RHODES UNIVERSITY
Where leaders learn

An Exploratory Investigation into an Integrated Vulnerability and Patch Management Framework

Submitted in partial fulfilment
of the requirements for the degree of

Master of Science

of Rhodes University

By: Duane Carstens

Grahamstown, South Africa
April 6, 2021

Abstract

In the rapidly changing world of cybersecurity, the constant increase of vulnerabilities continues to be a prevalent issue for many organisations. Malicious actors are aware that most organisations cannot timeously patch known vulnerabilities and are ill-prepared to protect against newly created vulnerabilities where a signature or an available patch has not yet been created. Consequently, information security personnel face ongoing challenges to mitigate these risks. In this research, the problem of remediation in a world of increasing vulnerabilities is considered. The current paradigm of vulnerability and patch management is reviewed using a pragmatic approach to all associated variables of these services / practices and, as a result, what is working and what is not working in terms of remediation is understood. In addition to the analysis, a taxonomy is created to provide a graphical representation of all associated variables to vulnerability and patch management based on existing literature. Frameworks currently being utilised in the industry to create an effective engagement model between vulnerability and patch management services are considered. The link between quantifying a threat, vulnerability and consequence; what Microsoft has available for patching; and the action plan for resulting vulnerabilities is explored. Furthermore, the processes and means of communication between each of these services are investigated to ensure there is effective remediation of vulnerabilities, ultimately improving the security risk posture of an organisation. In order to effectively measure the security risk posture, progress is measured between each of these services through a single averaged measurement metric. The outcome of the research highlights influencing factors that impact successful vulnerability management, in line with identified themes from the research taxonomy. These influencing factors are however significantly undermined due to resources within the same organisations not having a clear and consistent understanding of their role, organisational capabilities and objectives for effective vulnerability and patch management within their organisations.

Acknowledgements

I would like to thank my family, friends and professional associates for their support, contributions and encouragement throughout the process of writing this thesis. To all the information security practitioners who took the time and effort to respond to the research survey, being forthcoming and unreserved on their pragmatic understanding regarding this body of knowledge, I really am appreciative.

I also want to express a sincere gratitude to my supervisor, Dr. Yusuf Motara, for his patience, guidance and determination to assist me in completing this thesis. It really was a pleasure to work with someone as logical and as knowledgeable as Dr Motara. In addition, thank you to the Rhodes University Computer Science faculty leadership team for their valuable insight and subject proficiency.

Lastly, a special thank you to my dearest loved one, Lilani de Necker, who would always give me words of motivation when I needed it most and would always understand the sacrifices needed in order to complete this thesis. I sincerely hope that this research is a testament to all the support I have received, of which without, this research study would not have been possible.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The aim of this chapter is to provide an introduction into the specific research and understand the key areas of focus for this research. The domain of the research is thus discussed, followed by an explicit statement of the problem being investigated. The research questions and objectives are then further detailed for a more specific understanding of the research goals.

As various terms of vulnerability and patch management are used synonymously throughout this research, the following terms of reference which are key to the research are defined for ease of reference.

1.1 Research Area

Gauci, Michelin, and Salles (2017) highlight that cybersecurity is all about people, processes and technology. Security teams of large organisations or enterprises usually manage security controls such as patching, anti-virus and/or anti-malware applications, firewalls, etc., all of which work together to minimise exposure to threats (Beres *et al.*, 2008b). Namely (as per the research terms of reference), a threat is the potential to exploit a vulnerability (Shetty, McShane, Zhang, Kesan, Kamhoua, Kwiat, and Njilla, 2018). In addition, a vulnerability is a weakness or flaw in the software or hardware design that can result in loss if exploited (Shetty *et al.*, 2018). Most incidents today are caused by software flaws (Cavusoglu, Cavusoglu, and Zhang, 2008). In comparison, Cavusoglu *et al.* (2008) estimates that there are about twenty flaws per thousand lines of code.

Term	Definition
Vulnerability	A weakness or flaw in a software or hardware design, implementation and operation that can result in loss if exploited.
Threat	A threat is the potential to exploit a vulnerability.
Vulnerability Assessment	Process to identify and prioritise vulnerabilities according to criticality.
Vulnerability Management	A security practice specifically designed to proactively mitigate or prevent the exploitation of IT vulnerabilities which exist in a system or organisation.
Patch Management	A strategy for managing patches or upgrades for software applications and technologies.
Security Risk Management	A continuous process of identifying, measuring and prioritizing information systems security risk (threat, vulnerability and consequence), and implementing and monitoring controls (e.g. countermeasures, safeguards) that address those risks.

Table 1.1: Terms of reference

The main objective for system administrators, however, is to keep systems stable and secure (Singh *et al.*, 2016). To note, there are various system administrators and thus various teams usually responsible for various systems and systems management within an organisation. Nevertheless, software flaws continue to be a prevalent issue for small and large organisations, irrespective to the budget and resources available (Gianini, Cremonini, Rainini, Cota, and Fossi, 2015, Khouzani, Malacaria, Hankin, Fielder, and Smeraldi, 2016). If vulnerabilities are successfully exploited within an organisation's environment, the confidentiality, integrity and availability of systems and their data is at risk (Wen, Zhang, Dong, and Yang, 2015, Shetty *et al.*, 2018).

While "vulnerabilities" has a broad meaning in the information security context, the term in this work refers to flaws in the design, implementation and operations of Microsoft application security controls (Ganin *et al.*, 2017). Microsoft application security controls were selected for review because Microsoft Windows is a popular business operating system (Beres *et al.*, 2008b). Although patching is continuous, the number of published vulnerabilities continues to grow rapidly (Wen *et al.*, 2015). Furthermore, the number and type of cyber attacks changes dramatically as time progresses (Shetty *et al.*, 2018). Systems can be left without applicable patches for months or years after a patch has been released, regardless of the fact that most organisations deploy patches monthly within the environment (Cavusoglu *et al.*, 2008). Remediation of vulnerabilities through patching therefore remains a key activity of the organisation (Beres *et al.*, 2008b, Cavusoglu *et al.*, 2008, Okhravi and Nicol, 2008, Gianini *et al.*, 2015). Vulnerability management talks

to an organisation's ability to successfully identify and track a system threat and vulnerability, including the associated risk the vulnerability imposes on the system and the organisation (Nanda and Ghugar, 2017). For effective vulnerability management, an organisation must consider available security controls, including patch availability, whether the system cannot be patched and if so, what are the available compensating controls. Effective vulnerability management should also enable effective communication between IT operations teams and an integrated workflow to track remediation across the various teams (Nanda and Ghugar, 2017).

In terms of defects for tangible or intangible products, Arora, Forman, Nandkumar, and Telang (2010, p. 166) points out that "[u]nlike defects in physical goods, software defects can be mitigated even after product release via patch release". Patching therefore remains an important aspect of post-sales support and Arora *et al.* (2010) confirm this by mentioning that it remains profitable for software organisations to offer post-sale support after new software product releases. Moreover, the goal of patch management is to keep systems current in terms of security fixes (Nicolett and Colville, 2003). Patch management talks to an organisation's ability to deploy system patches, routine maintenance and necessary security updates, timeously to remediate a vulnerability identified in an operating system, device firmware, drivers and / or application software (Beres *et al.*, 2008b, Gauci *et al.*, 2017). Further to the understanding of the need to apply system patches, to apply effective patch management within the organisation, comprehensive knowledge of all assets within the organisation is required in terms of understanding asset components, operating systems and applications (Gauci *et al.*, 2017). This comprehensive knowledge allows for patches, which are released frequently through the month from different product vendors, to be applied with minimal impact to business functionality and security. What is also evident from the above, is that there are separate roles and responsibilities when considering the approach to remediating vulnerabilities within an organisation.

This global situation is reflected locally within multiple South African organisations and the remediation of vulnerabilities remains an ongoing issue. Monthly vulnerability scans continue to identify an increase in vulnerabilities for an organisation although patching teams continue to highlight the fact that they have met high patching service level agreements (SLAs) as per indicators from patch deployment tools such as Microsoft's System Center Configuration Manager (SCCM)[1].

Given the above, there seems to be a disconnect between the vulnerability management

[1] `https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager/`

component, managed by applications such as Qualys[2], Nexpose[3], Retina[4], Nessus[5], etc., and what Microsoft identifies and has available in the Microsoft catalog for download and deployment by the patching administrators.

This research reviews available engagement models between vulnerability management and patch management, taking into account all other facets of vulnerability management. The literature highlights a lot of work being done within each of these paradigms and the research will explore the question of whether there are any existing frameworks available to link these separate functions. If nothing is available, a working model must be defined based on an understanding of the literature and in line with empirical research. Empirical data will include opinions and perceptions from people to have a more pragmatic understanding of what is happening within organisations (Brady, 2015, Ganin *et al.*, 2017).

The scope of the proposed research includes organisations which have supporting elements for a vulnerability management program, including a risk management function across different business units. Security risk management is a "[c]ontinuous process of identifying and prioritising IS security risk, and implementing and monitoring controls (i.e. countermeasures and safeguards) that address those risks" (Spears and Barki, 2010, p. 505). Risk assessments, which form part of risk management, comprise of the following actionable elements: threat, vulnerability and consequence (HKSAR, 2008, Ganin *et al.*, 2017). With this understanding, this research reviews each of these elements to give suitable recommendations.

1.2 Problem Statement

Ideally, the information and communication technology (ICT) infrastructure of a business should operate with minimum risk. At present, vulnerabilities increase irrespective of the systems being patched. If patching and vulnerability management programs work effectively together, then vulnerabilities (and hence the organisational risk) should decrease. This research seeks to understand whether there are challenges between vulnerability and patch management in terms of successfully remediating vulnerabilities, and if there are, then why these challenges exist.

[2] `https://www.qualys.com/`
[3] `https://www.rapid7.com/products/nexpose/`
[4] `https://www.beyondtrust.com/products/retina/`
[5] `https://www.tenable.com/products/nessus/nessus-professional/`

1.3 Research Question and Goals

The primary research question is: what are the challenges that face vulnerability remediation through patch management within organisations, and why?

The primary research question has been formulated to explore and explain the current phenomena around remediating vulnerabilities. The following more detailed secondary research questions helped to construct and understand the primary question:

1. Does a silo approach between vulnerability management and patch management produce positive results in terms of remediating known vulnerabilities?
2. What are the advantages of an engagement model between vulnerability management and patch management?
3. What are the disadvantages of an engagement model between vulnerability management and patch management?

1.4 Research Objectives

The research will review the current effectiveness of vulnerability and patch management services, synthesise a taxonomy that includes all supporting facets of vulnerability management and assist in understanding any existing frameworks which further aids in vulnerability management. The focus is not on technology selection but rather the people and process component of vulnerability and patch management. A survey will be undertaken after the taxonomy generation to provide real-world data from the context of the study. The following steps will be taken in order to achieve these research objectives:

1. Identify influencing factors that impact successful vulnerability management.
2. Make recommendations regarding positively influencing each identified factor.
3. Identify whether effective risk management within a vulnerability management program actually benefits the approach to patching, further to patching what Microsoft has available in its catalog.
4. Identify and explore use cases where the decline of vulnerabilities remain progressive.

The benefits of the research are:

- Review current challenges - Establish current challenges for effective vulnerability remediation and areas of improvement.
- Revise patch management approach - Confirm whether there is a better approach to patch management on vulnerabilities that are not listed as critical and not listed with an exploit yet, i.e. be more proactive in approach rather than ignoring the less critical vulnerabilities and relying on compensating controls.
- Create a conceptual taxonomy - Create a conceptual taxonomy that will allow for further research and defining of suitable frameworks which can be used in organisations, initially focused for the financial sector. The taxonomy creates the basis for a suitable framework which can enhance the needs and requirements of the users.

1.5 Thesis Structure

The remainder of this document is structured as follows. Chapter 2 reviews the literature on the vulnerability and patch management paradigms, which includes all other associated variables of these services. Following this, Chapter 3 defines the research methodology which will include the research design, strategy, data collection and analysis process, research implementation and research limitations. Chapter 4 graphically defines what has been identified in the literature review into various themes, formulating a taxonomy which is then leveraged to generate survey questions. Chapter 5 details the analysis on the survey feedback as per the identified themes, after which Chapter 6 summarises the research findings and illustrates the current status of the target population. Finally, Chapter 7 provides conclusions on the research outcomes and proposes further research.

Chapter 2

Vulnerability and Patch Management

This chapter provides an understanding of the literature regarding vulnerability and patch management. All associated services and tasks which form part of the research topic are further understood. The chapter summarises the literature on barriers or challenges to the vulnerability and patch management services, the process flows or lines of communication between these services and concludes with the understanding of existing available frameworks and ways to measure progress on vulnerability remediation.

2.1 Vulnerability Management

Gianini *et al.* (2015) confirms that the number of classified vulnerabilities have exceeded 5000 per year in the previous 10 years, and the number of vulnerabilities that are classified as "high" have increased from 33% to 50%. According to a report by Secunia[1], reviewed by Abraham and Nair (2015c), vulnerabilities increased by 32% between the years 2012 and 2013.

Secunia's research team from Flexera[2] conducts their own vulnerability research on multiple products. Their 2018 report[3] continues to indicate the upward trend of vulnerabilities,

[1] https://secuniaresearch.flexerasoftware.com//?action=fetch&filename=secunia_vulnerability_review_2014.pdf/

[2] https://www.flexera.com/about-us/secunia-research.html/

[3] https://resources.flexera.com/web/pdf/Research-SVM-Vulnerability-Review-2018.pdf/

as seen in Figure 2.1, and shows that vulnerabilities have more than doubled between 2012 and 2017.

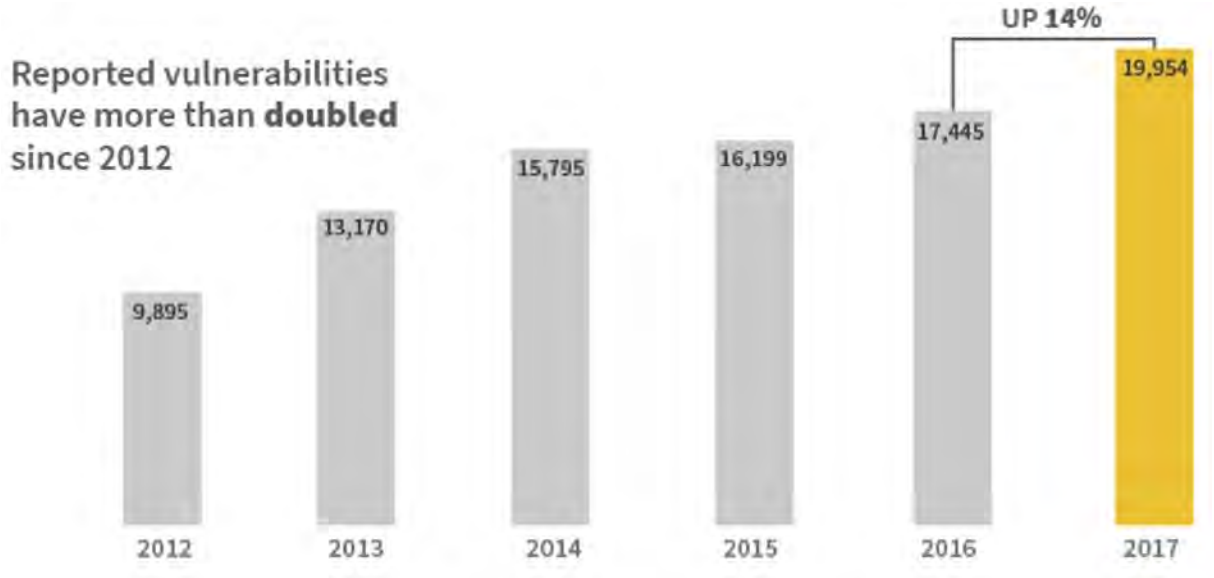

Figure 2.1: Increasing trend of vulnerabilities (reproduced from (FlexeraSoftware, 2018))

Vijayan (2018) summarises a report by Risk Based Security[4] that almost 17% of the 10644 disclosed vulnerabilities between January 2018 to August 2018 are classified as "critical". Risk Based Security provides analysis on data breaches, vendor risk ratings and vulnerability intelligence. The company's 2018 year-end vulnerability Quickview report highlighted a total of 22022 disclosed vulnerabilities for that year (RiskBasedSecurity, 2019).

New software vulnerabilities are being discovered almost daily (Okhravi and Nicol, 2008). With an increase in vulnerabilities over time, so have attack tools progressed (Cavusoglu *et al.*, 2008). As organisations' IT networks continue to grow and develop, vulnerability assessments are becoming more and more necessary (Wen *et al.*, 2015). Vulnerability management in this research refers to "[a] security practice specifically designed to proactively mitigate or prevent the exploitation of IT vulnerabilities which exist in a system or organisation" (Techopedia, 2019b, p. 1). Vulnerability assessments include identifying and prioritising the vulnerabilities whereas the vulnerability management will include these processes but also understand how to remediate the vulnerabilities.

Threats, however, are not correctly represented in risk assessment models due to the complexity of threats (Ganin *et al.*, 2017). Models tend to focus on vulnerabilities and the

[4] `https://www.riskbasedsecurity.com/`

consequence thereof versus the severity, means of exploitation and means to remediate. Similarly, risk management should provide a means to managing the rise in threats, and thus manage the associated risk to systems (Singh *et al.*, 2016). A lack of effective techniques to measure risk is evident (Abraham and Nair, 2015b). Spears and Barki (2010), however, suggests that although users are seen as a weak link in information security, a user's understanding of the organisation or the business contributes to more effective security controls or measures. Users thus add value to security risk management when "[t]hey participated in the prioritisation, analysis, design, implementation, testing, and monitoring of user-related security controls within business processes" (Spears and Barki, 2010, p. 520). The outcome of user participation then leads to greater organisational awareness of security risks and controls within the organisational processes. This leads to better development and management of security controls.

The attributes of a vulnerability are also dynamic and change over time, and thus the rating of perceived risk will also continuously change. Cyber attacks continue to rise and a patch not deployed timeously will increase the probability of a likely attack which, if successful, is likely to cause loss (Okhravi and Nicol, 2008, Arora *et al.*, 2010, Abraham and Nair, 2015c). Losses from a malicious event are caused by a deliberate action of an attacker who intends to inflict damage on an organisation (Shetty *et al.*, 2018). Malicious users exploit vulnerabilities to cause damage through unauthorised access, non-permitted modification of data (i.e. corruption or destruction), theft, disclosure of information, elevation of privileged access and causing system downtime (Cavusoglu *et al.*, 2008, Shetty *et al.*, 2018). Attacks exploit known vulnerabilities which have available patches or other remediation options (Cavusoglu *et al.*, 2008, Okhravi and Nicol, 2008, Afful-Dadzie and Allen, 2014), however, only 32.7% of the vulnerabilities disclosed in 2018 have public exploits (RiskBasedSecurity, 2019). Effective vulnerability management will thus allow the mitigation of security risks to the organisation (Singh *et al.*, 2016).

With the understanding of an increase in cyber attacks and an increase in vulnerabilities, organisations are falling behind in terms of protection due to budget constraints and weak security controls or processes (Abraham and Nair, 2015c). Abraham and Nair (2015a) mentions that we need to protect mission critical systems both from known and undiscovered vulnerabilities. Due to resource constraints for some organisations, only the relevant vulnerabilities that remain high are actually being focused on (Gianini *et al.*, 2015). Some organisations thus seem to only take care of a subset of all known vulnerabilities that could be relevant (Beres *et al.*, 2008b). In the same breath, it is also evident that other organisations are trying to apply more resources and more funding to the issue of vulnerability remediation, but without seeing positive results. Khouzani *et al.* (2016,

p. 3) highlights that an "[e]xhaustive implementation of controls at maximum intensity is likely neither economically feasible nor managerially desirable".

Gauci *et al.* (2017) summarises how to quantify an uncertain risk in a cybersecurity assessment using the following steps:

1. Inventory of critical assets, irrespective to vendor.
2. Identify threats and vulnerabilities for these assets.
3. Identify associated risk levels.
4. Define a mitigating action plan.
5. Implementation of mitigating actions.
6. Define a process to manage and maintain existing security levels.

Arora *et al.* (2010) was able to test the variables associated with a vendor releasing a patch, i.e. the speed, quality, cost and competition between vendors. This will not be the focus of this research. This research does not explore if vulnerabilities should be kept a secret, released or published to the public immediately after being identified or released sometime after, nor does it focus on the time a vendor takes, and any associated cost in terms of monetary or reputation, to release a patch after a vulnerability has been identified or how the vulnerability gets identified or reported to the vendor (Cavusoglu *et al.*, 2008). Instead, it focuses on all the variables associated with vulnerability management as highlighted in the literature to create a taxonomy in order to understand the correlation between vulnerability and patch management, including other areas or variables which impact both these services.

2.1.1 Vulnerability Timeline

Figure 2.2 summarises the lifecycle of a typical vulnerability, the associated timeline of events and the window of exposure (Beres, Griffin, and Shiu, 2008a, Beres *et al.*, 2008b, Okhravi and Nicol, 2008). The timeline depicts different points of awareness to a vulnerability and the different perceptions of risk. The key points of the timeline are the discovery of the vulnerability, disclosure or public awareness, the exploit becoming available for the vulnerability and then the correlating patch availability. The vulnerability

timeline is also color coded in order to understand the points of discovery and disclosure of a vulnerability (highlighted in black), the availability of exploits from a zero-day exploit to public code being available and the issuing of malware (highlighted in red) and, lastly, the availability of signatures for security controls, to remediate or compensate against known vulnerabilities, through to patches becoming available and finally deployed (highlighted in green).

Okhravi and Nicol (2008) adds extra points of awareness to the vulnerability timeline. Before the discovery of a vulnerability it is worthwhile mentioning the introduction of the vulnerability since it is present as part of the initial software creation, deployment and/or update. After discovery, the vendor then needs to develop the associated patch for the identified vulnerability. Okhravi and Nicol (2008) goes further to differentiate between private and public exploitation. Private exploitation occurs before disclosure of the vulnerability and public exploitation occurs after disclosure. Private exploitation refers to a small group of malicious users exploiting the vulnerability before public disclosure. Further to the vulnerability timeline, Okhravi and Nicol (2008) also provides additional detail to patch availability, i.e. patch release then patch testing and lastly patch deployment. This is summarised by the "patching process" as seen in Figure 2.2.

It is evident that the risk increases exponentially through the vulnerability timeline as the vulnerability becomes better known (Beres *et al.*, 2008a,b). The time of patch availability is the earliest point an organisation has to plan, prepare and deploy the necessary patch within their environment. This research thus measures the effectiveness of patch management from this particular point, to better understand an organisation's ability to deploy patches timeously.

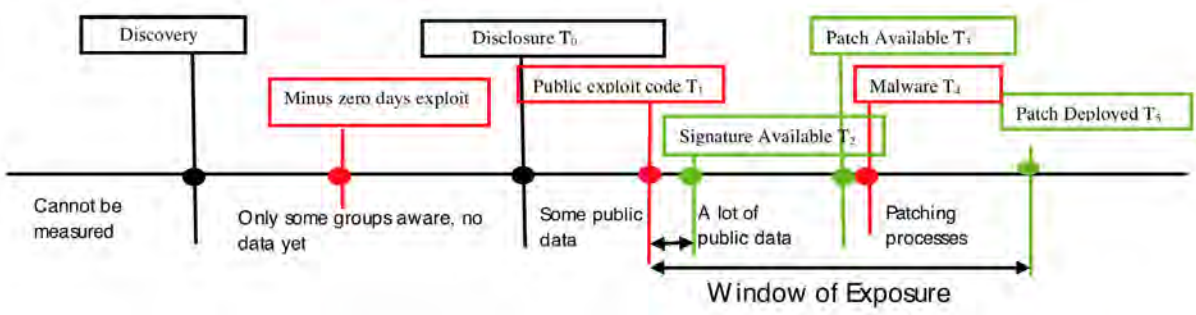

Figure 2.2: Vulnerability timeline

2.1.2 Effective Vulnerability Management

Vulnerability management needs to be proactive and automated as far as possible to ensure vulnerabilities are reviewed, prioritised and remediated as quickly as possible in order to avoid unnecessary exposure for an organisation (Singh *et al.*, 2016). Rouse (2017) reviewed vulnerability management, highlighted areas of concern and suggested a means to improve vulnerability management for organisations. The areas of concern or current limitations include access limitations, asset distribution and information overload (Rouse, 2017). When talking about access limitations the paper highlighted that most organisations are hesitant to scan their critical assets to avoid any unnecessary downtime. Asset distribution refers to maintaining and updating an asset inventory. Furthermore, in terms of asset distribution, asset location (cloud or mobile assets) can create a challenge for accessing assets. Lastly, vulnerability management scanners can create too much information through overly extensive reports which focus too little on the organisation's network context (Rouse, 2017).

Compensating, or alternative, security controls are seen as temporary solutions and might not cover all known vulnerabilities (Beres *et al.*, 2008b). Beres *et al.* (2008b) created a vulnerability management process that includes the understanding of external threats and the internal security decision points. They conclude their research by mentioning that changes in solutions, policies, timeous patch deployments and pre-patch mitigation measures all help improve vulnerability management. Additionally, developing cross-functional teams and competencies becomes key when securing technology (Gauci *et al.*, 2017). Protection against cyber threats requires "[t]houghtful, thorough, and ongoing analysis of many variables as well as an iterative vulnerability management process" (Gauci *et al.*, 2017, p. 2599). Rouse (2017) continues to summarise the suggested areas of improving an organisation's vulnerability management as follows:

- Analysis and validation - Analysis and validation is unique per organisation in terms of prioritising critical risks and avoiding wasting time on low risk items of investigation. A fast track list should be created which can be executed swiftly and eliminate any risk of a vulnerability being exploited.
- Intelligent risk rating - The current generic approach to vulnerability management focuses on predefined severity ratings and asset importance based on CVSS (see section 2.4.1). Instead, vulnerability management should focus on existing security controls, threat information, the organisation's assets and the impact of a potential attack.

- Effective remediation and tracking - Effective remediation should consider all available security controls. It should review patch availability, whether there are issues such as systems integration, location, availability requirements, bespoke application limitations, etc. Effective remediation should also review the system's susceptibility and whether the network architecture or access controls can be changed to mitigate a vulnerability. Lastly, in terms of effective remediation, the availability of other security controls should be determined. This is important when a patch is not available. Other security controls could include a firewall, intrusion prevention system (IPS), anti-malware signatures, etc. The availability of other security controls should be part of the vulnerability management prioritisation process.

In terms of vulnerability management, it is useful to prioritise easy to remediate vulnerabilities over vulnerabilities that are time-consuming and resource-intensive as the goal is to get the most protection in the shortest timeframe (Rouse, 2017). Rouse (2017) goes on to suggest points of consideration when deciding on a suitable vulnerability management solution. This work, however, will not focus on technology selection but rather the people and process component of vulnerability and patch management as mentioned in Chapter 1.

To further the understanding of effective vulnerability management, the following section details the paradigm of patch management and the associations between the vulnerability management and patch management services.

2.2 Patch Management

Keeping systems up-to-date with available patches could have prevented a high percentage of information security breaches (Cavusoglu *et al.*, 2008). However, Beres *et al.* (2008b) details that it is not a simple exercise to deploy patches to thousands of systems across an organisation in a timely manner. Fixing vulnerabilities remains a risk in itself to an organisation due to possible negative implications on application functions or crashing a system (Wen *et al.*, 2015). Therefore, further to the time spent on patch assessments and patch testing, the business usually places further restrictions on organisations with regards to operational reasons and allowed system downtime (Beres *et al.*, 2008b, Cavusoglu *et al.*, 2008, Okhravi and Nicol, 2008, Wen *et al.*, 2015).

Patch management in this research refers to "[a] strategy for managing patches or upgrades for software applications and technologies" (Techopedia, 2019a, p. 1). The patch

management lifecycle includes several steps, including preparation, vulnerability identification and patch acquisition, risk assessment and prioritisation, patch testing, patch deployment and verification (HKSAR, 2008). Patching a system will fix a vulnerability or improve functionality of the system. Undoubtedly, patch management between different organisations will differ depending on the available number of resources for patch management, the number of systems an organisation has and the organisation's risk appetite (Beres *et al.*, 2008b). With limited resources or resource capacity constraints, risk management will also help prioritise available patches to understand which patches should be deployed first (HKSAR, 2008). This prioritisation is based on understanding the threat (i.e. the potential danger to a system), vulnerability and risk or criticality to the application, system or environment. Systems facing more threats, are more vulnerable, or are mission critical should therefore be prioritised in the patch management process.

Furthermore, performing effective lifecyle management on all software-based assets in an environment entails having complete knowledge of the assets and its associated components (Gauci *et al.*, 2017). This highlights the need to have full details of an asset rather than simply knowing the owner and pushing a patch. Similarly, Nicolett and Colville (2003) states that patch management is not enough when effectively mitigating vulnerabilities. The following functional requirements should be considered with regards to patch management:

- Asset inventory - As security patches are specific to software components, an up-to-date asset inventory of servers and desktop needs to be available and should include installed software components and running services.
- Patch and service pack status - When revising patch installation requirements, information about installed service packs and patches for each installed component on a server or desktop should also be revised.
- Patch dependency analysis - Automated evaluation of patch dependencies should be considered. This is to review any pre-requisites or post patch requirements without the patch dependency analysis being time consuming. This analysis will also allow the understanding of superseded patches or post service pack dependencies.
- Patch inventory and patch classification - Patch management automation should include an inventory of available patches together with some detail about the patches. Depending on the nature of the vulnerability exposure, patch classification should also highlight priority.

- Patch matching reports or system baselining - Reporting should highlight the required patch per server and desktop, based on the asset's current installed software and the role of the system. Alternatively, patch management can also be expedited by comparing an asset to a desired state of configuration, i.e. baselining.
- Role based administration - A patch installation workflow should be followed where there are different roles/system owners for patch analysis and selection, quality assurance testing and implementation of system updates. A patch status should support this workflow depending on whether the patch is still being tested, deployed, post tests, etc.
- Patch distribution and installation - As patches may cause system or application issues, patch management tools should have roll-back options for system configurations to a prior known stable state.
- Platform and application support - Most organisations have multi-platform environments and thus patch management should focus on all operating systems, not just Windows. Patch management should also focus on database, server and application management.
- Agent versus agentless architectures - When reviewing a patch management process there are benefits of using an agent or agentless patch management architecture. Agent-based solutions provide more functionality and consume less network bandwidth but the deployment and management costs could be high, as opposed to the use of an agentless architecture being more feasible. On the other hand, if there is a machine with no agent, the solution will technically not know the asset exists which poses a risk to the patch management and vulnerability management program.

Gauci *et al.* (2017) also considers similar cases as above regarding how to improve patch management. Areas such as an up-to-date inventory of assets including information like network name, IP, firmware version, manufacturer, product, etc., can all aid in improving patch management processes (Gauci *et al.*, 2017). Other areas include correct revision of security bulletins, understanding and prioritising the risks of the vulnerabilities within an organisation's environment, and also to understand a patch management baseline (which is an outcome of the asset inventory). Creating a heat map can also help with the prioritisation by identifying and classifying areas for improvement.

Okhravi and Nicol (2008) details seven elements for successful patch management as well. These are executive support, dedicated resources and clearly defined responsibilities,

creation and maintenance of technology, identification of vulnerabilities and available patches, scanning and monitoring the network, testing of patches and post-deployment scanning and monitoring. In order for patch management to complement vulnerability management, patch management does require a strong security-oriented focus (Nicolett and Colville, 2003).

2.2.1 Barriers to Patch Management

Managing the patch management process can prove challenging due to its complexity and cost (Cavusoglu *et al.*, 2008). Patch management can be costly in terms of the resources or workforce and technology required. When talking about resources there are different levels of resources required to perform different functions within the patch management team.

Beres *et al.* (2008b) highlights the need to have policies for patch management and vulnerability management respectively, together with defined processes around how to perform effective patch management for the organisation. Beres *et al.* (2008b) also refers to International Organisation for Standardization (ISO) 17799:2000[8] and the National Institute of Standards and Technology (NIST)[9] which provide recommendations on principles and methodologies which can be used.

The challenge in the context of increasing vulnerabilities is the creation of policies and the effective, timely deployment of remediation measures (Afful-Dadzie and Allen, 2014). Vulnerabilities introduced due to a bad patch process add further complexity to patch management (Okhravi and Nicol, 2008). Gauci *et al.* (2017) lists several pain points for patch management, namely the following:

- User notifications - How users are informed of available patches, either through direct communication from a vendor or website subscriptions which provide public/member notifications. The detail of the notification should be extensive, including vulnerability information, patch information and vendor product information.
- Patch relevance - Trying to identify which patch would be applicable to a system in use by an organisation, i.e. patch relevance. Users need to review their asset inventory to ascertain whether a patch notification is relevant to them.

[8] `https://www.iso.org/home.html/`
[9] `https://www.nist.gov/`

- Testing patches - Patches should be tested in a test or non-production environment. These test environments must correctly mirror the production environment. There should also be clearly defined owners to confirm whether testing of an application is successful or not after the patch is applied.
- Post deployment reviews - Effective deployment of a patch should be confirmed. Post-deployment checks are required to confirm whether a patch was correctly applied and whether the vulnerability was effectively remediated.

Cavusoglu *et al.* (2008) highlights several operational points of concern with regards to patch management. Firstly, there are on average about 150 vulnerabilities together with vendor remediation suggestions released every week. Reviewing all of these to identify what is relevant to your organisation's environment can be a cumbersome and time consuming exercise. Secondly, testing of patches prior to deployment is critical to avoid unnecessary downtime within your organisation. This refers to any unplanned downtime. Cavusoglu *et al.* (2008) details both planned and unplanned downtime as separate operational points of concern for patch management. With this said, another operational point of concern with regards to patch management is that patching a system can prove costly with regards to planned downtime of any business critical systems.

However, not patching the system timeously can also have a cost associated with it when considering the effective exploitation of a vulnerability. Although critical, correct testing can prevent patches from being deployed timeously within the organisation. Okhravi and Nicol (2008) mentions that testing or pre-deployment testing is good practice. In particular, bringing down a system due to lack of testing can lead to loss of functionality or introduce further vulnerabilities into the system as mentioned earlier. When testing an available patch, a team must take into account the window of exposure (Okhravi and Nicol, 2008) as shown in Figure 2.2. Minimal testing could lead to a failed patch, but testing for too long can lead to a long window of exposure.

In addition, another operational point of concern with regards to patch management is that there is no standard way of deploying patches as patches can be made available by the vendor and some are made available by third parties. Reviewing a vendor's site can be time consuming. The time window for an available exploit once a vulnerability is published has greatly reduced over the years though (Cavusoglu *et al.*, 2008). Nevertheless, this research focuses on Microsoft patching and there are tools that allow a central point of management to effectively distribute patches still required for the organisation's environment. Microsoft

also has their own vulnerability database which lists all relevant published vulnerabilities for their products (Wen *et al.*, 2015).

In terms of responsibilities and in the context of this work we will distinguish between the patch management team who performs the patch management and the security operations team who will do the vulnerability management. With regards to responsibilities, Beres *et al.* (2008b) highlights some key activities for the patch management team. Beres *et al.* (2008b) says that a security operations team, which is responsible for patch assessments and testing, would need to review whether the current patch deployment process is exposing the organisation to an unacceptable risk and evaluate process improvements. Beres *et al.* (2008b) also highlights that the responsibility of such a team includes more than just deploying patches, but also tracking other means of mitigating vulnerabilities which reflect an immediate link between the patch management teams and the vulnerability management teams. Organisations unfortunately do not have the luxury of sharing resources from other IT functions with the patch management team as the planning, deploying and maintenance of patch management is a full time exercise (Cavusoglu *et al.*, 2008).

2.3 Process Flow between Vulnerability and Patch Management

Figure 2.3, as per Beres *et al.* (2008a,b), details an activity diagram of a typical vulnerability and patch management process. This could differ between organisations based on internal processes and requirements. However, it does provide a general understanding of the link between vulnerability and patch management.

The left hand side of Figure 2.3 indicates the decision points of a vulnerability assessment after it has been publicly disclosed (Beres *et al.*, 2008a). Based on the vulnerability assessment outcome, the right hand side of Figure 2.3 indicates three available patching policies for an organisation based on the risk and exposure of the vulnerability within the organisation's environment. Thereafter a decision around patch deployment urgency is made. It is important to note that patch preparation within this diagram takes the same time for all organisations, irrespective to the risk of a vulnerability, as most organisations do not have an appetite for unplanned downtime based on a failed patch.

While Figure 2.3 highlights three different patching policies, Cavusoglu *et al.* (2008) considers two types of stationary policies to understand patch management, how patches

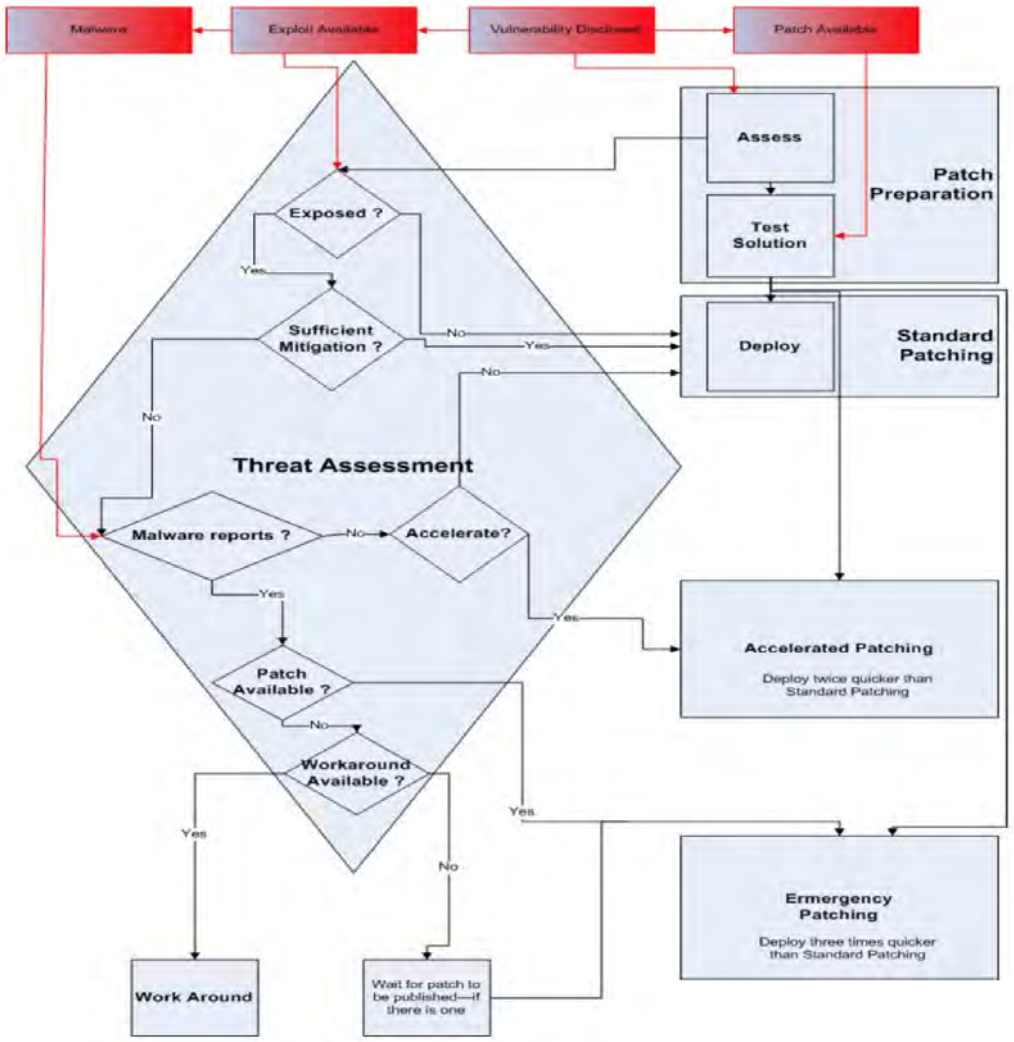

Figure 2.3: Vulnerability and patch management activity diagram (reproduced from (Beres *et al.*, 2008b))

should be released and how vulnerable systems should be updated. Standard, non complex and periodically updated patch procedures to manage the patch process are considered stationary in nature. The two types of stationary policies are:

- Time driven patch management - Patches are released in bulk after a certain time period has lapsed.
- Event driven patch management - The vendor releases patches in batches after identifying a fixed number of vulnerabilities.

Whether it be automatic patching with no administrator intervention or manual patching

with an administrator performing a checklist during and after applying a patch manually, Afful-Dadzie and Allen (2014) highlights other remediation options such as either replacing a system with a new host or taking a system offline and reformatting the host.

Having predictable schedules in terms of evaluating, testing, deploying and post checks of patch management helps with two things in an organisation (Cavusoglu *et al.*, 2008). Firstly, it helps with the resource uncertainty of the workforce required to perform patch management within the environment. Secondly, it balances the operational cost associated with patching a vulnerability with the the risk of not patching a vulnerability. Most vendors release patches periodically and this should further allow organisations to have predictable patching schedules. Provisioning for the required resources and effectively managing the associated operational costs for patching reduces the pressure for the patch management team to keep up with the high frequency of updates/patches.

2.4 Investigating Research Frameworks

As this research is regarding the identification or review of an integrated vulnerability and patch management framework, the following section will review elements similar to or relevant to the proposed topic. As per the above literature review, the research will delve into all elements of vulnerability and patch management services, with the inclusion and understanding of standards, frameworks and risk assessments, as investigated in the literature.

2.4.1 Common Vulnerability Scoring System

This research reviews vulnerabilities with the understanding of the Common Vulnerability Scoring System (CVSS) base score of a vulnerability, which is used to test either an existing or newly created framework. The CVSS scoring system was developed by the National Infrastructure Advisory Council (NIAC) and is applied to the National Vulnerability Database (NVD), a United States government repository of vulnerability management data (Arora *et al.*, 2010, Wen *et al.*, 2015). It was first released in 2004 for public use (Singh *et al.*, 2016). It is a technical framework to score vulnerabilities through a numeric scoring (severity score) value from 0 to 10 representing the intrinsic value of a vulnerability (Arora *et al.*, 2010, Afful-Dadzie and Allen, 2014, Wen *et al.*, 2015,

Singh *et al.*, 2016, Ganin *et al.*, 2017). CVSS allows others to rate, compare and understand the severity of different vulnerabilities thus allowing an organisation to understand the potential danger of a vulnerability specific to the organisation and thus to prioritise them (Singh *et al.*, 2016).

CVSS is considered a Quantitative Vulnerability Assessment Standard (QVAS), and unlike other vulnerability assessment standards, CVSS is objective, authoritative and transparent and promotes the standardization of vulnerability assessments (Wen *et al.*, 2015). CVSS considers the vulnerability's characteristics (base metric), the vulnerability's progression over time (temporal metric) and the organisation's security level (environmental metric) (Singh *et al.*, 2016, Shetty *et al.*, 2018). The base metric can be further split into exploitability and impact metrics. These manually entered metrics are applied against a given formula and a severity level of the vulnerability is calculated (Wen *et al.*, 2015).

There is some benefit in reviewing existing security controls, threat information, the organisation's assets and the impact of a potential attack together with the available CVSS scores (Rouse, 2017) and this has thus been kept in mind through the analysis of this research. There are however some disadvantages to the use of CVSS which need to be noted. As per Wen *et al.* (2015):

- Difficulty to re-assess older vulnerabilities - Organisations would not be able to re-assess vulnerabilities collected over a few years as you would need to find the individual who initially rated the different CVSS key metrics which produced the overall vulnerability severity score.
- Difficulty of objective assessments - A metric of CVSS is the complexity of exploiting a vulnerability. The person rating the vulnerability will have difficulty giving an objective rating for the complexity of exploiting a vulnerability as the person will not know the complexity of exploiting the tens of thousands of vulnerabilities available.
- Reviewing severities with lack of vulnerability information - A newly published vulnerability does not always have all the relevant information about the vulnerability as this can be completed days or months after the vulnerability was publicly disclosed. Due to the lack of information, the correct severity of the vulnerability cannot be assessed in this time period.

2.4.2 Quantitative Risk Model

Singh *et al.* (2016) summarises and tests a quantitative security risk level estimation

model, as represented in Figure 2.4.

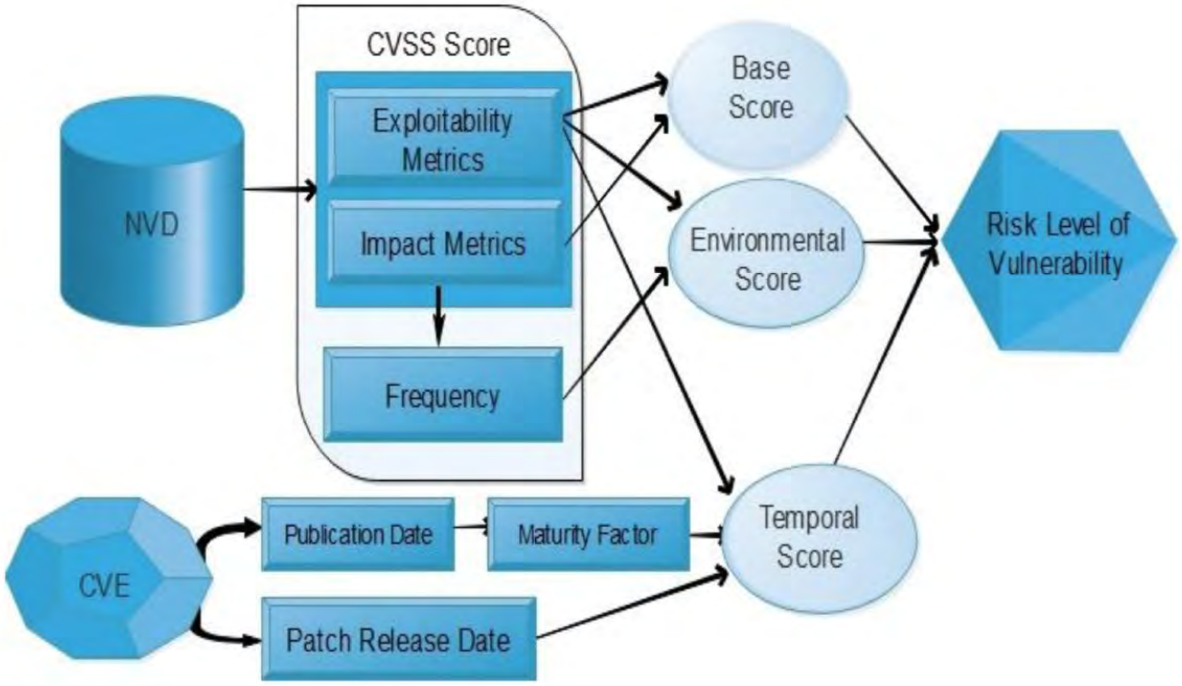

Figure 2.4: Quantitative security risk level estimation model (reproduced from (Singh *et al.*, 2016))

Figure 2.4 highlights the use of the Common Vulnerabilities and Exposures (CVE), the National Vulnerability Database (NVD) by the National Institute of Standards and Technology (NIST), and the Common Vulnerability Scoring System (CVSS) to develop a base score, environmental score and temporal score which ultimately provides a risk level for a vulnerability (Singh *et al.*, 2016). CVEs refer to Common Vulnerabilities and Exposures. CVE is a "[d]ictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE entries are comprised of an identification number, a description, and at least one public reference" (Mitre, 2018, p. 1). The vulnerabilities in the NVD are based on the CVE vulnerability naming standard. With regards to the CVSS score, the exploitability and impact metrics are used. Within the understanding of these metrics, the attack vector, the attack complexity, the required privileges and user interaction are considered as well. NVD is a repository of all known vulnerabilities and their associated CVSS scores (Shetty *et al.*, 2018). The change in risk of a vulnerability over time is also considered under the temporal score. The management of the risk identified is then either retained, mitigated or transferred (Shetty *et al.*, 2018).

2.4.3 Cyber Risk Scoring and Mitigation Tool

Shetty *et al.* (2018) defines five phases of a newly defined Cyber Risk Scoring and Mitigation tool (CRISM). CRISM is "[b]uilt over a platform optimised for vulnerability detection, attack graph analysis and risk assessment that produces cyber risk scores" (Shetty *et al.*, 2018, p. 7). Figure 2.5 represents the CRISM model.

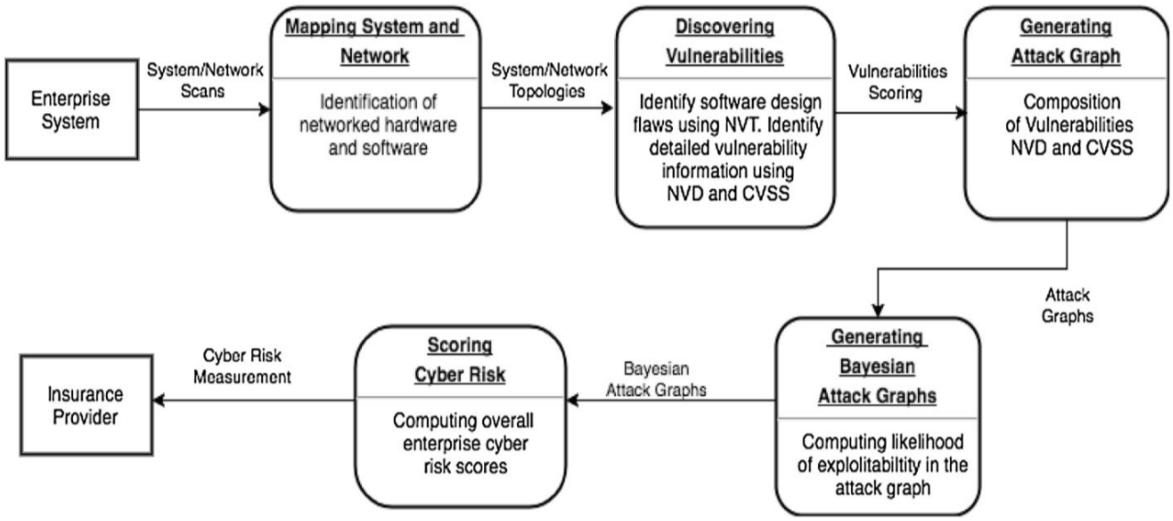

Figure 2.5: Five phases of the cyber risk scoring and mitigation tool

The five phases start by identifying all systems, hosts, ports and services through the use of Network Mapper (NMAP). Vulnerabilities are then discovered for all identified hosts through the use of OpenVAS[5]. An attack graph is then created highlighting all identified hosts and the available vulnerabilities not yet patched. The graph is based on actual exploits available from the identified vulnerabilities. CRISM models specific threats through the understanding of these attack graphs before assigning a cyber risk score regarding the overall risk posture for the organisation based on these metrics. Insurers also use this model for a better means to analyse the potential risk of an organisation and the correct balance of price premium to risk.

2.4.4 Methodologies

Ganin *et al.* (2017) identifies that a popular method to identify vulnerabilities is through expert elicitation. This means using questionnaires to quantify vulnerabilities, the probability of loss and the associated monetary value. The paper goes on to review available

[5] `http://www.openvas.org/`

risk assessment methodologies, identify vulnerabilities based on the potential attack techniques and to minimise any associated damage. Abraham and Nair (2015a,b) creates a predictive cybersecurity model, keeping into account the age of the vulnerability and the vulnerability discovery rate to highlight a practical means to remediate vulnerabilities. This paper continues to provide a better understanding of the lifecycle of vulnerabilities and takes into account available exploits and associated patches. With the mention of available frameworks, Ganin *et al.* (2017, p. 4) mentions that "[m]any of the frameworks published for cybersecurity risk management do not provide a means to characterise risk but rather focus on general practices enhancing the resilience of a system".

The summary of the aforementioned framework and the identified approach to assess risk in a cyber system can be seen in Figure 2.6, as per Ganin *et al.* (2017). Abraham and Nair (2015c) also created a "Cyber Situational Awareness" framework which provides a holistic approach to threats and vulnerabilities. Abraham and Nair (2015c) concludes their paper by highlighting that the defined model obtains security characteristics of vulnerabilities and optimises the application of patches.

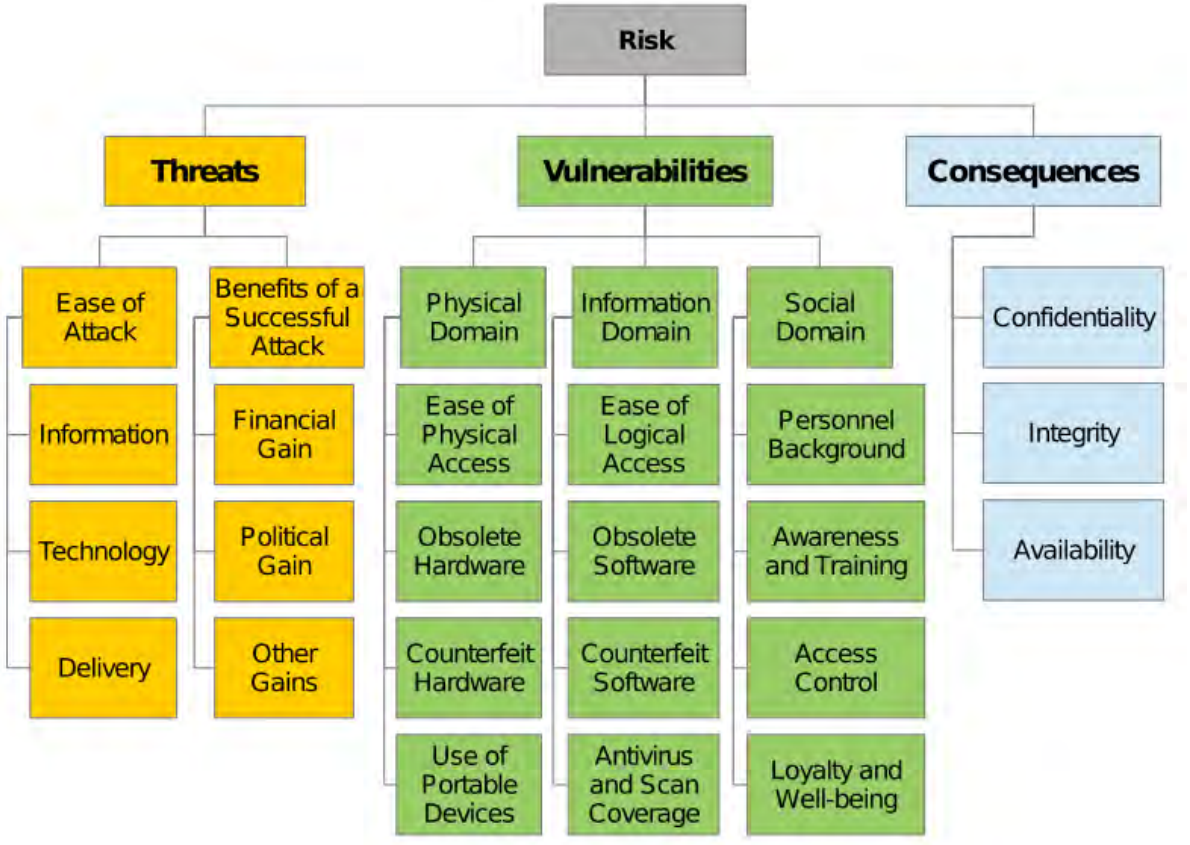

Figure 2.6: Approach to assess risk in a cyber system (reproduced from (Ganin *et al.*, 2017))

2.4.5 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) created a document that reviews a patch and vulnerability management program (Mell, Bergeron, and Henning, 2005). NIST furthermore created a group called the patch and vulnerability group (PVG) which could assist in answering the questions posed in this research. PVG is central to remediation efforts (i.e. patching and configuration changes) and their duties include the following:

- Asset inventory - Determine the organisation's hardware, operating systems and applications.
- Review security sources - Understand what security sources (public or private) are saying about vulnerabilities, the available remediation options and possible threats.
- Prioritising vulnerabilities - Prioritise the available remediation options for vulnerabilities.
- Track remediations - Create and manage a database of remediation options specific to the organisation.
- Patch testing - Test patches and other non patch related remediation options. Testing is performed on systems that have standardised configurations.
- Training - Training local IT administrators to apply vulnerability remediation options.

It is evident from the above that there are similarities to what has been detailed under section 2.2. Creating a group with responsibilities rather than creating a framework does have limitations, though. Large organisations may need multiple PVGs and anything not within the PVG scope will still need to be managed by the IT administrators.

2.4.6 Enhanced Vulnerability Patching Game

Gianini *et al.* (2015) worked off the hypothesis that both the organisations protecting themselves and the opposing malicious hackers are rational. As an organisation trying to prioritise which vulnerabilities they should remediate with priority, a malicious hacker

too is trying to prioritise which vulnerabilities they will exploit based on the effort and resources required. In particular, Gianini *et al.* (2015) continues to create an 'Enhanced Vulnerability Patching' game which tries to predict, through probability, which of the known vulnerabilities should be prioritised first. This paper then continues with a form of risk management but does not correlate that with what is taking place in the patch management service. It rather assumes, based on the "game" output, the patch will take place. Zhang, Zhang, and Ou (2014) also created a "game-like" framework to conduct a risk analysis of vulnerabilities and compare exploiting and patching strategies within a computing environment.

2.5 Vulnerability Management Metrics

Cavusoglu *et al.* (2008) highlights that patching, when released and when applied, can either be time driven or event driven. This research further evaluates the speed of remediating a vulnerability in order to understand the challenges and required collaboration between vulnerability and patch management.

2.5.1 To Measure Speed of Patch

Beres *et al.* (2008b) used the vulnerability timeline, referenced in Figure 2.2, as it affected the result of the paper's simulation based predictive modeling approach to test patching policies and mitigation strategies. The predictive modeling approach helped Beres *et al.* (2008b) answer two particular questions. Firstly, it helped them to review the effectiveness of patching processes against a vulnerability's exposure to an organisation and, secondly, it helped them to explore the impact of different policy decisions such as shorter patching timelines versus the introduction of further mitigating controls for vulnerabilities. Organisations "[o]ften regard the exposure window as closed when the proportion of systems patched is somewhere around 95%, as there will always be some number of systems that are either offline or unmanaged" (Beres *et al.*, 2008b, p. 36).

The above does not mean the exposure to risk is reduced to zero. It simply means that the patch was adequately and timeously deployed. A patch update cycle of an organisation might not be in sync with the patch release cycle of a vendor (Cavusoglu *et al.*, 2008). An attacker is more likely to exploit a vulnerability after it has been released via public disclosure, so it is important to review the speed of patching (time to patch) and how this

relates to the decrease of vulnerabilities found in the environment (Arora *et al.*, 2010). This research views "time to patch" as the time elapsed since the earlier of one of the following two times:

- Microsoft patch Tuesday - From the release of patches from Microsoft's "patch Tuesday".
- Zero-day vulnerabilities - When a "zero-day" exploit has been detected and an associated CVE has been issued for the zero-day vulnerability.

"Patch Tuesday" refers to the second Tuesday of every month when Microsoft releases their monthly patches. Microsoft began releasing patches monthly in October 2003 (Cavusoglu *et al.*, 2008). As per Rouse (2017, p. 1), "[p]atch Tuesday is the unofficial name of Microsoft's scheduled release of the newest security fixes for its Windows operating system and related software applications, as detailed in the Windows Security Updates Guide". Regarding the understanding of a "zero-day" attack, this is when an attacker creates an exploit for vulnerabilities that have not yet been disclosed (Abraham and Nair, 2015c).

Further to the discussion of the speed of patching, Gianini *et al.* (2015) mentions that the increased rate of vulnerable assets is correlated with the increased rate of available patches which cannot be managed manually. Further to the understanding of "speed to patch", the research reviews interconnecting processes related to patching in order to further identify challenges and possible areas for improvement.

2.6 The Implications of the Literature on the Research

Further to the understanding of the interlink between the vulnerability and patch management services and the available frameworks and process flows to augment these two services, what is evident from the above literature review is that the risk vulnerabilities impose on organisations remain prevalent although there are various elements authors talk to regarding the relationship and dependencies of the vulnerability and patch management services on each other to effectively remediate vulnerabilities in an organisation and thus reduce the associated risk on an organisation. These various elements or themes

that come out from the above literature (including the understanding of risk, challenges, the understanding that the risk of vulnerabilities change over time, suitable approach to each service/activity, and that the communication and actions between various managing teams play a critical role in successful vulnerability remediation) are further explored in this research and will aid in formulating the research taxonomy.

Further to the understanding of the interlink between the vulnerability and patch management services and the available frameworks and process flows to augment these two services, what is evident from the above literature review is that there is a consensus in most aspects of the research topic, thus no significant disagreement between authors. These various aspects holistically include the understanding that vulnerabilities continue to increase as organisations continue to grow and develop, vulnerability management (including the understanding of assets in your organisation, threats posed to your organisation, knowing the associated risks to your organisation, and the need to define a mitigation plan and track remediation progress which is interwoven with the intricacies of patch management) remains a critical practice in organisations and that inclusion of user / employee participation leads to greater organisational awareness of security risks and controls within the organisational processes and a better development and management of security controls. Furthermore, the risk vulnerabilities impose on organisations, if not remediated timeously, remains prevalent although there are various pragmatic elements authors talk about regarding the relationship and dependencies of the vulnerability and patch management services on each other to effectively remediate vulnerabilities in an organisation and thus reduce the associated risk on an organisation. What is not agreed upon from the research literature is the mention that attacks exploit known vulnerabilities. Zero-day vulnerabilities are however further discussed through the literature review. Various elements or themes that come out from the above literature (including the understanding of risk, challenges, the understanding that the risk of vulnerabilities change over time, suitable approach to each service/activity, and that the communication and actions between various managing teams play a critical role in successful vulnerability remediation) are further explored in this research and will aid in formulating the research taxonomy

Chapter 3

Research Taxonomy

The research survey (to be further explained in the following chapter) uses a taxonomy of distinct concepts or themes which represents an understanding of what vulnerability and patch management is and the relationship between the two, including associated paradigms of services or functions. To develop this taxonomy the literature was extensively reviewed, themes were identified and similarities were grouped where appropriate. Through the collation of data, the formulated taxonomy structures the identified themes and is thus data driven.

It is through the understanding of identified similarities in the literature and the associated paradigms of services or functions that the taxonomy themes can be sorted and represented in a pyramid type structure to help understand supporting characteristics between the themes. The development of the taxonomy and research survey also allows for appropriate questions to be asked and appropriate data to be collected, data which has an impact on the research questions. These themes are then further split into different areas of concise multiple choice questions, formulated based on the similarities or differences identified in the literature, and allows for an understanding of any correlation between questions of the various themes. The questions identified in each of the themes are referred to as categories of the research taxonomy. Themes have their own defined questions/categories together with associated multiple choice answers.

As the taxonomy is derived from the literature, the taxonomy exists as a reflection of the themes found in the literature review and includes supporting facets of vulnerability management. It is thus an overarching depiction of the research topic and the associated analysis thereof. For the purposes of this research and subsequent research, the research

taxonomy will be called “Vulnerability Management Resilience Taxonomy”. User participation is then considered for validation and testing of the reliability of the newly created taxonomy, which is improved through such industry feedback.

Figure 3.1 visualises the Vulnerability Management Resilience Taxonomy, highlighting the themes and the number of associated categories. Through the exercise of data analysis a working paper (in particular the questionnaire to citations list) was created through the literature review to document key themes and associated variables / questions, which are linked to the literature / citations (see Carstens (2021) for the dataset analysis). This working paper ultimately allowed for the creation of the thesis survey and the formulation of the research taxonomy to provide a graphical representation / holistic visualisation of all associated variables / themes to vulnerability and patch management. For each of the grouped similarities or categories, the relevant citations were correlated and referenced, and a variable was added explaining each of the survey items.

Figure 3.1: Vulnerability management resilience taxonomy

Literature highlights several influencing factors that impact vulnerability and patch management. As a result, seven themes were initially identified to form part of the Vulnerability Management Resilience Taxonomy of which each theme is associated with multiple categories. Table 3.1 describes the initially identified taxonomy themes.

With the understanding of the research taxonomy theme structure, Table 3.2 provides further detail to Figure 3.1, explaining the associated categories of the taxonomy. The categories correlate with the questions in the research survey.

Theme	Summary	Description
People and Team Structure	Respondent Roles and Experience	Respondents background section to understand the participant's current demographics, aptitude and experience in the industry, and their understanding of vulnerability management and patch management services, incl. team structures.
Incident Review	Reflection on Incidents	A section where respondents could acknowledge recent incidents in their environment and whether there were any associations with Microsoft Windows patching, or lack thereof.
Frameworks	Frameworks	A section to understand whether any frameworks, to create facilitation or a means of engagement between vulnerability and patch management, is being practiced in the organisations and whether the respondents can detail the advantages and disadvantages accordingly.
Vulnerability Management	Vulnerability Management Policy and Practice	A vulnerability management section created to understand policy, what is being practiced in the organisation in relation to defined policy, what the known challenges are, trending of vulnerabilities and whether (after contextualising vulnerability management within each organisation) the participants believe that there is still room for improvement required.
Risk Management	Risk Management Strategies	A section to understand whether risk management is being practiced in the organisations and whether the respondents can detail the advantages and disadvantages of this practice.
Patch Management	Patch Management Policy and Practice	A patch management section created to understand policy, what is being practiced in their organisation in relation to defined policy, their organisation's current patching SLA, what the known challenges are and whether (after contextualising patch management within each organisation) the participants believe that there is still room for improvement required.
Incident Management	Organisation Cyber Incident Management	Post incident review and the assurance that previous incidents of a similar nature will not occur through the vulnerability and patch management cycle.

Table 3.1: Taxonomy themes

Theme	Category
People and Team Structure	Experience in information & cybersecurity
	Aptitude through information security certifications or qualifications
	Team structures and responsibilities for vulnerability management and patch management
	Circumstances of communication for multiple teams
	Focus items of communication between multiple teams regarding what cannot be patched
	Advantages of separate teams
	Advantages of one multi-skilled team
Incident Review	Incidents experienced in last 5 years
	Incidents experienced in last 5 years which are associated with a Microsoft vulnerability
	Business consideration over incidents
Frameworks	ISO27001 compliance
	PCI compliance
	Utilisation of industry frameworks
	Understanding of frameworks being used in organisation
	Advantages of following a framework
	Disadvantages of following a framework
Vulnerability Management	Vulnerability management policy documents
	Detail of vulnerability management policy
	Vulnerability management policy items not being practiced in the workplace
	Number of vulnerabilities in organisations
	Trending of vulnerabilities being remediated
	Challenges of vulnerability management
	Contextualising vulnerability management and room for improvement
	Escalation of configuration issues identified through a vulnerability management process
	Monitoring of escalated configuration issues, post a vulnerability management process
Risk Management	Business considerations on risk management
	Risk management activities
	Advantages of risk management
	Disadvantages of risk management
	Improvements to system controls and processes
Patch Management	Centralised platform for patch deployment
	Patch management policy documents
	Detail of a patch management policy
	Patch management policy items not being practiced in the workplace
	Patch compliance
	Challenges of patch management
	Contextualising patch management and room for improvement
	Escalation of configuration issues identified through a patch management process
	Monitoring of escalated configuration issues, post a patch management process
	Superseded patch requirements
	Business consideration on superseded patch requirements
	Considerations on a centralised asset management solution
	Period of utilisation regarding a centralised asset management solution
	Functionality and applicability of a centralised asset management solution
Incident Management	Incident preparation, i.e. business continuity
	Understanding of business impact regarding incidents

Table 3.2: Taxonomy structure

Chapter 4

Research Methodology

Beres *et al.* (2008b) highlights the need to have policies for patch and vulnerability management, including defined processes on how to perform effective patch management for the organisation. The challenge in the context of increasing vulnerabilities is the creation of policies and the effective, timely deployment of remediation measures (Afful-Dadzie and Allen, 2014). As a result of the literature review, the research strategy includes the creation and use of a structured research survey to answer the proposed research questions. The research strategy creates a link between the research philosophy and the data collection and analysis (Saunders, Lewis, and Thornhill, 2012). Furthermore, a taxonomy is also formulated based on the literature review and tested through the use of the research survey.

The following section will continue to detail the research methodology used in order to perform the research, obtain empirical data, analyse the data and produce the final report. This section will start off with the research philosophy and approach, the research design, the purpose of the research and research target population. The research methodology section will then conclude with the data collection and analysis which was used to complete this research, the research limitations and ethics.

4.1 Research Philosophy and Approach

The research has an epistemological philosophical position, which questions what is considered acceptable knowledge (Saunders *et al.*, 2012). This included a positivism paradigm as data was collected through a structured data collection technique. Positivism, as per

Saunders *et al.* (2012, p. 134), collects "[d]ata about an observable reality and searches for regularities and causal relationships" in the data.

The research approach is inductive. An inductive approach allowed the research, as per Saunders *et al.* (2012, p. 48), to "[e]xplore a topic and develop a theoretical explanation as the data is collected and analysed". The researcher collected data to explore a phenomenon, identify themes and explain patterns to generate a new or explore an existing theory (Saunders *et al.*, 2012). An inductive approach was taken to allow meanings to emerge and identify whether patterns and relationships exist (what-type data) and why they exist (why-type data) through observation of empirical data.

4.2 Research Design

To operationalise the research questions and objectives, a fully integrated and concurrent mixed methods research design is used. This includes both a quantitative and qualitative methodology within a single phase of data collection and analysis (Saunders *et al.*, 2012). This could be done in a short timescale and was more practical to undertake than a sequential mixed methods research design.

A quantitative research design was used to review the survey results statistically, where the focus is on using data to test theory (Saunders *et al.*, 2012). The confirmation of vulnerabilities being reduced is also statistically revised together with associated variables as per the research taxonomy's defined themes and categories. In quantitative research, numerical data is analysed using statistical techniques, including that of probability sampling (see section 4.5). This allows for the identification of relationships between different statistical data. Qualitative data was also allowed through the completion of the survey. Results include what has been said and a formulation of any shared areas of concern, as identified by the sample population.

A concurrent mixed method research design is suited to the philosophical position of Epistemology (Saunders *et al.*, 2012). A mixed method is used as it is understood that there is a difference in culture and processes between organisations. The research can thus not assume that a complete answer to the primary research question is possible from either a subjective or objective point of view. The expected outcomes from using a mixed method design are to develop and extend existing theory and to identify, explore and/or measure case-specific variables.

4.3 Purpose of Research

The purpose of the research and the nature of the research design is exploratory and explanatory. Exploratory research explained the "what-type data", providing the ability to explore and discover what was happening in a particular case or scenario and gain knowledge or further insights about the topic of discussion (Saunders *et al.*, 2012). The explanatory research explained the "why-type data", establishing cause and effects between identified challenges and factors impeding the ability to successfully remediate vulnerabilities. Namely, the research survey allowed respondents an opportunity to provide further detail on any current processes or challenges. This allowed the research to gain insights further to what was received in the literature review, evaluate the feedback and then explain the relationships between these identified points, based on the respondents feedback.

The proposed research was achievable as the researcher has relationships with several financial services institutions (FSI). No travel was required as the survey, research discussions and review of the taxonomy with the target population were all done digitally, thus significant research funding was not required.

4.4 Research Target Population

The target population was FSIs. In particular, the target population included organisations that currently incorporates vulnerability and patch management services in their organisation, most of which would then also include a risk management function in their operations or management process. The target population being FSIs for this research does not imply that this industry has more importance over another. The challenge of effective vulnerability and patch management is understood to be an issue experienced across industry from the literature. The use of the industry does also not imply size of organisation was a deciding factor to include them in the research survey as FSIs of various organisational sizes provided feedback to the survey. The economical impact of a potential cyber breach on an FSI due to a potentially unpatched vulnerability was however considered when deciding a target population for this research.

These organisations are comprised of different business units between which operational and/or service level agreements have already been defined. An operational level agreement (OLA) is the agreement of how a required service will be delivered between internal

departments or business units within an organisation (Esmaili, Gardesh, and Sikari, 2010). A service level agreement (SLA) refers to the level of service promised to a client to deliver a service. A client can be served by an internal business unit delivering a product or service as well as an outsourced partner delivering a service or product. The aim was to get at least four organisations to complete the survey, and the participants were selected to provide a complementary set of data when compared with the literature. The selection of participants also allowed for a diverse set of experiences, backgrounds and perspectives to be understood.

4.5 Data Collection and Analysis

Further to the understanding that the research design was quantitative, allowing a statistical analysis of the feedback (numerical data) to the research survey, the observed empirical data also included opinions and perceptions from people which gave the researcher an opportunity to understand reality (Brady, 2015, Ganin *et al.*, 2017). As a result of this expected subjective feedback, probability sampling was used to obtain a sample population to complete the research survey. Probability sampling is a technique where the participants or respondents for the interview will be sampled based on their expertise and availability (Saunders *et al.*, 2012, Glen, 2015, Dudovskiy, 2018). This allowed for the identification of relationships between different statistical data.

Beres *et al.* (2008b) argues that it is difficult to evaluate how well security processes and controls are affecting your information security. Evaluating the change of these controls or incorporating new solutions or policies proves just as difficult. The data needed to assess the effectiveness of vulnerability management is also difficult to come across due to organisations' security concerns around sharing this information (Afful-Dadzie and Allen, 2014). As a consequence hereof, a structured research survey was created to answer the proposed research questions and was directly correlated with the research taxonomy.

Data was scored based on a score out of 100, calculated against the number of answers to each question, and averaged to allow comparison between the data and allow for conclusions. This means that whether a question had one answer or ten, the approach of averaging the answer out of 100 allows for comparison with other sections where the number of available answer may have been different. As mentioned earlier, qualitative data was also allowed through the completion of the survey. Results therefore included what has been said and a formulation of any shared areas of concern, as identified by the sample population. Data was analysed in the following ways:

- Summaries per question - To help understand the percentages of responses for the different questions.
- Comparisons per question - To compare some of the questions based on the maturity of the organisations that participated in this survey.
- Normalised question rating scales - To compare responses between questions more easily.
- Highlights of answers - To draw attention to answers that are, for various reasons, particularly interesting in the context of this research.

4.6 Research Survey

The research follows the creation and use of a structured research survey, derived by summarising the literature review and which directly correlates with the proposed taxonomy of this research. The available answers were based on what the literature considers to be working or not working.

A survey is widely associated with exploratory research (Saunders *et al.*, 2012). As per Saunders *et al.* (2012, p. 177), "[s]urveys using questionnaires are popular as they allow the collection of standardised data from a sizable population in a highly economical way, allowing easy comparison". The use of a survey thus allowed the research to reach beyond the target of four organisations with 12 participants, allowing participants to provide feedback to the questionnaire at their own convenience and allowing the researcher to receive multiple responses in parallel. Based on the research feedback, a revised research taxonomy will be detailed and explained in Chapter 6 and 7.

A close-ended (static) survey with static answers was utilised for this research survey and split into themes which formulated the research taxonomy (as found in Table 3.1). Figure 4.1, as defined by Sauro (2019), helps define specific classes of surveys which are used in research papers.

A close-ended (static) survey, with multiple choice options and multiple choice responses, was used for this research to allow for an effective analysis of what has been found in the literature and to create the final taxonomy of data. The survey was shared online, all questions were optional and took the respondents about 15-25 minutes to complete. Some

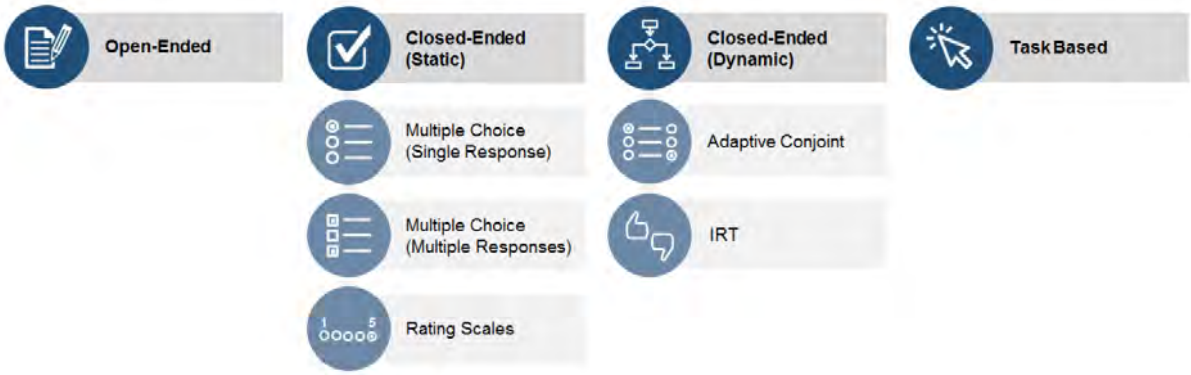

Figure 4.1: Survey classes

questions only allowing a single choice and other questions having multiple available options to choose from. Some questions allowed respondents to add further detail/comments to answers, in the event that the survey and taxonomy had missed something. Rating scales were used for this research to allow for effective comparisons between various answers and taxonomy themes.

4.7 Research Limitations

The target population for the research was South African organisations, more specifically FSIs as mentioned earlier, and the research sample was a subset of the target organisations with whom the researcher collaborated with. The research sample does not reflect all industries or sectors in South Africa, but may be generalised to other enterprise-level South African FSIs. As all data collection occurs in South Africa, a possible limitation is the in-applicability to other contexts. There is, however, no prima facie reason for this to be true. As noted in Chapter 7, further research is welcomed in order to attempt in replicating the research results in other organisational contexts and in other geographical areas.

A threat to the reliability of data is that of a biased researcher, due to the researchers current working relationships within the target population. Researcher bias is revealed when "[a] researcher may allow her or his subjective view or disposition get in the way of fairly recording and interpreting participants' responses" (Saunders *et al.*, 2012, p. 192). This was avoided by creating the survey based on the literature review, allowing participants to add their feedback in addition to the available multiple choice options and accepting

all submissions online through a solution which does not allow the manipulation of the data feedback.

A thematic analysis has also allowed a consensus of common sentiments to be derived from the feedback of the target population. Braun, Clarke, and Terry (2014) refers to a thematic analysis as "[a] method for systematically identifying, organising, and offering insight into patterns of meaning (themes) across a data set" (Braun *et al.*, 2014, p. 57). The thematic analysis was done manually to correlate all data and illustrate patterns and relationships between each identified theme. The above helped to avoid any prejudiced data analysis.

4.8 Ethics

Ethics approval was requested from the Rhodes University ethics board before continuing with the research.

To overcome any organisational concern and to improve the research data quality, the participants/respondents had an opportunity to ask questions and had sufficient time to consider any questions without being coerced (Saunders *et al.*, 2012). An introductory letter was provided to clarify the nature of the research and a consent form was signed confirming that participants are not obligated to participate.

4.8.1 Privacy and Confidentiality

In order to comply with the Protection of Personal Information Act (POPI Act), respondents were informed about what data will be required, why it is required, how it will be processed and how it will be stored. Respondents were also educated on how to request the provided data at a later stage.

Due to the nature of the study, the respondents were not obligated to provide the researcher with a form of identifiable information. However, an understanding of their expertise and role in the field was required. All responses were kept confidential and used for the purposes of this research only. Confidentiality and anonymity were assured through anonymizing and aggregating data, the use of pseudonyms and generalization in order to remove personal identifiers (Saunders *et al.*, 2012). Direct quotes herein will therefore be attributed to anonymous respondents.

User participation implies that the respondents read and understood the research information sheet, that they were aware they could ask questions, that they understood that their participation is voluntary and that they were free to choose not to participate at any stage. It was also understood that the data collected may be reused in further research. The information provided by the respondents was strictly for the completion of the aforementioned degree. While their knowledgeable contribution was valued, there were no benefits to participation and the respondents were not disadvantaged in any way if they chose not to participate.

Data stored was protected on an encrypted hard-drive with password authentication and secured behind a Windows firewall. Data will only be released to the respondents when requested. All paperwork was digitised and then shredded. The summary of findings can be requested from the researcher, at any stage, by emailing the researcher.

4.9 Research Implementation

The research implementation was in line with the research design, in particular a mixed methods research design which includes both a quantitative and qualitative methodology, and the survey was deployed using a well-established internet based survey service. The identification of prospective respondents, the total number of survey respondents and the analysis of their responses will be further discussed in the next chapter.

Chapter 5

Data Analysis

This chapter presents the results of analysing the data collected through a research survey and relates these to the research questions and objectives. The following sections detail each theme of the research taxonomy, the associated survey questions and the respondents feedback. The multiple choice answers of the research survey correlate with the subcategories of the taxonomy and the comparison of the questions, or taxonomy categories, are reviewed based on the mentioned risk score rating.

Most sections do provide interpretation of the results including the relevance of questions (e.g. Sections 5.1, 5.2, 5.5.1), the assumption of what it means if someone did not respond to a question (e.g. Sections 5.1-5.4), the correlation of users from the same organisation having different opinions or answers to questions, filtering on any additional survey feedback (either adding the feedback in the main responses or articulating what is in addition to the literature / unique discussion points), and any needed similarities / comparison in the data where appropriate, (e.g. Section 5.2 - "The patch management team referring back periodically to the vulnerability management team on items that cannot be patched" was listed in the top three areas of communication circumstances, including being mentioned in additional feedback by respondents) has been detailed in Chapter 5. Table 5.9 and Table 5.10 are further examples of comparing the survey results data, and briefly discussing some of the significant results before the summary of the findings being discussed in Chapter 6.

Chapter 5 will also talk to various included graphs about the survey standard responses and additional responses, as depicted in the graphs, and if there were any responses best placed in a different section in the research (e.g. Figure 5.9 "Circumstances of communication between separate teams", and where the respondent rather provided feedback to

the advantages they see in having multiple teams). The data results in terms of where there are multiple responses from the same organisation is also discussed, or where they may be a significance in lack of response, e.g. Section 5.5.2 - note that neither vulnerability nor patch management feedback had a focus on "creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet" when referring to policies.

Comparing responses to other areas of the results where significant, e.g. Section 5.5.3 - "Three of the 21 respondents were not sure" in terms of whether they practiced certain aspects of the patch management policy or not in their environment. However, the same organisations had concise feedback from other respondents. At least 18 out of the 30 respondents (60%) are therefore currently practicing some form of their defined patch management policy. There are three points worthwhile to note from the above feedback. A "patch management lifecycle", was one of the top five items listed by organisations' patch management policy or similar document, at 86.7% of the 30 respondents. However, 38.1% of the 21 respondents stated that they are not currently practicing this item.

Due to Figures 5.24, 5.25, 5.27, 5.37 and 5.43 being quite large with data representation, the tables that summarise these figures, e.g. Table 5.12 and 5.13 etc., provide a shorter and more concise summary of the significant survey results. For consistency throughout Chapter 5, all remaining figures are summarised with a respective table.

To summarise, Chapter 5 allows for results to be compared where appropriate however, Chapter 6 will then discuss the findings in comparison to what the literature review had revealed and thus is able to contextualise the survey feedback from Chapter 5, detailing the significance and implication of the data analysis.

5.1 Identification of Prospective Respondents

The research was provisionally intended for 12 participants in total from four FSIs. The researcher was able to reach out to 67 information security practitioners or professionals in the information security field, from 26 different organisations. From this total outreach, 14 gatekeepers from the different organisations accepted/approved the use and sending of the survey to the leaders and employees of their organisations who have a pragmatic understanding of the research based on their skillset and current roles and responsibilities.

The research analysis below is from 30 responses, obtained from 12 of the 14 approved reputable FSIs as delegates from two of the approved organisations did not respond in

the allocated time-frame for this research data collection. The roles who took part in this survey include Chief Information Security Officer (CISO), other C-level positions (such as Chief Technology Officer (CTO), Chief Operational Officer (COO) and Chief Information Officer (CIO)), Information Security Officer (ISO), Information Security Manager, IT Manager, consultant, engineer, analyst and risk and audit officer. From the total research survey feedback, 56.7% of the respondents listed themselves as non-technical.

Figure 5.1 shows that although South African FSIs were selected, 60% of the organisations who completed the survey do have a global footprint when considering the remediation of vulnerabilities. This talks to the earlier mentioned possible research limitations and allows for further research to be better adapted.

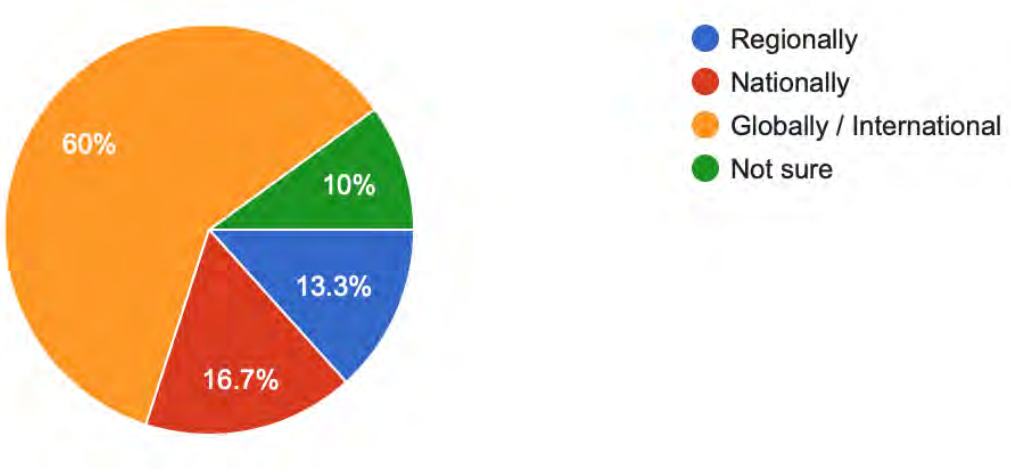

Figure 5.1: Operational size of participating organisations

Figure 5.2 represents the number of employees who work for each of the organisations that took part in this survey. It is important to understand the relation between the number of employees and assets the organisation needs to protect in order to understand the scope of each organisation's vulnerability and patch management service.

Figure 5.3 represents the number of assets, including workstations and servers for the participating organisations, and thus the magnitude of what they need to protect. It is evident from the employee graph and the asset graph that over half (58.6%) of the participating organisations have more than 10000 employees. However, the asset graph illustrates that 41.4% have to protect almost double the number of assets, i.e. more than 20000 assets.

Figure 5.4 summarises the number of years that most respondents have been in the information security industry. Noticeably, most respondents have been in the industry for

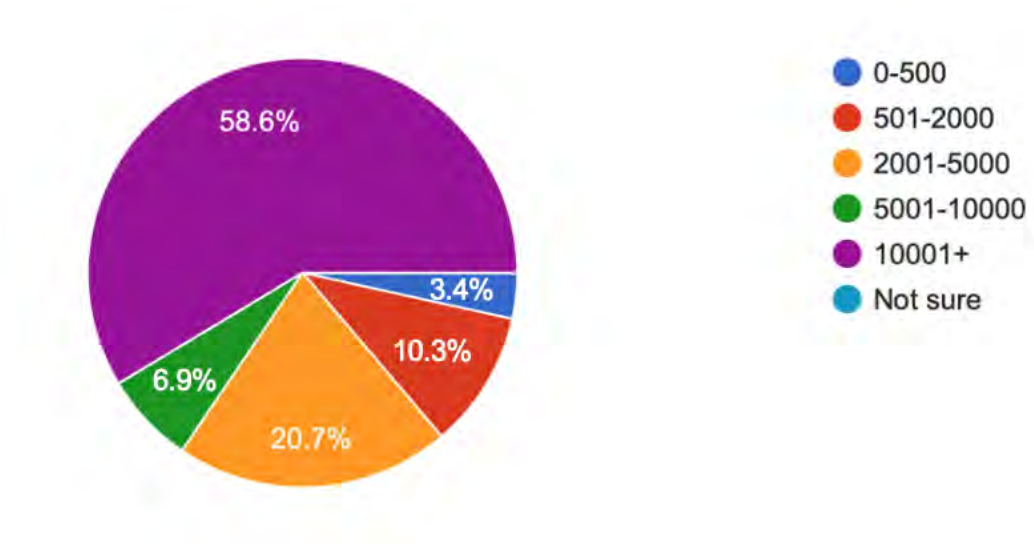

Figure 5.2: Employee count for participating organisations

13+ years which illustrates the expansive knowledge of the respondents and their expected pragmatic approach to the topic of this survey and its questions.

Figure 5.5 represents some of the qualifications the survey respondents currently have. A large majority of the respondents have not only been in the industry for more than 13 years, they also hold leading international qualifications in the field such as Certified Information Systems Security Professional (CISSP) (47.6%), Certified Information Security Manager (CISM) (52.4%) and ISO27001 (Foundation, Lead Implementer, etc.) (38.1%).

5.2 Team Structure

As earlier reviewed, Table 3.2 provides detail on the themes and associated categories for this research taxonomy. The themes and categories are now summarised through the following sections and graphs for a better understanding of what the respondents currently practice and find benefit from.

The team structure within each of the participating organisations is reviewed in this section. This section details what the respondents' understanding is of team structures and the organisational benefit(s) thereof.

5.2.1 Single Service Teams to Multiple Service Teams

Q. How have you been involved with vulnerability management?

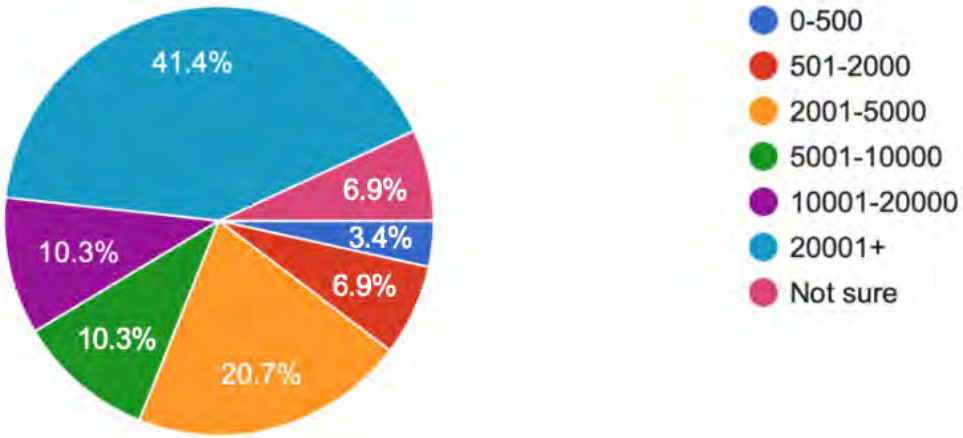

Figure 5.3: Asset count of organisations

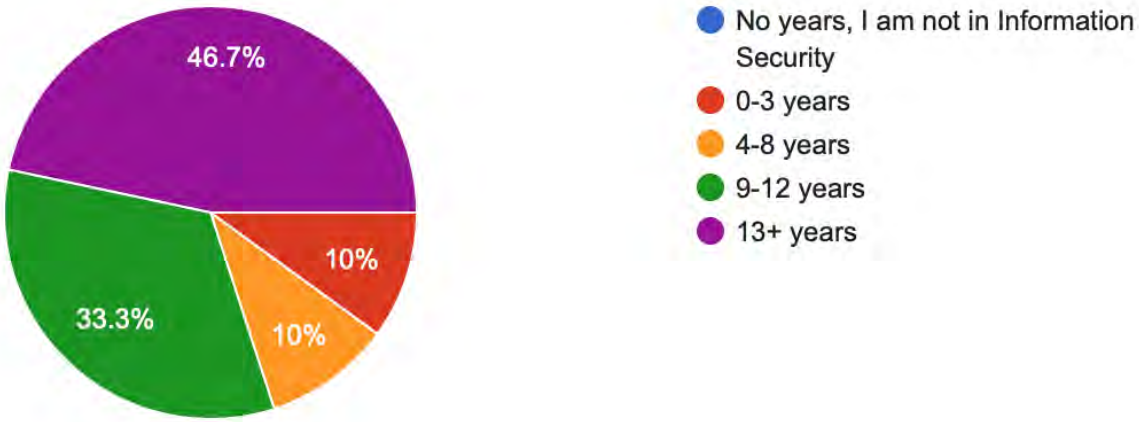

Figure 5.4: Respondents' years in information security

☐ No involvement

☐ Worked with managing teams

☐ Led the managing teams

☐ Created / improved service for organisation

Q. How have you been involved with patch management?

☐ No involvement

☐ Worked with managing teams

☐ Led the managing teams

☐ Created / improved service for organisation

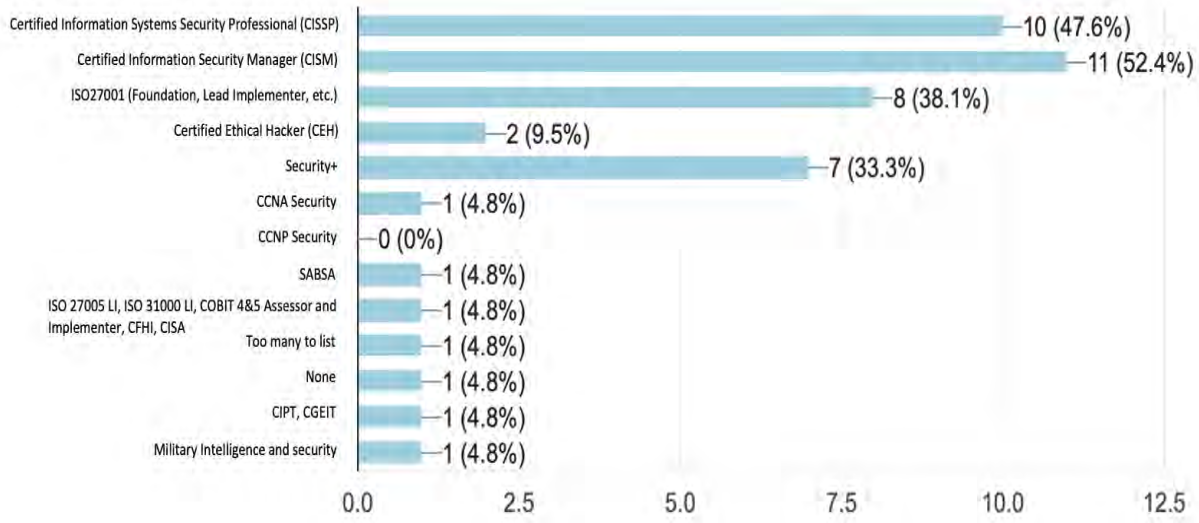

Figure 5.5: Respondents' current information security qualifications

Q. In your organisation, does one cross-functional team have responsibility for vulnerability management and patch management?

- ◯ Yes
- ◯ No
- ◯ Not sure
- ◯ Other: (*write-in answer*)

Figure 5.6 represents how the respondents have been involved in the vulnerability and patch management services for their organisation. As you will see, separate graphs for each of the mentioned services are detailed in Figure 5.6. Their involvement, or available answers to the question, could include "no involvement", "worked with managing teams", "led the managing teams" and "created or improved service for organisation". Respondents were able to select multiple options since more than one could be applicable.

Out of the 30 respondents, 19 have been involved in "working with the team" and 13 were involved with either "creating" or "improving" the service for the "Vulnerability Management" section. With regard to patch management, 17 have been involved in "working with the team" and 13 were involved with either "creating" or "improving" the service. "Working with managing teams" and "created or improved services" in each of these areas continues to indicate the experience of the respondents.

Figure 5.7 shows that, of the 30 respondents, 63% of the participating organisations have multiple teams attending to their vulnerability and patch management services rather than one cross-skilled team.

Figure 5.6: Respondents involvement in vulnerability and patch management services

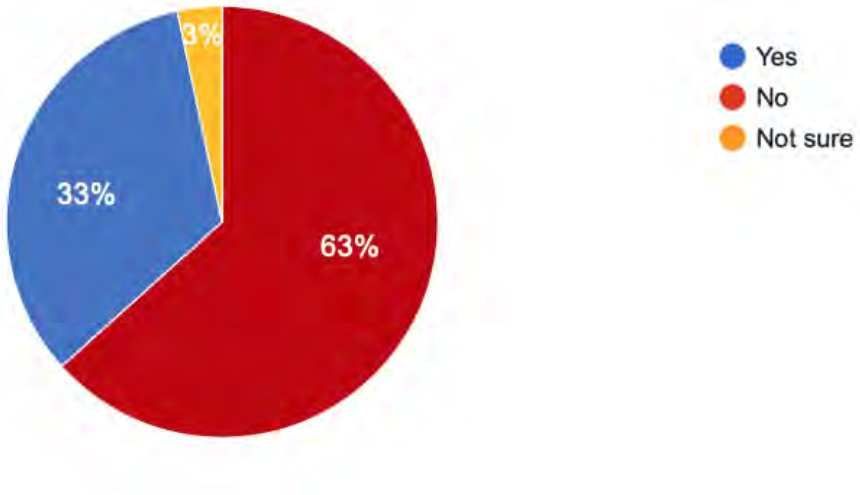

Figure 5.7: A cross-functional team having responsibility for vulnerability management and patch management services

There were additional responses when questioning whether the respondents had a cross functional team within their organisation for the questioned services. These responses were included in the main options presented based on how the respondent answered additional questions. In particular, the additional responses and the associated data correlation included the following:

- Additional response - “Do-er (IT) and Checker (IS)”. This was placed as “no” as the respondent continued to answer questions based on if they had separate teams and how they communicated with one another.
- Additional response - “Yes and no”. This was placed as “not sure”.
- Additional response - “There is a software release team responsible for testing and deploying patches, then there is the Core security team responsible for vulnerability

management within the organisation". This was placed as "no" as the respondent continued to answer questions based on if they had separate teams and how they communicated with one another.

Additional feedback implies that the number of respondents who utilise separate teams for the vulnerability and patch management services is 63%, as seen above. Twenty of the 30 respondents have indicated that they are aware of multiple teams being utilised in their organisation to manage the vulnerability and patch management services. These 20 respondents represent 11 of the 12 participating organisations in the survey. It is noticeable, however, that there are participants within the same organisation who have responded with different answers to this question. Some said that there are multiple teams and others said that they only have one managing team for the vulnerability and patch management services. As a result of respondents from the same organisation providing different answers, the resulting figures indicate that respondents from six of the participating organisations confirmed they utilise one cross-functional team for both their vulnerability and patch management services.

5.2.2 Advantages of Different Structured Teams

Q. What do you see as the benefit(s) of having separate teams?

- ☐ Separate teams with more resources allows more tasks to be completed timeously, i.e. improved capacity constraints
- ☐ Dedicated resources with clearly defined roles and responsibilities
- ☐ Able to split costs between different costs centres
- ☐ Having one team is not suited for large organisations
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Figure 5.8 details what the respondents believe are the advantages of utilising multiple teams to manage their vulnerability and patch management services.

The top three advantages, as per the survey feedback, are listed in Table 5.1. Two respondents from two different organisations did not respond to this question which may imply that they saw no advantage from having multiple teams to manage vulnerability and patch management within their organisations.

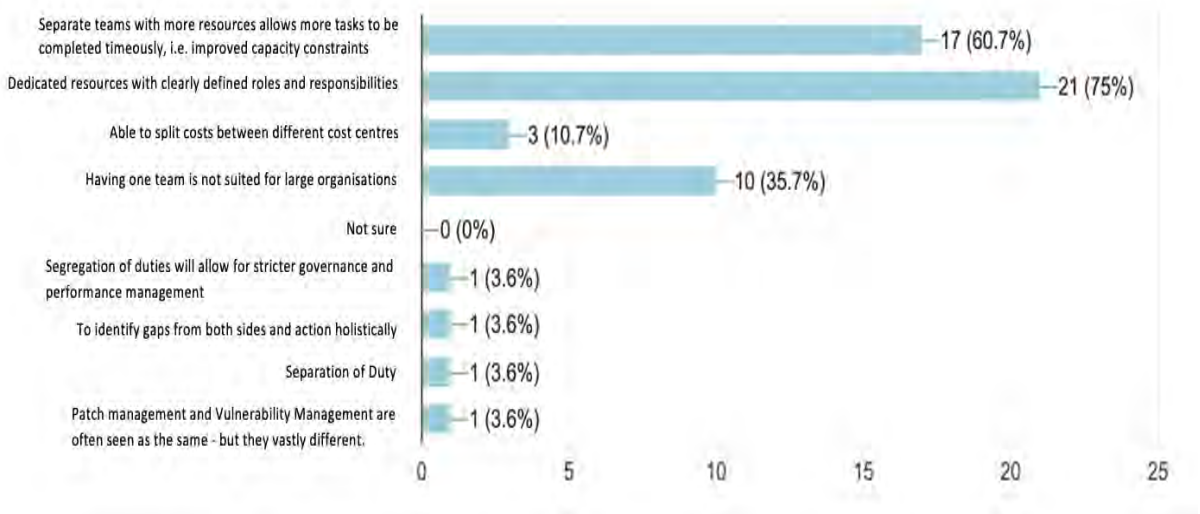

Figure 5.8: Advantages of having separate teams

	Advantages of separate teams	Percent
Top three	Dedicated resources with clearly defined roles and responsibilities	75%
	Separate teams with more resources allows more tasks to be completed timeously, i.e. improved capacity constraints	60.7%
	Having one team is not suited for large organisations	35.7%

Table 5.1: Advantages of separate team structures

Further to the defined multiple choice options in the survey, four respondents from three different organisations provided additional comments on the advantages of utilising separate teams. The additional feedback does reflect similar perceptions from the respondents on the advantages, in particular the segregation or separation of duties, and the understanding that patch and vulnerability management are different services and having separate teams allows for gaps to be correctly identified in each service offering and actioned accordingly. This does correlate with what was found in the literature review with regards to having dedicated resources with clearly defined roles and responsibilities.

One respondent provided two further suggestions, after the survey review, around process and effective vulnerability management:

- A collaboration page for everyone to communicate and have visibility on challenges or tasks with positive results would result in the correct principles being utilised through the organisation.
- The organisation's SIEM solution, including the vulnerability scanning tool, can facilitate vulnerability management by issuing tasks to review remediation and also

gives users in the business the capability of testing whether their response to remediating a vulnerability was successful.

5.2.3 Communication of Separate Teams

Q. If you have separate teams, under what circumstances do they communicate?

- ☐ The vulnerability management team providing the patch management team with a list of specific vulnerabilities to action
- ☐ The patch management team referring back periodically to the vulnerability management team on items that cannot be patched

  Q. What would these items which cannot be patched include?

  - ☐ Interoperability issues
  - ☐ Operating systems that have reached EOL
  - ☐ Machines that require configuration updates
  - ☐ Service pack restrictions
  - ☐ Upgrade requirements
  - ☐ Not sure
  - ☐ Other: (*write-in answer*)
- ☐ The vulnerability management team doing a post scan to confirm the patch management cycle was successful for the patch management team
- ☐ Prioritising remediation options with identified vulnerabilities
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Figure 5.9 provides an understanding of communication circumstances from 27 respondents across 12 organisations.

As per Figure 5.9, the top three answers of circumstances for communication are listed in Table 5.2.

The last two options in Figure 5.9 were identified by separate respondents from different organisations, but not found in the literature. In the first case, various application development teams would have their own patch management capability and thus not be part of the Microsoft patch management team or require a need for communication to different teams. Although this does not associate with the advantages or disadvantages

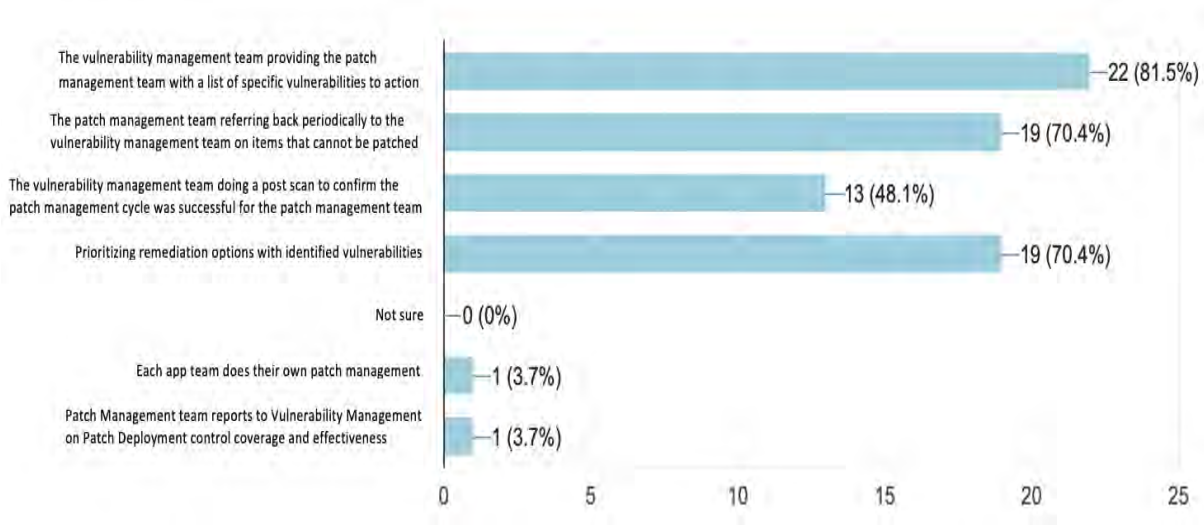

Figure 5.9: Circumstances of communication from separate teams

	Circumstances of communication from multiple teams	Percent
Top three	The vulnerability management team providing the patch management team with a list of specific vulnerabilities to action	81.5%
	The patch management team referring back periodically to the vulnerability management team on items that cannot be patched	70.4%
	Prioritising remediation options with identified vulnerabilities	70.4%

Table 5.2: Circumstances for team communication

of having multiple teams involved in the vulnerability and patch management teams, the survey respondent continued to highlight the advantages they see in having multiple or separate teams, namely: "separate teams with more resources allows more tasks to be completed timeously, i.e. improved capacity constraints", and "having one team is not suited for large organisations".

The second case spoke to communication between vulnerability and patch management teams that included the patch management team giving feedback to the vulnerability management team regarding operational effectiveness, in particular the transparency on patch control coverage and effectiveness.

"The patch management team referring back periodically to the vulnerability management team on items that cannot be patched" was listed in the top three areas of communication circumstances, including being mentioned in additional feedback by respondents. Figure 5.10 provides an understanding of what cannot be patched, as per 23 respondents from 11 of the participating organisations.

Table 5.3 details what the top four items that cannot be patched are. Four items are

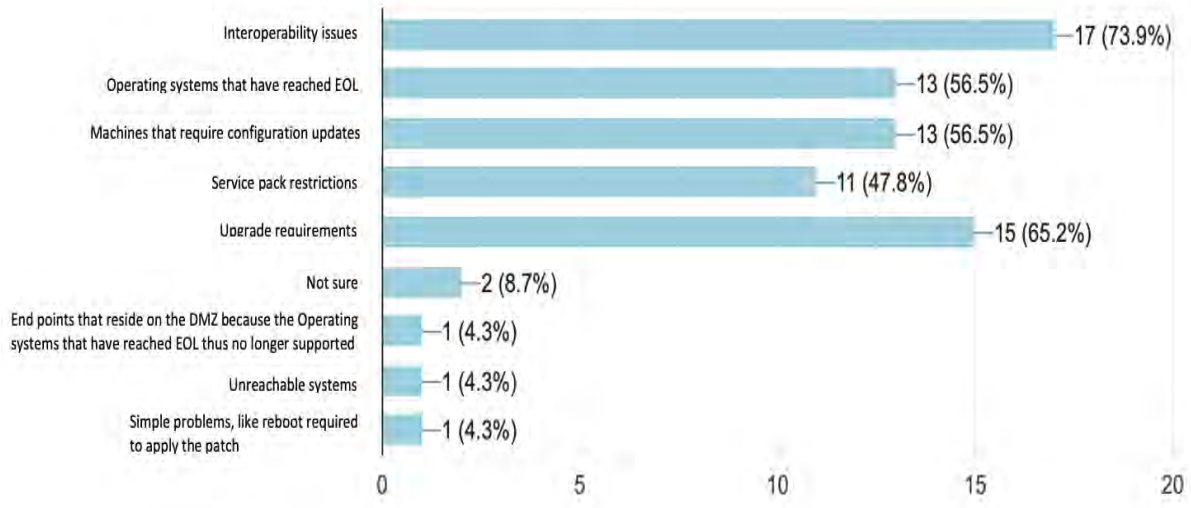

Figure 5.10: The patch management team referring back to the vulnerability management team on items which cannot be patched

	Communication of what cannot be patched	Percent
Top four	Interoperability issues	73.9%
	Upgrade requirements	65.2%
	Operating systems that have reached EOL	56.5%
	Machines that require configuration updates	56.5%

Table 5.3: Team communication of what cannot be patched

listed due to the last items having the same percentage of respondent responses.

Three respondents from three different organisations specified the following additional items that could not be patched:

- Unreachable systems.
- End points that reside on the DMZ because the operating systems that have reached end of life (EOL) thus no longer supported.
- Simple problems, like reboot required to apply the patch.

The advantages of a single team were also interrogated.

Q. What do you see as the benefit(s) of having one team?

☐ Improved competency with one cross functional team

- ☐ One team with one goal
- ☐ One team allows there to be no barrier between patching and monitoring other means of mitigation
- ☐ One team reduces any possible miscommunication on requests
- ☐ One team reduces the time for tasks to be requested and completed between each service
- ☐ Easier collaboration
- ☐ Better skills transfer
- ☐ One team creates a stronger security oriented focus
- ☐ Dedicated resources with clearly defined roles and responsibilities
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Figure 5.11 details the advantages of having one team, as per 30 respondents. It is evident from Figure 5.11 that there seem to be multiple reasons for having one team to manage the vulnerability and patch management services.

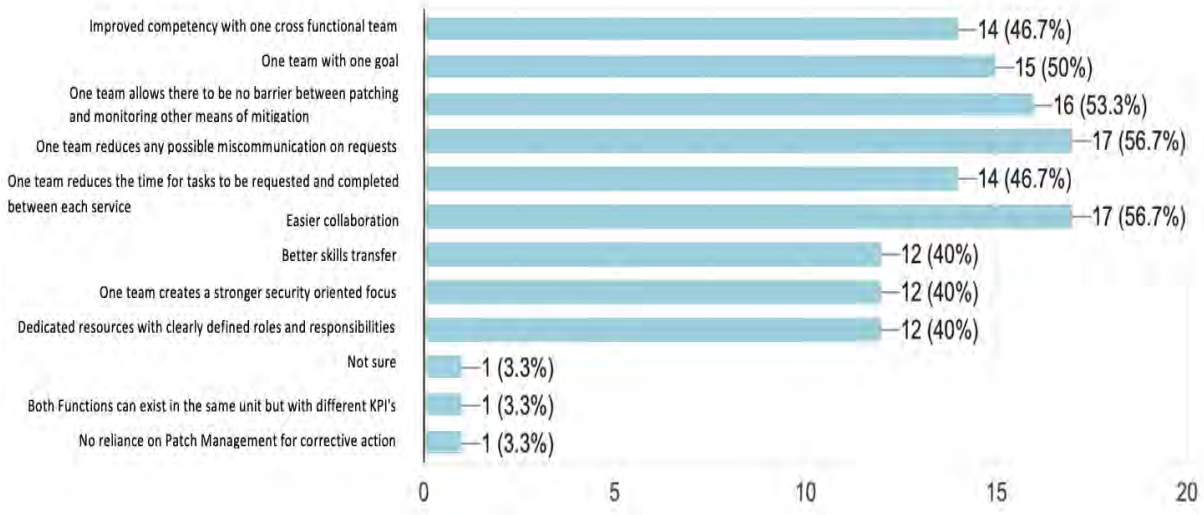

Figure 5.11: Advantages of having one cross functional team

Table 5.4 details what the top three advantages listed of having one team are, as per the total 30 respondents.

	Advantages of a single team	Percent
Top three	Easier collaboration	56.7%
	One team reduces any possible miscommunication on requests	56.7%
	One team allows there to be no barrier between patching and monitoring other means of mitigation	53.3%

Table 5.4: Advantages of one team

5.3 Incident Management

The next theme of analysis is the number of previous incidents within each of the participating organisations. This section provides an understanding of any previous information security incident(s) the participating organisations may have had and their relation to known vulnerabilities or available Windows patches.

5.3.1 Incidents in Organisations

From the 27 respondents from 10 participating organisations for this section, nine respondents from five organisations were able to give actual numbers regarding the vulnerabilities and the possible number of these vulnerabilities related to Microsoft Windows patches.

Out of a total of 33 incidents, 23 vulnerabilities were related to a Windows vulnerability which had a relevant patch available at the time of the incident that equates to about 39.39% of the vulnerabilities the respondents are willing to share about or are aware of.

Only two respondents from two separate organisations experienced high business impacts from incidents related to a Microsoft vulnerability which had a relevant Windows patch available at the time of the incident. Both these respondents gave further feedback stating that they were well-prepared for the incident(s). From the total number of incidents experienced by these two respondents and its relation to an available Windows patch, it is understood that between 25% and 50% of the incidents which were Windows patch related caused a high business impact on the effected organisations.

Medium impacts were mostly associated with a Windows patch requirement. From the medium line items, 50% of the respondents, whom are associated with one organisation, seemed prepared for the incidents. In contrast, from the respondents who mentioned they were not prepared for the particular incident(s) in their organisation (although these correlate with “low” or “medium” business impact), one respondent mentioned they had

to bring down a production cloud environment in order to investigate and calculate the impact of the incident.

Although the above review was done on organisations that responded regarding their known incident statistics, several organisations were able to add further information on the topic, the most relevant of which are:

- The environment within which the impact is felt (e.g. cloud, dev/test, virtualised, etc.) makes a difference to how severe the impact is.
- Issues such as old OS versions and deployment of incorrect PC images continue to affect patching.
- Impacts often had a transitive impact on other systems that depended on the affected ones.
- The involvement of multiple teams on the patch management side sometimes made it difficult to commit to a resolution time for an incident.
- Other best practices, such as backups, become very important from a security point-of-view when ransomware attacks occur, especially if such attacks affect shared resources.
- Custom software adds to the complexity of testing during patch rollout.

5.3.2 Organisations Prepared for Incidents

Figure 5.12 shows that, from 27 responses across 12 organisations, 74.1% believe they were well prepared for the incidents that took place in their environment.

Being prepared refers to either having a computer security incident response team (CSIRT) or computer emergency response team (CERT), or having further business continuity plans, ITIL process, the ability to apply new security controls for incident management, and so on.

It does remain a positive experience to receive the above feedback from a group of respondents who can be seen as experts in their field. The following sections will complete the analysis on the remaining taxonomy themes.

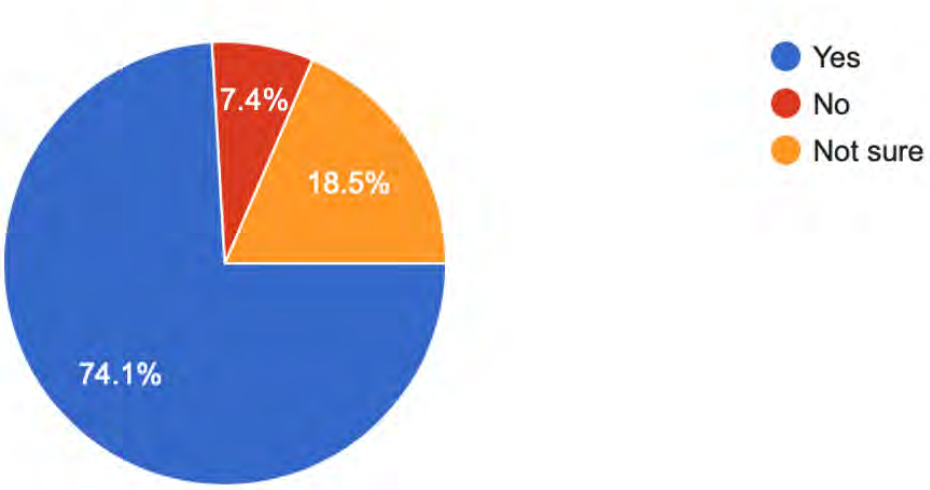

Figure 5.12: Organisations prepared for incidents

5.4 Vulnerability Management

5.4.1 Vulnerability Management Policy

Figure 5.13 is a summary from 30 respondents on whether they have a vulnerability management policy within their organisation. It does not detail who currently has a policy but is not using it. The 86.7% refers to 26 respondents from 12 of the organisations currently using a vulnerability management policy. Three respondents from different organisations state that they are using similar documents and only one organisational member is currently not sure about whether they have a policy.

These responses are from a total of 12 participating organisations in the survey which, again, implies that there are respondents from the same organisation who have different views or understandings of what is taking place and available in their organisations.

Q. Does your vulnerability management policy or similar document cover...

- ☐ A vulnerability management lifecycle (i.e. scan - prioritise - analyse - report - remediate - validate)
- ☐ Requirement to create a vulnerability management monthly council/forum
- ☐ Detail your vulnerability management strategy

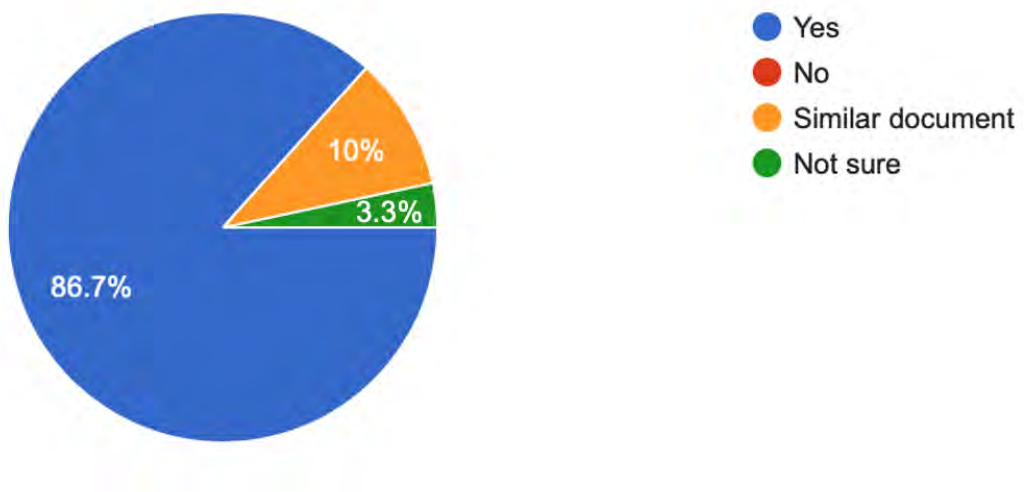

Figure 5.13: Respondents who confirmed they currently have a vulnerability management policy or a similar document

- ☐ Daily automated scan schedules
- ☐ Weekly automated scan schedules
- ☐ Monthly automated scan schedules
- ☐ Scan schedules longer than a month
- ☐ Ad hoc manual scanning
- ☐ Internal scans
- ☐ External scans
- ☐ Authenticated scans
- ☐ Logging calls with respective teams to remediate vulnerabilities
- ☐ Service levels/timelines for patching different vulnerability severities
- ☐ Post checks to confirm a vulnerability is remediated
- ☐ Risk assessments on threat, available patch and other remediation options
- ☐ Daily/weekly/monthly review of failed scans, i.e. health checks
- ☐ A risk dispensation/exemption process for assets that cannot be scanned, i.e. due to access issues or operational restrictions, downtime restrictions
- ☐ Creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet
- ☐ A separate process to tackle zero-day vulnerabilities or otherwise expedite patches

☐ Creating periodic management and/or operational reports for action

☐ Not sure

☐ Other: (*write-in answer*)

Figure 5.14 illustrates what some of the key focus areas of an existing policy are.

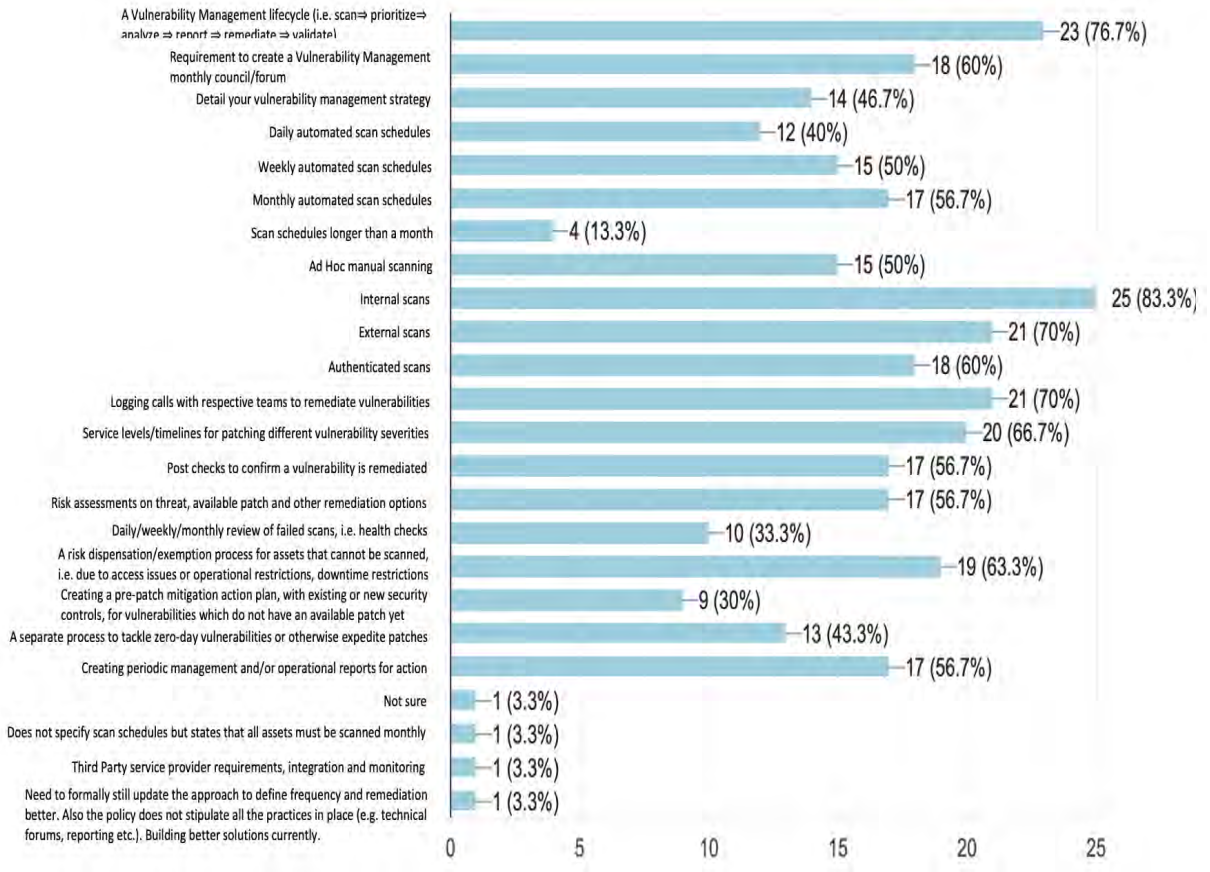

Figure 5.14: Items of a vulnerability management policy or similar document

Table 5.5 summarises Figure 5.14 and illustrates that from the 21 available subcategories or available drop down/multiple choice answers, the five most favourable topics within the respondents vulnerability management policies, as per the feedback from the 30 respondents of the participating organisations.

Respondents noted that policies were sometimes not as well-defined and detailed as they could be, especially in terms of process, or regularly updated and also mentioned the following items covered by such policies which were not present in the literature:

- Third-party service provider requirements, integration and monitoring

	Vulnerability management policies, most common	Percent
Most common	Internal scans	83.3%
	A vulnerability management lifecycle (i.e. scan, prioritise, analyse report remediate validate) sitting	76.6%
	External scans	70%
	Logging calls with respective teams to remediate vulnerabilities	70%
	Service levels/timelines for patching different vulnerability severities	66.7%

Table 5.5: Vulnerability management policies, most common

	Vulnerability management policies, least common	Percent
Least common	Scan schedules longer than a month	13.3%
	Creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet	30%

Table 5.6: Vulnerability management policies, least common

- Policies to stipulate all practices, i.e. technical forums, reporting, etc.

By contrast, Table 5.6 summarises two items which are the least common when the survey respondents articulate what is included in their vulnerability management policies.

5.4.2 Vulnerability Management Policy Items not being Practiced

Figure 5.14 provided detail on what organisations are including in their vulnerability management policies. Figure 5.15 will now detail what organisations are not practicing with respect to their defined organisational policies.

Table 5.7 summarises the six key topic areas of feedback from the respondents, rather than the top three due to several items having the same score or same number of feedback. Responses were obtained from 28 respondents across 11 organisations.

Three of the 28 respondents were “not sure” in terms of whether they practiced certain aspects of the vulnerability management policy or not in their environment. These three individuals represented two organisations from which other respondents had more assured feedback. It was also noted in the survey feedback that the remaining two respondents who did not respond to this question represent two organisations where other respondents from

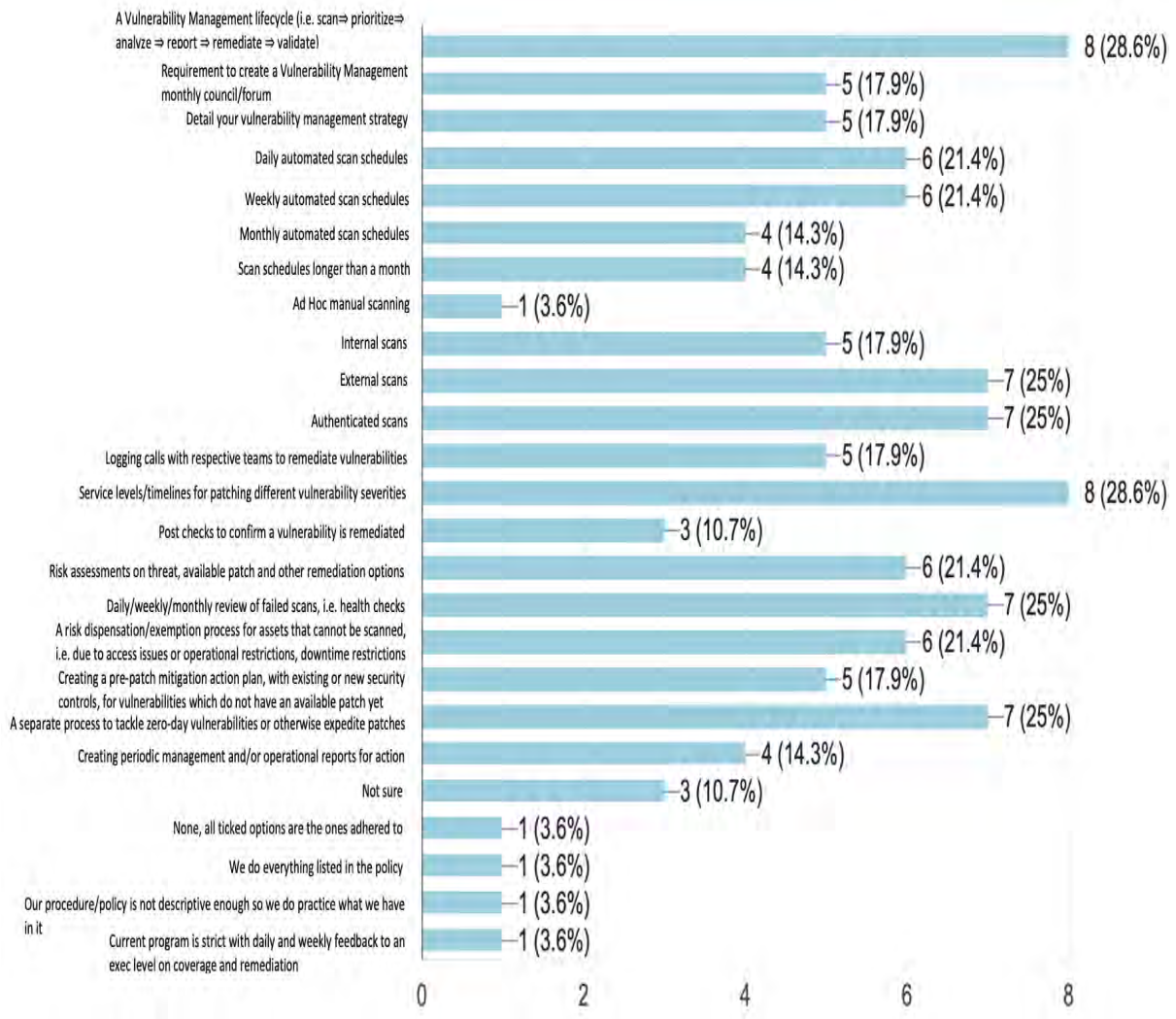

Figure 5.15: Items not being practiced from a defined vulnerability management policy or similar document

the same organisation did provide feedback. This means that 25 out of the 30 respondents (83.3%) are currently practicing forms of their defined vulnerability management policy.

Lastly, to summarise from the above feedback it is worthwhile noting two points. As per Table 5.5, a "vulnerability management lifecycle" was one of the top five items listed in the participating organisations' vulnerability management policy or similar document, at 76.6% of the 29 responses. However, 28.6% of 28 responses then mentioned that they are not currently practicing this item, as per Table 5.7.

Similarly, "service levels/timelines for patching different vulnerability severities" was one of the top five items listed in the participating organisations' vulnerability management policy or similar document, at 66.7% of the 29 responses. However, 28.6% of 28 responses

	Vulnerability management policies, not practiced	Percent
Top "not practiced" items	A vulnerability management lifecycle (i.e. scan, prioritise, analyse report remediate validate)	28.6%
	Service levels/timelines for patching different vulnerability severities	28.6%
	External scans	25%
	Authenticated scans	25%
	Daily/weekly/monthly review of failed scans, i.e. health checks	25%
	A separate process to tackle zero-day vulnerabilities or otherwise expedite patches	25%

Table 5.7: Vulnerability management policies, not being practiced

then mentioned that they are not currently practicing this.

Additionally, four respondents noted that they adhered fully to policy, with one noting that daily and weekly feedback at an executive level — with regard to coverage and remediation — was practiced. A respondent did however continue to mention that as their policy was not descriptive enough, the team was able to adhere to the policy.

5.4.3 Vulnerability Management Trending

This section considers how progressive the participating organisations are with their vulnerability management based on the above feedback.

Figure 5.16 shows the total number of vulnerabilities in the participating organisations' environments.

It seems that from the 29 responses, 24.1% are actually not even sure what their total number of vulnerabilities are within their organisation. You will notice that 41.4% believe their vulnerabilities are sitting between 0 and 10 000. In addition, 20.7% of the responses believe their vulnerabilities are sitting at 10 001 to 250 000. There was one response from the 29 responses who believes their vulnerabilities are more than a million.

Further to the above understanding of the total number of vulnerabilities in the participating organisations, Figure 5.17 illustrates how many of the 28 responses believe that their vulnerabilities currently being remediated are actually increasing or decreasing.

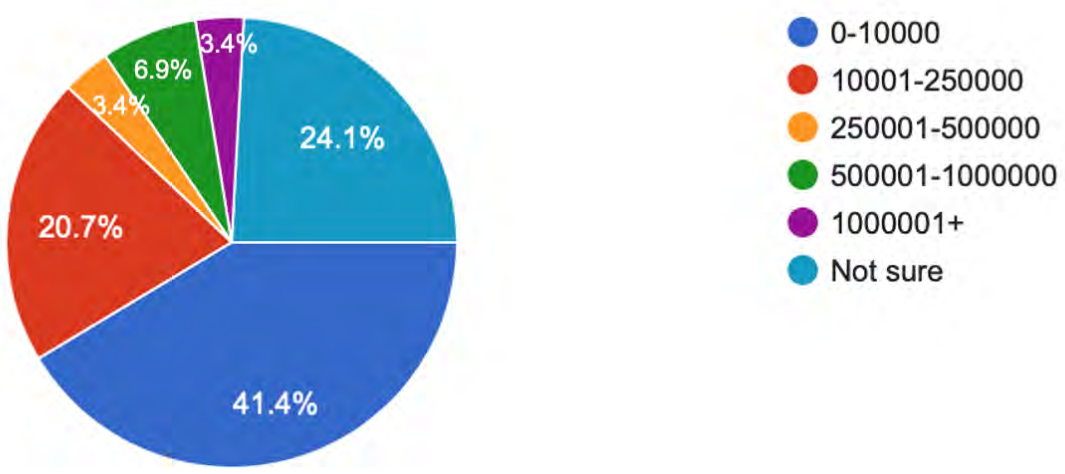

Figure 5.16: Total number of vulnerabilities per organisation

5.4.4 Vulnerability Management Challenges

A significant aspect of this research is determining what the current challenges within vulnerability management are. Figure 5.18 helps to detail exactly that.

Q. What challenges do you face with vulnerability management within your organisation?

- ☐ Budget
- ☐ Lack of executive/management support
- ☐ Resource constraints, i.e. lack of resources, skills shortage, capacity issues or poorly defined responsibilities, etc.
- ☐ Lack of collaboration between the patching and vulnerability management teams
- ☐ One cross functional team not producing positive results on vulnerability remediation
- ☐ Lack of ownership for remediation tasks
- ☐ Lack of or poorly defined vulnerability management policy
- ☐ Lack of or poorly defined patch management policy
- ☐ Lack of communication and user awareness on policies and procedures
- ☐ Processes (not defined or not efficient)
- ☐ Security controls (not available or not effective)

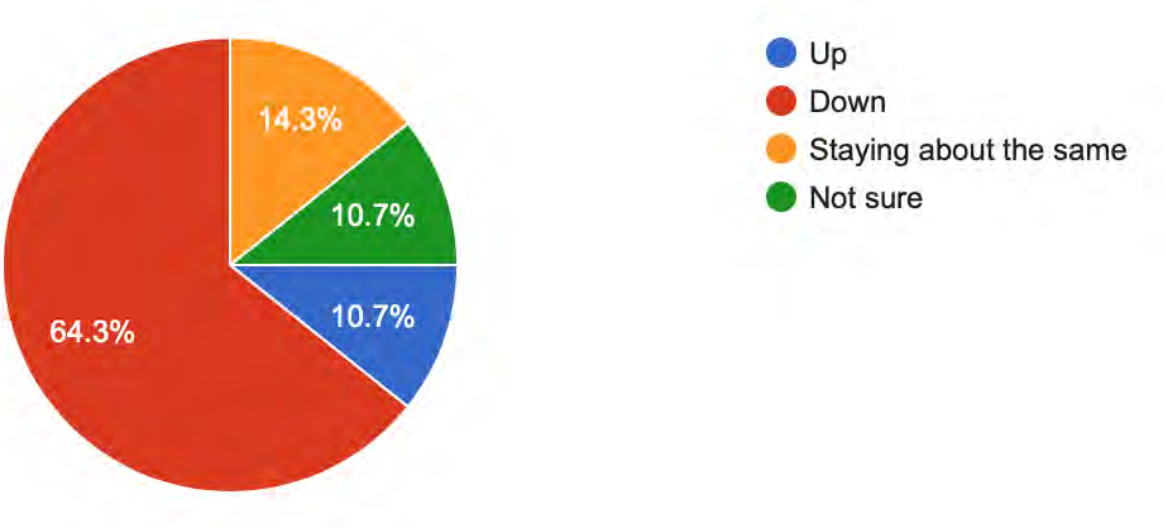

Figure 5.17: Monthly trend of vulnerabilities being remediated

- ☐ Environment too complex
- ☐ Vulnerability management is time consuming
- ☐ Operational restrictions (such as limiting scans or downtime for critical assets)
- ☐ Patching not consistent or timeously applied
- ☐ Scanning or visibility of assets in the cloud
- ☐ The vulnerabilities you trying to remediate in the organisation are not to be remediated by a patch, but rather upgrades, config updates, etc.
- ☐ Superseded patches highlighted in vulnerability management scan although current patches have been applied
- ☐ Identified vulnerabilities causing an upward trend all have risk dispensation/exemption approved, thus removed from reporting and not effectively remediated
- ☐ Organisation only focusing on Critical and High severity vulnerabilities
- ☐ Information overload (from completed scan reports or publicly available vulnerabilities)
- ☐ Vulnerabilities increasing quicker than they can be remediated
- ☐ Technical issues (such as access issues to scan assets, machines offline/unmanaged or technology issues/outdated)
- ☐ Risk assessment not completed to ensure correct priority on remediation
- ☐ Patch teams not having a strong security oriented focus
- ☐ Asset database (such as incorrect or incomplete information of assets, i.e. asset ownership, installed components, services, versions)

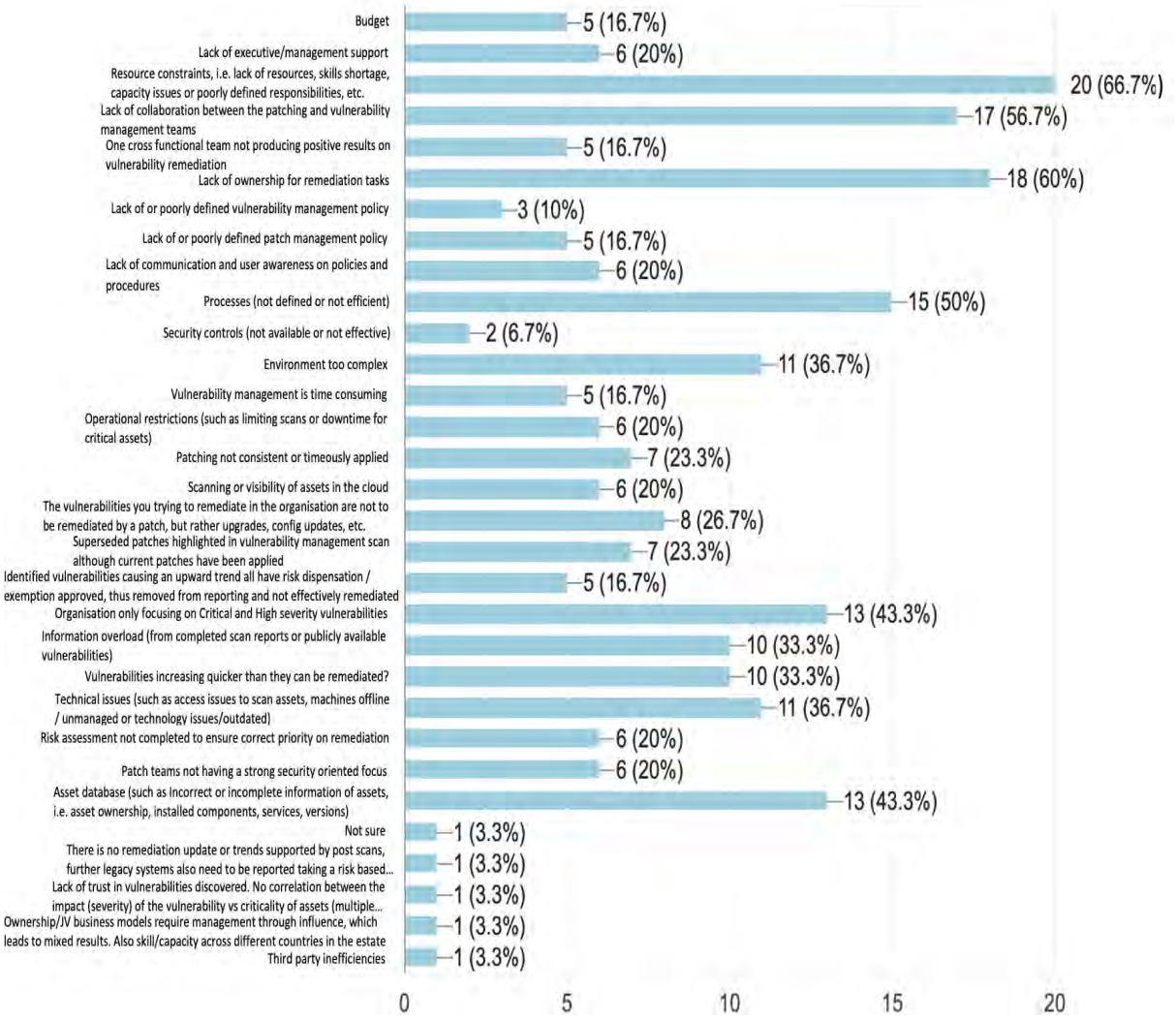

Figure 5.18: Vulnerability management challenges

☐ Not sure

☐ Other: (*write-in answer*)

Table 5.8 summarises the feedback of the top six current challenges from all 30 respondents.

Four respondents from three organisations provided additional feedback to the challenges they were facing in vulnerability management. The following summarises these additional notes into separate points of consideration:

- Lack of trust in vulnerabilities discovered.

Vulnerability management challenges		Percent
Top challenges	Resource constraints, i.e. lack of resources, skills shortage, capacity issues or poorly defined responsibilities, etc.	66.7%
	Lack of ownership for remediation tasks	60%
	Lack of collaboration between the patching and vulnerability management teams	56.7%
	Processes (not defined or not efficient)	50%
	Organisation only focusing on Critical and High severity vulnerabilities	43.3%
	Asset database (such as incorrect or incomplete information of assets, i.e. asset ownership, installed components, services, versions)	43.3%

Table 5.8: Summary of vulnerability management challenges

- No correlation between the severity of a vulnerability and critical or non business critical asset.
- Disconnect between organisations and the outsourcing of vulnerability management activities.
- Skill shortage or skill variances across various teams managing multiple geographics.
- Capacity constraints across teams managing multiple geographics.
- Disconnect between post scans and the identified vulnerabilities which were remediated successfully or not.
- Legacy systems are not being reported through a risk based approach.
- Organisations focus on the high and critical vulnerabilities however there is no tracking of the low and medium vulnerabilities as they may potentially become a high or critical vulnerability for the organisation over time.
- Vulnerability management scans are not part of the development and post production deployment of S-SDLC iterations.
- Third party inefficiencies in performing the vulnerability management tasks.

Although there are items detailed in the additional feedback which do correlate with what was found in the literature, specifically that organisations seem to only take care of a subset of all known vulnerabilities that could be relevant (Beres *et al.*, 2008b), there are a few unique points that stand out. Namely, the lack of trust in vulnerabilities discovered, the disconnect between the organisations and their associated third parties or vendors

to which they outsource the vulnerability management function, the disconnect between post scans and identified vulnerabilities being remediated, legacy systems not being appropriately reported on and the need to include vulnerability management through an organisation's SDLC.

With the understanding of utilised vulnerability management policies in each of the participating organisations and with the total feedback of current challenges being faced, Figure 5.19 illustrates that from the feedback of 30 respondents, there is a balance (50% agree and 50% do not agree) in understanding or perception of whether there is still room for improvement in vulnerability management for their organisations.

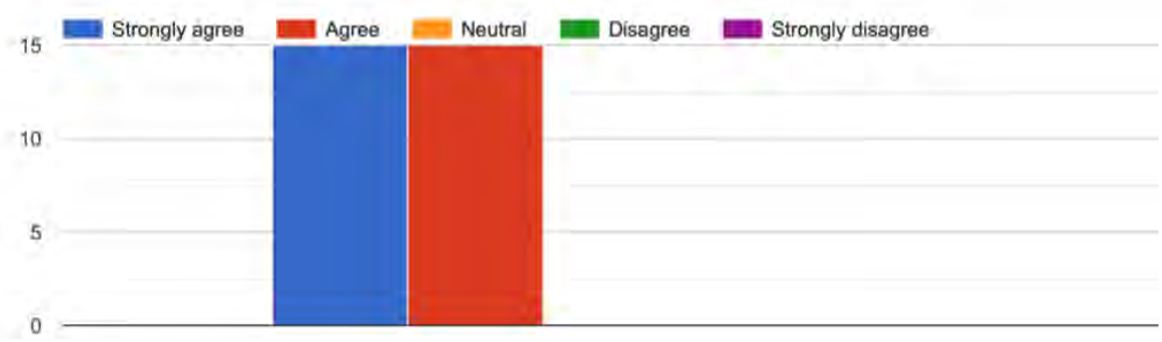

Figure 5.19: Vulnerability management room for improvement

Table 5.9, before going to the "Patch Management" theme of the taxonomy, will help correlate a few aspects. This table is filtered on who is using a vulnerability management policy or has a similar document. This leaves a total of 29 respondents of which certain data-sets are then correlated with their initial feedback that they actually have a policy in place. The score columns for column B and column E is taking the number of answers the respondent gave and calculating a 100% response based on the number of answers or subcategories available for the respondents to select. This score aids to understand 1) respondents with the highest percentage of not following items as dictated in the vulnerability management policy (column B), and 2) the respondents who have indicated the highest number of challenges they currently facing based on the multiple choice option available to them (column E).

From Table 5.9, it is evident which of the respondents have detailed whether they have more than 500 000 vulnerabilities in their organisation and whom of the respondents have between 10 000 and 250 000 vulnerabilities in their environment.

To summarise for the respondents whom have confirmed they have more than 500 000 vulnerabilities, the highest number of vulnerabilities reported (column C), and although

Do you have a vulnerability management policy or similar document?	Score of companies not practicing what is in their VM policy	Number of vulnerabilities in your organisation	Monthly trend of vulnerabilities being remediated in your organisation moving up or down?	What challenges do you face with vulnerability management within your organisation? The average score is used below.	Do you agree that there is still room for improvement required?
Yes	9.52	10001-250000	Down	58.62	Strongly agree
Yes	9.52	500001-1000000	Down	24.14	Strongly agree
Yes	0.00	Not sure	Down	17.24	Strongly agree
Yes	14.29	10001-250000	Down	17.24	Agree
Yes	4.76			37.93	Strongly agree
Yes	9.52	10001-250000	Staying about the same	17.24	Agree
Yes	61.90	0-10000	Down	20.69	Agree
Yes	38.10	0-10000	Down	3.45	Agree
Yes	19.05	10001-250000	Up	55.17	Strongly agree
Yes	23.81	Not sure	Not sure	34.48	Strongly agree
Yes	0.00	1000001+	Down	48.28	Strongly agree
Yes	0.00	Not sure	Down	13.79	Agree
Similar document	14.29	Not sure	Down	10.34	Agree
Yes	38.10	0-10000	Staying about the same	10.34	Strongly agree
Yes	4.76	Not sure	Down	13.79	Agree
Yes	9.52	250001-500000	Down	27.59	Agree
Yes	4.76	500001-1000000		44.83	Strongly agree
Yes	28.57	10001-250000	Staying about the same	27.59	Agree
Yes	0.00	0-10000	Up	13.79	Agree
Yes	4.76	0-10000	Down	13.79	Agree
Yes	33.33	0-10000	Not sure	17.24	Strongly agree
Yes	4.76	0-10000	Down	6.90	Agree
Yes	28.57	Not sure	Not sure	10.34	Agree
Similar document	9.52	0-10000	Staying about the same	48.28	Strongly agree
Yes	4.76	0-10000	Up	13.79	Agree
Yes	95.24	Not sure	Down	89.66	Strongly agree
Yes	4.76	0-10000	Down	34.48	Strongly agree
Similar document	52.38	0-10000	Down	24.14	Agree
Yes	4.76	10001-250000	Down	31.03	Strongly agree

Table 5.9: Vulnerability management review on policies being used vs current challenges in the organisation

Do you have a vulnerability management policy or similar document?	Score of companies not practicing what is in their VM policy	Number of vulnerabilities in your organisation	Monthly trend of vulnerabilities being remediated in your organisation moving up or down?	What challenges do you face with vulnerability management within your organisation? The average score is used below.	Do you agree that there is still room for improvement required?
Yes	9.52	500001-1000000	Down	24.14	Strongly agree
Yes	0.00	1000001+	Down	48.28	Strongly agree
Yes	4.76	500001-1000000		44.83	Strongly agree

Table 5.10: Vulnerability management review on policies being used vs current challenges vs top vulnerabilities

they all understand there is a vulnerability management (VM) policy (column A), they utilise most of what is being indicated in their VM policy as indicated by the low score (column B). The low score refers to the least number of selected items available from the drop down multiple choice options. These respondents also tend to suggest the trend of their remediated vulnerabilities is moving down. Their challenges are below 50% of what was available for selection and lastly, they "strongly agree" (75% of the 4 organisations being analysed) there is still room for improvement in their organisation for their vulnerability management service. Table 5.10 summarises the above.

Further to Table 5.9, the following Table 5.11 illustrates a similar data structure but is focused on per organisation rather than per respondent. The scores are averaged based on the number of respondents per participating organisation. If there was a balance of yes or no answers from respondents of the same organisation, the response of the most senior respondent in that organisation was used for the below analysis.

It is evident from Table 5.11 that on average, organisations are sitting at a score of 21.89% regarding not practicing what is in their vulnerability management policy or similar document. With that said, 16.67% of the 12 organisations who responded, are sitting above 60% in terms of their score on not practicing what is in their vulnerability management policy. Of this 16.67%, the respondents of these organisations still believe the trending of vulnerabilities within their organisation is decreasing. Of the organisations with a high rating in terms of not practicing all items listed in their vulnerability management policy, 50% of these organisations also mentioned their vulnerability management challenges are sitting at 62.07% which is the highest scoring received. In general, however, 58.33% of the participating organisations believe the vulnerabilities within their organisation are

Organisation	Do you have a vulnerability management policy or similar document?	Score of companies not practicing what is in their VM policy	Number of vulnerabilities in your organisation	Monthly trend of vulnerabilities being remediated in your organisation moving up or down?	What challenges do you face with vulnerability management within your organisation? The average score is used below.	Do you agree that there is still room for improvement required?
A	Yes	14.29	250000	Up	41.38	Strongly agree
B	Yes	64.29	Not sure	Down	62.07	Strongly agree
C	Yes	61.9	0-10000	Down	20.69	Agree
D	Yes	4.76	10001-250000	Down	31.03	Strongly agree
E	Yes	9.12	Not sure	Down	25.29	Agree
F	Yes	0	0-10000	Up	13.79	Agree
G	Yes	9.52	10000	Staying about the same	53.45	Strongly agree
H	Yes	9.52	10001-250000	Staying about the same	17.24	Agree
I	Yes	38.10	0-10000	Staying about the same	10.34	Strongly agree
J	Yes	4.76	0-10000	Down	13.79	Agree
K	Yes	17.86	0-10000	Down	8.62	Agree
L	Yes	28.57	0-10000	Down	29.31	Strongly agree

Table 5.11: Vulnerability management review on policies being used vs current challenges in the organisation - Statistics per organisation

decreasing.

5.4.5 Escalation of Configuration Issues Identified Through a Vulnerability Management Process

The research acknowledges that there are several other aspects to vulnerability management, other than patch management. There are also issues such as configuration management issues, systems end of life, systems requiring upgrades, etc. With this said, is the review of configuration or system update requirements being picked up in our respondents vulnerability management scans, is this being escalated, is there ownership between teams and are these vulnerabilities being monitored to completion? Figure 5.20 highlights that 76.7% of the 30 respondents believe this task is happening and there is ownership of who escalates these issues. However, Figure 5.21 depicts that 80.8% from only 26 responses believe this is being monitored successfully to conclusion.

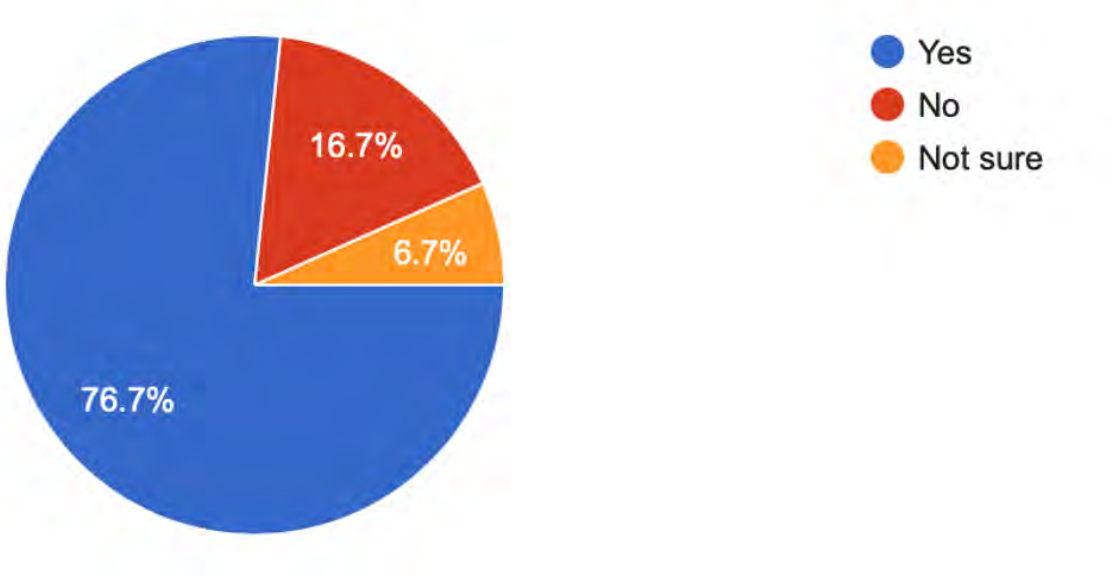

Figure 5.20: Escalation of configuration issues identified through a vulnerability management process

5.5 Patch Management

The above was to retrieve feedback and analyse the theme of "Vulnerability Management" and testing of the research taxonomy. The following section of this taxonomy will help to

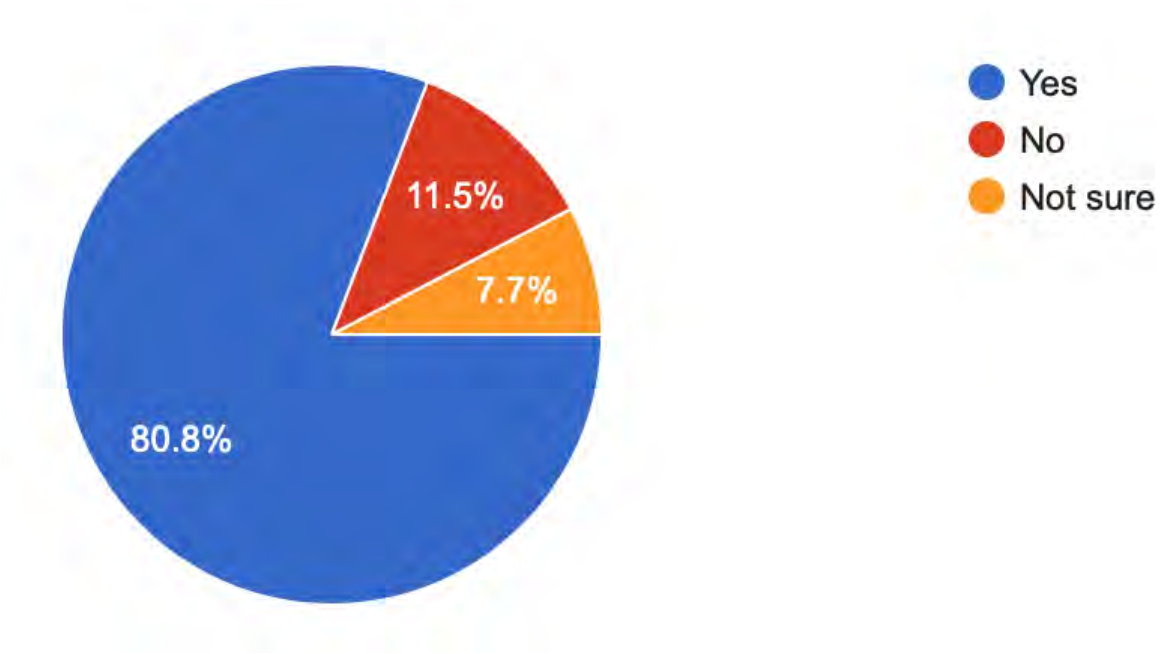

Figure 5.21: Monitoring of configuration escalations, post vulnerability management, to completion

understand the different patch management statuses in the participating organisations. As mentioned earlier these summaries of the themes in the research taxonomy will also allow us to correlate data between the different themes, find similarities and also help ensure the taxonomy is created correctly from the understanding of the literature review.

5.5.1 Utilising a Central Patch Management Platform

Figure 5.22 illustrates that with regards to the utilisation of available solutions to deploy patches to large organisations, 29 out of 30 respondents (96.7%) confirmed that they do use a system/solution for this purpose.

These tools provide several benefits. For larger organisations this is an easier approach to deploying patches, which are made available monthly for Windows. However, this still does not mean that the issue of vulnerabilities within the organisation is resolved or can easily be tackled because vulnerabilities are not all resolved by deploying a patch as mentioned in the earlier sections.

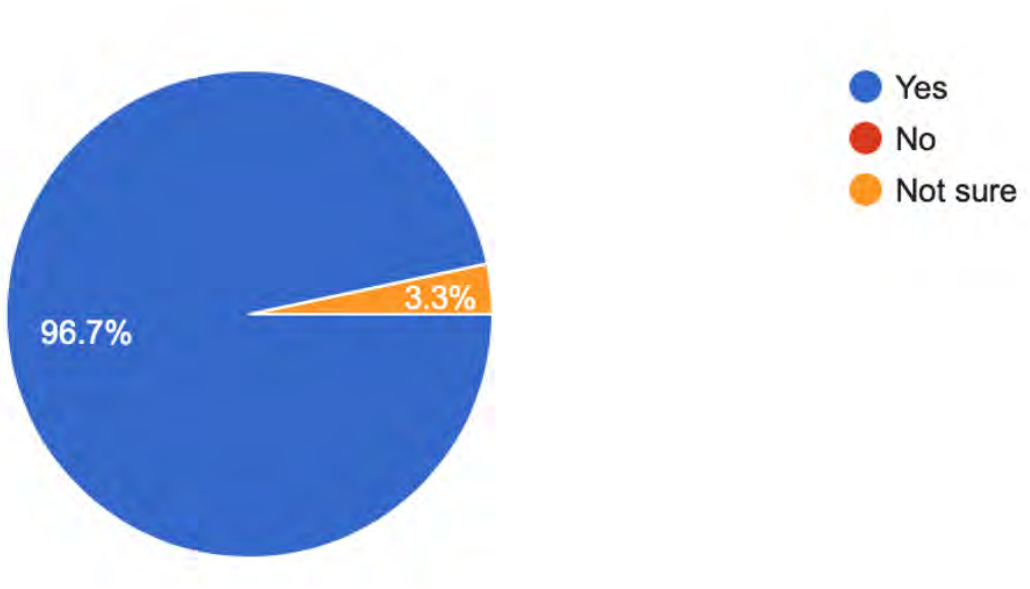

Figure 5.22: Central platform for managing and deploying Microsoft patches

5.5.2 Patch Management Policy

Figure 5.23 summarises feedback from 30 respondents. The 86.7% refers to 26 respondents from 11 of the participating organisations currently using a patch management policy. Two respondents from different organisations, however, are using similar documents and two respondents from the same organisation are currently not sure whether they have a policy or similar document. This from a total of 12 participating organisations in this survey, with multiple respondents per organisation.

With regard to the "not sure" responses, both respondents work for the same participating organisation where other members within their organisation could give more precise feedback on this question. With regard to the responses where a "similar document" was in use, the respondents of each of these two answers also work for the participating organisations where other members within their organisation could give more precise feedback.

Figure 5.24 illustrates what some of the key focus areas are in which their existing policy currently covers.

Q. Does your patch management policy or similar document cover...

- ☐ A patch management lifecycle (i.e. patch analysis/selection - risk assessment & prioritisation - quality assurance/testing - implementation/deployment of updates - post checks/verification - reporting)

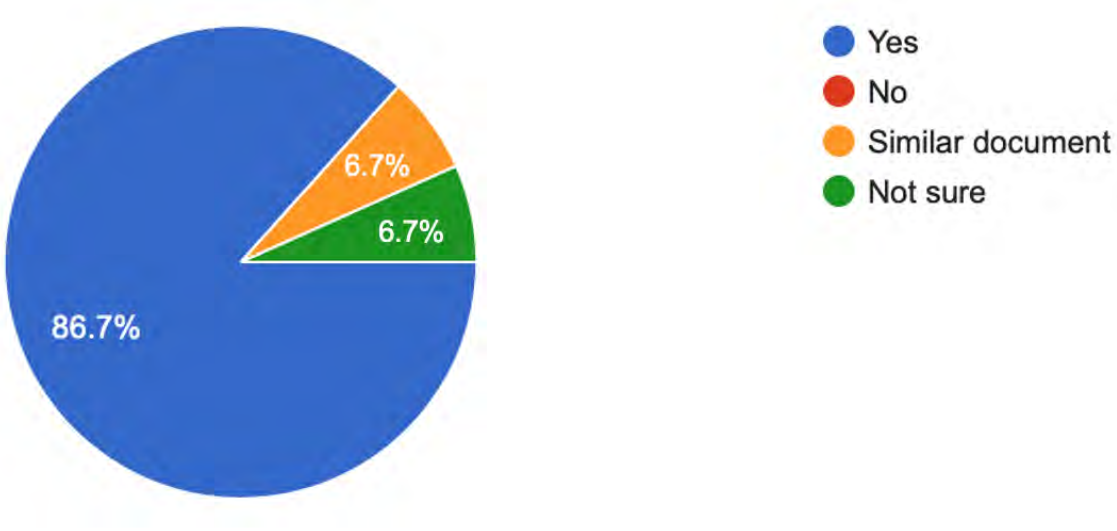

Figure 5.23: Respondents who confirmed they currently have a patch management policy or a similar document

- ☐ Detail your patch management strategy
- ☐ Daily patch schedules
- ☐ Weekly patch schedules
- ☐ Monthly patch schedules
- ☐ Patch schedules longer than a month
- ☐ Automated patching
- ☐ Manual patching
- ☐ Patch management baselines for workstations and servers
- ☐ Patching all servers and workstations
- ☐ Performing test management of patches
- ☐ Service levels/timelines for patching different vulnerability severities
- ☐ Patching only Critical and High vulnerabilities, or
- ☐ Patching all vulnerability severities
- ☐ Only patching vulnerabilities with a known exploit
- ☐ Risk assessments on threat, available patch and other remediation options
- ☐ Patch dependency analysis, i.e. understanding of superseded patches or post service pack dependencies
- ☐ Roll back options for system configurations to a prior known stable state
- ☐ Daily/weekly/monthly review of agent coverage, i.e. health checks

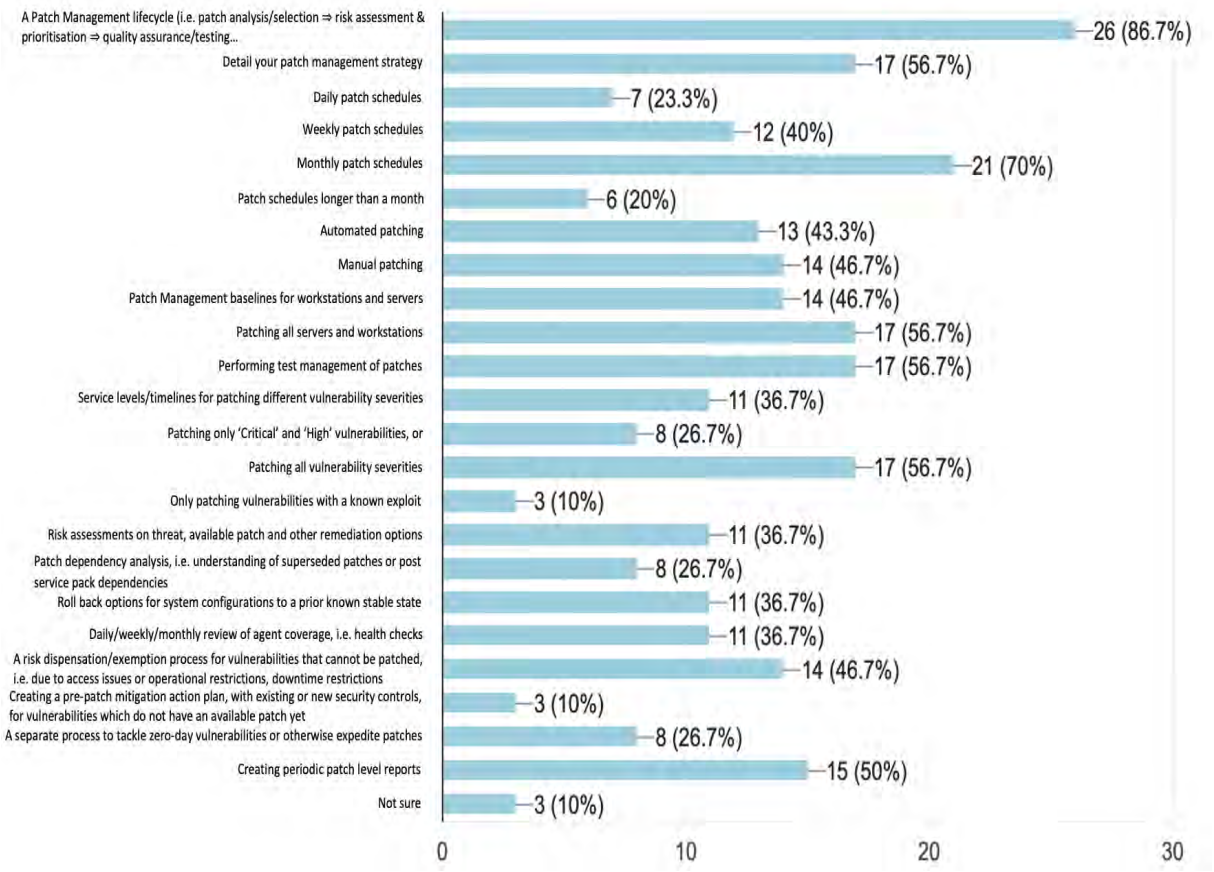

Figure 5.24: Items of a patch management policy or similar document

- ☐ A risk dispensation/exemption process for vulnerabilities that cannot be patched, i.e. due to access issues or operational restrictions, downtime restrictions
- ☐ Creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet
- ☐ A separate process to tackle zero-day vulnerabilities or otherwise expedite patches
- ☐ Creating periodic patch level reports
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Table 5.12 summarises Figure 5.24 and highlights the six most favourable or most common topics within the respondents patch management policies. The top six are listed as four of the items have similar feedback results.

There were 24 subcategories or available answers to the discussion or category of having a patch management policy being used in the organisations. With the top six being listed,

	Patch management policies, most common	Percent
Most common	A patch management lifecycle (i.e. patch analysis/selection, risk assessment & prioritisation, quality assurance/testing, implementation/deployment of updates, post checks/verification, reporting)	86.7%
	Monthly patch schedules	70%
	Detail your patch management strategy	56.7%
	Patching all servers and workstations	56.7%
	Performing test management of patches	56.7%
	Patching all vulnerability severities	56.7%

Table 5.12: Patch management policies, most common

	Patch management policies, least common	Percent
Least common	Only patching vulnerabilities with a known exploit	10%
	Creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet	10%
	Patch schedules longer than a month	20%
	Daily patch schedules	23.3%
	Patching only Critical and High vulnerabilities	26.7%
	Patch dependency analysis, i.e. understanding of superseded patches or post service pack dependencies	26.7%
	A separate process to tackle zero-day vulnerabilities or otherwise expedite patches	26.7%

Table 5.13: Patch management policies, least common

Table 5.13 will help indicate what was the least common or least selected from answers detailing available sections to a patch management policy. The data analysis excludes the two "not sure" responses to who has a policy within their organisation. These two responses are from the same organisation.

Note that neither vulnerability nor patch management feedback had a focus on "creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet" when referring to policies.

5.5.3 Patch Management Policy Items not being Practiced

Figure 5.25 explores what organisations are not practicing with reference to their defined organisational policies.

Table 5.14 summarises the five key topic areas of feedback from the respondents, rather

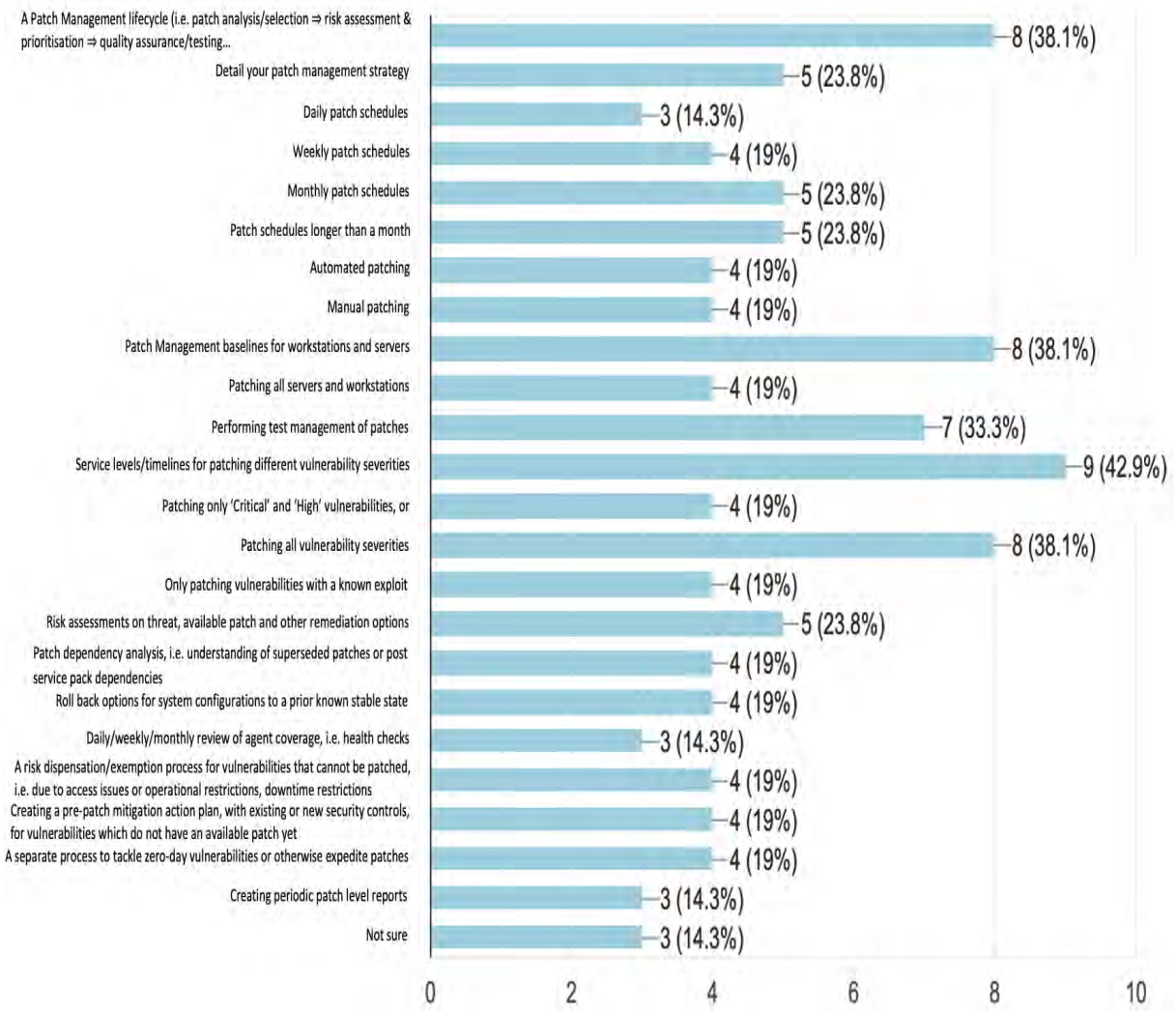

Figure 5.25: Items not being practiced from a defined patch management policy or similar document

than the top three due to several items having the same score or similar number of feedback. Responses were obtained from 21 respondents across 10 organisations.

Three of the 21 respondents were "not sure" in terms of whether they practiced certain aspects of the patch management policy or not in their environment. However, the same organisations had concise feedback from other respondents. At least 18 out of the 30 respondents (60%) are therefore currently practicing some form of their defined patch management policy.

There are three points worthwhile to note from the above feedback. A "patch management lifecycle", was one of the top five items listed by organisations' patch management policy or similar document, at 86.7% of the 30 respondents. However, 38.1% of the 21

	Patch management policies, not practiced	Percent
Top "not practiced" items	Service levels/timelines for patching different vulnerability severities	42.9%
	A patch management lifecycle (i.e. patch analysis/selection, risk assessment and prioritisation, quality assurance/testing, implementation/deployment of updates, post checks/verification, reporting)	38.1%
	Patch management baselines for workstations and servers	38.1%
	Patching all vulnerability severities	38.1%
	Performing test management of patches	33.3%

Table 5.14: Patch management policies, not being practiced

respondents stated that they are not currently practicing this item.

Similarly, "performing test management of patches" was one of the top five items listed in organisations' patch management policy or similar document, at 56.7% of the 30 respondents. However, 33.3% of 21 responses then mentioned that they are not currently practicing this either.

Lastly, "patching all vulnerability severities" was one of the top five items listed in organisations' patch management policy or similar document, at 56.7% of the 30 respondents. However, 38.1% of 21 responses then mentioned that they are not currently practicing this item.

5.5.4 Organisations' System Patch Level Compliance

Further to the understanding of who currently has a patch management policy and is practicing tasks against the service based on their policy, the following will help understand whether the respondents and their organisations believe they are patching Windows systems to the best of their ability.

Figure 5.26 indicates that from 28 responses, 53.6% believe that their systems are not patched at a compliance level of 95%, based on their Windows patching status. This does not directly refer to the vulnerability management status. As mentioned in Chapter 2, attacks often exploit known vulnerabilities which have available patches or other remediation options (Cavusoglu *et al.*, 2008, Okhravi and Nicol, 2008, Afful-Dadzie and Allen, 2014). Risk increases exponentially through the vulnerability timeline as the vulnerability becomes better known (Beres *et al.*, 2008a,b). Only 25% of the respondents, however, believe they have a patching compliance higher than 95%.

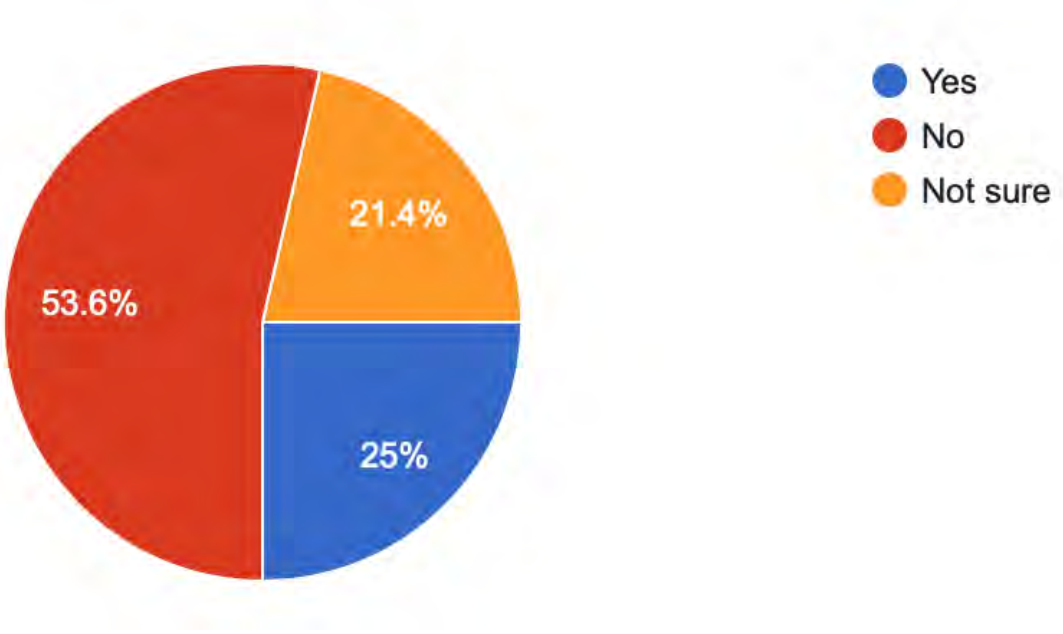

Figure 5.26: Systems patch level compliance

5.5.5 Patch Management Challenges

Q. What challenges do you face with patch management within your organisation?

- ☐ Budget
- ☐ Lack of executive/management support
- ☐ Resource constraints, i.e. lack of resources, skills shortage, capacity issues or poorly defined responsibilities, etc.
- ☐ Lack of collaboration between the patching and vulnerability management teams
- ☐ One cross functional team not producing positive results on vulnerability remediation
- ☐ Lack of ownership for remediation tasks
- ☐ Lack or poorly defined vulnerability management policy
- ☐ Lack or poorly defined patch management policy
- ☐ Lack of communication and user awareness on policies and procedures
- ☐ Processes (not defined or not efficient)
- ☐ Security controls (not available or not effective)
- ☐ Environment too complex
- ☐ Patch management is time consuming

- ☐ Operational restrictions (such as downtime restrictions on critical assets)
- ☐ Patch testing is cumbersome
- ☐ Patching of assets in the cloud
- ☐ No standard way of deploying patches
- ☐ Maintaining assets in the cloud
- ☐ IT Support teams using incorrect images for machines builds
- ☐ Inability to manage zero-day vulnerabilities
- ☐ Legacy patches causing issues
- ☐ Information overload (from completed patch reports or publicised vulnerabilities and patches)
- ☐ Issues with understanding bespoke application limitations
- ☐ Issue is not with deploying patches but prioritising config updates or upgrades
- ☐ Technical issues (such as access issues, coverage issues, machines offline/unmanaged or technology issues/outdated)
- ☐ Maintenance and upgrades of utilised technology
- ☐ Risk assessment not completed to ensure correct priority on remediation
- ☐ Patch teams not having a strong security oriented focus
- ☐ Asset database (such as incorrect or incomplete information of assets, i.e. asset ownership, installed components, services, versions)
- ☐ Not sure
- ☐ Other: (*write-in answer*)

As mentioned earlier, one of the key questions in this research is what are the current challenges not just within vulnerability management but also patch management. Figure 5.27 helps detail the challenges the participating organisations are currently facing.

Table 5.15 summarises Figure 5.27 into the top six current challenges from all 30 respondents.

Figure 5.28 illustrates that from the feedback of 30 respondents, and similarly to the balance of 50% "agree" and 50% "do not agree" statistics found in the "Vulnerability Management" section, 53.3% "strongly agree" that there is still room for improvement in their patch management service.

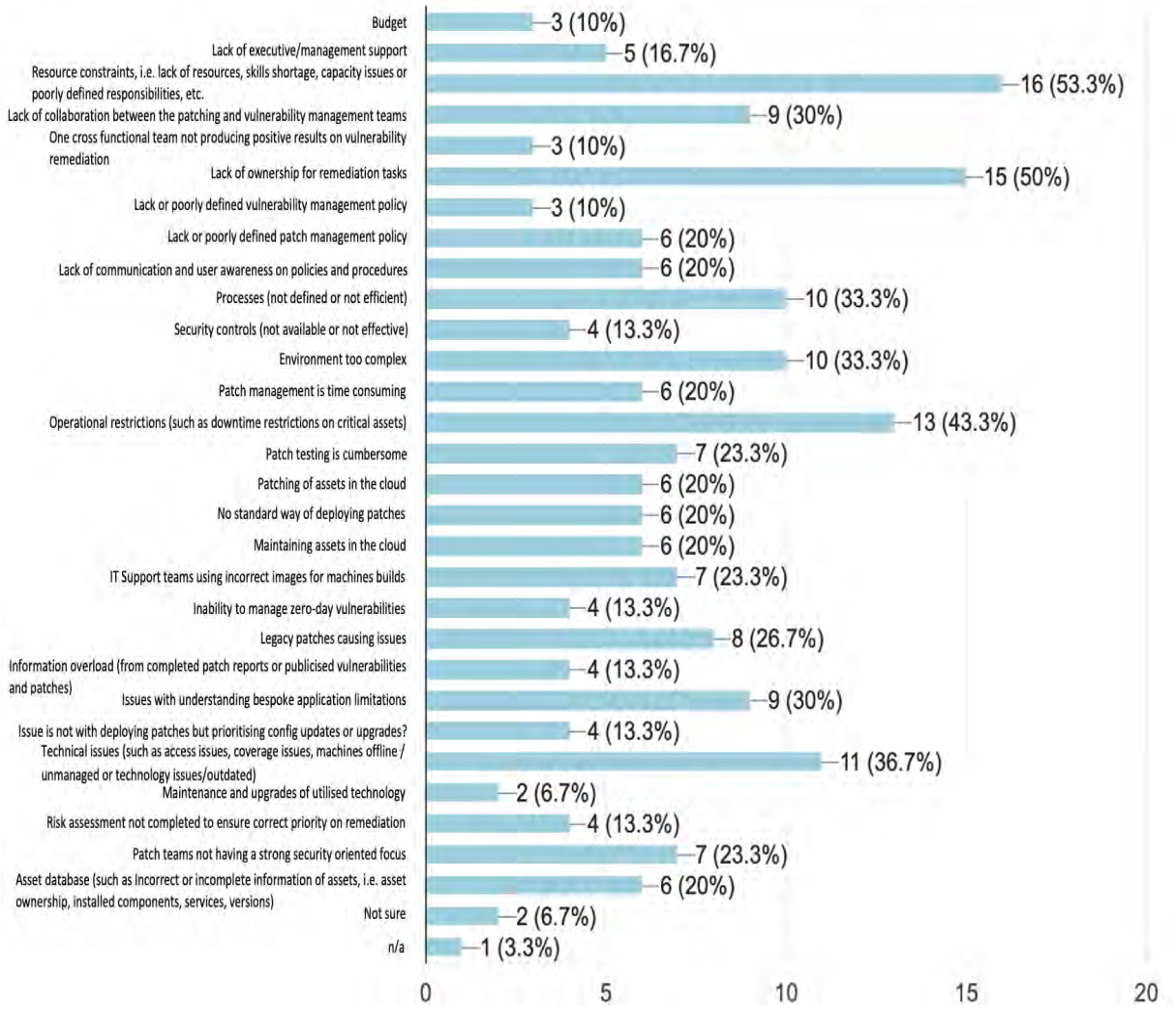

Figure 5.27: Patch management challenges

Table 5.16 correlates several of the already reviewed aspects. This table is filtered on who is using a patch management policy or has a similar document. The table was also filtered on users who were "not sure" or left this field blank regarding their patch compliance. This leaves a total of 21 respondents from 11 organisations, of which certain data-sets are then correlated with their initial feedback that they actually have a policy in place.

The score columns for column B and column D are calculated by taking the number of answers the respondent gave and calculating a 100% response based on the number of answers or subcategories available for the respondents to select. This score helps to understand 1) respondents with the highest percentage of not following items as dictated in the patch management policy (column B), and 2) the respondents who have indicated the highest number of challenges they currently facing based on the multiple choice option available to them (column D).

	Patch management challenges	Percent
Top challenges	Resource constraints, i.e. lack of resources, skills shortage, capacity issues or poorly defined responsibilities, etc.	53.3%
	Lack of ownership for remediation tasks	50%
	Operational restrictions (such as downtime restrictions on critical assets)	43.3%
	Technical issues (such as access issues, coverage issues, machines offline/unmanaged or technology issues/outdated)	36.7%
	Processes (not defined or not efficient)	33.3%
	Environment too complex	33.3%

Table 5.15: Summary of patch management challenges

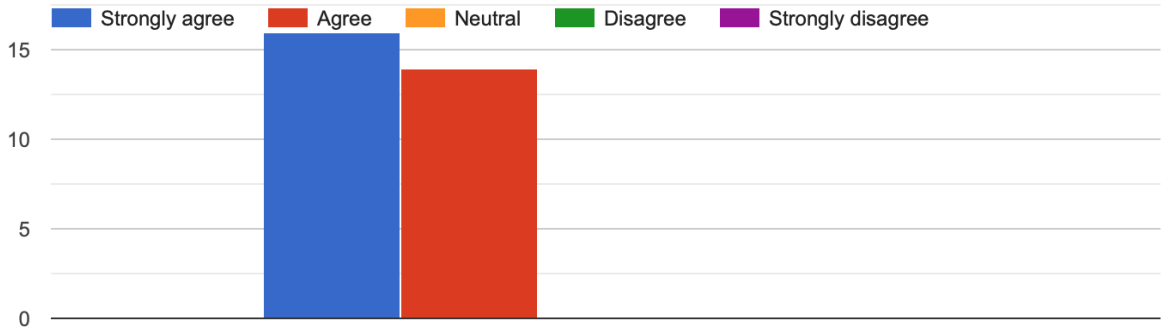

Figure 5.28: Patch management room for improvement

From Table 5.16, column C indicates the respondents whom said their compliance on systems patched is above 95%. Six out of the 21 respondents (28.5%) thus believe they are above 95% patch compliance, all of whom "agree" or "strongly agree" that there is still room for improvement within the organisations for their patch management service.

Table 5.16 also illustrates for the respondents whom mentioned their patch compliance is above 95%, the six out of 21 respondents, that the challenges faced equates to an average of 8.62% (average of column D) of what was available for selection from the subcategories. The remaining 15 respondents who do not agree that their patch compliance is sitting above 95% indicate that the challenges faced equates to an average of 34.25%. However, 80% "strongly agree" that there is still room for improvement in their patch management service.

Lastly, from Table 5.16 you will notice that the respondents who confirmed their patch compliance is above 95% on average do not practice 18.84% of what is listed in their patch policy. The remaining 15 respondents do not practice about 27.54% of what is listed in their patch management policy.

Do you have a patch management policy or similar document?	Score of companies not practicing what is in their patching policy	Proportion of systems patched (patch compliance) above 95%	What challenges do you face with patch management within your organisation?	Do you agree that there is still room for improvement required?
Yes	21.74	No	44.83	Strongly agree
Yes	100.00	No	34.48	Strongly agree
Yes	4.35	No	3.45	Agree
Similar document	0.00	No	34.48	Strongly agree
Yes	34.78	No	27.59	Strongly agree
Yes	82.61	Yes	0.00	Agree
Yes	17.39	No	72.41	Strongly agree
Yes	21.74	No	37.93	Strongly agree
Yes	0.00	No	41.38	Agree
Yes	0.00	Yes	10.34	Agree
Yes	43.48	No	6.90	Strongly agree
Yes	17.39	Yes	13.79	Agree
Yes	0.00	Yes	13.79	Agree
Yes	8.70	No	17.24	Agree
Yes	21.74	No	6.90	Strongly agree
Yes	8.70	Yes	3.45	Agree
Similar document	21.74	No	27.59	Strongly agree
Yes	4.35	Yes	10.34	Agree
Yes	100.00	No	86.21	Strongly agree
Yes	0.00	No	24.14	Strongly agree
Yes	17.39	No	48.28	Strongly agree

Table 5.16: Patch management review on policies being used vs current challenges in the organisation

Organisation	Do you have a patch management policy or similar document?	Score of companies not practicing what is in their patching policy	Proportion of systems patched (patch compliance) above 95%	What challenges do you face with patch management within your organisation?	Do you agree that there is still room for improvement required?
A	Yes	10.87	No	43.10	Strongly agree
B	Yes	60.87	No	46.55	Strongly agree
C	Yes	43.48	Not sure	13.79	Agree
D	Yes	17.39	No	48.28	Strongly agree
E	Yes	13.77	No	20.69	Agree
F	Yes	0.00	Yes	13.79	Agree
G	Similar document	21.74	No	36.21	Strongly agree
H	Yes	34.78	No	27.59	Strongly agree
I	Yes	43.48	No	6.90	Strongly agree
J	Yes	8.70	No	17.24	Agree
K	Yes	45.65	Yes	1.72	Agree
L	Yes	0.00	No	24.14	Strongly agree

Table 5.17: Patch management review on policies being used vs current challenges in the organisation - Statistics per organisation

Further to Table 5.16, the following Table 5.17 illustrates a similar data structure but is focused on per organisation rather than per respondent. Two respondents, from one organisation, whom said they were "not sure" as to whether they had a patch management policy or similar document being used in their organisation were removed from the below data analysis. However, there were two further respondents from the same organisation of the above who could indicate that they indeed were using a patch management policy within their organisation. The scores are averaged based on the number of respondents per participating organisation. If there was a balance of yes or no answers from respondents of the same organisation, the response of the most senior respondent in that organisation was used for the below analysis.

It is evident from Table 5.17 that on average, organisations are sitting at a score of 25.06% regarding not practicing what is in their patch management policy or similar document.

With that said, 33.33% of the 12 organisations who responded, are sitting above 40% at an average of 48.37%. Of this 33.33%, 50% believe their patch compliance is below 95%.

The participating organisations are on average sitting at 25% regarding the patch management challenges they are facing. The above 33.33% of organisations with a high rating in terms of not practicing all items listed in their patch management policy are sitting at an average of 17.24% of patch management challenges being faced. In general, however, 58.33% of the organisations "strongly agree" that there is still room for improvement in their patch management service.

5.5.6 Escalation of Configuration Issues Identified Through a Patch Management Process

As mentioned in the "Vulnerability Management" section, this research acknowledges that there are several other aspects to vulnerability management, other than patch management. The following paragraph will highlight that if after patching, it is identified that the patch did not work or there was no patch required for the vulnerability in question, are these systems, servers or applications escalated to the correct managing team to remediate the vulnerability. Further to simply escalating, the following also identifies whether there is ownership between teams and whether the remediation of vulnerabilities are being monitored to completion. Figure 5.29 highlights that 80% of the 30 respondents believe this task is happening and there is ownership of who escalates these issues.

Nicolett and Colville (2003) states that patch management is not enough when effectively mitigating vulnerabilities. The following functional requirements should be considered with regards to patch management: asset inventory, patch and service pack status, patch dependency analysis, patch dependency analysis, patch inventory and patch classification, patch matching reports or system baselining, role based administration, patch distribution and installation, patch and application support, and agent vs agentless architectures.

Figure 5.30 depicts that 64.3% of 28 respondents believe that the escalation of configuration issues is being monitored successfully to conclusion.

5.5.7 Superseded Patches

Figure 5.31 illustrates how many of the participating organisations and respondents are aware of superseded patches within their environment. Figure 5.31 highlights that 40%

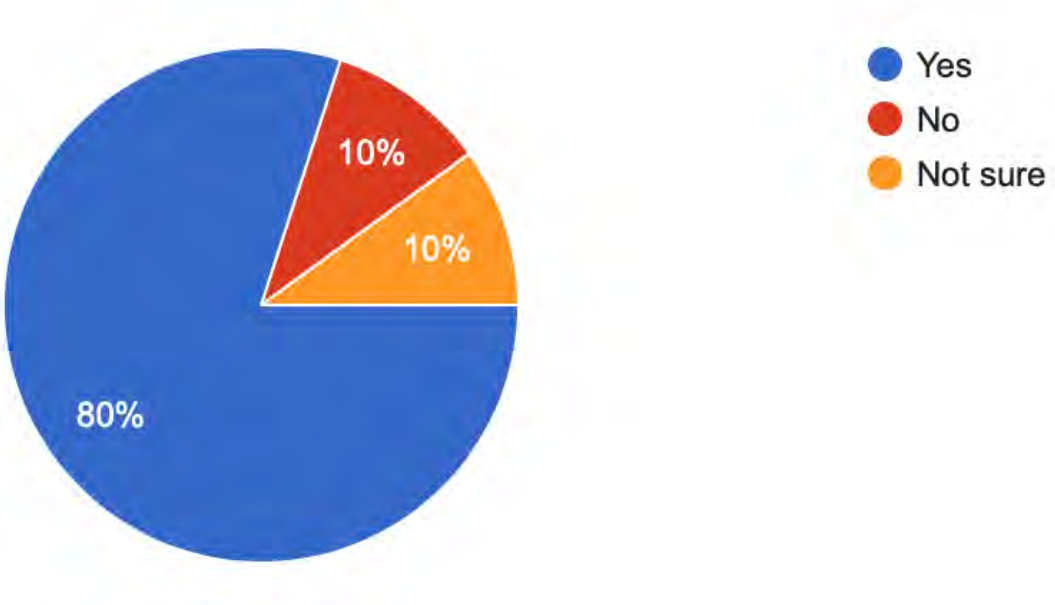

Figure 5.29: Escalation of configuration issues identified through the patch management process

of the 30 respondents have confirmed that superseded patches do exist within their organisations.

Respondents' additional feedback spoke more about the contentious nature of superseded patches. Some respondents refer to the understanding of what compensating controls exist in their organisation as an extra layer of protection to assets with superseded patch requirements, and state that a formal risk acceptance approach and a defined risk scoring matrix should be used to appropriately define the risk of the asset not being patched to the organisation. In contrast to the this view, one respondent mentioned that risk dispensations may delay or prevent patches from being deployed timeously, and another respondent stated that an informal investigation and escalation process exists in their organisation due to the vast number of assets with a superseded patch requirement.

5.5.8 Utilising a Centralised Asset Management Solution

Section 5.3.1 highlighted a link between incidents experienced in organisations and the requirement for an asset management tool. In particular, a respondent did provide additional feedback regarding issues with phasing out old OS versions across their estate. This section explores how organisations know their environment and provide suitable data for risk management. The literature asserts that to apply effective patch management within

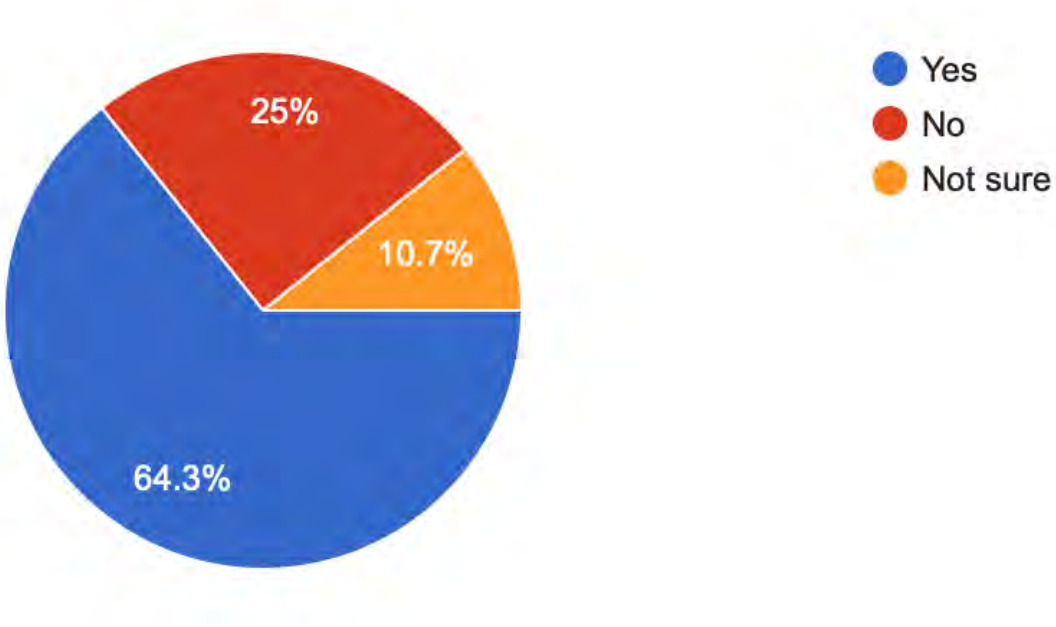

Figure 5.30: Monitoring of configuration escalations, post patch management, to completion

the organisation, comprehensive knowledge of all assets within the organisation is required in terms of understanding asset components, operating systems and applications (Gauci *et al.*, 2017).

Figure 5.32 provides an indication of whether the respondents know that their organisations have a centralised asset management solution such as a configuration management database (CMDB) which details full asset details (installed components, versions & services) and ownership for their assets.

Figure 5.33 explores the duration of a centralised asset management system being utilised in the participating organisation's environment.

Out of the 29 respondents 17.2% believe they have had an asset system for more than 11 years whereas 48.3% are "not sure" of how long they have had a centralised asset management system. Figure 5.34 points out that 55.2% believe their solution is not up to date and only 17.2% are sure that their asset management solution is up to date. This seems to indicate that although 60% of the respondents confirmed they have a centralised asset management solution, 55.5% of the respondents believe their centralised asset management solution is not up to date.

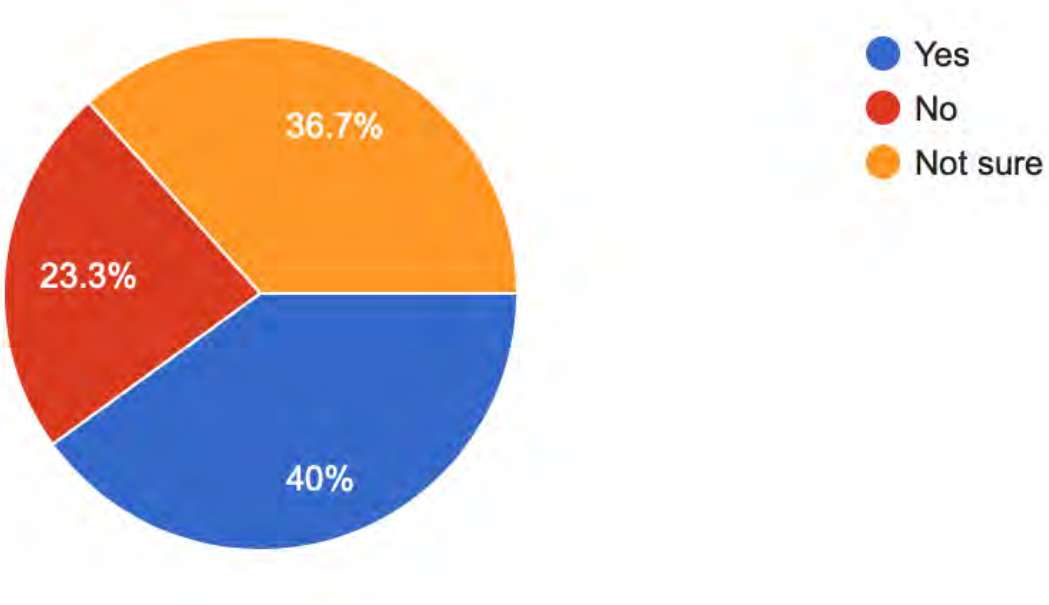

Figure 5.31: Organisations with superseded patch requirements

5.6 Risk Management

The following section will review the "Risk Management" theme of the taxonomy and aid in the understanding of the current risk management status in the participating organisations.

5.6.1 Performing Risk Management before Deploying Patches

Figure 5.35 provides an understanding of whether the participating organisations and respondents perform risk management before patch deployment. From the 30 respondents, 50% indicated that they perform this task before patch management and 33.3% are aware that they do not perform risk management before deploying patches. The following graphs will delve into some of the reasons for this.

5.6.2 Risk Management Functional Activities

Figure 5.36 summarises responses from 24 respondents across 12 organisations about what is included in their risk management function.

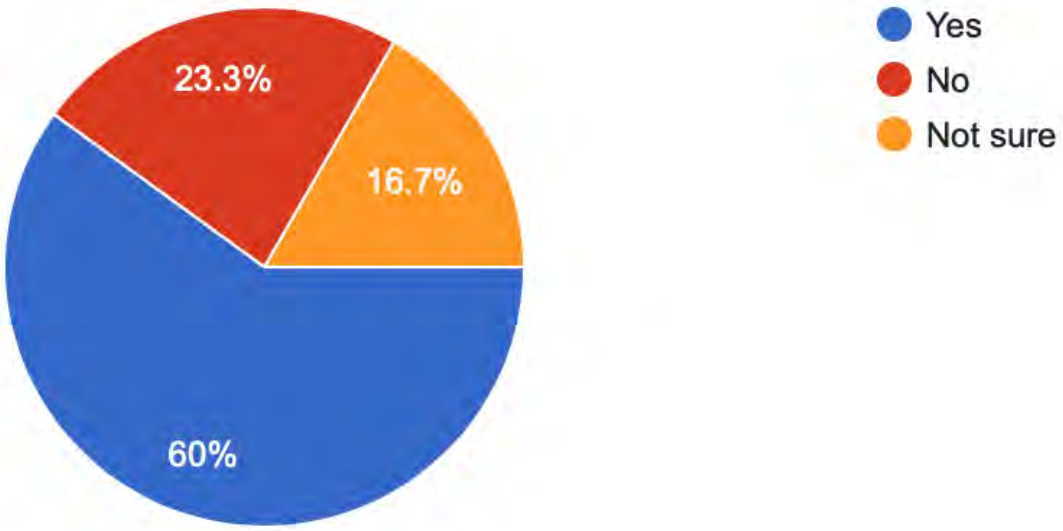

Figure 5.32: Utilising a centralised asset management solution

Q. Does the risk management function within your organisation include the following activities?

- ☐ Documenting business processes or transactions for risk evaluation
- ☐ Ensuring key controls exist to mitigate specific types of risks
- ☐ Defining procedural controls (for example, rules for access control)
- ☐ Implementing controls
- ☐ Reviewing or testing controls
- ☐ Remediating defective controls
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Four respondents from two organisations responded with "not sure". Considering that 15 respondents responded to utilising a risk management function, but 24 respondents responded to this question, it seems that in some organisations the risk management function is available but not used at the correct times before patch deployment.

Table 5.18 illustrates the top three most common activities which their risk management function performs, as per the 24 respondents.

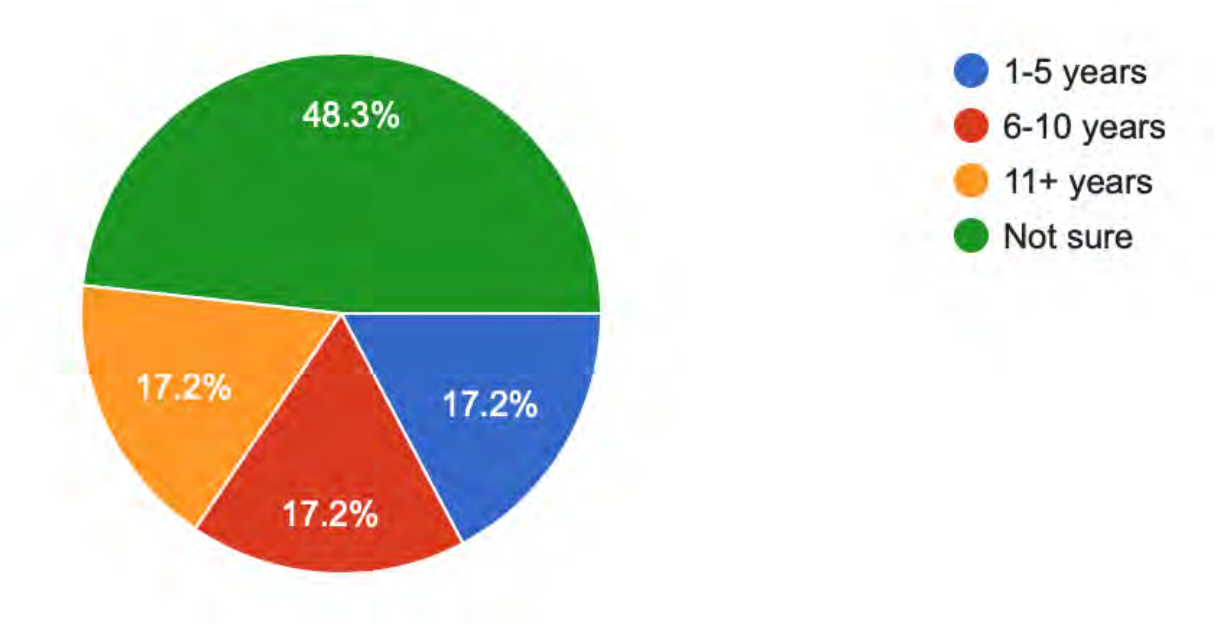

Figure 5.33: Duration of utilising a centralised asset management solution

Most common risk management activities		Percent
Activities	Ensuring key controls exist to mitigate specific types of risks	78.6%
	Reviewing or testing controls	57.1%
	Documenting business processes or transactions for risk evaluation	53.6%

Table 5.18: Top listed risk management functions

5.6.3 Advantages of Risk Management

Further to the earlier review of challenges both within vulnerability and patch management, the following will now review the advantages and disadvantages (in sequential order) of performing risk management within the participating organisations.

Q. What do you see as the advantages of risk management for your organisation?

- ☐ Understanding threat, vulnerability and consequence
- ☐ Continuous review and management of risks and threats
- ☐ Patch and risk prioritisation, based on exploitability, attack vector, attack complexity, etc.
- ☐ Improved organisational awareness on risks to the environment
- ☐ Improving control deficiencies
- ☐ Being able to monitor change in risk over time for a vulnerability

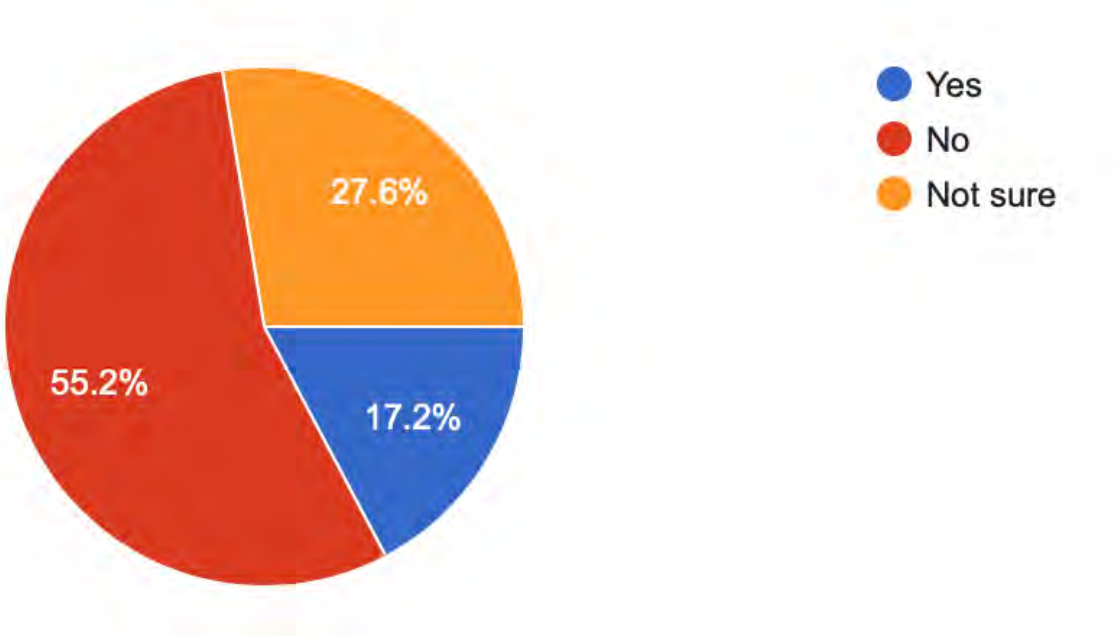

Figure 5.34: Up-to-date centralised asset management solution

	Risk management advantages	Percent
Advantages	Understanding threat, vulnerability and consequence	75.9%
	Continuous review and management of risks and threats	75.9%
	Improving control deficiencies	69%

Table 5.19: Top advantages of risk management

- ☐ Management of the risk identified can then either be retained, mitigated or transferred
- ☐ Allows a means for other mitigation strategies to be considered
- ☐ Understanding overall risk posture for organisation
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Figure 5.37 details the advantages of risk management activities, as per 26 respondents from 12 organisations. There were three respondents from two organisations who were "not sure", and one respondent who did not complete this question.

Table 5.19 illustrates the top three advantages of risk management, as per the respondents' feedback.

From the above it is evident that respondents are stipulating that controls and risk evaluation are some of the activities performed in their organisation. However, the advantages

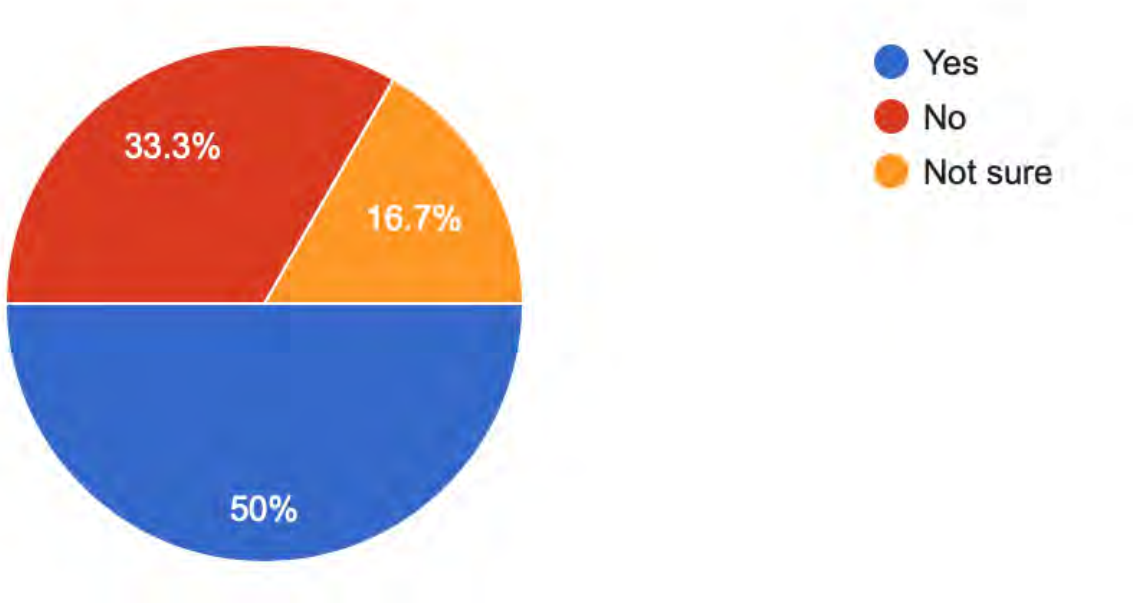

Figure 5.35: Performing risk management before deploying patches

touch more on high level summaries such as understanding threat vulnerability and consequence.

A respondent also provided another advantage through additional feedback: "facilitating the organisations strategy in either defining or supporting their strategy".

5.6.4 Disadvantages of Risk Management

Figure 5.38 details the feedback from 29 respondents regarding the disadvantages of performing risk management.

Q. What do you see as the disadvantages of risk management for your organisation?

- ☐ Time consuming
- ☐ Resource intensive
- ☐ Inability to characterise risk
- ☐ Inability to measure risk
- ☐ Inability to represent threats due to the complexity of threats
- ☐ The IT Risk team not fully aware of the cyber threats to the organisation and the existing compensating controls in the organisation

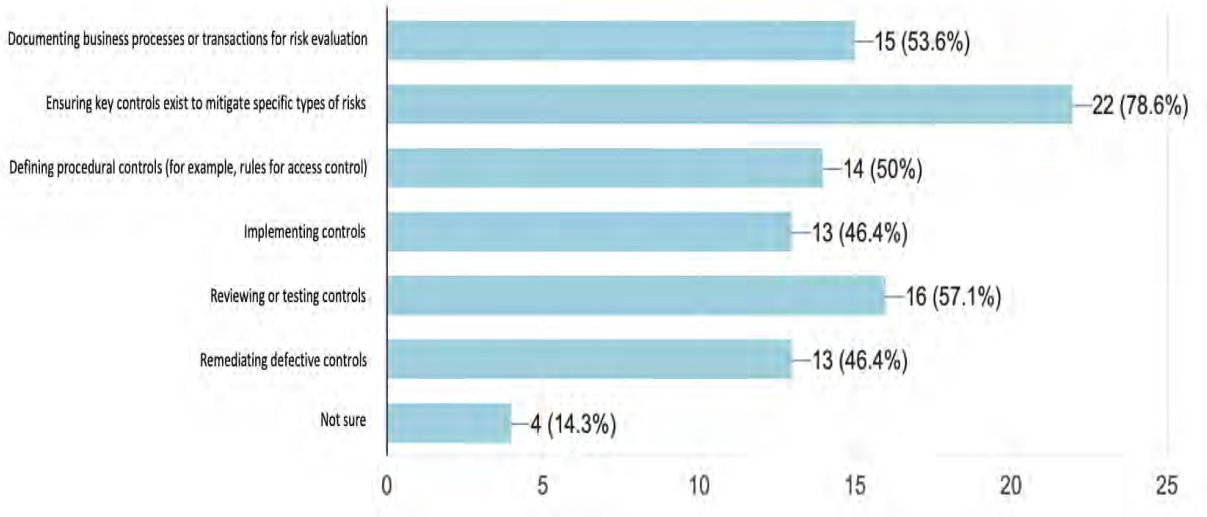

Figure 5.36: Activities the risk management function includes

	Risk management disadvantages	Percent
Disadvantages	Resource intensive	48.3%
	Time consuming	44.8%
	Inability to measure risk	37.9%

Table 5.20: Top disadvantages of risk management

☐ Not sure

☐ Other: (*write-in answer*)

Table 5.20 illustrates the top three disadvantages of risk management, as per the respondents feedback.

While the advantages touch more on high level summaries such as understanding threat vulnerability and consequence, it seems the disadvantages are illustrating more focus on lack of time and resources to perform this activity. More importantly, it seems 37.9% of the respondents believe that risk management has an inability to actually measure risk.

5.6.5 Risk Management Control and System Improvements

Figure 5.39 summarises, from 29 respondents, whether during the past 12 months and to what degree have there been efficiency improvements made (or are in-progress) to the system of controls and processes, taken as a whole, by redesigning, consolidating, or automating key controls used to manage risk in the organisation.

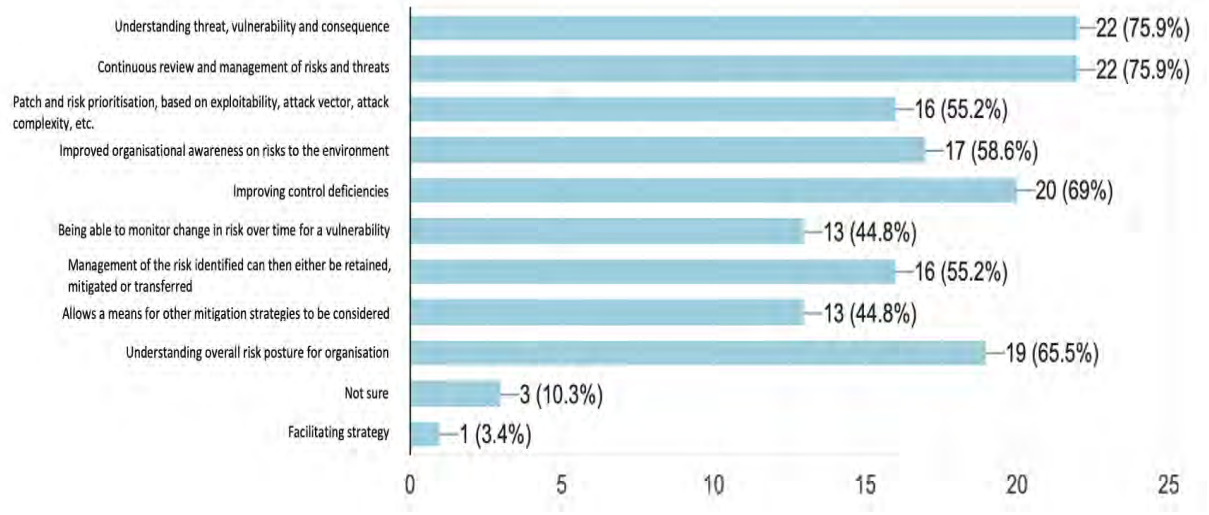

Figure 5.37: Advantages of risk management

Twenty-seven respondents believe that a "little better" and "significantly better" improvements have been made. The "significantly better" refers to 12 respondents from seven organisations, thus 41.37% of the feedback remains extremely positive about improvements over the last 12 months. There are two respondents from two different organisations, however, who believe there has been "no change in improvement" to their risk management over the last 12 months.

Table 5.21 provides a comparative view of organisations who perform risk management before patch deployment.

Table 5.21 can be translated with an understanding of the following bullet items:

- Column A - Indicates with a high score that particular respondents have selected the most available options with regards to the questions available multiple choice options.
- Column B - Indicates particular respondents' perception on the advantages of utilising risk management within their organisation. Again, the higher the score indicates that particular respondents selected a high number of available answers or subcategories from the questions multiple choice options.
- Column C - Indicates particular respondents' perception on the disadvantages of utilising risk management within their organisation. Again, the higher the score indicates that particular respondent selected a high number of available answers or subcategories from the questions multiple choice options.

Score of organisations where their risk management include various activities	Score of organisations highlighting items of advantage to risk management	Score of organisations highlighting items of disadvantage to risk management	To what degree have there been efficiency improvements made (or are in-progress) to the system of controls and processes, taken as a whole, by redesigning, consolidating, or automating key controls used to manage risk?
33.33	20.00	16.67	A little better
33.33	60.00	33.33	A little better
83.33	80.00	16.67	Significantly better
50.00	100.00	50.00	A little better
0.00	0.00	0.00	No response
83.33	70.00	16.67	Significantly better
33.33	20.00	33.33	No change in improvement
50.00	40.00	0.00	A little better
83.33	40.00	66.67	A little better
100.00	90.00	33.33	Significantly better
100.00	90.00	66.67	Significantly better
0.00	30.00	16.67	A little better
66.67	70.00	16.67	Significantly better
100.00	0.00	0.00	Significantly better
83.33	90.00	33.33	A little better

Table 5.21: Comparison on organisations utilising risk management

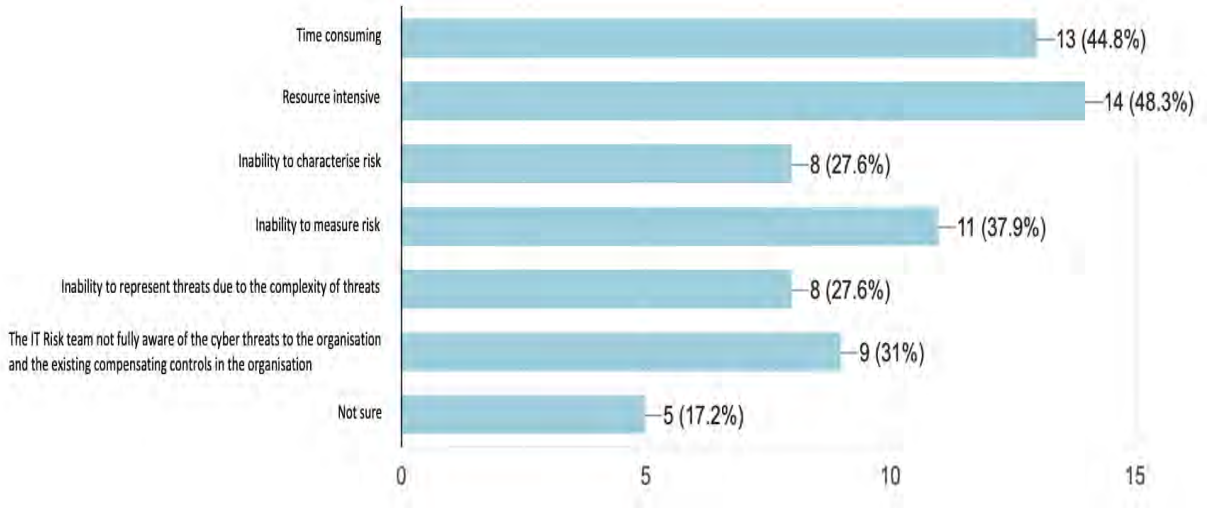

Figure 5.38: Disadvantages of risk management

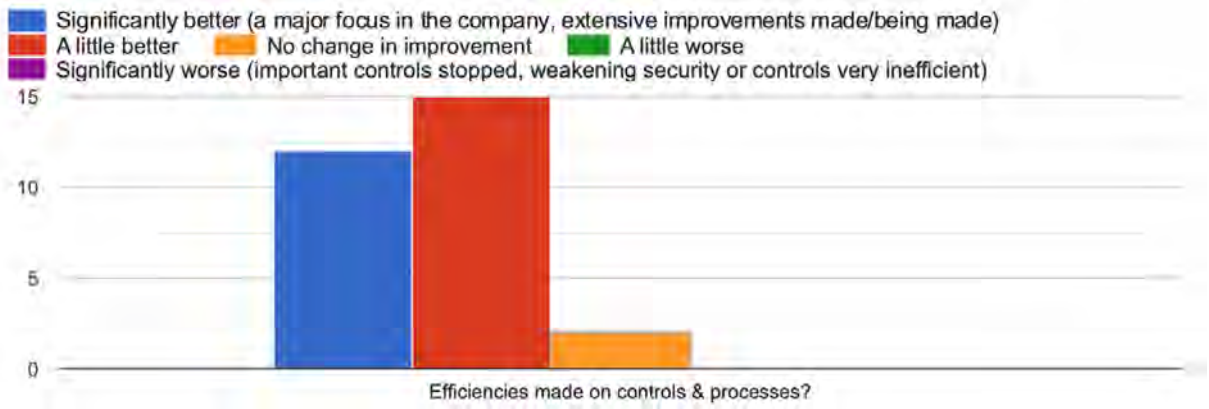

Figure 5.39: Risk management control efficiencies

- Column D - Indicates particular respondents' perception on the improvement efficiencies that have taken place within their organisation over the last 12 months. The higher the score indicates that particular respondents selected a high degree of improvement for their organisations.

Table 5.21 shows that as per column B, three respondents from three different organisations perform 100% of the risk management activities. Of these three respondents, two find risk management very advantageous to their organisation however, there is a disparity in what disadvantages these respondents consider from risk management. Disparity meaning a high degree of difference between the respondents in terms of what they believe are the disadvantages of utilising risk management in their organisation. Lastly, all of these respondents believe their improvement efficiencies are "significantly better".

5.7 Utilisation of Frameworks

The below final graphs of the survey and taxonomy review will continue to summarise the 'Frameworks' theme and associated categories to allow for a more effective understanding of what is currently being practiced in the industry.

The following two graphs provide a brief summary of who follows certain standards. To clarify, a standard is used as best practice or principles whereas a framework provides guidelines for an organisation to follow (Olivia, 2019). The below two questions on standards indicates the controls required but does not dictate how these controls should be applied.

5.7.1 ISO27001 Compliant

Figure 5.40 provides an understanding of whether the participating organisations and respondents are ISO27001 compliant. This means that in addition to each organisation having the required controls or principles of the standard, they have been externally evaluated on their compliance to this standard.

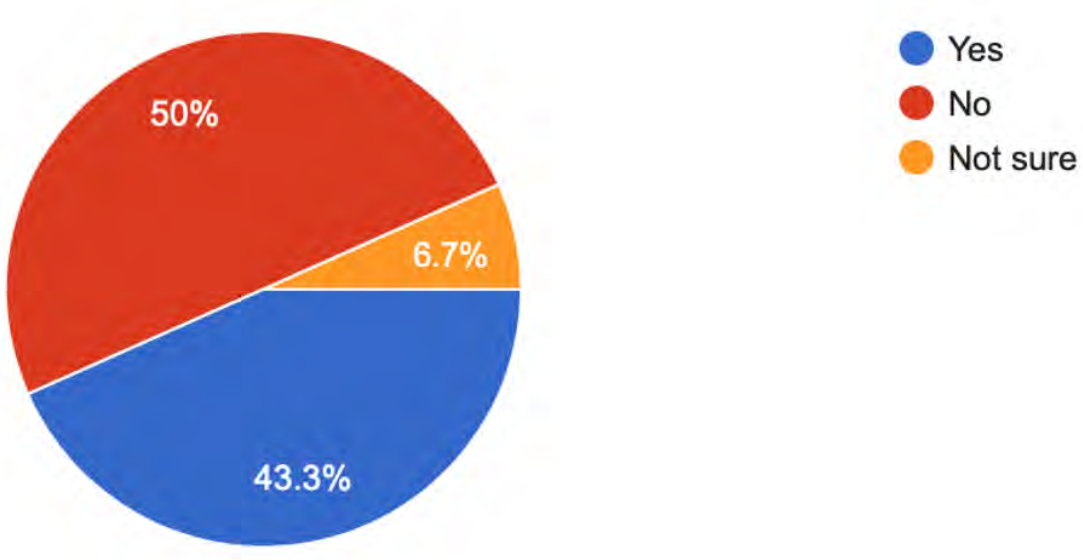

Figure 5.40: ISO27001 compliant organisations

From the 30 respondents, 43.3% confirmed that they are compliant. However, 50% of the respondents indicated that they are not compliant, with 6.7% "not sure". The 43.3% who confirmed that they are compliant equates to 13 respondents from eight organisations.

5.7.2 PCI Compliant

Figure 5.41 indicates whether the participating organisations and respondents are PCI compliant. This means that in addition to each organisation having the required controls or principles of the standard, they have been externally evaluated on their compliance to this standard.

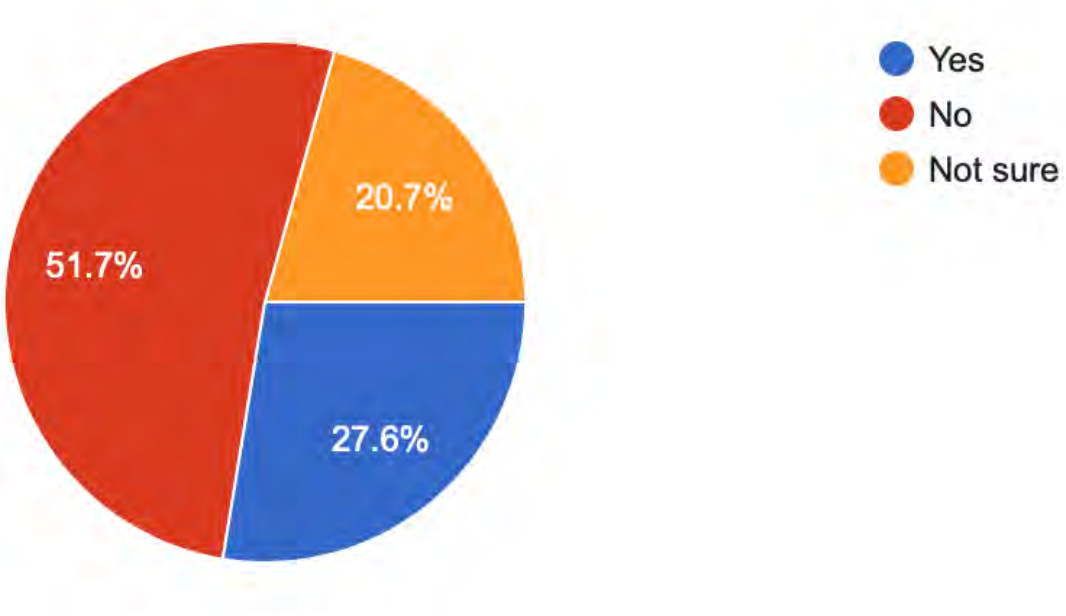

Figure 5.41: PCI compliant organisations

From the 29 respondents, 51.7% confirmed that they are not PCI compliant. Note that only organisations who process and store card transactions are meant to be PCI compliant so this implies that, from the FSI participating organisations for this research, just over a quarter (27.6%) need to be PCI compliant.

5.7.3 Utilise Frameworks for Effective Collaboration

Figure 5.42 illustrates whether the respondents utilise any existing frameworks within their organisation which further assists in the collaboration between the vulnerability management and Windows patch management teams and activities.

From the 30 respondents, 46.7% confirmed that they do utilise a framework. This refers to 14 participants from nine organisations. However, 30% of the respondents are saying that they do not use a framework and 23.3% are “not sure”. From the 14 respondents whom

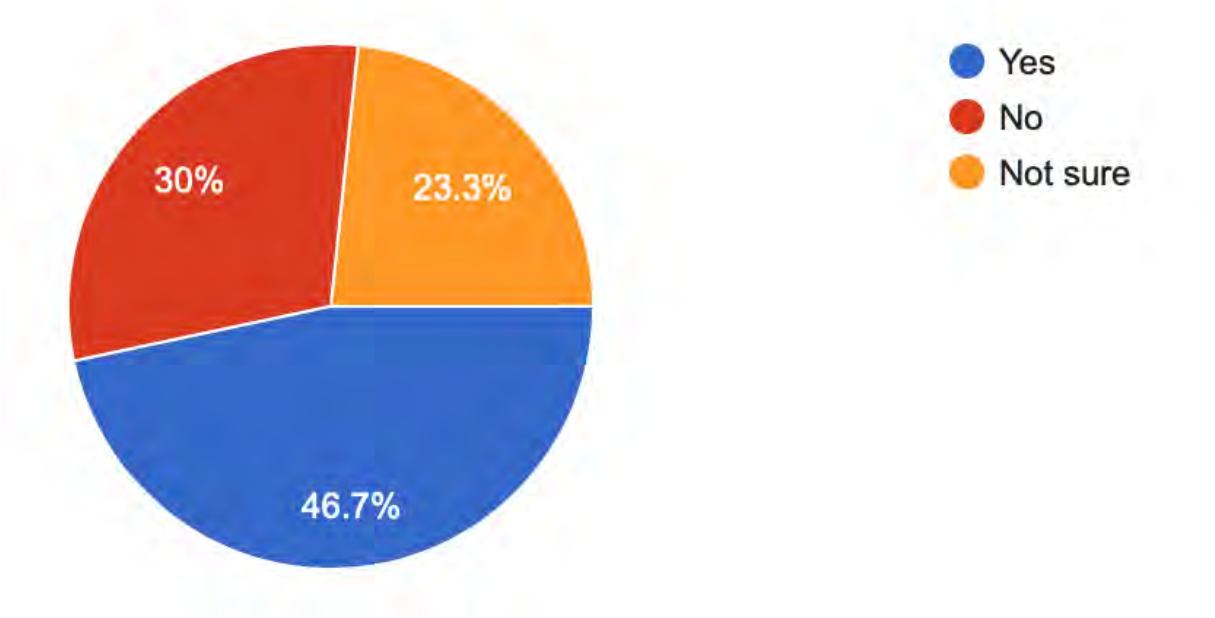

Figure 5.42: Organisations utilising existing frameworks

confirmed they do utilise a framework, only six of these respondents from four organisations mentioned their organisations are ISO27001 compliant and only four respondents from three organisations mentioned they are PCI compliant.

5.7.4 Current Frameworks being Utilised

Table 5.22 details, as per the feedback of 14 respondents from nine organisations, what frameworks are currently being utilised in the organisations. Table 5.22 is filtered on who currently is utilising a framework, what framework they currently using and correlates that with who is ISO27001 or PCI compliant.

As per Table 5.22, 57.14% of the respondents (8 out of 14 respondents) are using NIST.

5.7.5 Advantages of a Framework

Figure 5.43 provides insight into what the respondents of the participating organisations have stated are the advantages of utilising a framework in their organisations.

> Q. What do you see as the advantages of following a framework for your organisation?

ISO27001 compliant?	PCI compliant?	If yes, what is the name of the framework being used?	Score of organisations who highlighted items of advantage for following a framework within their organisations
Yes	Yes	NIST	25.00
No	No	NIST	8.33
Yes	No	NIST	25.00
No	No	CIS Benchmarks and internal	33.33
No	No	NIST	50.00
Yes	Yes	NIST / ISO27001	50.00
No	No	Follow key control and criticality for now based on risk rating score.	33.33
No	Not sure	NIST	33.33
Yes	Yes		25.00
No	No	Aligned to ISO and NIST	91.67
Yes	Yes	ISO 27000 Series (IT Security) and NIST	25.00
No	Not sure	Hybrid	0.00
Yes	No response	ISF framework	75.00
No	No	ISF Standards of Good Practice	41.67

Table 5.22: Summary of frameworks being used in the organisations

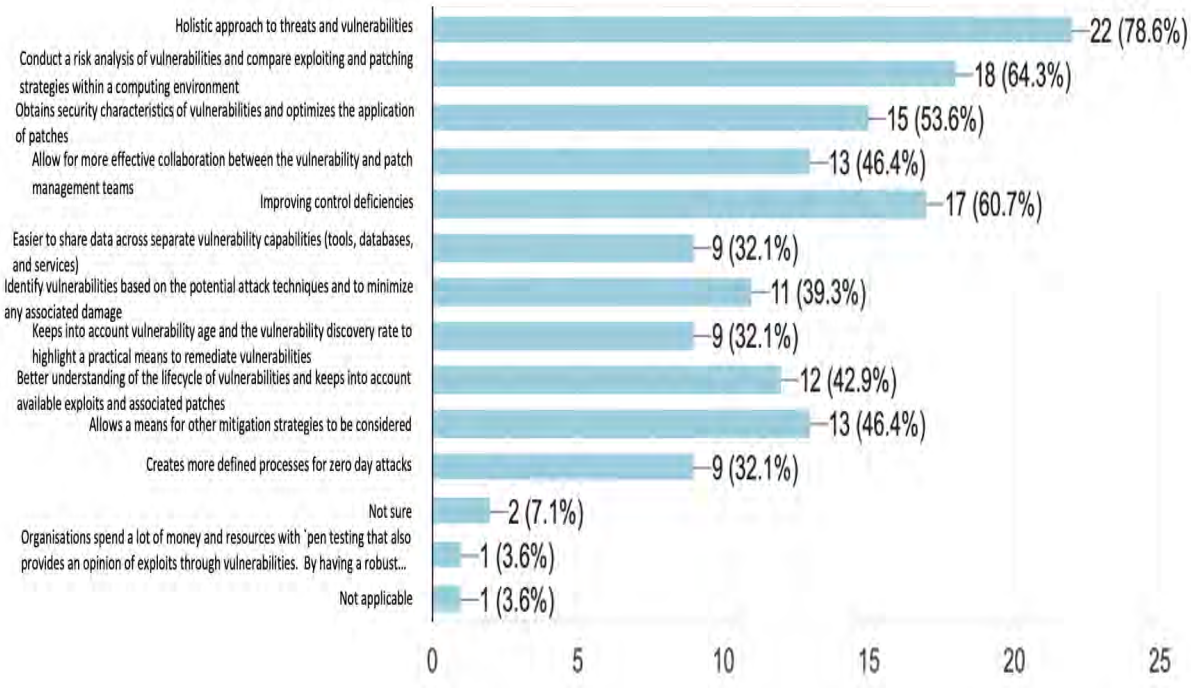

Figure 5.43: Advantages of a framework

- ☐ Holistic approach to threats and vulnerabilities
- ☐ Conduct a risk analysis of vulnerabilities and compare exploiting and patching strategies within a computing environment
- ☐ Obtains security characteristics of vulnerabilities and optimises the application of patches
- ☐ Allow for more effective collaboration between the vulnerability and patch management teams
- ☐ Improving control deficiencies
- ☐ Easier to share data across separate vulnerability capabilities (tools, databases, and services)
- ☐ Identify vulnerabilities based on the potential attack techniques and to minimise any associated damage
- ☐ Keeps into account vulnerability age and the vulnerability discovery rate to highlight a practical means to remediate vulnerabilities
- ☐ Better understanding of the lifecycle of vulnerabilities and keeps into account available exploits and associated patches
- ☐ Allows a means for other mitigation strategies to be considered

	Framework advantages	Percent
Advantages	Holistic approach to threats and vulnerabilities	78.6%
	Conduct a risk analysis of vulnerabilities and compare exploiting and patching strategies within a computing environment	64.3%
	Improving control deficiencies	60.7%
	Obtains security characteristics of vulnerabilities and optimises the application of patches	53.6%
	Allow for more effective collaboration between the vulnerability and patch management teams	46.4%
	Allows a means for other mitigation strategies to be considered	46.4%

Table 5.23: Most commonly accepted advantages of a framework

☐ Creates more defined processes for zero-day attacks

☐ Not sure

☐ Other: (*write-in answer*)

Table 5.23 summarises the feedback from 28 respondents on the top six advantages of utilising a framework.

A respondent who confirmed that they do not currently utilise a framework within their environment gave further feedback by stating the following advantage of utilising a framework. The respondent indicated that penetration testing was often used to validate or provide an opinion of vulnerability exploits, and could be better-focused through a risk-based framework for vulnerability management. This complementary use allows for logic and insight into planning the focus of penetration testing, which improves risk management within technology that is linked to cyber exposure, and makes the best use of monies spent on penetration testing.

5.7.6 Disadvantages of a Framework

Figure 5.44 will now detail what the respondents of the participating organisations believe are the disadvantages of utilising a framework in their organisations. This is as per feedback from 25 respondents across 10 organisations. To further detail the respondents who replied to this question, five respondents from four organisations left their response blank, one respondent stated “not applicable” and five respondents from four organisations responded “not sure”.

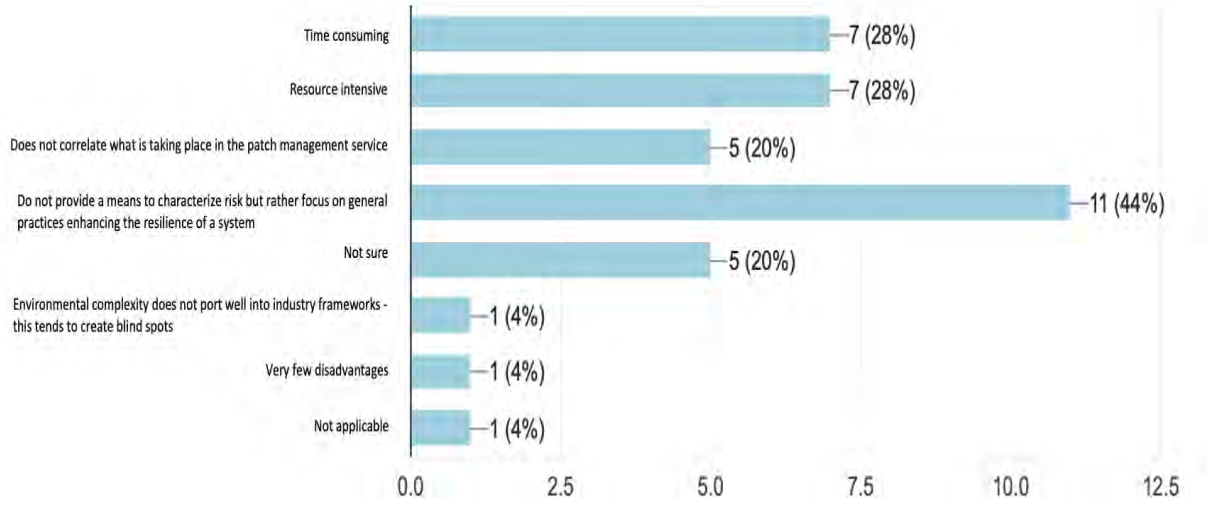

Figure 5.44: Disadvantages of a framework

	Framework disadvantages	Percent
Disadvantages	Do not provide a means to characterise risk but rather focus on general practices enhancing the resilience of a system	44%
	Time consuming	28%
	Resource intensive	28%

Table 5.24: Most commonly perceived disadvantages of a framework

Q. What do you see as the disadvantages of following a framework for your organisation?

- ☐ Time consuming
- ☐ Resource intensive
- ☐ Does not correlate what is taking place in the patch management service
- ☐ Do not provide a means to characterise risk but rather focus on general practices enhancing the resilience of a system
- ☐ Not sure
- ☐ Other: (*write-in answer*)

Table 5.24 summarises the top three items listed as disadvantages of utilising frameworks within the respondents environments. This is as per 19 respondents from nine organisations.

It seems there is disparity between the advantages of utilising a framework which provides a holistic approach to threats and vulnerabilities and also allowing a risk analysis to take

place whereas the disadvantages of utilising a framework itself does not allow a means to characterise risk, further to being resource and time consuming. Further feedback from a respondent who did not use a framework indicated the more complex an organisation's environment is, the the greater the possibility of potential blind spots being created through the use of a predefined framework, and this makes the integration or usage of an industry framework more complicated.

Chapter 6

Research Findings

With the understanding of the data analysis from the previous chapter, this chapter will now be able to discuss the findings in line with what the literature review had revealed.

It is clear from various sections of the previous chapter that from the received feedback of the different respondents, some working for the same organisation as other participants of this survey, there seems to be a mis-alignment in what each participant understands both about their vulnerability and patch management services and what they are practicing in the organisation, i.e. the operational side. This could however indicate the participants could be in different roles and responsibilities, and thus could not possibly have the same visibility into key areas of these services.

Further evidence for the above is the number of respondents providing feedback of "not sure" for questions related to service challenges and what they currently not practicing in each of these services. In particular, one respondent from an organisation with multiple responses to the survey was "not sure" whether they had a vulnerability management policy and two respondents from two organisations mentioned they were "not sure" of what they were not practicing in their vulnerability management service. However, it seems all respondents provided feedback regarding what the challenges are in their vulnerability management service, thus there were no "not sure" responses for this category. Similarly, two respondents from one organisation which also had multiple responses to the survey mentioned they were "not sure" whether they had a vulnerability management policy, three respondents from two organisations mentioned they were "not sure" about what they were not practicing in their patch management service and two respondents from two separate organisations mentioned they were "not sure" of the challenges faced in their patch management service.

The following insights provides some further evidence for this hypothesis:

- Team structure - Team members have different answers to some questions from the same organisations which is a concern regarding the suitability of single or multiple team structures being utilised for vulnerability and patch management services.
- Team structure advantages - It is noticeable in the total count for organisations, there was one organisation that had responses and non responses from its respondents which could indicate different mindsets of the service or expectations of the service.
- Vulnerability management policies differences - A summary from 30 respondents on who knows they have a vulnerability management policy within their organisation was detailed. This item of discussion referred to the respondents' understanding of whether their organisation had a vulnerability management policy. The 86.7% listed referred to 26 respondents from 12 of the organisations currently using a vulnerability management policy. However, three respondents from different organisations mentioned that they are using similar documents and only one organisational respondent is currently "not sure" whether they have a policy. The above is from the total of 12 participating organisations in this survey which again implies there are respondents from the same organisation who have different views or understandings of what is taking place and available in their organisations.
- Vulnerability and patch management policies - There are discrepancies in what respondents from the same organisation are practicing and discrepancies in what items are listed as most important in their vulnerability management.
- Risk management - Figure 5.36 summarises from 24 respondents across 12 organisations, on who knows what is included in their risk management function. Four respondents from two organisations had listed "not sure". Considering 15 respondents responded to utilising a risk management function whereas 28 respondents responded to the question of what is included in their risk management function, as reflected in Figure 5.36, it seems in some organisations the risk management function is available but not formally understood or possibly not used across the organisation.

6.1 Team Structure

Now, with a better understanding of the industry and their preference for having multiple teams in the organisation, the research reflects on some of the initially identified areas of the literature review on the topic. There are several citations in the literature that review the use of multiple teams to manage the vulnerability and patch management services separately, including the detail of technical and non-technical respondents being involved. Gauci *et al.* (2017) mentions that developing cross-functional teams and competencies becomes key when securing technology. Beres *et al.* (2008b) highlights multiple functions between both the patch management and the security operations team who do the vulnerability management. Security teams of large organisations or enterprises usually manage security controls such as patching, anti-virus or anti-malware applications, firewalls, etc., all of which work together to minimise exposure to potential threats (Beres *et al.*, 2008b). With this said, software flaws continue to be a prevalent issue for small and large organisations, irrespective to the budget and resources available (Gianini *et al.*, 2015, Khouzani *et al.*, 2016).

Okhravi and Nicol (2008) details seven elements for successful patch management of which dedicated resources and clearly defined responsibilities are some of the listed reasons. With an increase in vulnerabilities over time, so have attack tools progressed (Cavusoglu *et al.*, 2008) which provides a further requirement for defined roles and responsibilities. Users add value to security risk management when, "[t]hey participated in the prioritisation, analysis, design, implementation, testing, and monitoring of user-related security controls within business processes" (Spears and Barki, 2010, p. 520). The outcome of user participation then leads to greater organisational awareness of security risks and controls within the organisational processes. This leads to better development and management of security controls.

The top three rows of Figure 5.8 refer to "dedicated resources with clearly defined roles and responsibilities" sitting at 75% of the feedback, "separate teams with more resources allows more tasks to be completed timeously, i.e. improved capacity constraints" sitting at 60.7% and lastly "having one team is not suited for large organisations" sitting at 35.7%. This feedback indicates that, as far as the industry is concerned, there is a pragmatic rather than an idealistic preference to having separate teams managing the vulnerability and patch management services within organisations.

Organisations, unfortunately, do not have the luxury of sharing resources from other IT functions with the patch management team as the planning, deploying and maintenance

of patch management is a full time exercise (Cavusoglu *et al.*, 2008). Abraham and Nair (2015a) mentions that organisations are trying to apply more resources and more funding to the issue of vulnerability remediation. In order for patch management to complement vulnerability management, patch management requires a strong security-oriented focus (Nicolett and Colville, 2003).

Nevertheless, Figure 5.7 indicates that most organisations are using multiple teams to manage their vulnerability and patch management, with Figure 5.8 indicating why. Spears and Barki (2010) suggests however that although users are seen as a weak link in information security, a user's understanding of the organisation or the business contributes to more effective security controls or measures. It is thus evident from the survey feedback, and the implication for the literature, that users with defined roles and skill-sets continue to play a critical role in the vulnerability and patch management function.

Regarding team structure or team responsibilities, a respondent of the research survey gave post survey feedback to consider the structure of the organisation, i.e. is the organisational structure centralised, federated or a combination of both. The structure of the organisation directly impacts the effectiveness of the IT risk and security function in its ability to execute its various tasks or functions. The respondent continues to highlight that there is an observed tension between the digital teams and the more conservative risk management functions. The digital teams look to expedite the execution of a task or function with often little regard for governance or external collaboration to mitigate risks. The respondent highlighted the above to contexualise the challenge where the IT risk and security teams are seen as an inhibitor to innovation and progress, which further compounds the challenges of vulnerability management if the IT risk and security teams are circumvented in business decisions or activities. The above two key points understood is 1) the structure of the organisation directly correlates with the effectiveness of vulnerability and patch management, and 2) the noticeable disconnect between the business and the security teams. These two points are considered as additions to what was identified in the literature when reviewing the effectiveness of vulnerability and patch management as the above points provide a link between the business structure and objectives to the effective requirement of a vulnerability and patch management service.

6.2 Incident Management

The number and types of cyber attacks changes dramatically as time progresses (Shetty *et al.*, 2018). As mentioned in Chapter 1, security teams of large organisations or en-

terprises usually manage security controls such as patching, anti-virus or anti-malware applications, firewalls, etc., all of which work together to minimise exposure to potential threats and cyber incidents (Beres *et al.*, 2008b). Microsoft application security controls were selected for review because Microsoft Windows is a popular business operating system (Beres *et al.*, 2008b). The data analysis of incident management experienced by the participating organisations provides an understanding of the percentage of vulnerabilities which caused an incident, some not only referring to Windows patching.

From the total of 33 incidents across nine organisations, detailed in Chapter 5, at least 23 were related to a Microsoft vulnerability which had a relevant Windows patch available at the time of the incident. That equates to 39.39% of the vulnerabilities the respondents are willing to share or are aware of. It is evident from the data analysis in Chapter 5 that the lack of effective vulnerability and patch management leads to or is the cause of under 40% of the incidents being experienced by the respondents. Of the related Windows patch incidents experienced, the following business impact was experienced:

- High business impact - 22.22% of the incidents have had a high impact on the organisations which implies a significant impact that was non-manageable and resulted in some form of failure for the organisation and its assets.
- Medium business impact - 44.44% of the incidents have had a medium impact which implies a significant impact on the organisations, however the impact was manageable.

Of the reported incidents by the respondents who confirmed the incident was related to Windows patch not being applied, 66.66% had mentioned that they have multiple / separate teams managing their vulnerability and patch management services. All respondents of the above statistics however mentioned that they do have a vulnerability and patch management policy available in their organisation and 55.55% believe that the monthly trend of vulnerabilities being remediated in their organisations is moving down but only 33.33% believe their organisation's proportion of systems patched (patch compliance) is above 95%.

As mentioned earlier, Nicolett and Colville (2003) states that patch management is not enough when effectively mitigating vulnerabilities. The following functional requirements should be considered with regards to patch management: asset inventory, patch and service pack status, patch dependency analysis, patch dependency analysis, patch inventory

and patch classification, patch matching reports or system baselining, role based administration, patch distribution and installation, patch and application support, and agent vs agentless architectures. Patching based on the incidents seen also implies that patch management should not only be reviewed under vulnerability management as there are other remediation requirements.

6.3 Vulnerability Management

As mentioned earlier in the research literature review on vulnerability and patch management, Spears and Barki (2010) suggests that although users are seen as a weak link in information security, a user's understanding of the organisation or the business contributes to more effective security controls or measures. However, it seems from the 29 responses, 24.1% are actually not even sure what their total number of vulnerabilities are within their organisation. This implies that around a quarter of the respondents are not actually monitoring or measuring the effectiveness of their required action or role in their organisation's vulnerability and patch management services, even though new software vulnerabilities are discovered almost daily (Okhravi and Nicol, 2008).

Furthermore, according to the literature, the expectation is that organisations need to remain proactive when reviewing vulnerabilities through identifying critical assets, its associated risk levels and, defining and implementing a process for mitigating actions. This can be understood as having a defined expectation through a defined policy of which an organisation and its vulnerability and patch management stakeholders should have an understanding and effective adherence towards. Beres *et al.* (2008b) highlights the need to have policies for patch management and vulnerability management respectively, together with defined processes around how to perform effective patch management for the organisation. As per the survey results, organisations continue to create and implement policies with an average of 52.22% of the available options (subcategories) having been selected as part of their policy. However, 82.22% of the participating organisations are practicing all items as listed in their vulnerability management policy.

Regarding the understanding of policies, both from a vulnerability and patch management perspective, a respondent provided additional feedback regarding the understanding that all individuals involved in these services need to contribute to these policies, including standards, as this will allow for everyone having accountability for these services and the progression thereof. This further supports what was identified in the literature as

	Summary of vulnerability management policy review	Percent
Most common	Internal scans	83.3%
	A vulnerability management lifecycle (i.e. scan, prioritise, analyse report remediate validate) sitting	76.6%
	External scans	70%
	Logging calls with respective teams to remediate vulnerabilities	70%
	Service levels/timelines for patching different vulnerability severities	66.7%
Not practicing	A vulnerability management lifecycle (i.e. scan, prioritise, analyse report remediate validate)	28.6%
	Service levels/timelines for patching different vulnerability severities	28.6%
	External scans	25%
	Authenticated scans	25%
	Daily/weekly/monthly review of failed scans, i.e. health checks	25%
	A separate process to tackle zero-day vulnerabilities or otherwise expedite patches	25%

Table 6.1: Summary of vulnerability management policy review

items were noted based on user expertise and users identifying challenges through the vulnerability and patch management process. The lessons learned through the operational activity thus may allow organisational policies to be more effectively adapted based on the organisation and industry requirements.

The trend of vulnerabilities being remediated within organisations is moving down, indicating that the success in remediation is not improving. It is also evident from the vulnerability and patch management reviews that there is ownership of escalating configuration issues identified through a vulnerability management process to the correct team for action. Further to the escalation hereof, it seems these items are being monitored to conclusion.

Table 6.1 helps summarise the most common items listed in the respondents' defined vulnerability management policy. This table also shows the most common items from the policy which the respondents are not practicing in their environments. It is further highlighted that 3 of the 6 most common items listed in an organisation's policy are not actually being practiced in the organisation. A key item of what is not being practiced, i.e. "a vulnerability management lifecycle", can be found in various sections of the literature review where it is mentioned as a requirement for effective vulnerability and patch management.

Further to the above regarding vulnerability management, a respondent of the research

survey continued to give post survey feedback to consider systems which have reached end of life (EOL). You may find systems and operating systems in legacy environments that have reached end of life which cannot be patched/updated. The respondent then continues to mention that in these instances they rely completely on compensating controls until such time that the functionality of the system can be replaced, budget and internal governance or politics willing. Compensating security controls, however, are seen as temporary solutions and might not cover all known vulnerabilities (Beres *et al.*, 2008b). Nevertheless, the literature also mentions that patch management is not enough when effectively mitigating vulnerabilities. The above additional feedback also talks to the fact that operational challenges identified through vulnerability and patch management should be clearly communicated between the teams to understand what is being identified in the vulnerability management service and what are the required actions to remediate the vulnerability, may that be with the associated patch management team or not.

Regarding the theme of "Vulnerability Management", and further to the additional feedback from a respondent in Chapter 5 regarding vulnerability management being part of a program where regular feedback is provided at an executive level for review, a separate respondent's post survey feedback touched on the same topic suggesting this theme to be a board level item of discussion. Within the taxonomy, this could indicate a requirement for executive team awareness of the vulnerability and patch management service levels, which could be defined either through the defining of the "people and team structure" or included through various layers of the taxonomy.

To conclude on the theme of "Vulnerability Management", a respondent gave several other suggestions for effective vulnerability management. These reflects as several key items to consider as indicated in the literature review. This includes, 1) effective communication and collaboration between teams, 2) lessons learned through operations being shared to allow for correct principles to be utilised in the organisation, and 3) the need for effective analysis and analytics of what is taking place in the vulnerability and patch management services. With this mentioned, the use of a specific security technology such as a security information and event management (SIEM) solution to monitor and provide analytics on the vulnerability management does add further context to what was understood in the literature.

	Summary of patch management policy review	Percent
Most common	A patch management lifecycle (i.e. patch analysis/selection, risk assessment & prioritisation, quality assurance/testing, implementation/deployment of updates, post checks/verification, reporting)	86.7%
	Monthly patch schedules	70%
	Detail your patch management strategy	56.7%
	Patching all servers and workstations	56.7%
	Performing test management of patches	56.7%
	Patching all vulnerability severities	56.7%
Not practicing	Service levels/timelines for patching different vulnerability severities	42.9%
	A patch management lifecycle (i.e. patch analysis/selection, risk assessment and prioritisation, quality assurance/testing, implementation/deployment of updates, post checks/verification, reporting)	38.1%
	Patch management baselines for workstations and servers	38.1%
	Patching all vulnerability severities	38.1%
	Performing test management of patches	33.3%

Table 6.2: Summary of patch management policy review

6.4 Patch Management

Within the understanding of the "Patch Management" theme, Table 6.2 helps summarise the most common items listed in the respondents defined patch management policy. This table also shows the most common items from the policy which the respondents are not practicing in their environments. As per the analysis of the last section, it is evident that 3 of the 6 most common items listed in an organisation's policy are not actually being practiced in the organisation.

Further to the above summary, a subcategory "creating a pre-patch mitigation action plan, with existing or new security controls, for vulnerabilities which do not have an available patch yet" is least common in both the "Vulnerability Management" and "Patch Management" sections of the previous chapter. This item, however, does not show up in the number of items not being practiced, based on most responses. This implying that although only 10% of the respondents confirmed this to be listed in their patch management policy, it seems this item may still be practiced in the participating organisations which is positive as it reflects what was identified in the literature talking to patch management not being enough when effectively mitigating vulnerabilities.

To apply effective patch management within the organisation, comprehensive knowledge of all assets within the organisation is required in terms of understanding asset components,

operating systems and applications (Gauci *et al.*, 2017). With this said, the data indicates that although a centralised asset management tool is being used in the participating organisations, less than 16.6% believe this data is up to date. Not just the understanding of the asset configuration details but also location was mentioned by a respondent through their additional feedback post the survey review. To quote, "the location of assets could involve bandwidth issues and concerns around assets not being reachable for patching". This adds further detail to the understanding of the patch management challenges category of the research taxonomy. Taking the above into consideration, not having an up to date inventory of critical assets in the organisation and not being able to identify threats and vulnerabilities for these assets based on its specifications or attributes does not allow organisations to quantify an uncertain risk to the organisation, as mentioned in the literature.

In addition to understanding the importance of an up to date asset management solution, another respondent confirmed they use added solutions to understand assets connecting to their network. There are other solutions available that provide device visibility on the network. This visibility enables an accurate device inventory, continuous compliance enforcement, policy-based access control and rapid response to security incidents.

6.5 Risk Management

From the 12 participating organisations, nine organisations are not performing risk management as per the survey feedback. For those that do practice risk management, the creation and testing of key controls together with documentation for risk evaluation comes out key from the survey.

Further to the available statistics for this theme based on the feedback to what was found in the literature review, a respondent also confirmed that "facilitating strategy" is a benefit from the use of risk management before patch management. This continues to touch on what was said in the literature review and earlier section on "Team Structure". Users add value to security risk management when, "[t]hey participated in the prioritisation, analysis, design, implementation, testing, and monitoring of user-related security controls within business processes" (Spears and Barki, 2010, p. 520).

There are also additional mentions of risk as highlighted in the feedback of the "Vulnerability Management" theme and the category on challenges. More specifically the additional challenges, which were highlighted, are namely the following:

- Lack of trust in vulnerabilities discovered - No correlation between the impact (severity) of the vulnerability vs critical of assets (multiple "medium" vulnerabilities on mission critical systems with higher severity and impact vs "critical" vulnerabilities on less or non business critical assets).
- Risk based approach - Legacy systems also need to be reported taking a risk based approach.
- Inefficiencies - Third party inefficiencies

All of the above areas highlighted identified the relevance and requirement for risk management to be practiced in organisations. This is also noted in addition to the literature, namely, the lack of trust in vulnerabilities discovered, the disconnect between the organisations and their associated third parties or vendors to which they outsource the vulnerability management function, and legacy systems not being appropriately reported on.

The patch management lifecycle includes several steps, including preparation, vulnerability identification and patch acquisition, risk assessment and prioritisation, patch testing, patch deployment and verification (HKSAR, 2008). The challenge in the context of increasing vulnerabilities is the creation of policies and the effective, timely deployment of remediation measures (Afful-Dadzie and Allen, 2014). Vulnerabilities introduced due to a bad patch process add further complexity to patch management (Okhravi and Nicol, 2008). Gauci *et al.* (2017) lists several pain points for patch management such as user notifications, patch relevance, testing patches and post deployment reviews. Effective vulnerability management will thus allow the mitigation of security risks to the organisation (Singh *et al.*, 2016). As per the disadvantages of risk management, as highlighted in Chapter 5 Figure 5.38, feedback from the respondents are again very similar to the literature review which mentions that threats are not correctly represented in risk assessment models due to the complexity of threats (Ganin *et al.*, 2017).

Similarly to the review of the vulnerability and patch management policy, Figure 5.36 summarises from 28 respondents on who knows what is included in their risk management function. Considering 15 respondents responded to utilising a risk management function however 28 respondents responded to this question, as reflected in Figure 5.36, it seems in some organisations the risk management function is available but not used efficiently or at an appropriate time before patch management.

As mentioned earlier, 37.9% of the respondents believe that risk management has an inability to actually measure risk. As per the literature review, by contrast, Gauci *et al.* (2017) summarises how to quantify an uncertain risk in a cybersecurity assessment which includes knowing the following variables for an organisation. Firstly the identification or inventory of the organisations critical assets. Thereafter, the identification of threats and the associated risk levels, defining and implementing a mitigation plan and lastly the maintenance of these tasks to continue the quantification of uncertain risk and the implementation of existing security controls.

Risk Management continued to be mentioned in the "Patch Management" category when talking about superseded patches. To note from the additional feedback, respondents do refer to the understanding of what compensating controls exist in their organisation as an extra layer of protection to assets with superseded patch requirements. Further to the understanding of compensating controls, a formal risk acceptance approach and a defined risk scoring matrix should be used to appropriately define the risk of the asset not being patched to the organisation. In contrast, one respondent did mention that risk dispensations may delay or prevent patches from being deployed timeously, and another respondent did mention that an informal investigation and escalation process exists in their organisation due to the vast number of assets with a superseded patch requirement.

6.6 Utilisation of Frameworks

It is evident there is disparity in knowledge of individuals who know their compliance and whether they use frameworks or standards in their organisations, almost sitting at 25% of the respondents feedback. Being resource intensive with respect to the use of risk management, it seems the same applies to the use of a framework in the participating organisations.

As per Table 5.22, NIST seems to be mostly used. NIST is considered a standard providing best practices or principles in the participating organisation's vulnerability and patch management services (Beres *et al.*, 2008b). The participating organisations are using this as a framework rather between the mentioned services in terms of following certain guidelines to continue to manage these services. This implies a framework that includes all facets of this research taxonomy, i.e. a framework which encompasses all the themes of the taxonomy and provides process flows to allow more efficient communication and task handovers between themes and the responsible teams, is not currently being utilised.

Whereas NIST created a document that illustrates a patch and vulnerability management program (Mell *et al.*, 2005), the survey feedback does not correlate with what NIST had created in terms of a group which the professional body considers central to remediation efforts (i.e. patching and configuration changes).

The topic of this research is "An exploratory investigation into an integrated vulnerability and patch management framework". With this said, and with the revision from Table 5.22 of all respondents who confirmed they are using a framework, what standards they follow and what they believe are the advantages of using a framework, Table 6.3 and Table 6.4 help to illustrate a thread between those who are using a framework and some associated comparisons with categories from the "Vulnerability and Patch Management" themes.

Table 6.3 and Table 6.4 were filtered on all respondents whom confirmed they are using multiple teams to manage their vulnerability and patch management services. From the 19 respondents, the tables are then also filtered on who confirmed they are using a framework. This resulted in nine respondents from six organisations, 30% of the participants, being illustrated in the below tables. Due to the number of associated variables being compared separate tables were created, for the vulnerability and patch management services respectively, to review an integrated vulnerability and patch management framework however the line items per table refer to the same respondents. Only columns C, D, E, F and G are changed per table, based on the vulnerability and patch management statistics currently being compared.

Further to the earlier statement that this research implies a framework that includes all facets of this research taxonomy, i.e. a framework which encompasses all the themes of the taxonomy and provides process flows to allow more efficient communication and task handovers between themes and the responsible teams, is not currently being utilised, Table 6.3 and Table 6.4 actually gives an understanding of where the use of a framework actually correlates with a positive downward trend of vulnerabilities.

Table 6.3 confirms successful progress being made in the vulnerability management service based on 1) the high average score of communication between multiple teams (column A), 2) the low score of vulnerability management policy items not being practiced in the workplace (column C, total respondents average is 17.46%) and 3) the low score of challenges faced with vulnerability management (column F, total respondents average is 21.07%). There seems to be ownership of escalating configuration issues identified through vulnerability management (column G) and the majority of the respondents do perform risk management before deploying patches (column H).

Separate teams level of communication	Incidents, over the last 5 years, related to a MS vulnerability which had a relevant patch available at time of incident	Score of vulnerability management policy items not being practiced in the workplace	Number of vulnerabilities in your organisation	Trend of vulnerabilities being remediated in organisation moving up or down	Score of challenges faced with vulnerability management	Are configuration issues, identified through VM, escalated and monitored to completion?	Perform risk management before deploying patches?	What is the name of the framework being used?
80.00	Not sure	9.52	500001-1000000	Down	24.14	Yes	No	NIST
20.00	0	0.00	Not sure	Down	17.24	Not sure	Not sure	NIST
20.00	10+	14.29	10001-250000	Down	17.24	Yes	Yes	NIST
60.00	0	61.90	0-10000	Down	20.69	Yes	Yes	CIS Benchmarks and internal
60.00	1	0.00	Not sure	Down	13.79	Yes	Yes	NIST / ISO27001
20.00	4	9.52	250001-500000	Down	27.59	Yes	Yes	
80.00	0	4.76	0-10000	Down	13.79	Yes	Yes	ISO 27000 Series (IT Security) and NIST
80.00	0	52.38	0-10000	Down	24.14	Yes	Yes	ISF framework
80.00		4.76	10001-250000	Down	31.03	Yes	No	ISF Standards of Good Practice

Table 6.3: Vulnerability management review with utilisation of frameworks

Separate teams level of communication	Incidents, over the last 5 years, related to a MS vulnerability which had a relevant patch available at time of incident	Score of patch management policy items not being practiced in the workplace	Systems patched (patch compliance) above 95%?	Score of challenges faced with patch management	Are configuration issues, identified through patch management, escalated and monitored to completion?	Superseded patch requirements within your environment	Perform risk management before deploying patches?	What is the name of the framework being used?
80.00	Not sure	100.00	No	34.48	No	Yes	No	NIST
20.00	0	0.00		0.00	Not sure	Not sure	Not sure	NIST
20.00	10+	4.35	No	3.45	Yes	Not sure	Yes	NIST
60.00	0	43.48	Not sure	13.79	Yes	No	Yes	CIS Benchmarks and internal
60.00	1	0.00	Not sure	17.24	Yes	Not sure	Yes	NIST / ISO27001
20.00	4	4.35	Not sure	13.79	Yes	Yes	Yes	
80.00	0	8.70	No	17.24	Yes	No	Yes	ISO 27000 Series (IT Security) and NIST
80.00	0	0.00	Not sure	24.14	Yes	No	Yes	ISF framework
80.00		17.39	No	48.28	Yes	No	No	ISF Standards of Good Practice

Table 6.4: Patch management review with utilisation of frameworks

Similarly, Table 6.4 confirms successful progress being made in the patch management service based on 1) the high average score of communication between multiple teams (column A), 2) the low score of patch management policy items not being practiced in the workplace (column C, total respondents average is 19.8%) and 3) the low score of challenges faced with patch management (column E, total respondents average is 19.15%). There also seems to be ownership of escalating configuration issues identified through patch management (column F) and the majority of the respondents do perform risk management before deploying patches (column H).

The correlation between the above two tables indicates that in relation to incidents being experienced in the organisations which relate to a vulnerability where an available Windows patch needed to be applied, there continues to be a high level of communication between separate teams which manage their vulnerability and patch management services, respondents believe most of what is being stipulated in the organisations vulnerability and patch management policies are being practiced, challenges faced within the vulnerability and patch management services remain under a score of 34%, configuration issues are generally being escalated and monitored to completion, frameworks are being used and risk management is mostly being performed before deploying patches. However, with this form of alignment to the literature, although systems are not patched above a level of 95% compliance, the trend of vulnerabilities being remediated indicates a downward trend. This may imply although vulnerabilities are successfully being attended to, it is not directly as a result of a high patch compliance in the organisations.

6.7 Research Findings Summary

Because there are multiple themes with multiple categories and subcategories of the Vulnerability Management Resilience Taxonomy, a rating scale was defined which further to allowing correlation of summaries from the feedback received, the scoring also helped in creating a quadrant of where most of the respondents are performing in terms of progressive remediation of vulnerabilities within their environments. Figure 6.1 is a result of this analysis. The X axis details from left to right, “not aligned with the literature” to “aligned with the literature”. The Y axis details from bottom to top “what is not working” and “what is working” in the environments based on the understanding of the above analysis. This scoring was done by understanding the available options from the survey’s multiple choice, verses what the user has selected or provided further information on and then a mark out of 100% was calculated.

Table 6.5 and Table 6.6 summarises which categories were included in the calculation of the quadrant. The X axis helps understand where the respondents are sitting in terms of following the literature review verses not following the literature review. The Y axis helps understand where the respondents are sitting in terms of what is working and what they are practicing within their environments. The averaged scores for the following categories were used in the quadrant calculations.

Figure 6.1 provides a graphical representation of the summary from Table 6.5 and Table 6.6 by placing the summarised scoring per category, per respondent, on a scatter map to help visualise what is considered working in an organisation and is (or is not) in line with what the literature currently suggests.

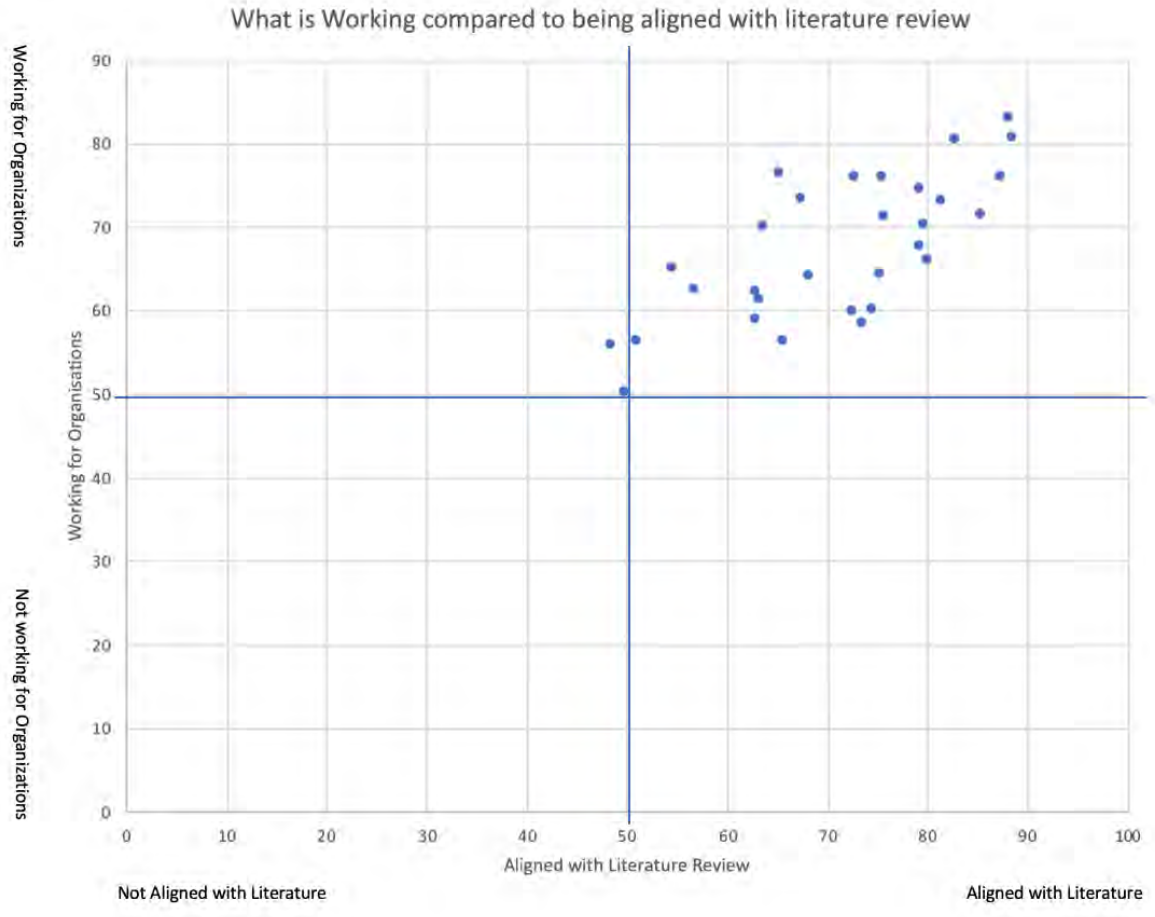

Figure 6.1: Organisational capability based on literature

It is evident from Figure 6.1 that most of the respondents fall within the top right of the quadrant which refers to the respondents having listed that they mostly do follow what the literature review has revealed, as most of the answers or taxonomy subcategories were listed as identified in the literature. What they are currently practicing verses

X Axis	Detail
Team Structure1	In your organisation, does one cross-functional team have responsibility for vulnerability management and patch management?
Separate Teams	If you have separate teams, under what circumstances do they communicate?
VM Policy	Do you have a vulnerability management policy or similar document?
VM Policy Items	What items does your vulnerability management policy or similar document cover?
Ownership of Configuration Escalations	Is there ownership of who escalates configuration issues identified through a vulnerability management process to the correct team for action?
Conclusions of Configuration Escalations	Are such queries monitored to completion?
Patch Deployments	Do you have a central platform for managing and deploying Microsoft patches?
Patch Management Policy	Do you have a patch management policy or similar document?
Patch Management Policy Items	What items does your patch management policy or similar document cover?
Configuration Escalations Identified through Patch Management	Is there ownership of who escalates configuration issues identified through a patch management process to the correct team for action?
Conclusions of Configuration Escalations identified through Patch Management	Are such queries monitored to completion?
Centralised Asset Management Systems	Do you have a system to centralise asset management such as a configuration management database (CMDB) which details full asset details (installed components, versions \& services) and ownership?
Up to date Centralised Asset Management Systems	Is your centralised asset management solution up to date?
Risk Management	Does your organisation perform risk management before deploying patches?
Risk Management Activities	What activities does the risk management function within your organisation include?
Frameworks	Do you utilise any existing frameworks (or engagement model) that allows for effective collaboration between vulnerability management and patch management teams?

Table 6.5: Defined quadrant detail on literature review vs current practice, X Axis

Y Axis	Detail
Team Structure1	In your organisation, does one cross-functional team have responsibility for vulnerability management and patch management?
Separate Teams	If you have separate teams, under what circumstances do they communicate?
Incidents	How many incidents were related to a Microsoft vulnerability which had a relevant MS Windows patch available at the time of recent incidents?
Incident Impact	What was the general business impact of these incidents?
Preparation for Incident	In general, were you well prepared for the incident, i.e. incident response?
VM Policy	Do you have a vulnerability management policy or similar document?
VM Policy Items	Please list items which you have listed is in your vulnerability management policy (above) however of which you are not practicing in the workplace?
Vulnerabilities Trend	Monthly trend of vulnerabilities being remediated in organisation?
VM Challenges	Vulnerability management challenges within your organisation?
Room for VM Improvement	After contextualising vulnerability management within your organisation, do you agree that there is still room for improvement required?
Config Escalations Identified through VM	Is there ownership of who escalates configuration issues identified through a vulnerability management process to the correct team for action?
Config Escalations identified through VM	If yes, are such queries monitored to completion?
Patch Deployment	Do you have a central platform for managing and deploying Microsoft patches?
Patch Management Policy	Do you have a patch management policy or similar document?
Patch Management Policy Items	Please list items which you have listed is in your patching policy (above) however of which you are not practicing in the workplace?
Patch Compliance	Organisation's proportion of systems patched (patch compliance) above 95 percent?
Patch Management Challenges	Patch management challenges within your organisation?
Patch Management Improvement	After contextualising patch management within your organisation, do you agree that there is still room for improvement required?
Config Escalations Identified through Patch Management	Is there ownership of who escalates configuration issues identified through a patch management process to the correct team for action?
Config Escalations identified through Patch Management	If yes, are such queries monitored to completion?
Superseded Patches	Do you have any superseded patch requirements within your environment?
Asset Management	Do you have a system to centralise asset management?
Asset Management Updates	Is your centralised asset management solution up to date?
Risk Management	Does your organisation perform risk management before deploying patches?
Risk Management Activities	What activities does the risk management function within your organisation include?
Improvements in Managing Risks	To what degree have there been efficiency improvements made (or are in-progress) to the system of controls and processes, taken as a whole, by redesigning, consolidating, or automating key controls used to manage risk?
ISO27001 Compliance	Is your organisation, or a division, ISO27001 compliant?
PCI Compliance	Is your organisation, or a division, PCI compliant?
Frameworks	Do you utilise any existing frameworks (or engagement model) that allows for effective collaboration between vulnerability management and patch management teams?

Table 6.6: Defined quadrant detail on literature review vs current practice, Y Axis

their number of vulnerabilities and patch compliance implies that what they currently performing within their environment is producing positive results.

6.7.1 Team Structure Impact

Further to the above direct feedback from the respondents, and the summaries of the themes and their respective categories of the research taxonomy, Table 6.7 provides insight to the first secondary research question, whether "a silo approach between vulnerability management and patch management produces positive results in terms of remediating known vulnerabilities". Table 6.7 summarises all respondents who utilise one cross-functional team in their organisation and is then also filtered by removing all "0", "not sure" or blanks in terms of "how many incidents were related to a MS vulnerability which had a relevant MS Windows patch available at the time of the incident" The resulting data included respondents whom only had one incident related to a Windows vulnerability. The respondents from Table 6.7 were also not sure whether they were PCI compliant.

The end result of Table 6.7 is to indicate whether having one team to manage the vulnerability and patch management services is producing positive results. It is clear from Table 6.7 that one cross-functional team, from the respondents' feedback, only had one incident in the last five years related to a Windows vulnerability which had a relevant Windows patch available at the time of the incident. The business impact for 66.6% of these respondents remained low and 66.6% were prepared for this incident. The answer to whether a silo approach works however can be understood by looking at the number of vulnerabilities within their organisation, which 66.6% of the respondents have confirmed are less than 10 000. Also, 66.6% of the respondents confirmed they do perform risk management before their patch deployment. None of these respondents however are familiar with standards being followed in their organisation and only 33.3% of the respondents confirmed they use a framework.

Table 6.7 can then be compared to Table 6.8 which details all respondents who work with multiple teams to manage their vulnerability and patch management services. Table 6.8 is then also filtered by removing all "0", "not sure" or blanks in terms of "how many incidents were related to a MS vulnerability which had a relevant MS Windows patch available at the time of the incident".

Business impact?	Prepared for Incidents?	Number of vulnerabilities in your organisation?	Trend of vulnerabilities being remediated in your organisation moving up or down?	Room for improvement required in your VM Service	Systems patched (patch compliance) above 95%?	Room for improvement required in your patch management service?	Perform risk management before deploying patches?	Efficiency improvements made (or are in-progress) to the system of controls and processes used to manage risk?	ISO 27001 compliant?	Existing frameworks (or engagement model) being utilised?	What is the name of the framework being used?
Low	No	0-10000	Down	Agree	Yes	Agree	Yes	A little better	Not sure	Not sure	No response
Low	Yes	0-10000	Up	Agree	Yes	Agree	No	Significantly better	Not sure	Not sure	No response
High	Yes	Not sure	Down	Strongly agree	No	Strongly agree	Yes	Significantly better	No	Yes	Hybrid

Table 6.7: Review of one cross functional team structure

Incidents related to a MS vulnerability?	Business impact?	Prepared for Incidents?	Number of vulnerabilities in your organisation?	Trend of vulnerabilities being remediated in your organisation moving up or down?	Room for improvement required in your VM Service	Systems patched (patch compliance) above 95%?	Room for improvement required in your patch management service?	Perform risk management before deploying patches?	Efficiency improvements made (or are in-progress) to the system of controls and processes used to manage risk?	ISO 27001 compliant?	PCI compliant?	Existing frameworks (or engagement model) being utilised?	What is the name of the framework being used?
10+	Medium	No	10001-250000	Down	Agree	No	Agree	Yes	A little better	Yes	No	Yes	NIST
2	High	Yes	10001-250000	Staying about the same	Agree	No	Strongly agree	Not sure	A little better	Yes	No	No	No response
1	Medium	Yes	Not sure	Down	Agree	Not sure	Agree	Yes	Significantly better	Yes	Yes	Yes	NIST / ISO 27001
4	Low	Yes	250001-500000	Down	Agree	Not sure	Agree	Yes	A little better	Yes	Yes	Yes	No response
1	Medium	Yes	10001-250000	Staying about the same	Agree	Yes	Agree	No	Significantly better	Yes	No	No	No response
2	Medium		0-10000	Not sure	Strongly agree	No	Strongly agree	No	A little better	No	No	Not sure	No response

Table 6.8: Review of one multiple team structure

6.7.2 Review on Primary Research Question

Although Chapter 5 identifies the answer to the primary research question which is "what are the challenges that face vulnerability remediation through patch management within organisations", and most of the previous graphs indicate why from a team structure and other associated variables perspective, the following section will delve further into why there are challenges currently being experienced as per the respondents feedback.

Table 6.1 illustrated the most common items listed in the respondents' defined vulnerability management policy and also the top number of items which the respondents are not practicing in their environments. Table 6.2 then continued to illustrate the most common items listed in the respondents defined patch management policy and also the top number of items which the respondents are not practicing in their environments. These tables can imply answers as to why organisations could be failing. However, the following review provides a further understanding of the feedback to answer "why" there are challenges within the organisations.

Vulnerability management is a continuous cycle of revision and action, unlike a project which will have a start and end task. Vulnerability management will also be an ongoing requirement if we consider the possibility of software never being released without bugs. With this understanding of an ongoing effort, it is vital to have all personnel involved in this exercise working towards common goals. Otherwise, when trying to correlate the tasks between the vulnerability and patch management teams, inefficient processes will be evident, pulling the different teams into different directions and not effectively dealing with the cybersecurity issues at hand.

To summarise through a separate means of understanding the challenges faced through vulnerability management, the research data was filtered off all respondents who mentioned their vulnerabilities trend is increasing. This is a separate approach to the tables listed earlier in this section. Out of the three respondents highlighted, two of the three respondents mentioned they have multiple teams dealing with vulnerability and patch management. Table 6.9 details what they were not practicing from what was being highlighted in the vulnerability management policy. Table 6.10 details what the respondents were not practicing from what was being highlighted in the patch management policy.

Item not being practiced	Detail of item
Logging calls	Logging calls with respective teams to remediate vulnerabilities.
Service level agreements	Service levels/timelines for patching different vulnerability severities.
Health Checks	Daily/weekly/monthly review of failed scans, i.e. health checks.
Expedite patches	A separate process to tackle zero-day vulnerabilities or otherwise expedite patches

Table 6.9: Vulnerabilities increasing, Vulnerability management policy, Items not being practiced

Item not being practiced	Detail of item
Test Patches	Performing test management of patches.
Service level agreements	Service levels/timelines for patching different vulnerability severities.
Reviewing all vulnerability severities	Patching all vulnerability severities.
Expedite patches	A separate process to tackle zero-day vulnerabilities or otherwise expedite patches.

Table 6.10: Vulnerabilities increasing, Patch management policy, Items not being practiced

6.7.3 Influencing Factors

From a research objective perspective, "influencing factors that impact successful vulnerability management" can also be derived from Table 6.7. To summarise, single teams being used for vulnerability and patch management, whom are well prepared for incidents, i.e. business continuity management, are some of these influencing factors which correlates with low vulnerabilities within the respondent's environments. This also ensures the majority have a patch level compliance status above 95%, although the respondents still believe there is room for further improvement in their environment. As earlier summarised, these respondents do not seem to focus on being compliant in aspects such as ISO27001 and PCI, however 33.3% does utilise a hybrid of frameworks and 66.6% of this data sample also do risk management before patch deployment.

To summarise the above, Table 6.11 details the respondents who have confirmed they have less than 500 000 vulnerabilities, the lowest number of vulnerabilities reported (column C), and mostly all of which understand there is a vulnerability management (VM) policy (column A), they utilise most of what is being detailed in their VM policy as indicated by the low score (column B). The low score refers to the least number of selected items available from the drop down multiple choice options. This list of multiple choice options are identical to what the selection option was for respondents to confirm what is in their VM policy. These respondents also tend to suggest the trend of their remediated vulnerabilities is moving down. Most of their challenges are below 50% of what was available for selection and lastly, they "strongly agree" there is still room for improvement in their organisation for their vulnerability management service.

6.7.4 Risk Management Review

A further full review of the dataset, as per Table 6.12 gives an indication of the number of vulnerabilities each respondent has answered and whether they perform risk management or not before patching, keeping into account the number of Windows patch related vulnerabilities.

Table 6.12 is filtered on all organisations who mentioned their vulnerability total in their organisation (column A) and also filtered on removing all the "0", blanks and "not sure" values for column B. It is evident from Table 6.12 that there is a balance between respondents that perform risk management, their associated number of vulnerabilities in the

Do you have a vulnerability management policy or similar document?	Score of organisation's not practicing what is in their VM policy	Number of vulnerabilities in your organisation	Monthly trend of vulnerabilities being remediated in your organisation moving up or down?	What challenges do you face with vulnerability management within your organisation? The average score is used below.	Do you agree that there is still room for improvement required?
Yes	9.52	10001-250000	Down	58.62	Strongly agree
Yes	14.29	10001-250000	Down	17.24	Agree
Yes	9.52	10001-250000	Staying about the same	17.24	Agree
Yes	61.90	0-10000	Down	20.69	Agree
Yes	38.10	0-10000	Down	3.45	Agree
Yes	19.05	10001-250000	Up	55.17	Strongly agree
Yes	38.10	0-10000	Staying about the same	10.34	Strongly agree
Yes	9.52	250001-500000	Down	27.59	Agree
Yes	28.57	10001-250000	Staying about the same	27.59	Agree
Yes	0.00	0-10000	Up	13.79	Agree
Yes	4.76	0-10000	Down	13.79	Agree
Yes	33.33	0-10000	Not sure	17.24	Strongly agree
Yes	4.76	0-10000	Down	6.90	Agree
Similar document	9.52	0-10000	Staying about the same	48.28	Strongly agree
Yes	4.76	0-10000	Up	13.79	Agree
Not sure	0.00	0-10000	Down	13.79	Strongly agree
Yes	4.76	0-10000	Down	34.48	Strongly agree
Similar document	52.38	0-10000	Down	24.14	Agree
Yes	4.76	10001-250000	Down	31.03	Strongly agree

Table 6.11: Vulnerability management review on policies being used vs current challenges vs least vulnerabilities

Number of vulnerabilities in your organisation?	How many incidents were related to a Microsoft vulnerability which had a relevant MS Windows patch available at the time of the incident?	Superseded patch requirements within your environment?	Perform risk management before deploying patches?
10001-250000	10+	Not sure	Yes
10001-250000	2	No	Not sure
250001-500000	4	Yes	Yes
10001-250000	1	No	No
0-10000	2	Not sure	No
0-10000	1	Yes	Yes
0-10000	1	No	No

Table 6.12: Risk management correlated with vulnerabilities

organisation and the associated number of Windows related patch incidents as opposed to respondents that do not perform risk management prior to patch deployment.

6.7.5 Progressive Vulnerability Management

Table 6.13, Table 6.14 and Table 6.15 all indicate associated variables with three respondents from three organisations whom confirmed their monthly trend of vulnerabilities being remediated in their organisation is moving up. Due to the number of the associated variables, three tables were created, however the line items from each table refer to the same respondent.

6.7.6 Taxonomy Review

The structure and different levels of the taxonomy is further confirmed through the review of the survey feedback. Firstly with the understanding of having a correct team structure with people whom have the right focus or aptitude for the services they are managing. Through the research literature review on vulnerability and patch management, Spears and Barki (2010) suggests that although users are seen as a weak link in information security, a user's understanding of the organisation or the business contributes to more effective security controls or measures. It was mentioned earlier that it remains vital to have all personnel involved in this exercise whom are educated and working towards

Monthly trend of vulnerabilities being remediated moving up	Score of VM items not being practiced in the workplace?	Number of vulnerabilities in your organisation?	Score of number of challenges faced with vulnerability management	Are configuration issues identified in vulnerability management monitored to completion?	Do you have a central platform for managing and deploying Microsoft patches.	Score of patch management items not being practiced in the workplace?
Up	19.05	10001-250000	55.17	Yes	Yes	17.39
Up	0.00	0-10000	13.79	Yes	Yes	0.00
Up	4.76	0-10000	13.79	Yes	Yes	4.35

Table 6.13: Progressive use cases of vulnerability management-1

Monthly trend of vulnerabilities being remediated moving up	Organisation's systems patched (patch compliance) above 95%?	Score of number of challenges faced with patch management	Are configuration issues identified after patch management monitored to completion?	Superseded patch requirements	Centralised asset management solution up to date	Organisation perform risk management before deploying patches?
Up	No	72.41	Yes	Yes	No	Not sure
Up	Yes	13.79	Yes	Yes	Yes	Yes
Up	Yes	10.34	Yes	No	Not sure	No

Table 6.14: Progressive use cases of vulnerability management-2

Monthly trend of vulnerabilities being remediated moving up	ISO27001 compliant	PCI compliant	Utilise any existing frameworks (or engagement model)	Does one cross-functional team have responsibility for vulnerability management and patch management? (please select one)	How many incidents were related to a Microsoft vulnerability which had a relevant MS Windows patch available at the time of the incident?	General business impact of these incidents?	Well prepared for the incident, i.e. incident response
Up	No	No	No	No	No response	Medium (significant effect but manageable)	Yes
Up	Yes	Yes	No	No	0	Low (minor effect or consequence)	Yes
Up	Not sure	Not sure	Not sure	Yes	1	Low (minor effect or consequence)	Yes

Table 6.15: Progressive use cases of vulnerability management-3

common goals. If everyone is not working with similar goals, inefficient processes will be evident, pulling the different teams into different directions and not effectively dealing with the cybersecurity issues at hand.

As mentioned in the Introduction of this research, security teams of large organisations or enterprises usually manage security controls such as patching, anti-virus or anti-malware applications, firewalls, etc., all of which work together to minimise exposure to potential threats (Beres *et al.*, 2008b). An understanding of ownership is required for the different components of the taxonomy. This would tie in with understanding ownership of assets and understanding the critically of those assets, and may potentially allow a more effective and holistic approach to vulnerability and patch management.

It is important to have comprehensive knowledge of all assets within the organisation, in terms of understanding asset components, operating systems and applications (Gauci *et al.*, 2017). With this said the above research does indicate that although a centralised asset management tool is being used in the participating organisations, less than 18% believe the data of the solution is up to date. The discussion of asset management was also raised as additional feedback from a respondent when talking about virtualised assets and monitoring of operating system versions.

Further to what was detailed in the "Summary of Vulnerability Management Challenges" table, referenced in Chapter 5, an asset database (such as incorrect or incomplete information of assets, i.e. asset ownership, installed components, services, versions) remain an issue at 43.3% of the responses.

The above research also reviewed and provides an understanding of the percentage of vulnerabilities which caused an incident within the target population. From the earlier mentioned research objectives, the research highlights that an influencing factor that impacts vulnerability management is where multiple teams are well prepared for incidents, i.e. business continuity management being of the highlighted influencing factors. Past critical incidents and current critical incidents remain key when reviewing the effectiveness of vulnerability management and the prevention of vulnerabilities from being exploited.

With the above in mind, incident management is placed at level three and eight of the taxonomy to allow a review of previous incidents and post incidents, its relation to critical assets and the following layers then focus on the assurance that previous incidents of a similar nature will not reoccur. Incident management is thus seen twice in the taxonomy to allow continuous review of current issues or challenges in the organisations. Also previous incidents with the understanding of required frameworks, possibly not being

followed, needs to be evaluated as a principle the organisation follows before deciding on the controls and how to apply them, i.e. vulnerability and patch management.

As earlier mentioned, it seems there is disparity between the advantages of utilising a framework which provides a holistic approach to threats and vulnerabilities and also allowing a risk analysis to take place whereas the disadvantages of utilising a framework itself does not allow a means to characterise risk, further to being resource and time consuming. This does, however, reflect that should your organisation be utilising a framework, this should be decided before defining your means to identify threats and vulnerabilities.

Attacks exploit known vulnerabilities which have available patches or other remediation options (Cavusoglu *et al.*, 2008, Okhravi and Nicol, 2008, Afful-Dadzie and Allen, 2014). Again, a relation to the understanding of vulnerability management being applied before the prioritisation of patching takes place. Effective vulnerability management will thus allow the mitigation of security risks to the organisation (Singh *et al.*, 2016). It is for this reason once the vulnerability management takes place, risk management is performed to allow for a more effective prioritisation and patch deployment. Risk increases exponentially through the vulnerability timeline as the vulnerability becomes better known (Beres *et al.*, 2008a,b).

As listed under the "Effective Vulnerability Management" section of Chapter 2, there is benefit in reviewing existing security controls, threat information, the organisation's assets and the impact of a potential attack together with the available CVSS scores (Rouse, 2017) and this has thus been kept in mind through the analysis of this research. CVSS considers the vulnerability's characteristics (base metric), the vulnerability's progression over time (temporal metric) and the organisation's security level (environmental metric) (Singh *et al.*, 2016, Shetty *et al.*, 2018). The base metric can be further split into exploitability and impact metrics.

Risk Management, similarly to the review of the vulnerability and patch management policy, summarises from 24 respondents from 12 organisations, on who knows what is included in their risk management function and four respondents from two organisations have listed "not sure". Considering 15 respondents responded to utilising a risk management function however 28 respondents responded to this question, as reflected in Figure 5.36, it seems in some organisations the risk management function is available but not used at the correct times before patch deployment.

Regarding the understanding of the respondents feedback in terms of what they are not practicing further to their defined patch management policy, items such as not defining

service levels/timelines for patching different vulnerability severities and another item on respondents not patching all vulnerability severities can only be done effectively once the vulnerability management and risk management approach takes place.

Gauci *et al.* (2017) summarises how to quantify an uncertain risk in a cybersecurity assessment which includes knowing the following variables for your organisation, i.e. inventory, identify threats, risk levels, define mitigation, implement mitigation and maintain processes for existing controls. This also continues to then define the understanding of risk management to be performed before patch management. This statement also helps clarify the need to know your inventory, i.e. asset management and identify threats and risk levels, through the themes of "Incident Review" and "Incident Management" of the taxonomy.

As mentioned in Chapter 6, Nicolett and Colville (2003) states that patch management is not enough when effectively mitigating vulnerabilities. Further to the theme of "Patch Management", a "pre-patch mitigation plan" seems to be uncommon among the respondents and superseded patches remain an issue in organisations. Further to the available statistics for this theme based on the feedback to what was found in the literature review, a respondent also confirmed that "facilitating strategy" is an advantage from the use of risk management before patch management.

The patch management lifecycle includes several steps, including preparation, vulnerability identification and patch acquisition, risk assessment and prioritisation, patch testing, patch deployment and verification (HKSAR, 2008). The following functional requirements should also be considered with regards to patch management: asset inventory, patch and service pack status, patch dependency analysis, patch dependency analysis, patch inventory and patch classification, patch matching reports or system baselining, role based administration, patch distribution and installation, patch and application support and agent vs agentless architectures. As mentioned in the literature review, Okhravi and Nicol (2008) also details elements for successful patch management. These are executive support, dedicated resources and clearly defined responsibilities, creation and maintenance of technology, identification of vulnerabilities and available patches, scanning and monitoring the network, testing of patches and post-deployment scanning and monitoring. The above assists in defining the several layers of the taxonomy, from the clearly defined responsibilities of dedicated resources, to firstly the identification of vulnerabilities and the available patches which would include scanning and monitoring the network, to the testing and deployment of patches to the post monitoring whether the patch cycle was effective.

To conclude on the "Incident Management" theme of the taxonomy, the mention of incident management at layer three and layer eight is because this is what we ultimately trying to avoid. Any incidents after a successful patch cycle will need to be reviewed and the possibility of revising all layers from one to eight again after picking up new vulnerabilities remains an option. Further research can allow cycles to take place between the different layers. As mentioned earlier, the taxonomy is meant to outlay all paradigms of activities required in vulnerability and patch management.

Chapter 7

Conclusion

This was primarily an exploratory study which assisted the researcher to accomplish research objectives and ultimately review a framework where available, that integrates an understanding of processes and activities between the vulnerability and patch management services of an organisation. Through the above empirical research, vulnerability and patch management services within FSIs were reviewed, testing the initially proposed taxonomy with the target population to obtain their feedback on the categories of the taxonomy and formulate results on the efficacy of the taxonomy. The taxonomy exists as a reflection of the research survey, formulating a basis of understanding regarding aspects of vulnerability management and includes associated paradigms of services or functions. The taxonomy assists in understanding any existing frameworks being utilised, giving guidance on process and cyclic behaviours between the different themes of the taxonomy.

To summarise the questions this research wanted to answer:

1. Primary question - What are the challenges that face vulnerability remediation through patch management within organisations, and why?
2. Secondary question - Does a silo approach between vulnerability management and patch management produce positive results in terms of remediating known vulnerabilities?
3. Secondary question - What are the advantages of an engagement model between vulnerability management and patch management?
4. Secondary question - What are the disadvantages of an engagement model between vulnerability management and patch management?

7.1 Conclusion on Research Questions

Regarding some of the direct feedback received from the respondents, 1) the challenges that face vulnerability and patch management, 2) the preference by the participants on using multiple teams and the advantages thereof, 3) advantages and 4) disadvantages of using frameworks in the respondents environments are answered by several of the figures and tables listed in chapter 5.

Table 6.8 indicates that, of the respondents using multiple teams in their organisations to manage vulnerability and patch management, several incidents were experienced in the last five years that were related to a Windows vulnerability which had a relevant Windows patch available at the time of the incident. The business impact for 66.6% of these respondents remained medium and 66.6% were prepared for these incidents. The answer to whether an approach of using multiple teams effectively works however can be understood with the number of vulnerabilities within their organisation, which 66.6% of the respondents have confirmed is more than 10 000. 50% of the respondents also confirmed they do perform risk management before their patch deployment. As opposed to the respondents utilising one cross-functional team, the respondents utilising multiple teams for their vulnerability and patch management are familiar with standards being followed in their organisation, 83.3% confirming they are ISO27001 compliant and 50% of the respondents confirmed they use a framework, mostly NIST.

The comparison of the above mentioned tables clarifies the differences between using one team verses using multiple teams to manage the vulnerability and patch management services. Further to the understanding of previous incidents which happened in the organisations related to a missing Windows patch and the associated business impact, these tables then also compared the following:

1. Current vulnerability count from each respondent.
2. Whether there is an improvement in their vulnerability and patch management services.
3. What their patch compliance is.
4. Whether they perform risk management before patching.
5. What standards or frameworks do they follow.

The respondents whom confirmed they use multiple teams actually have more vulnerabilities in their environment and their trend of remediating vulnerabilities are mostly either "staying about the same" or are going "down". They also have less certainty that their systems have a patch compliance of over 95%.

A respondent provided further feedback to also consider the structure of the organisation, i.e. is the organisational structure centralised, federated or a combination of both. The structure of the organisation directly impacts the effectiveness of the IT risk and security function in its ability to execute its various tasks or functions.

Chapter 5 and the analysis of the survey feedback found in Chapter 6 continues to provide direct answers to the remaining two secondary research questions, i.e. 1) the advantages, and 2) the disadvantages of an engagement model/framework between vulnerability management and patch management. The "Review on Primary Research Question" section detailed in Chapter 6 then continues to provide clarity from respondents, who confirmed their organisations are not progressively remediating vulnerabilities, on what their organisations are not doing of which their vulnerability and patch management policies dictates. These would, from the understanding of the themes being analysed in this research, allow us to understand why there are challenges in the organisations.

7.2 Conclusion on Research Objectives

The research objectives helped identify the evaluative criteria for the research questions and formulate the research in terms of the structure taken to answer the research questions. The following interconnected research objectives were obtained through the research:

1. Influencing factors - Identify influencing factors that impact successful vulnerability management.
2. Recommendations - To make recommendations regarding positively influencing each identified factor.
3. Risk management - Identify whether effective risk management within a vulnerability management program actually benefits the approach to patching, further to patching what Microsoft has available in its catalog.
4. Explore use cases - Identify and explore use cases where the decline of vulnerabilities remain progressive.

"Influencing factors that impact successful vulnerability management" can be derived from various tables detailed in Chapter 6. The second research objective, "to make recommendations regarding positively influencing each identified factor", is at an organisations discretion to decide on how to positively influence each identified factor further to their security strategy and their importance of the themes reviewed in this research. The research analysis does provide clarity in terms of not only the respondents from same organisations having different interpretations or different mindsets to certain categories of the taxonomy; there are also vulnerability and patching policy disparities on what is currently being practiced in the participating organisations and what is not being practiced further to what is defined in their vulnerability and patch management policies. This would be the first focus area when trying to improve vulnerability management and patch management, and that is the review of policy to what is being practiced and the assurance of the correct people having the same understanding of the research service variables where appropriate. Different roles within an organisation that touch on vulnerability and patch management (including the difference in perception of the services between a junior or senior employee), needs to be resolved and the understanding of everyone having a joint responsibility in the research topic needs to be clarified and agreed upon by all parties involved. A respondent confirmed post the survey feedback that "if security fails then we all fail as it is a shared responsibility, there needs to be an agreed cadence between all teams involved with mutually agreed targets and SLAs". Once these categories are understood, the challenges can then be reviewed and prioritised based on an organisation's risk appetite.

The third research objective is to "identify whether effective risk management within a vulnerability management program actually benefits the approach to patching, further to patching what Microsoft has available in its catalog". It seems from the earlier mentioned tables in Chapter 6 "Research Findings Summary", that most of the respondents do perform risk management prior to patching and vulnerabilities are not higher than 500 000.

The last research objective is to "identify and explore use cases where the decline of vulnerabilities remain progressive". This has been reviewed and illustrated in the last chapter however the summarised tables, from Chapter 6, on utilising single or multiple teams also provides clarity on some of the associated variables where the respondents mention their vulnerability remediation is increasing or decreasing. Lastly, through this research it has been identified whether there are mechanisms currently in place for the patching team to refer back to the vulnerability management team on items that cannot be patched, either due to possible interoperability issues, operating systems which have

reached end of life, machines that require configuration updates, service pack restrictions, upgrade requirements, etc. Between 70% to 80% of the respondents do believe there are escalations taking place of configuration issues identified either through the vulnerability management or the patch management processes however a lessor percentage of these respondents believe these escalations are being monitored successfully to conclusion.

7.3 Research Contribution

The data collected from the survey has helped the researcher to understand the important relationship between vulnerability and patch management and other associated variables.

The benefits of the research were the following:

- Review current challenges - Establish current challenges for effective vulnerability remediation and areas of improvement.
- Revise patch management approach - Confirm whether there is a better approach to patch management on vulnerabilities that are not listed as critical and not listed with an exploit yet, i.e. be more proactive in approach rather than ignoring the less critical vulnerabilities and relying on compensating controls.
- Create a conceptual taxonomy - Create a conceptual taxonomy that will allow for further research and defining of suitable frameworks which can be used in organisations, initially focused for the financial sector. The taxonomy creates the basis for a suitable framework which can enhance the needs and requirements of the users.

Further to the research questions and objectives, the research was able to produce a logical and concise taxonomy, allowing the classification of multiple themes associated with the research (Ely, Osheroff, Gorman, Ebell, Chambliss, Pifer, and Stavri, 2000). The taxonomy is flexible as it not only provides a theoretical comparison but also allows for additional themes to be applied or for a theoretical framework to be developed based on the taxonomy.

The research allowed empirical data to include opinions and perceptions from people and allowed the researcher to understand reality (Brady, 2015, Ganin *et al.*, 2017). The taxonomy was reviewed and validated based on the scoring on the feedback to the research

survey. Deviations from the initial draft of the taxonomy were considered based on the analysis of the feedback. Figure 7.1 details an updated taxonomy based on the feedback of this research. To note, the taxonomy is not a framework and thus the use of the different layers to be performed in cycles or if something happens in a certain layer to go to another layer for review is not what this research is advising. It is, however, structuring all paradigms related to vulnerability and patch management.

Figure 7.1: Vulnerability management resilience taxonomy updated

Table 7.1 describes the final summary of the research taxonomy themes. This research acknowledges that there are several other aspects to vulnerability management, other than patch management and particularly to one operating system. There are also issues such as configuration management issues, systems end of life, systems requiring upgrades, etc. This was also highlighted in the configuration escalation issues further to patching. With this said, the research includes configuration management at both levels or themes of "Vulnerability and Patch Management".

In addition, it was listed that asset management is a key foundational aspect, as per the feedback of the survey and the associated benefits in successful vulnerability remediation. There are thus three updates to the initial proposed taxonomy, namely the following. To note, "Configuration Management" refers to two updates in separate themes of the taxonomy, namely the following:

- Asset Management - As per the research survey feedback, asset management is a key foundational aspect when performing effective vulnerability remediation. The

research will not further elaborate on the differences between asset management and a configuration management database as this can be reviewed in further research.

- Configuration Management - This point of discussion revolves around both 1) the vulnerability management and 2) the patch management services. It seems through both of these services, further to patch management, anything not patch related should be correctly owned, escalated and monitored so that positive results from the escalation takes place.

Table 7.2 illustrates the final research detail to Figure 7.1, providing further detail on the additional and associated categories of the taxonomy.

7.4 Practical Implications

As there are various teams responsible for vulnerability and patch management within an organisation, the practical implications of the research will allow for a detailed understanding of the various paradigms of the two services. This means that whether one is technical or not, the research and its findings should allow information security practitioners, IT or the Risk team to be able to understand the implications of their actions on their organisations goals to remediate vulnerabilities in the organisation, thus reducing the associated risk for the organisation.

The following practical suggestions have been drawn from Chapter 6.

- A cross-functional team may result in fewer overall vulnerabilities.
- Daily practices and routine processes, such as logging calls, reviewing failed scans, maintaining SLA levels, security control reviews, and testing patches, are key to ongoing success.
- "Emergency" processes such as a process to expedite patches for zero-day vulnerabilities are important.
- Up-to-date record-keeping infrastructure such as an asset database can be a key resource for both vulnerability management and patch management.
- It is not necessary to utilize a risk framework. However, if a framework is being used, this should be decided before defining a means to identify threats and vulnerabilities.

Theme	Summary	Description
People and Team Structure	Respondent Roles and Experience	Respondents background section to understand the participant's current demographics, aptitude and experience in the industry, and their understanding of vulnerability management and patch management services, incl. team structures.
Asset Management	Asset and Configuration Management	A section to detail the assets and associated configuration in the organisation to understand critical assets within the organisation.
Incident Review	Reflection on Incidents	A section where respondents could acknowledge recent incidents in their environment and whether there were any associations with Microsoft Windows patching, or lack thereof.
Frameworks	Frameworks	A section to understand whether any frameworks, to create facilitation or a means of engagement between vulnerability and patch management, is being practiced in the organisations and whether the respondents can detail the advantages and disadvantages accordingly.
Vulnerability Management and Configuration Management	Vulnerability Management Policy and Practice	A vulnerability management section created to understand policy, what is being practiced in the organisation in relation to defined policy, what the known challenges are, trending of vulnerabilities and whether (after contextualising vulnerability management within each organisation) the participants believe that there is still room for improvement required.
Risk Management	Risk Management Strategies	A section to understand whether risk management is being practiced in the organisations and whether the respondents can detail the advantages and disadvantages of this practice.
Patch Management and Configuration Management	Patch Management Policy and Practice	A patch management section created to understand policy, what is being practiced in their organisation further to their defined policy, their organisation's current patching SLA, what the known challenges are and whether (after contextualising patch management within each organisation) the participants believe that there is still room for improvement required.
Incident Management	Organisation Cyber Incident Management	Post incident review and the assurance that previous incidents of a similar nature will not occur through the vulnerability and patch management cycle.

Table 7.1: Taxonomy final themes

Theme	Category
People and Team Structure	Experience in information & cybersecurity
	Aptitude through information security certifications or qualifications
	Team structures and responsibilities for vulnerability management and patch management
	Circumstances of communication for multiple teams
	Focus items of communication between multiple teams regarding what cannot be patched
	Advantages of separate teams
	Advantages of one multi-skilled team
Asset Management	Considerations on a centralised asset management solution
	Period of utilisation regarding a centralised asset management solution
	Functionality and applicability of a centralised asset management solution
Incident Review	Incidents experienced in last 5 years
	Incidents experienced in last 5 years which are associated with a Microsoft vulnerability
	Business consideration over incidents
Frameworks	ISO27001 compliance
	PCI compliance
	Utilisation of industry frameworks
	Understanding of frameworks being used in organisation
	Advantages of following a framework
	Disadvantages of following a framework
Vulnerability Management and Configuration Management	Vulnerability management policy documents
	Detail of vulnerability management policy
	Vulnerability management policy items not being practiced in the workplace
	Number of vulnerabilities in organisations
	Trending of vulnerabilities being remediated
	Challenges of vulnerability management
	Contextualising vulnerability management and room for improvement
	Escalation of configuration issues identified through a vulnerability management process
	Monitoring of escalated configuration issues, post a vulnerability management process
Risk Management	Business considerations on risk management
	Risk management activities
	Advantages of risk management
	Disadvantages of risk management
	Improvements to system controls and processes
Patch Management and Configuration Management	Centralised platform for patch deployment
	Patch management policy documents
	Detail of a patch management policy
	Patch management policy items not being practiced in the workplace
	Patch compliance
	Challenges of patch management
	Contextualising patch management and room for improvement
	Escalation of configuration issues identified through a patch management process
	Monitoring of escalated configuration issues, post a patch management process
	Superseded patch requirements
	Business consideration on superseded patch requirements
Incident Management	Incident preparation, i.e. business continuity
	Understanding of business impact regarding incidents

Table 7.2: Taxonomy final structure

- There is broad consensus on what constitutes "good practice" within the literature, and organizations that follow these practices are more successful. The implication is that following the guidance of any peer-reviewed and well-cited literature may be practically better than spending too much time selecting between the details of largely-equivalent pragmatic guidance.

7.5 Further Research

As per Whittle, Hutchinson, Rouncefield, Burden, and Heldal (2017, p. 317), "[a] taxonomy can be used in a variety of ways. It can be used as a checklist of issues to consider when developing tools. It can be used as a framework to evaluate existing tools". It must be noted that this research focused on Windows patching and the associations with this patching to ensure effective remediation of vulnerabilities. Microsoft application security controls were selected for review because Microsoft Windows is a popular business operating system (Beres *et al.*, 2008b). The number and types of cyber attacks changes dramatically as time progresses (Shetty *et al.*, 2018). Nicolett and Colville (2003) states that patch management is not enough when effectively mitigating vulnerabilities. Vulnerability management, however, includes several other areas rather than just Windows patch management and this can thus be reviewed as part of further research of the taxonomy and any associated frameworks.

There were several areas mentioned through the final chapters of this research where further research would be an option. This includes 1) additions to the taxonomy (including items not patch related, items not Windows patch related for databases, servers, other operating systems, third party application vulnerabilities, bespoke application vulnerabilities, vulnerable development repository downloads, threat modelling, etc.), or 2) to create a framework that weaves its way through the different levels of the taxonomy and then getting that framework tested with key stakeholders in the industry. With the result of the formation of a conceptual framework, the researcher can then deductively test the framework and any associated cyclic process with a target population. Process flows as illustrated in Figure 2.3, as per Beres *et al.* (2008a,b), can detail an activity diagram of a typical vulnerability and patch management process which can assist in defining a suitable framework.

Testing can be performed during the development of a conceptual framework, in particular as the framework is defined into smaller tasks or processes, it can be reviewed by subject

matter experts. The Delphi method can be utilised to develop and explore the effectiveness of a defined framework. As per Brady (2015, p. 1), "[t]he Delphi method emphasizes structured anonymous communication between individuals who hold expertise on a certain topic with a goal of arriving at a consensus in the areas of policy, practice, or organisational decision making". The Delphi method provides a pragmatic and more inclusive means to obtain information and validation from the target population.

Further to the above mention of creating a conceptual framework, Manshaei, Zhu, Alpcan, Bacşar, and Hubaux (2013) summarised a number of security related problems within their paper and their adopted game theoretical approach for each of the security related problems. The static non-zero-sum game approach is specific to the vulnerability management security problem and the approach leads to an understanding of vulnerability disclosure policies or processes. Game theory helps to understand the actions of an attacker and helps to determine the decisions of a defender (Liang and Xiao, 2013). Game theory also deals with problems where there are multiple players or users within an organisation, with contradictory objectives (Roy, Ellis, Shiva, Dasgupta, Shandilya, and Wu, 2010). This can then be a further review not just of a conceptual framework but also an understanding of areas lacking maturity or misconception. This implies the improved maturity of the different levels of the taxonomy could relate to how effective each service of the taxonomy is and whether the "pyramid" type figure can grow with maturity.

With the understanding of game theory and the revision of maturity, NIST SP 800-26 details targeting metrics used to review the maturity of vulnerability and patch management (Mell *et al.*, 2005). NIST provides a table of metric values to be used based on the number of vulnerabilities as opposed to the number of hosts an organisation has, patches applied and not applied, response times, costs, etc. These metrics would then substantiate further research and the understanding of a maturity level for the vulnerability and patch management program. The review of maturity of the taxonomy's various themes can then also include previous respondents feedback regarding the additional understanding of other categories per theme such as organisational structure for theme one, "People and Team Structure", or also include the understanding of compensating controls in themes five and six of the research taxonomy, i.e. "Vulnerability Management" and "Risk Management".

Further research can also include the addition of subjective variable topics for each of the Vulnerability Management Resilience Taxonomy's categories. Adding this variable topic per category should allow correlation between the different subcategory items or questions and give an understanding of relationships between the categories of the different themes.

The resulting data can be split to better understand the key areas of what is and what is not working. The areas of dissection of the research feedback can then be reviewed under 1) technical factors, 2) internal organisational factors, 3) external organisational factors and 4) social factors (Whittle *et al.*, 2017).

Finally, as all data collection occurs in South Africa, further research is welcomed in order to attempt in replicating the research results in other organisational contexts and in other geographical areas.

Bibliography

Abraham, S. and Nair, S. Exploitability analysis using predictive cybersecurity framework. In *Cybernetics (CYBCONF), 2015 IEEE 2nd International Conference on*, pages 317–323. IEEE, 2015a.

Abraham, S. and Nair, S. Predictive cyber-security analytics framework: A non-homogenous markov model for security quantification. *arXiv preprint arXiv:1501.01901*, 2015b.

Abraham, S. and Nair, S. A predictive framework for cyber security analytics using attack graphs. *arXiv preprint arXiv:1502.01240*, 2015c.

Afful-Dadzie, A. and Allen, T. T. Data-driven cyber-vulnerability maintenance policies. *Journal of Quality Technology*, 46(3):234–250, 2014.

Arora, A., Forman, C., Nandkumar, A., and Telang, R. Competition and patching of security vulnerabilities: An empirical analysis. *Information Economics and Policy*, 22(2):164–177, 2010.

Beres, Y., Griffin, J., and Shiu, S. Security analytics: Analysis of security policies for vulnerability management. Technical Report HPL-2008-121, HP Labs, 2008. Conference version to appear , 2008a.

Beres, Y., Griffin, J., Shiu, S., Heitman, M., Markle, D., and Ventura, P. Analysing the performance of security solutions to reduce vulnerability exposure window. In *2008 Annual Computer Security Applications Conference (ACSAC)*, pages 33–42. IEEE, 2008b.

Brady, S. R. Utilizing and adapting the delphi method for use in qualitative research. *International Journal of Qualitative Methods*, 14(5):1609406915621381, 2015.

Braun, V., Clarke, V., and Terry, G. Thematic analysis. *Qual Res Clin Health Psychol*, 24:95–114, 2014.

Carstens, D. An exploratory investigation into an integrated vulnerability and patch management framework (thesis) - questionnaire to citations list (working paper). Apr 2021. doi:10.6084/m9.figshare.14374052.v1.
URL `https://figshare.com/articles/dataset/An_Exploratory_Investigation_into_an_Integrated_Vulnerability_and_Patch_Management_Framework_thesis_-_Questionnaire_to_citations_list_working_paper_/14374052/1`

Cavusoglu, H., Cavusoglu, H., and Zhang, J. Security patch management: Share the burden or share the damage? *Management Science*, 54(4):657–670, 2008.

Dudovskiy, J. Non-probability sampling. 2018.
URL `https://research-methodology.net/sampling-in-primary-data-collection/non-probability-sampling/`

Ely, J. W., Osheroff, J. A., Gorman, P. N., Ebell, M. H., Chambliss, M. L., Pifer, E. A., and Stavri, P. Z. A taxonomy of generic clinical questions: classification study. *Bmj*, 321(7258):429–432, 2000.

Esmaili, H. B., Gardesh, H., and Sikari, S. S. Strategic alignment: Itil perspective. In *Computer Technology and Development (ICCTD), 2010 2nd International Conference on*, pages 550–555. IEEE, 2010.

FlexeraSoftware. Vulnerability review 2018, global trends. 2018.
URL `https://resources.flexera.com/web/pdf/Research-SVM-Vulnerability-Review-2018.pdf`

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., and Linkov, I. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 2017.

Gauci, A., Michelin, S., and Salles, M. Addressing the challenge of cyber security maintenance through patch management. *CIRED-Open Access Proceedings Journal*, 2017(1):2599–2601, 2017.

Gianini, G., Cremonini, M., Rainini, A., Cota, G. L., and Fossi, L. G. A game theoretic approach to vulnerability patching. In *Information and Communication Technology Research (ICTRC), 2015 International Conference on*, pages 88–91. IEEE, 2015.

Glen, S. Non-probability sampling: Definition, types. 2015.
URL `https://www.statisticshowto.datasciencecentral.com/non-probability-sampling/`

HKSAR. Patch management. 2008. Honk Kong Government.
URL `https://www.infosec.gov.hk/english/technical/files/patch.pdf`

Khouzani, M., Malacaria, P., Hankin, C., Fielder, A., and Smeraldi, F. Efficient numerical frameworks for multi-objective cyber security planning. In *European Symposium on Research in Computer Security*, pages 179–197. Springer, 2016.

Liang, X. and Xiao, Y. Game theory for network security. *IEEE Communications Surveys & Tutorials*, 15(1):472–486, 2013.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25, 2013.

Mell, P., Bergeron, T., and Henning, D. Creating a patch and vulnerability management program. *NIST Special Publication*, 800:40, 2005.

Mitre. Common vulnerabilities and exposures. 2018.
URL `https://cve.mitre.org/about/faqs.html`

Nanda, S. and Ghugar, U. Approach to an efficient vulnerability management program. 2017.

Nicolett, M. and Colville, R. Robust patch management requires specific capabilities. *Technology*, 19:4570, 2003.

Okhravi, H. and Nicol, D. Evaluation of patch management strategies. *International Journal of Computational Intelligence: Theory and Practice*, 3(2):109–117, 2008.

Olivia. Difference between standard and framework. 2019.
URL `https://www.differencebetween.com/difference-between-standard-and-vs-framewo`

RiskBasedSecurity. More than 22000 vulnerabilities disclosed in 2018. 2019.
URL `https://www.riskbasedsecurity.com/2019/02/more-than-22000-vulnerabilities-disclosed-in-2018`

Rouse, M. Patch tuesday. 2017.
URL `https://searchsecurity.techtarget.com/definition/Patch-Tuesday`

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE, 2010.

Saunders, M., Lewis, P., and Thornhill, A. Research methods for business students. Pearson Education Limited, sixth edition edition, 2012. ISBN 978-0-273-75075-8.

Sauro, J. 4 classes of survey questions. 2019.
URL `https://measuringu.com/survey-question-classes/`

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., and Njilla, L. L. Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 43(2):224–238, 2018.

Singh, U. K., Joshi, C., and Gaud, N. Information security assessment by quantifying risk level of network vulnerabilities. *International Journal of Computer Applications*, 156(2):37–44, 2016.

Spears, J. L. and Barki, H. User participation in information systems security risk management. *MIS quarterly*, pages 503–522, 2010.

Techopedia. Patch management. 2019a.
URL `https://www.techopedia.com/definition/13835/patch-management`

Techopedia. Vulnerability management. 2019b.
URL `https://www.techopedia.com/definition/16172/vulnerability-management`

Vijayan, J. Vulnerability disclosures in 2018 so far outpacing previous years'. 2018.
URL `https://www.darkreading.com/vulnerabilities---threats/vulnerability-disclosures-in-2018-so-far-outpacing-previous-years/d/d-id/1332545`

Wen, T., Zhang, Y., Dong, Y., and Yang, G. A novel automatic severity vulnerability assessment framework. *Journal of Communications*, 10(5):320–329, 2015.

Whittle, J., Hutchinson, J., Rouncefield, M., Burden, H., and Heldal, R. A taxonomy of tool-related issues affecting the adoption of model-driven engineering. *Software & Systems Modeling*, 16(2):313–331, 2017.

Zhang, S., Zhang, X., and Ou, X. After we knew it: empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pages 317–328. ACM, 2014.