☐ Yes
- ☐ No

g) If Yes to (f), are they (tick all that apply):

- ☐ External
- ☐ Internal

h) If yes to (f), what are their motivations?

- ☐ To steal and (or) sell information
- ☐ To disrupt service (make audit evidence unavailable)
- ☐ Other

i) If motivation is information above, what information are they interested in obtaining from the office?

- ☐ Audit Evidence
- ☐ Research & Development Information
- ☐ Human Resource (Auditors personal data)
- ☐ Other.....

j) What strategies and technologies are they using?

- ☐ Physical access to premises (unauthorised entry)
- ☐ Hacking
- ☐ Malware
- ☐ Unauthorised copying of data by employees
- ☐ Other

k) To your knowledge what steps has the office taken in anticipation of attempts on information assets?

- ☐ Physical security measures
- ☐ Antivirus/Antimalware software
- ☐ Other.....

l) In your opinion is data protected throughout its life cycle, i.e. from the time it is captured/obtained, through transmission (including being carried on laptops at client premises) to the time it is achieved?

- ☐ Yes
- ☐ No

If NO why.....

3. Incident and Disaster Management

Establish an inter-departmental incident identification and response plan for active crisis handling

- m) In your knowledge are there contingency plans in place for cyberattack?
- ☐ Yes
 - ☐ No
- n) If yes how is staff informed of these
- ☐ Training
 - ☐ Apprised through emails/memos
 - ☐ Other.....
- o) Does the contingency plan include malware attacks like virus, ransomware etc.
- ☐ Yes
 - ☐ No
- p) What contingency response steps are you to carry out during cyberattack?
-
-
-
-

4. Monitoring and Detection

Improve institutional detection and responsiveness to security events

- q) Are there measures in place to advance awareness of both internal and external security events and activities?
- ☐ Yes
 - ☐ No
- If yes above, how is staff notified of this new trends?.....
-
- r) Do feel that you are sufficiently notified and made aware to cyber risks?
- ☐ Yes
 - ☐ No
- s) The years 2016 and 2017 headlines were dominated by ransomware outbreaks, in your opinion, is ransomware currently a significant threat to the OAG?
- ☐ Yes
 - ☐ No

Questions to Chief Systems Analyst

Attached to every Government Ministry, holders of the designation are seconded/attached from the DIT. They are responsible for support of ICT within the Ministry.

1. What is the role of the Chief Systems Analyst:

a. With regards to the OAG?

.....

.....

.....

.....

b. In relation to the DIT?

.....

.....

.....

.....

2. Do you have a formal security strategy for the OAG?

.....

.....

.....

.....

3. In devising the strategy:

a. What steps were taken to identify threats and (or) risks to the OAG's mission?

.....

.....

.....

.....

b. Did the OAG identify the most mission critical information assets?

.....

.....

.....

.....

c. What measures have been taken to prioritize and secure these mission critical assets?

.....

.....

.....

.....

d. Do you consider client or audit data to be a mission critical asset?

.....

.....

.....

.....

Annexure 3

4. According to you are these mission critical assets adequately protected given the workflows and procedures at the OAG e.g. is data protected throughout its life cycle?
-
-
-
-
5. Do you consider yourself to be knowledgeable at all times about:
- a. Where sensitive data copies are?
-
-
-
-
- b. Who has access to this data?
-
-
-
-
- c. What users are doing with the data?
-
-
-
-
6. In your opinion is Management involved and dedicated to addressing cyber threats at the OAG?
-
-
-
-
7. In your opinion, is ransomware currently a significant threat to the OAG?
-
-
-
-
8. Does your security strategy take into consideration the ransomware threat?
-
-
-
-
9. How confident are you that your current defences are proficient in detecting and stopping ransomware attempts?
-
-

-
.....
10. What other security interventions do you presently employ to fight ransomware? (Select where applicable)
- a. Data backup and recovery
 - b. User awareness
 - c. Email and web gateways
 - d. Operating systems and software are current with latest patches
 - e. Incident detection and disaster management plan
 - f. Any other
-
.....
.....
11. If (d.) above is positive, what steps are in place to ensure core platforms and technology are upgraded and patched in a timely manner?
-
.....
.....
.....
.....
12. Are there change management procedures for adopting new technology and ensuring they meet the appropriate security?
-
.....
.....
.....
13. How are vulnerabilities with your legacy technology managed?
-
.....
.....
.....

Questions to DIT

As the facilitator and administrator of ICT services across the public sector, the DIT plays a pivotal role in the securing of the government ICT environment. Their vision is to deliver a reliable, secure and responsive ICT network.

1. Are there documented Service Level Agreements or Memorandum of Agreements between the DIT and other government entities? (Obtain copies)

.....

If not:

- ☐ What is the DIT's role with regards to security within government?

.....

- ☐ How is performance documented (Key Performance Indicators)?

.....

2. The years 2016 and 2017 headlines were dominated by ransomware outbreaks, did any of the government entities fall victim?

- ☐ How hard were we hit as a government? (Productivity loss, System downtime, Data loss, No business impacts, negative publicity)

.....

- ☐ Any reports/statistics? (Obtain copies)

.....

3. In your opinion, is ransomware currently a significant threat to government?

.....

4. In your assessment what was the root cause?

.....

-
-
5. Typically speaking how does ransomware attempt to enter your enterprise?
.....
.....
.....
6. What are we doing as DIT to mitigate the risk against future attacks?
.....
.....
.....
7. How confident are you that your current defences are proficient in detecting and stopping ransomware attempts?
.....
.....
.....
8. What other security interventions do you presently employ to fight ransomware? (e.g.)
- ☐ Data backup and recovery
 - ☐ User awareness
 - ☐ Email and web gateways
 - ☐ Operating systems and software are current with latest patches
 - ☐ An incident detection and disaster management plan
 - ☐ Any other
-
9. In your opinion what is the biggest lesson(s) from the ransomware surge of the last couple of years?
.....
.....
.....