Data-centric security: towards a utopian model for protecting corporate data on mobile devices

A thesis submitted in partial fulfilment of the

requirements for the degree of

MASTER of SCIENCE

of

RHODES UNIVERSITY

Simphiwe Hector Mayisela

July 2013

Abstract

Data-centric security is significant in understanding, assessing and mitigating the various risks and impacts of sharing information outside corporate boundaries. Information generally leaves corporate boundaries through mobile devices. Mobile devices continue to evolve as multi-functional tools for everyday life, surpassing their initial intended use. This added capability and increasingly extensive use of mobile devices does not come without a degree of risk - hence the need to guard and protect information as it exists beyond the corporate boundaries and throughout its lifecycle.

Literature on existing models crafted to protect data, rather than infrastructure in which the data resides, is reviewed. Technologies that organisations have implemented to adopt the data-centric model are studied. A utopian model that takes into account the shortcomings of existing technologies and deficiencies of common theories is proposed.

Two sets of qualitative studies are reported; the first is a preliminary online survey to assess the ubiquity of mobile devices and extent of technology adoption towards implementation of data-centric model; and the second comprises of a focus survey and expert interviews pertaining on technologies that organisations have implemented to adopt the data-centric model. The latter study revealed insufficient data at the time of writing for the results to be statistically significant; however; indicative trends supported the assertions documented in the literature review. The question that this research answers is whether or not current technology implementations designed to mitigate risks from mobile devices, actually address business requirements. This research question, answered through these two sets qualitative studies, discovered inconsistencies between the technology implementations and business requirements.

The thesis concludes by proposing a realistic model, based on the outcome of the qualitative study, which bridges the gap between the technology implementations and business requirements. Future work which could perhaps be conducted in light of the findings and the comments from this research is also considered.

Acknowledgements

First and foremost, I thank God for the opportunity to embark on such a rewarding exercise.

Thanks to Dr Barry Irwin for his invaluable assistance, supervision, and guidance over the course of this project.

I would also like to thank my employer, T-Systems, and my immediate manager, Melusi Gumbi, for providing me the opportunity to complete this research, and for supporting me both financially and by allowing me to take leave, often at very short notice, when required throughout the course of the entire degree.

A special thanks to the late Jeremiah Mbatsana for taking this journey with me and for providing inspiration and backing until his passing on 27 November 2012 – this piece of work is indisputably dedicated to him.

Several colleagues and friends have given of their time to proofread and review the project. Thanks to Dr Jill Slay, Dr Laura Budler, Dr David Taylor and Dr Alapan Arnab. All remaining defects are entirely my responsibility, but many more would have remained without their scrutiny and meticulous attention.

Finally, I want to thank my spouse, Nompumelelo, for being with me throughout all of this and more.

Table of Contents

List of Figures

List of Tables

Glossary of Acronyms and Abbreviations

API: Application Programming Interface

AR: Augmented Reality

ASLR: Address Space Layout Resolution

BDC: Business Data Classification

BYOD: Bring Your Own Device

CA: Certificate Authority

CAPEX: Capital Expenditure

C & C: Command and Control

CKM: Constructive Key Management

COA: Collaboration Oriented Architecture

CSR: Certificate Service Request

DCR: Data Control Rules

DCSM: Data Centric Security Model

DEP: Data Execution Prevention

DLL: Dynamic-Link Library

DLP: Data Loss Prevention

DOS: Disk Operating System

EAS: Exchange ActiveSync

ECC: Elliptic Curve Cryptosystem

E-DRM: Enterprise Digital Rights Management

EJB: Enterprise Java Beans

ERP: Entity Resource Planning

EUL: End User License

FPGA: Field Programmable Gate Array

HIPPA: Healthcare Information Portability and Accountability Act of 1996 (USA)

NDES: Network Device Enrolment Service

RIM: Research in Motion

IAM: Identity and Access Management

IEC: International Electrotechnical Commission

ILM: Information Lifecycle Management

IRM: Information Rights Management

IPS: Intrusion Prevention Systems

ISMS: Information Security Management System

ISO: International Organisation for Standardisation

J2EE: Java 2 Platform Enterprise Edition

MAM: Mobile Application Management

MDM: Mobile Device Management

MSMQ: Microsoft Message Queuing

NAC: Network Access Control

NTP: Network Time Protocol

OTP: One-Time Password

PDM: Product Data Management

PED: Portable Electronic Device

PKI: Public Key Infrastructure

RA: Registration Authority

ROI: Return on Investment

TIFF: Tag Image File Format

SCEP: Simple Certificate Enrolment Protocol

SDK: Software Development Kit

SMS: Short Messaging Service

SSH: Secure Socket Shell

SOA: Service Oriented Architecture

SOS: Service Oriented Security

SSO: Single Sign-on

VDI: Virtualised Desktop Infrastructure

VPN: Virtual Private Network

W3C: World Wide Web Consortium

Chapter 1 : Introduction

The traditional security paradigm envisions layers of perimeter-focused security defences like Firewalls, Intrusion Prevention Systems (IPS), Anti-malware solutions, host-based firewalls, and encrypted network tunnels. This exemplar is comparable to an urban house dweller with burglar-proof doors and windows, an armed-response alarm system, high walls, electric fence, and a Rottweiler barking viciously in the back yard. However, regardless of the security of the resident's house, ultimately he still has to leave this secure confine to travel to work or to frequent the shops. Similarly, an organisation can create "defence in depth" perimeter security, but its information will invariably leave this well-guarded environment.

Information that leaves organisations through mobile devices present a growing concern for organisations as more employees are using mobile devices for work and to access corporate data. Mobile devices exist as small-sized, affluent gadgets that are often attractive to thieves and therefore prone to being lost or stolen (Disabato & Berenbaum, 2012). According to a survey conducted by Credant Technologies between June 2011 and June 2012, approximately 8000 mobile devices were left behind by travellers at seven of the largest airports in the United States (Gill, 2011). Extrapolating the figures into global context shows that it is not only the vast *number* of mobile devices that are lost, but also the *data* within those mobile devices that is lost. In an earlier independently commissioned survey conducted by TSN in August of 2011, 67% of the surveyed respondents did not have password-enabled mobile devices to protect their stored information (Enzer, 2011). Therefore, organisations are required to craft security approaches to mitigate the risks of unauthorised disclosure of confidential information, unauthorised access to sensitive corporate application, or malicious code that steals information from mobile devices.

There is an understanding that the traditional approaches to security **do** have the potential to provide hitherto unparalleled protection to an organisation's infrastructure (Smith, 2003). As a matter of fact, traditional approaches **do** provide adequate protection of the network, servers, and applications that surround data (Grandison, T., Bilger, M., T., O'Connor, L., Graf, M., Swimmer, M., Schunter, M., Wespi, A. & Zunic, N., 2007). However, such approaches fail to protect the *data* itself (Hoffman, 2006). In fact, these traditional approaches face increasing challenges as data moves out of an organisation, carried out on employee mobile devices (Neuman, 1991), leading to a necessity of a concept of protecting data away from the infrastructure; this concept, relatively new, is known as 'data-centric security'.

‘Data-centric security’ is a term used to describe the implementation of appropriate controls in an effort to protect data or information, taking into consideration its business value and flow, with the goal of ensuring that controls are cost effective and not excessive, (Bilger, M., O'Connor, L., Schunter, M., Swimmer, M. & Zunic, N., 2006). ‘Data-centric security’ is defined by Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009) as an approach to protecting data from within, rather than protecting data from outside (i.e. protecting the actual data and application data, rather than protecting applications and infrastructure within which the data resides). Put simply, this means protecting the data or information, not merely the physical mobile device. A basic presupposition of this concept was first introduced in 2006 at IBM’s Security and Global Privacy Department to describe the protection of information within a device, rather than protecting the device itself. Indeed, in order for an organisation to adopt a data-centric security model, this organisation must be able to protect its data throughout its life cycle, irrespective of where it resides or where it is destined to travel (Grandison *et al*., 2007).

One current challenge faced by information security professionals is to constantly adapt to ever-changing business requirements by ensuring that the security strategy is in line with business requirements and that it is definitely able to protect information (Marko, 2008) in the manner that the particular business requires (McFadzean, Ezingeard & Birchall, 2007). The proliferation of mobile devices and the requirements by business to allow employees to access corporate information using their mobile devices means that the security professionals *must* revise their traditional layered ‘perimeter defence’ approach to accommodate this change and become more flexible, all the while ensuring that the information on mobile devices remains protected.

In order for data-centric security paradigm to be fully realised, and for organisation to benefit from this distributed data sharing concept, challenges concerning the introduction of mobile devices within businesses needs to be thoroughly investigated and carefully evaluated. According to ISACA (2010), introduction of mobile devices into the organisation may be harmful in the following ways:

- reduce an employee’s capability of performing daily tasks due to network communication problems;
- put corporate information at risks;
- hinder daily operations as a result of an employee’s inability to use the technology for protecting information on mobile devices;

- impact existing security controls that may lead to implementation interoperability issues;
- be unsuited for the corporate culture;
- be difficult to manage due to multiple platforms (e.g. Android, Symbian, iOS, and Windows Mobile) as well as multiple devices per user; and
- result in difficulty segregating personal data from corporate data on a mobile device.

Likewise, the drivers that lead to the implementation of a data-centric security model are hugely influenced by the inevitable trends within the information technology landscape. These drivers (explained in detail in Section 2.3) have been determined to be:

- expansion of the IT scope and the evolution of the threat landscape;
- consumerisation of IT and Bring Your Own Device (BYOD);
- cost; and
- 'Data sprawl' and 'Big Data'.

1.1 Scope of Research

This research examines the data-centric security paradigm and the technologies that have been implemented for adopting this paradigm. Furthermore, this research focuses on the application of the following technologies by organisations to implement data-centric security:

- Virtual Desktop Infrastructure (VDI)
- Information Rights Management (IRM)
- Mobile Device Management (MDM)

The aforementioned technologies are selected because they **do not** focus on the traditional approach of defending the device and network infrastructure (infrastructure-centric security approach), but **do** focus, to some extent, on protecting the actual data (data-centric security approach).

The scope of the research, however, is not limited to the above-mentioned technologies. Based on the gaps that will be identified with these technologies, the proposed architecture model may include additional technologies that will complement through integration with the technologies mentioned.

Mobile devices can mean many different things to people. For the purpose of this research, the scope will be limited to the following devices:

- High-featured mobile communication; devices with computer-based functionality commonly referred to as smartphones; and
- Laptop, tablet, netbook, notebook computers, or any similar mobile computing device that connects to a wireless career for communication.

1.2 Problem Statement

Mobile devices provide organisations with the capability of keeping their employees connected *at all times*. These devices give today's mobile workforce the ability to conduct business from any location, regardless of whether an employee is home-based, office-bound, or even travelling between destinations.

IT Departments have significantly revised their mobile computing strategies to accommodate the support of mobile devices. IT is now struggling to meet and satisfy business requirements while also, quite importantly, ensuring that the information residing on mobile devices remains secure and manageable regardless of whether the device is company-liable or employee-owned. Check Point, in partnership with ITWeb (ITWeb Surveys, 2012), conducted a survey in South Africa to determine, amongst other things, the percentage of corporate-liable and personal devices present in the enterprise. The majority of respondents (86.04%) said that their organisations allow company-issued mobile devices to connect to the corporate network, while 77.48% said that they even allow personal mobile devices to do so (ITWeb Surveys, 2012).

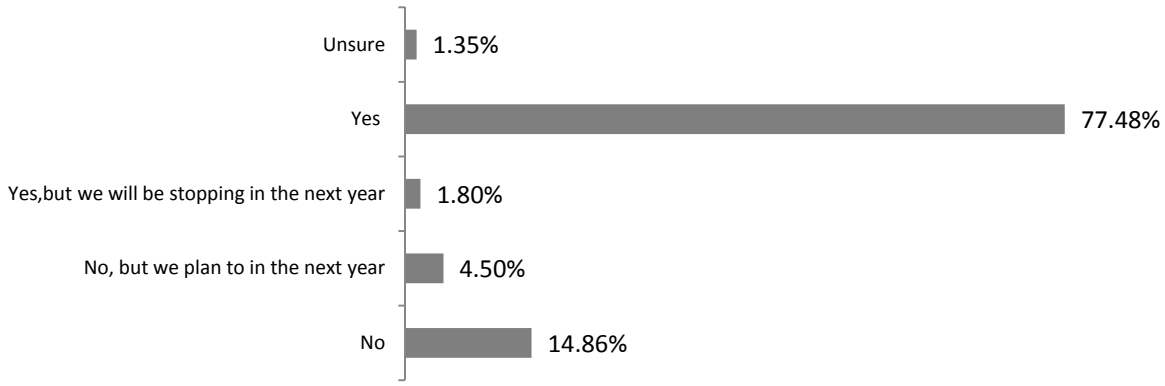


Figure 1-1: Percentage of Personal Devices Allowed in Organisations (ITWeb Surveys, 2012)

The 2012 Mobile Security Survey was run online on by ITWeb in late June 2012. Figure 1-1 depicts responses to whether or not organisations allow personal mobile devices to connect to the network. It is evident that IT departments have diminishing control with regards to managing the devices that connect to an organisation's network.

Mobility certainly is required by business to accommodate the mobile workforces that need to do their work anywhere, anytime, using any possible mobile device. Furthermore, mobility is becoming a business enabler by supporting new consumer engagement models. For instance, consumer product strategy professionals are starting to use Augmented Reality (AR) to engage consumers throughout the procurement life-cycle through advanced digital interactivity (Ask, 2011). Augmented Reality is defined by Forrester Research as the "virtual overlay of contextual digital information generated by a computer on to a physical world object seen in the device display as it is captured real time by the camera" (Ask, 2011, p. 2). Augmented Reality, now implemented in mobile devices, allows consumers to ascertain a feel of the product, and to obtain pricing information in an extremely convenient manner, prior to the commencement of a transaction. For example, Marketing Professionals at BMW used the "BMW X3 Anywhere" application to communicate new innovations within the new X3 brand, and to simulate ownership and drive discovery, thus strongly influencing a purchaser's decision (Husson, 2011).

Still, in the midst of this paradigm shift, like shoes that refuse to go out of style, organisations continue to rely on classic infrastructure-centric technologies like firewalls and network intrusion prevention systems to protect their digital assets. And the organisations that *have* begun to implement the aforementioned technologies to protect data on mobile devices follow a reactive approach. Most organisations *do not* have a security strategy or framework that maximises its business, financial, and operational benefits while still protecting the business from risk (McFadzean, Ezingeard & Birchall, 2007). Consequently, the technologies used for protecting data *outside* the organisation's infrastructure are not driven by business requirements and do not implement the correct level of protection necessary to result in both effective and cost-efficient controls. The dilemma, of course, is how the organisation should determine the tools and technologies in which to invest, when almost all come with claims of enhanced security. All too often, a wrong decision is made and organisations invest time and money in technologies that fail to address the desired business requirements. Tools and technology, it must be noted, fail for different reasons:

- They are not implemented according to a pre-determined mobile device management strategy and policy.
- They do not protect information based on an approved data classification policy.
- They do not provide adequate authentication or encryption.

1.3 Research Objectives

The objectives of this study are as follows:

1) to understand the drivers for the implementation of data-centric security controls;
2) to examine the data-centric security model and understand how it can be used to mitigate risks that mobile devices bring to corporate information;
3) to analyse the shortcomings of each technology in an effort to identify gaps in technologies used to implement this model; and
4) to propose a reference architecture framework that will address the identified gaps and ensure effective implementation of the data-centric security model that is consistent with the business requirements and objectives.

In light of the problem statement previously described, it is clear that organisations rely heavily on technology to protect information and yet tend to neglect processes and people. Even the state-of-the-art technology fails if it is not implemented according to procedures, processes and policies that fortify an organisation's business requirements or if it is implemented without people who support those business requirements and without people who live up that culture (Andress, 2003). To quote Bruce Schneier (Mann, 2002, p. 3):

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"

When organisations do adopt the data-centric security approach and implement a certain degree of data-centric control or technology, they do not integrate those technologies with existing information management processes, resulting in inconsistency between the security technology and the organisation's business requirements (Hoffman, 2006). While the newly implemented technologies may be successful in providing *some level* of security, this still leaves uncertainty about whether or not the technology has fully addressed the risk, and whether or not the cost of that technology is proportionate to the benefit (Sherwood, Clark & Lynas, 2005). In other words, while technology may offer some information security, it often does so to the neglect of the business requirements.

The question that this research seeks to answer is whether or not current technology implementations designed to mitigate risks from mobile devices, actually address business requirements. This research question, answered through a qualitative study described in Chapter 4, determined some level of inconsistency between the data-centric security controls

and business requirements. As described in detail in Section 4.7, this inconsistency is instigated by the fact that organisations implement the information security controls on a very reactive and tactical basis. The mobile security architecture models proposed in this research allow organisations to bridge this gap between information security controls and the objectives of the business strategy, in particular by using SABSA[1] as the underpinning framework. The proposed models take into account both general business requirements as well as specific business requirements for security, and relate security controls and security services directly to business requirements – a relationship that is too often concealed by presenting security controls and security services as the only solutions to the problem.

1.4 Conceptual Hypothesis

Technologies implemented to protect information *outside* the corporate infrastructure do not necessarily simultaneously implement the correct level of protection to result in controls that effectively address the business requirements *within* an organisation.

1.5 Significance of the Research

The research is significant for two primary reasons:

- It intends to improve public understanding of the role of a data-centric security model in the achievement of fulfilling business objectives.
- It intends to fortify literature on successful and implementable data-centric security models.

1.6 Structure of Document

The remainder of this document is structured as follows:

- Chapter 2 recasts the reader's attention to the research objectives raised in Section 1.3, and provides adequate historical background to the study. This chapter starts by providing a broad perspective of the subject area and eventually narrows in on concepts clearly related to these research objectives.
- Chapter 3 introduces an almost impracticably ideal (utopian) architecture model required to implement data-centric security. The justification of the proposed model is also provided.
- Chapter 4 examines the proposed model through a real-world survey. Details pertaining to the survey's construction are described, along with limitations. This

[1] http://www.sabsa.org/

chapter presents the results, analysis and findings of the survey. The collected data is presented to answer research questions.

- Chapter 5 compares the utopian model introduced in Chapter 3 with the real-world model described in Chapter 5 in an effort to produce the so-called ‘final model’ that is a true reflection of the current implementations.
- Chapter 6 concludes the research by identifying areas through which the research questions were answered. Areas warranting future research are also presented.

Chapter 2 : Literature Review

2.1 Introduction

In this chapter, we expand on the risks and drivers introduced in the previous Chapter, review related work on the key models that were designed for data-centric model, and describe the technologies implemented to achieve a data-centric security model.

The theory in all related work is compared, criticised and connected with this area of research in an effort to identify gaps in the literature. This chapter reviews four aspects from literature:

- risks regarding introduction of mobile devices;
- drivers towards the adoption of data-centric security model;
- related work; and
- current implementations of data-centric security toolsets.

The next section summarises the risks regarding the introduction of mobile devices in the enterprise. In Section 2.3, the drivers that the Researcher believes to be the fundamental drivers towards the implementation of data-centric security controls are discussed using supporting literature. Related work on the implementations of data-centric security model is visited in Section 2.4 with the intention to learn and identify any gaps with the existing models prior to proposing a utopian architecture model. Finally, the remaining sections of this Chapter look at the current implementations of data-centric security controls; again with the intention of identifying loopholes that can be closed using other existing toolsets.

2.2 Risks Regarding the Introduction of Mobile Devices

The introduction of mobile devices presents numerous risks to organisations. Table 2-1 outlines a threat model on mobile devices from an adversary perspective. This threat model, developed by Information Systems Audit and Control Association (ISACA)[2], while not exhaustive, illustrates both the vulnerabilities and threats that are imperative to understand when dealing with mobile devices.

Each risk highlighted in Table 2-1 pertains to data loss, data leakage, data corruption, data exposure, or data breach; thus clearly emphasizing the risks mobile devices pose to corporate data.

[2] http://www.isaca.org

Table 2-1: Threat Model on Mobile Devices from an Adversarial Perspective

Vulnerability	Threat	Risk
Information travels across wireless networks, which are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation, legal action.
Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this Malware into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data.
Bluetooth technology is very convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information.
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees.
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up.
The device has no authentication requirements applied.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues.
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with e-mail or store sensitive documents.	Data leakage, malware propagation, unknown data loss in the case of device loss or theft.
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage, intrusion on enterprise network.

Source: (ISACA, 2010)– Verbatim.

The risks that mobile devices bring to the organisation can be categorised as follows:

2.2.1 Physical Risk

Mobile devices are generally small in appearance and can easily be lost or stolen, particularly in public areas (as target for pickpockets). This does not only result in data loss (emails, saved attachments, text messages, call logs, calendar items, confidential presentations and spreadsheet, but also to loss of productivity as an employee is often left unable to work (Von Roessing *et al.*, 2012). Identity thieves analyse the data retrieved from mobile devices in an effort to steal the owner's digital identity and to execute further malicious activities. While strong passwords provide a certain degree of protection against this type of data loss, some mobile devices do not support complex passwords and encryption (Von Roessing *et al.*, 2012).

2.2.2 Organisational Risk

Executive managers usually enjoy the privileges of corporate-issued mobile devices and are often the highest users of mobile device resources (Von Roessing *et al.*, 2012). A successful compromise of their mobile devices can result in data leakage that could be detrimental to the organisation at large.

The increasing complexity and diversity in mobile devices, coupled with constantly evolving generation of mobile devices results in employees not being able to keep up with ever-changing mobile device features. Consequently, this creates an environment that is prone to human error and ultimately impacting on the quality of business (Von Roessing *et al.*, 2012).

2.2.3 Technical Risk

This type of risk requires some form of technical mechanism to exploit the mobile device. This includes the retrieval and monitoring of GPS positional data, eavesdropping on text, email and call messages, and insertion of malicious code and spyware (Von Roessing *et al.*, 2012).

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) jointly published a collection of information security standards based on good practices observed across various industries. One of the standard within this information security management systems (ISMS) family of standards, ISO27001:2005 (Boehmer, 2008), provides a set of requirements for ISMS. ISO27001:2005 proposes, in Section 11.7.1, that the risks of business data on mobile devices being compromised should be mitigated using mobile computing policy and security measures proportionate to the risk (Boehmer, 2008). The mobile computing policy should not only take into account the above-mentioned risk categories, but should also include clear guidelines on

the usage of mobile devices outside the protected environments of the organisation's premises (Freeman, 2007). The standard clearly states that the focus should not only be on the security measures (technology) and policies (processes), but also on the human (people) component through arranged training for mobile workforce to raise awareness about the risks of mobile computing.

The impact of the above-mentioned risk categories results in organisations adopting a data-centric security approach to mitigate these risks. The following section seeks to fulfil the first research objective of exploring and understanding the drivers to adopt data-centric security controls.

2.3 Implementation Drivers

Allowing employees to bring their own personal devices introduces devices that may not have adequate security features into the corporate infrastructure. For instance, a large proportion of Android devices do not possess default encryption capabilities (Zumerle, 2012). Likewise, employees use their own personal devices in a manner that is deemed acceptable to them. They visit any website and install any applications that are desirable to their needs, thus increasing exposure to malware infections and information leakage (Friedman, 2012; Graziano, 2012). Employees also choose weak passwords to unlock their mobile devices (Amitay, 2011); and sometimes choose not to use any password, thus increasing further risks of data leakage in an event of a device being stolen or getting lost (Gill, 2011).

Another challenge faced by IT today is not to necessarily train business users about how to use new technology, but to prevent business users from involving IT when the features of the new technology no longer yield the desired situation. Consequently, IT becomes indebted to supporting the full features of mobile devices from different manufacturers (Pelino, 2010).

The afore-mentioned challenges drive businesses to apply enterprise-grade security controls to devices that are owned and controlled by users (Zumerle, 2012). These enterprise-grade security controls must therefore focus on protecting enterprise data residing on mobile devices, rather than protecting the device itself – an approach known as 'data-centric security'.

The following sections outline the elements that the researcher believes to be the fundamental drivers leading towards the adoption of data-centric security model.

2.3.1 Expansion of the IT scope and Evolution of Threat Landscape

The responsibility of IT has changed over time (Lewis, 2011):

- **In the 1960's and early 1970's**: IT's fundamental functions were focussed around the fundamental accounting functions such as general ledger, billing systems, accounts payable and payroll.
- **In the mid 1970's through to the mid 1980's**: IT took over the same responsibility but added the automation of fundamental non-accounting processes such as inventory management, purchasing or supply chain, and order entry.
- **In the mid 1980's through to the early 1990's**: IT added the responsibility of office applications like word processors, email, spreadsheet and presentations.
- **In the mid 1990's through to the late 2000's:** IT added e-commerce, work process management, content management, and further expanded communication technologies (e.g. Web conferencing).
- **In the late 2000's to the present**: IT saw an introduction of social media, expanded media (e.g. YouTube, and Podcast), as well as an increase in mobile platforms to support.

According to Forrester's Enterprise and SMB Networks and Telecommunications Survey, North America and Europe, Q1 2010, half of the surveyed enterprises' IT departments already support two or more mobile platforms as shown in Figure 2-1.

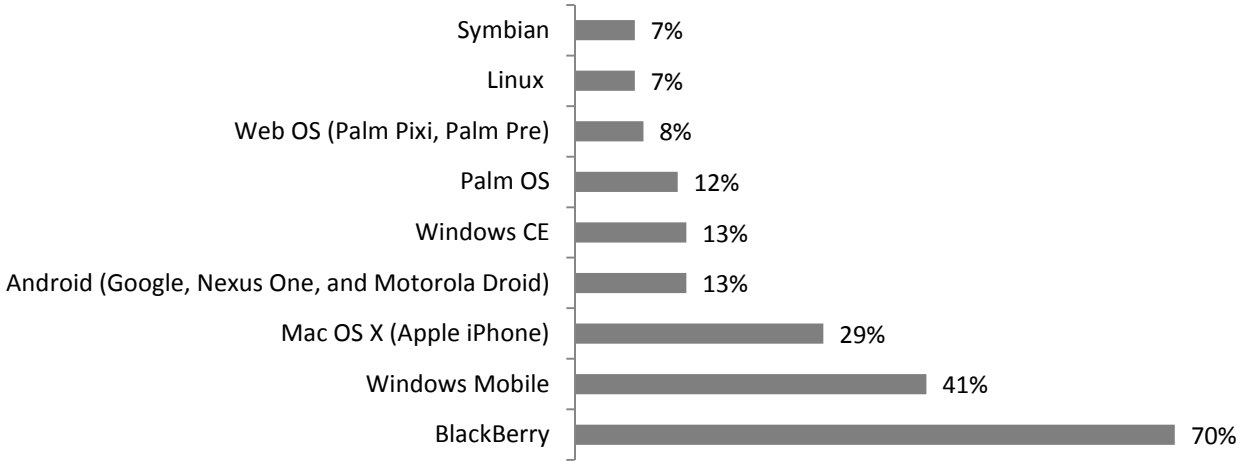


Figure 2-1: Proliferation Trend in Mobile Operating Systems (Pelino, 2010)

This expansion in IT scope is proportional to evolution in security landscape. The larger the IT scope, the larger the scope of digital assets needing to be secured. Likewise, as IT devices evolve, so does the threat landscape. This trend is illustrated in Figure 2-2. The birth of Ethernet Networks in the early 1970's marked the beginning of malicious activity in a form of software (malware) that allowed attacks to propagate from one host to another host through

the network (Gupta, Kuppili, Akella & Barford, 2009). Creeper was the first virus to propagate itself over the network in a harmless fashion, by displaying simple messages on infected machines (Loebenberger & Wielputz, 2006). Time advanced to clear the way for affordable personal computers that saw another generation of malware encompassed of Disk Operating System (DOS) viruses and boot-sector viruses in the mid 1980's to 1995 (Tippett, 2006).

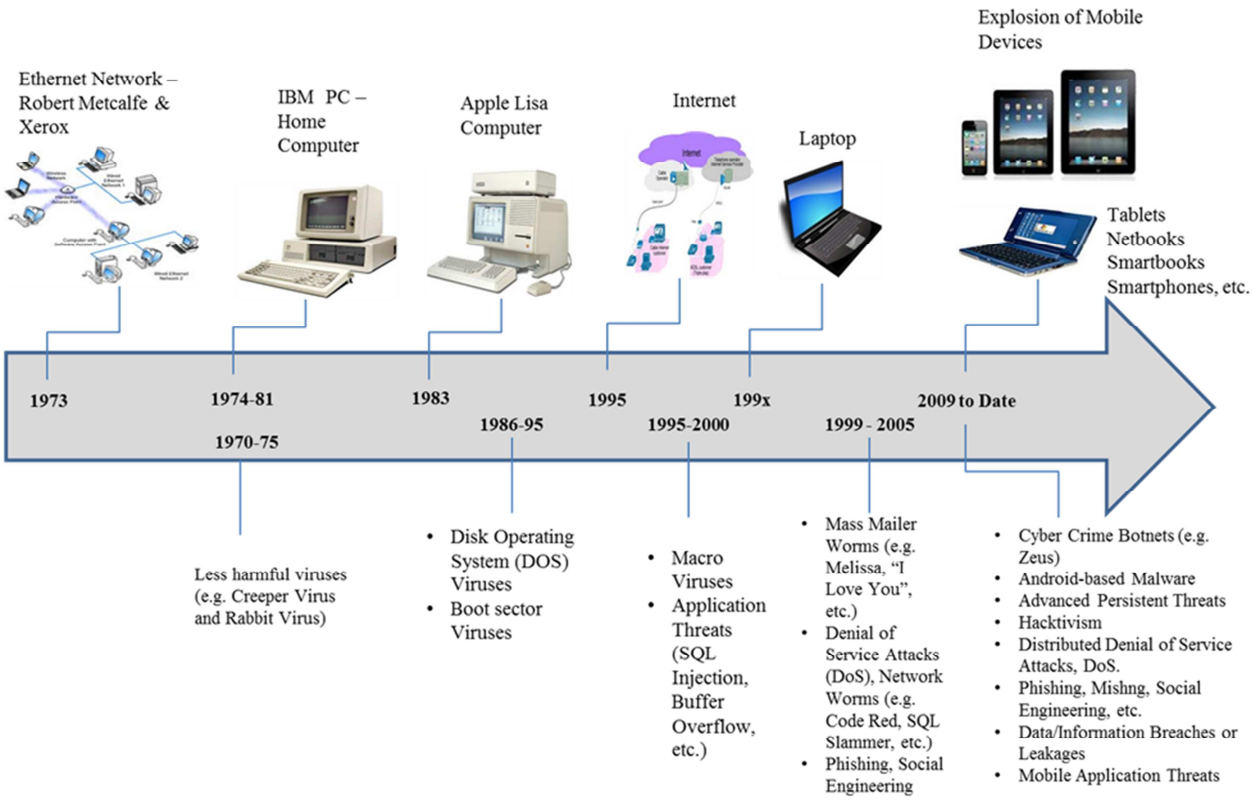


Figure 2-2: Evolution of Threat Landscape

In 1995, the Internet became ubiquitous and became a vehicle for macro viruses like Melissa Worm to spread (Loebenberger & Wielputz, 2006). The next phase saw the explosion of mobile devices with newer malware that had reached a relatively increased level of sophistication and additional means of propagation such as Bluetooth (Wang, González, Hidalgo& Barabási, 2009). In addition to threats that exist on traditional IT devices, it is vital for organisations to deal with imminent threats presented by mobile devices such as 'Jailbreaking' and 'Android Rooting' (Kravets, 2009). 'Jailbreaking' is the process of modifying the system kernel of the mobile operating system, developed and distributed by Apple Inc. (iOS) in order to allow file system read and write access (Mukhopadhyay, 2012). This allows end users to install customised applications that are not signed and approved by Apple Inc. (Magaudda, 2010). 'Android Rooting', on the other hand, is the process of gaining

privileged access to the Linux-based operating systems developed by Google (Android) allowing the user to remove or replace the operating system (Mukhopadhyay, 2012). Jailbreaking is a very popular attack in the mobile device space. For instance, the Absinthe 2.0 Jailbreak tool for iOS 5.1.1 was used to compromise over 1 million devices on the first weekend after its release in May 2012 (Jeff, 2012) – approximately three weeks after iOS version 5.1.1 was released.

Threats that target multiple operating systems have now incorporated mobile platforms into their list of targets. In the mid-to-late 1990's when Microsoft Office was made available to non-Windows platforms, Microsoft Word Macro Viruses became pervasive. On the same wavelength, attackers are taking advantage of vulnerabilities on Adobe Flash, Acrobat, and Reader because of their multi-platform ubiquity. More recently, attackers have been using Java as their avenue to multiple operating systems (Fischer, 2012). A good example is the one described by Ferrer (2012) where a malicious code was carried through the Internet to multiple platforms by exploiting vulnerabilities referred to in CVE-2011-3544 and CVE-2012-0507.

Apple Inc. signs and approves applications that are made available through the application store. The application, or Library, can only load if it has been signed by Apple's private encryption key (Miller, 2011). Once the application is downloaded onto the device, it runs in a sandbox. 'Sandboxing' refers to the practice in which potentially dangerous code is run in an environment that prevents it from carrying out dangerous actions, in such a way that applications execute in isolated environments with no access to each other's data (Blasing, Batyuk, Schmidt, Camtepe & Albayrak, 2010).

Conversely, applications that are made available through the Android Market and Google Play Store are not reviewed and signed. Although the Android Market necessitates that applications be signed, it does allow applications that are self-signed to be uploaded, thus allowing Android users to download applications from any source, not just from the Android Market (Miller, 2011). Android also adopts the sandbox architecture model, but permits the user to decide what type of access the application requires. Users often blindly grant the application any permission it requires, much as users blindly accept the end user licensing agreement without reading it (Miller, 2011).

In July 2011, more than 50 applications in the Android Market were found to contain malware that could leak sensitive personal information (Chansanchai, 2011). According to a research

conducted by Kaspersky Labs, the volume of malicious software that infects Android devices grew threefold in the second quarter of 2012 (Graziano, 2012).

Within a period of three months in the first quarter of 2012, Kaspersky Labs discovered more than 14 900 Android-based malware that could steal information from mobile devices. The malware could also download and install programs from remote servers (Graziano, 2012). In earlier studies conducted by Felt, Finifter, Chin, Hanna& Wagner (2011) and Töyssy & Helenius (2006) on mobile malware, it was similarly revealed that the main drive behind the mobile malicious code is the desire to steal user data and credentials. These studies showed that the other stronger desire to send premium-rate SMS messages that are charged to the victim's phone bill could not be exploited on a large scale due to the fact that this requires user confirmation.

Other research conducted by McAfee Labs found that mobile malware is popular within Android devices. The McAfee threat report also revealed that majority of infections on the mobile platform are due to unintended download of malicious software from the Internet, a vector commonly known as drive-by download (Bu, 2012). Mobile drive-by downloads are comparable to drive-by downloads on the workstations in that malicious code infects the mobile device when an infected site is visited. The infected downloaded files are given less suspicious names such as "Android System Update 4.0.apk" as opposed to "EvilMalware.apk" in order to trick the user into installing the file (Bu, 2012).

A new variant of 'botnets' that uses Twitter as the command and control (C&C) entity was reported in the second quarter of 2012 (Bu, 2012). This new 'botnet' (Android/Twikabot.A) requests commands from other attacker-controlled Twitter accounts running on Android OS, instead of connecting to a dedicated C&C web server, thereby leveraging the resources of other victims. A majority of threats targeting mobile devices are looking at stealing consumer and business information that resides on mobile devices, primarily targeted at Android devices due to the openness of the platform and dominance in the marketplace (Bu, 2012). Likewise, Microsoft's drive to make Windows-8 a developer-friendly platform will also be embraced by malware developers. Blackberry as well has received its fair share of attacks despite its 6% share on the market. According to Websense ThreatSeeker 2012 Report, bogus emails targeting Blackberry customers were distributed with attachments that supposedly contain instructions for enjoying the benefits of Blackberry. The attachment, however, actually contained malicious code while the body of the email was an exact replica of a legitimate email from Blackberry as shown in Figure 2-3.

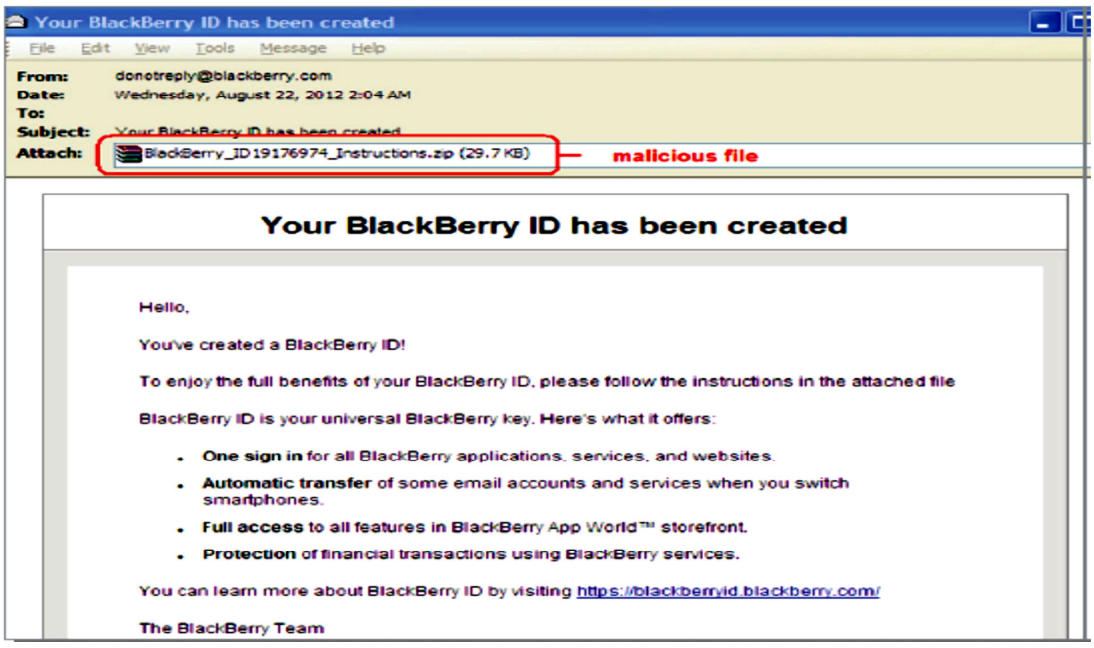


Figure 2-3: Phishing Email to Blackberry Customers (Websense ThreatSeeker, 2012)

Android followed Apple's layered defence approach to prevent malware exploitation by employing Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) on Android version 4.1 (Protalinski, 2012). DEP is a technique used to prevent an application or service from running malicious code by ensuring that the particular application or service does not execute code from a non-executable memory region (Engler, 2011). ASLR is a technique that increases security by increasing the search space of memory addresses thereby affording the attacker a low chance of guessing where the randomly placed memory areas are located (Whitehouse, 2010). Several instantiations of a programme containing the same flaw cannot be compromised using the same exploit code if the address space of the software programme has been randomised (Schamam, 2004). Instead of removing the actual flaw or vulnerability, the technique increases the strain of exploiting the flaw. This is useful in protecting unknown vulnerabilities or vulnerabilities that have not been remediated. ASLR complements DEP in providing protection against memory manipulation vulnerabilities. Despite this layered defence approach, Apple iOS has been breached in more than one occasion due to the fact that Apple runs most of the installed applications as root privileges. The first breach exploited by Farrow (2009) took advantage of stack buffer overflow vulnerability on version 3.9.2 of LibTIFF, included in versions of Apple iOS earlier than version 1.1.2. LibTIFF is an open source image library that enables the display and manipulation of Tag Image File Format image data (TIFF). The breach starts by Jailbreaking the iPhone and reverse engineering how the iPhone communicates over its USB channel in an effort to circumvent the communication channel and install rogue programs that can install

other programs (Farrow, 2009). The programmes are controlled remotely using basic command line tools and Secure Shell (SSH) over a Wi-Fi network. In a command line interface resembling that of a Mac-OS, a command was issued to find recently modified files and easily located a directory containing personal information such as contact details, recent calls, voice messages, web browsing history, bookmarks and email (Farrow, 2009). The breach extends even further exploiting MobileSafari web browser using Metasploit and IPWN files. Another breach known as SMS Fuzzing was demonstrated by Miller & Mulliner (2009) at the Black Hat USA Conference in 2009, where SMS messages were injected into iPhone, Android and Windows Mobile devices.

Breach of privacy is another serious concern with regards to mobile applications. A lawsuit was filed against an iPhone game manufacturer called Storm8 that secretly collected user's phone numbers without their consent and sent them in Plaintext (Goodin, 2009). The initial releases of a video game called "Aurora Feint the Beginning" also collected phone numbers and emails and used those details for a community feature that locates the user's friends, without informing the users (Macenstein, 2008). Apple iPhone users who downloaded a free application from App Store called 'MogoRoad' received phone calls from the Vendor persuading the users to purchase a full version of the application (Moren, 2009). The Vendor claimed to have received the information from Apple, but Apple is prohibited by their privacy policy from disclosing personal information to App Store Vendors. Even though Apple iPhone's software development kit does not provide a default way to access personal information, this can still quite easily be retrieved. Every application installed on the iPhone contains a hidden symbolic link between the application's sandboxed preferences and global preference property list (Sadun, 2009). All personal information retrieved from this location is in plaintext and readable, notwithstanding Apple's sandbox architecture (Sadun, 2009).

These software programmes that collect information from mobile devices without users' knowledge have marked the rise of mobile spyware (Lawton, 2008a). Mobile spyware refers to programmes installed on mobile devices that collect information about an individual or organisations without their knowledge: Spyphone, StealthGenie and MobiStealth, for example (Macenstein, 2008). This mobile spy software records activities, logs, and GPS locations and send this information to a remote account.

Another risk that is prevalent on mobile devices concerns the ease of guessing the passcode used to access mobile devices. A free application called Big Brother Camera Security was employed to gather the most commonly used iPhone passcodes (Amitay, 2011). Out of the

204 508 passcodes that were recorded, the top 10 most commonly used passcodes are depicted in Figure 2-4.

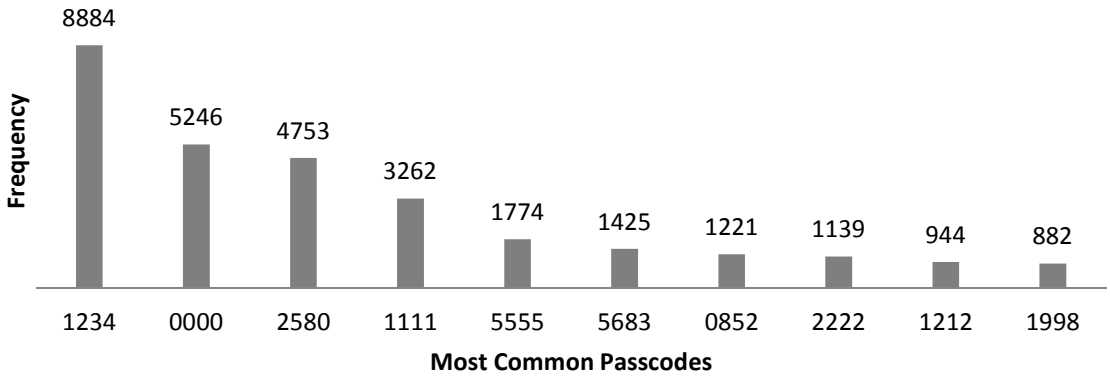


Figure 2-4: Commonly Used Passcodes (Amitay, 2011)

These top 10 passcodes constitute 15% of the entire population of collected passcodes. The very top most commonly used passcode, 1234, resembles the Internet's most common password, 123456 (Vance, 2010). Analysis of these common passcodes shows that mobile users are inclined to choose obvious patterns such as four identical digits, digits that line up or line down the key pad, or repetitive digits. The only most common passcode with a less obvious pattern is 5683, a numerical representation of the word LOVE (Amitay, 2011). Passcodes in the range 1990 to 2000 are all in the top 50, and those in the range 1980 to 1989 are in the top 100 – this could be attributed to the fact that mobile users frequently select their birth year or graduation year as their passcodes (Amitay, 2011).

2.3.2 Consumerisation of IT and Bring Your Own Device (BYOD)

There is a remarkable convergence of consumer electronics with the Information Technology (IT) industry where the consumer devices and consumer applications are spreading to business. Employees are, without a doubt, bringing their own mobile devices and connecting them to the corporate network. IT departments often find themselves supporting an increasingly decentralised and mobile workforce comprised of various user segments, each with its own unique set of requirements. This shift has led to newly coined phrases such as "Consumerisation of IT" and "Bring Your Own Device (BYOD)" (Edwards, 2011). Traditionally, Information Technology has been viewed as an infrastructure required to support the operations of business, not that of the individual. Consumerisation of IT, though, initiated a paradigm shift that has now made IT relevant to individuals as well as business. In October of 2005, Gartner Analysts projected that the bulk of new technologies that organisations would adopt for their IT systems between 2007 and 2012 would have origins in

consumer applications (Pettey, 2005). The traditional boundaries between work and play are readily disappearing as the same devices that employees use for work are the same devices that they use for entertainment, thus transforming IT from a business tool to a social medium.

Unsurprisingly then, the applications and devices that workers request from their employers are increasingly becoming consumer-centric (Kane & Gray, 2012). Employees are becoming empowered to respond to consumers who have been empowered by groundswell technologies: mobile, social, video, and cloud (Schadler & Bernoff, 2010). The Forrester Research refers to these workers as highly empowered and resourceful operatives (HERO) as these are the type of employees that use consumer-centric applications to solve consumer problems at work. The HERO Index, as depicted in Figure 2-5, illustrates how the HERO workers compare to other information worker types.

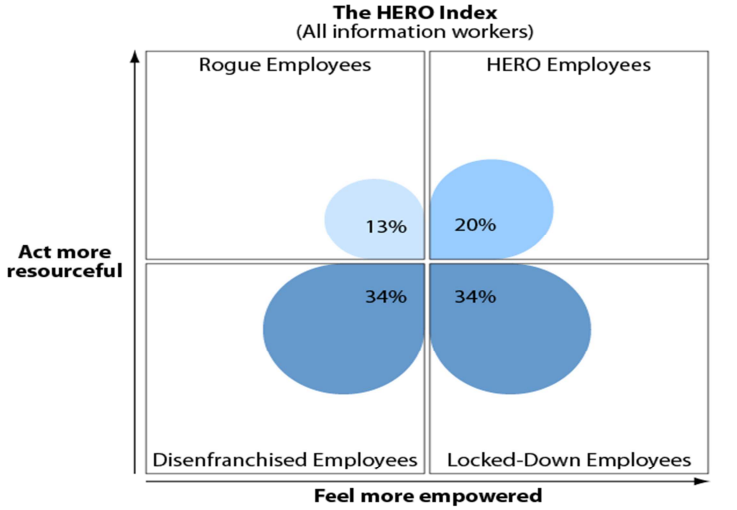


Figure 2-5: The HERO Index (Schadler & Bernoff, 2010)

The term ‘disenfranchised employee’ refers to employees who just do their job with little innovation. Rogue employees, conversely, innovate through unauthorised applications to resolve consumer problems, often without receiving support from their employer. The remaining group, ‘Locked-Down Employees’, refers to people who are eager to resolve consumer problems but are hindered by corporate technology lock-down.

Forward-thinking companies are embracing their empowered employees and reviewing their mobile workforce strategies. Notwithstanding that reviewing a mobile workforce strategy often takes time because of budget approvals and IT leadership sign-off, the workforce is moving forward, with or without IT’s guidance and sign-off. In most cases, the drive to

operate with much-needed innovation and critical flexibility in the workforce far surpasses IT executive's leadership and decision-making process (Kane & Gray, 2011).

The workforce and consumers are driving what they require from technology, so waiting for IT to keep up with innovation or to deliver on it is no longer an option. IT departments are known for adopting structured, well-controlled, and conventional approaches (e.g. SDLC: interview stakeholders, collect requirements, build a project plan, review it with the customer). While this approach is well-suited for internal infrastructure projects or for applications driven by a top-down business requirement, it is far from ideal for discretionary everyday use technologies like smartphone and employee portals. Indeed, this approach fails dismally in capturing requirements from a diverse workforce and consumers at large (Schadler, 2010).

An independent South African benchmarking exercise conducted with various companies by Wolfpack's research team in Q4 of 2011, found that the organisations are already embracing the concept of BYOD by allowing multi-platform mobile devices to access corporate emails and calendars (Rosewarne, 2011).

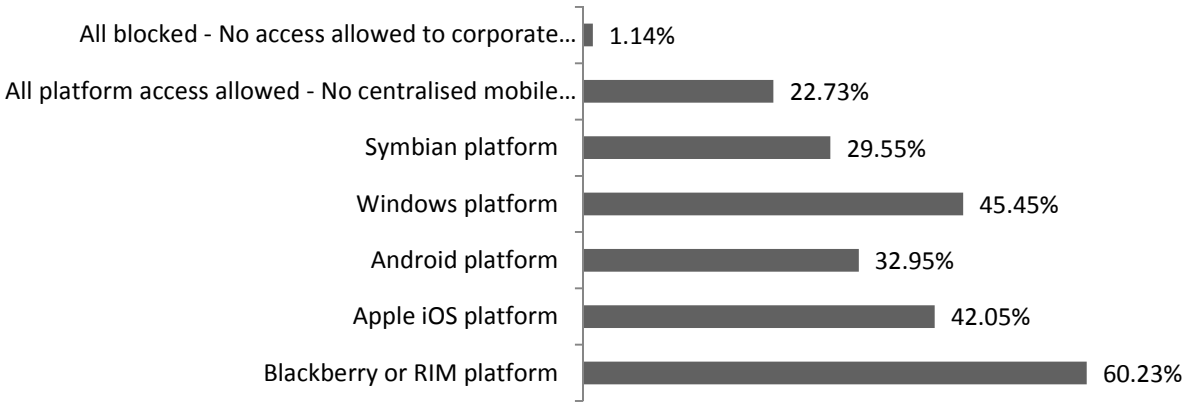


Figure 2-6: Mobile Devices Allowed into the Corporate Network - A South African View (Rosewarne, 2011)

Figure 2-6 shows that only 1.14% of the surveyed companies blocked access to corporate emails and calendars, whereas 22.73% of the companies provided all platforms access to the corporate resources without implementing mobile device management solutions to monitor or control that access.

Checkpoint South Africa in partnership with ITWeb, conducted an online survey in late June of 2012, with a total of 231 people responding to the survey. The survey showed that 86% of the respondents' organisations allow company-issued mobile devices to connect to the

network, and 77% of the respondents' organisations allow personal mobile devices to connect to the corporate network. About 56% of the respondents use mobile devices to access web-based business applications, while a significant majority (98.45%) use mobile devices to access corporate emails, calendars and contacts. About 32% of the respondents use mobile devices to connect remotely to corporate desktops. Only 12%, however, admitted that mobile devices have led to an increase in the number of security incidents within their organisation.

Along with consumerisation of mobile devices, came along consumerisation of cloud-based file sharing services such as Egnyte, iCloud, SugaSync, Skydrive, and Dropbox allowing employees to share files from any mobile device platform. While this service has the benefit of replacing on-premise file servers and reducing the costs associated with remote virtual private network (VPN) access, it exposes an organisation to severe information breaches (Disabato & Berenbaum, 2012). In July of 2012, passwords stolen from other websites were used to access several Dropbox accounts, one of which contained customer email addresses (Rash, 2012). The breach signifies that cloud-based file sharing systems still hinge on username and password to provide protection for information stored on the cloud.

2.3.3 Cost

Organisations that allow employees to bring their own devices save on the costs of the devices that it would normally be required to procure for its employees. Surveys conducted by Forrester Research in the last quarter of 2011, show that an average of 64% of mobile devices used within organisations are fully procured by employees themselves. The results of the survey are shown in Figure 2-7.

Self-provisioning of software trails hardware: according to the same survey, with a total population of 9,912 of small and medium-sized businesses across the globe, 28% of these global workers are paying for software they are using for work purposes.

On the other hand, some researchers believe that the cost of supporting employee-owned mobile devices might outweigh the cost of not supporting them (Schadler, Gray& Wang, 2012). This inherent cost mostly emanates from mobile applications used for business purposes. IT is required to upgrade and license the mobile application on each mobile device user. For instance, a business that uses tablets and client computers to access enterprise applications may be required to support and license two versions of the client software.

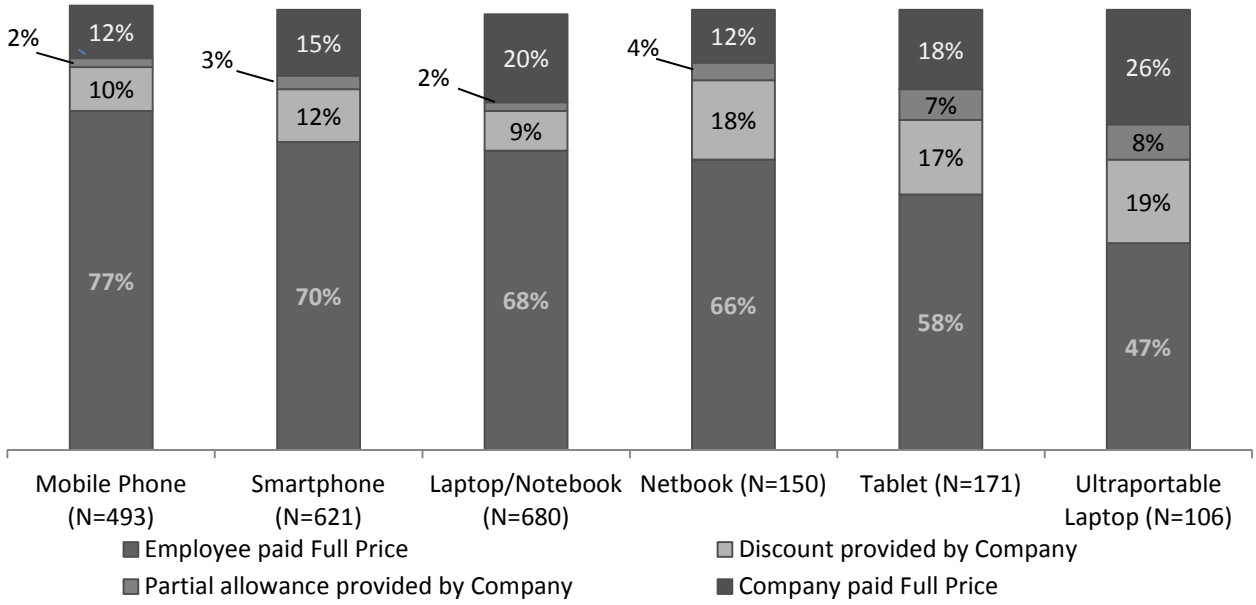


Figure 2-7: Employee Spending on Mobile Devices (Sherman, 2012))

2.3.4 Data Sprawl and Big Data

In the distant past, before the prevalence of information and communication technology, most information was stored in paper form. Control of access to the information on the paper was regulated by physically controlling access to the paper itself. Today, information is stored in digital form, making it exceptionally easy to copy and disseminate. This digital information exists in various forms, stored on numerous folders, on multiple folders, and on various machines and platforms. Likewise, the large amount of digital data that organisations need to share and process on a daily basis results in organisations not always being able to keep track of where confidential data is situated, and consequently not always being able to protect data that cannot be located and controlled (Nosseir, 2010). This ultimately leads to situations known as 'Data Sprawl' and 'Big Data'. 'Data Sprawl' is the explosion of data with no significant control (Thea, 2008). 'Big Data', on the other hand, refers to sets of skills and techniques for processing extreme data volumes, comprised of various data formats, with agility and affordability (Kindervarg, 2012).

'Big Data' and 'Data Sprawl' are not only consequences of uncontrolled information that previously existed in paper form, but also consequences of formation of new digital data that previously never existed. Advanced mobile devices consist of embedded sensors and applications that generate new digitised data (Laurila *et al.*, 2012), sensors which include Geographical Positioning System (GPS), accelerometer, Bluetooth, microphone, gyroscope

and camera (Laurila *et al.*, 2012). While such new mobile data input gives rise to new research areas by allowing Computer and Social Scientists to derive a better understanding of real-life phenomena such as human mobility, interaction patterns and communication (Chittaranjan, Blom& Gatica-Perez, 2012; Eagle, Pentland& Lazer, 2009; Gonzalez, Hidalgo& Barabasi, 2008), it also extends data-sharing beyond the perimeters of the organisation, adding to the complexity of data control. Data contained in these massive data stores could be detrimental to an organisation if it leaves the organisation's control as some of the data includes personal data and sensitive intellectual properties (Kindervarg, 2012).

In this section the business drivers that may ultimately lead to the implementation of data-centric security controls are explained. The benefit of implementing data-centric security controls to enable these business drivers is, however, not adequately communicated by IT security teams; as a result, the business becomes more concerned about the costs associated with implementing data-centric security controls and costs associated with supporting diverse device types rather than the benefits that these mobility investments have on employee productivity and at mitigating mobile risks (Pelino, 2012). This is because IT security teams have not as of yet developed metrics to measure the business impact of these controls, as well as schemes to measure the return on investment (ROI) of these mobility investments (Pelino, 2012). Consequently, to answer our research question, inconsistencies *do* arise between the data-centric security controls implemented by IT security teams and the business drivers.

2.4 Related Work

This section examines the related work of widely published aspects of information-sharing concepts that have a significant impact on data-centric security.

2.4.1 TecSec Incorporated Information-centric Security Model

The literature review begins by exploring the work done by Tsang, Scheidt & Burkardsmaier, (2004), hereby referred to as TecSec Team, from July 2003 to February 2004, in applying the concept of data-centric security into a healthcare environment in order to comply with Healthcare Information Portability and Accountability Act of 1996 (HIPPA) regulations. TecSec' s secondary objective was to preserve the confidentiality, integrity and availability of medical information within a portable electronic device (PED) by addressing the misuse of access privileges and consequent unauthorised dissemination of medical information by Navy and medical services personnel (Tsang *et al.*, 2004). The use of electronic mechanisms of storing and transmitting data (e.g. PED) supports the health organisations business requirements to accurately capture and access medical information in a timely fashion,

thereby reducing costs (from manual processing of paper records and forms) and improving quality of healthcare. The challenge was to apply the following data-centric security controls while ensuring that the business requirements were met:

- authentication;
- authorization;
- access control;
- encryption; and
- audit trail.

The TecSec team posed three set of questions; "*Who?* Knew *What*? And *When?*"

The "*Who*?" refers to the identification and authentication of the PDA user using either shared public key root key(s), or real-time shared secret. The "*What?*" refers to what medical information requires either confidentiality protection or integrity protection. That is, some medical information may require confidential protection as per HIPPA privacy regulations (e.g. patient billing information), while other medical information may require integrity protection due to its sensitivity (e.g. electronic patient records, laboratory data, and other pharmacological information). The "*When?*" refers to the exact time that the particular medical information was accessed, that is, audit logging as well as the protection of the audit log files (Tsang *et al.*, 2004).

As a use case, a physician using HP/Compaq iPAQ Pocket PC h5550 installed with medical software packages and Microsoft Mobile Office software was utilized. The proposed data-centric solution was a hardware-based cryptographic platform, commonly known as Field Programmable Gate Array (FPGA) hosted on a PED platform. Two groups of Elliptic Curve Cryptosystems (ECC) were chosen for distributing public keys and for generating digital signatures, thereby enforcing non-repudiation (Tsang *et al.*, 2004). These two families of ECC were chosen primarily because of their small circuit area and minimal power consumption making them appropriate for wireless networks and portable electronic devices (Tsang *et al.*, 2004).

In addition to the hardware-based cryptographic platform, the key management component was included as part of the solution. Constructive Key Management (CKM), detailed in ANSI X9.69 was chosen because of its split knowledge capabilities (Tsang *et al.*, 2004). Split knowledge refers to the practice of splitting a cryptographic key into '*n*' multiple components while hiding the knowledge of the original key, and subsequently using those several key

components in constructing the final original key (Barker, Barker, Burr, Polk & Smid, 2011). Constructive Key Management was used for authorisation or role-based access control, while Public Key Infrastructure (PKI) was used for authentication.

The TecSec team proposed that the data-centric security solution be segregated and hosted in a stand-alone encryption module that in turn connects to the PED platform (Tsang *et al.*, 2004). A trust model that provides different levels of trust between security domains was also proposed (Tsang *et al.*, 2004). According to Sherwood Applied Business Security Architecture (SABSA), a security domain is a set of logical and physical entities that are subjected to similar security policies and architecture (Lynas, 2012). The security domains that Tsang *et al.* (2004) proposed were comprised of the following:

- Untrusted domain: a foreign domain with which the reference domain has not established any security associations with;
- Second Party Domain: a domain that has a different owner to that of the reference domain and that has already established security associations with the reference domain; and
- Third Party Domain: a domain that has a same owner as that of the reference domain.

2.4.2 Service Oriented Security Architecture

The section explores an architecture model that was proposed by Peterson (2005) to address the lack of security within web services and service orientated architecture (SOA), a model he termed 'service oriented security' (SOS) architecture. This particular architecture model is chosen because it intends to bring an additional layer of security to SOA's decentralised peer-to-peer architecture, as the security models that existed at that time focussed only on perimeters and centralised security models, rather than catering for the diminishing perimeter.
The introduction of web services and service oriented architecture left software developers with no mechanism to secure client's and server's transactions, largely due to the fact that traditional programming styles such as object oriented programming provided developers with options to configure the same languages, technologies, and security models on both the client and the server. For example, the developers could configure the EJB client and server to use the same J2EE security standard for authentication and authorisation. However, with Web services and SOA, the systems may be configured differently and separately, resulting in decentralised peer-to-peer systems that cannot be adequately protected using centralised perimeter-focused security mechanisms (Peterson, 2005). Consequently, SOS was proposed

as a solution that is not solely perimeter-focus, and as a solution that protects the actual data, services, and identities.

SOS consists of five architecture views, one of which (message view) deals with risks associated with data throughout its lifecycle. The SOS views can be used in conjunction with the six architecture views of SABSA to design a comprehensive data-centric security architecture model (Peterson, 2005)

2.4.3 IBM's Data-Centric Security Model

The first and most extensive clarification of the data-centric security model came from Bilger *et al.* (2006) who did an extensive work in tracing progressions in security rational from infrastructure-based to host-based defences (Marko, 2008).

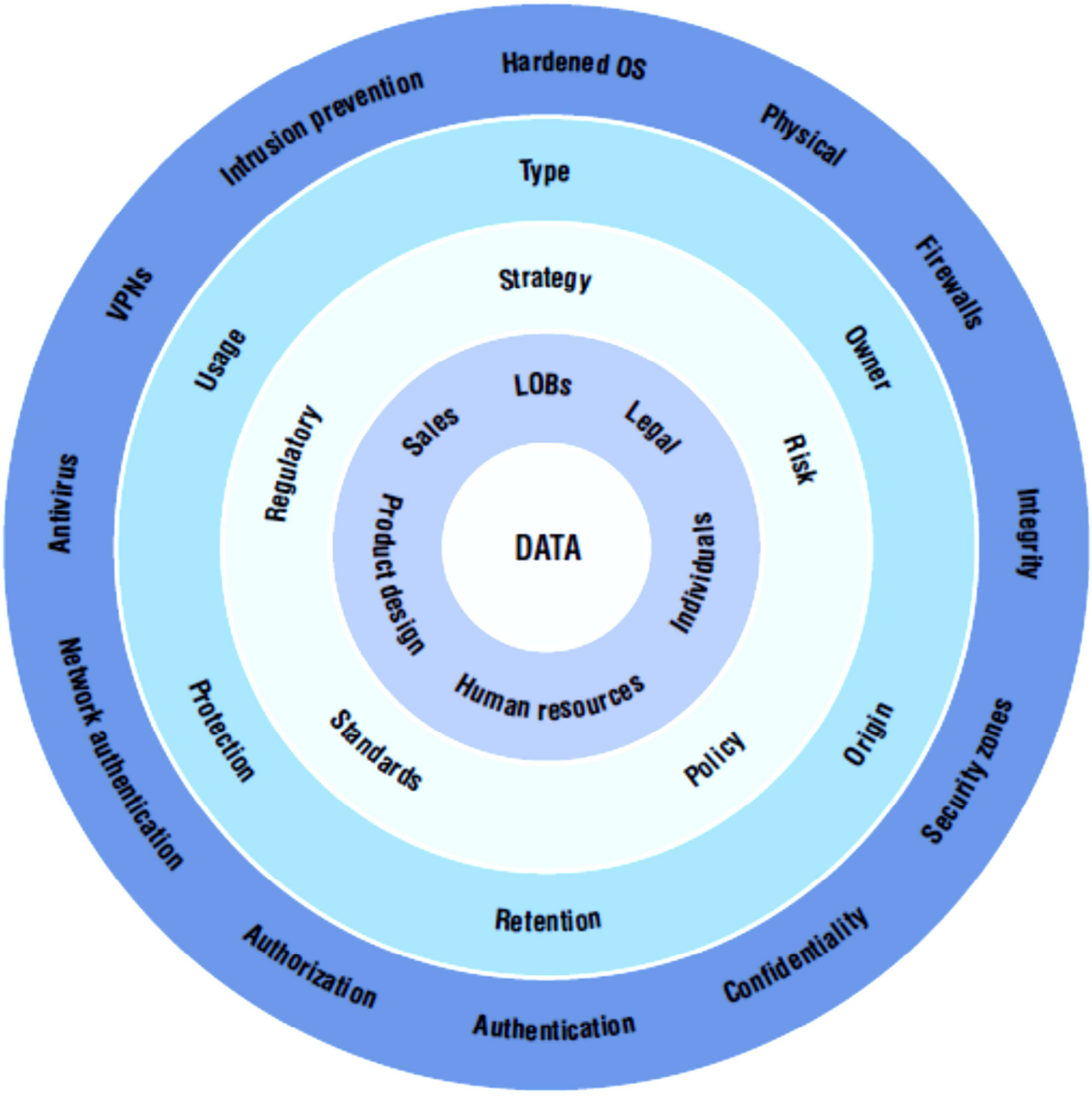


Figure 2-8: IBM Data-centric Security Model (Bilger *et al.*, 2006).

They note that*: "If we extend this layered defence approach further, beyond host-based security to the data that is protected on those hosts, we arrive at the Data Centric Security Model"* (Bilger *et al.*, 2006, p.10). The data-centric security model is illustrated in Figure 2-8, where data is placed at the centre of the model.

The access control policies applied on the data are driven by business requirements and defined using organisational roles. This model is based on the understanding of the business value of data, its type, as well as the ownership of the data.

Figure 2-9 illustrates the two components of DCSM, the policy pillar and data pillar. The policies on the policy pillar are made up of business requirements and regulations, expressing data-handling policies in terms of requirements, both internal and external to the enterprise (Bilger *et al.*, 2006). These requirements are then used to define an overall business data classification (BDC), which gets encoded into data control rules (DCR) together with the policy rules. Briefly, the data control rules define how data is going to be handled given its data classification level.

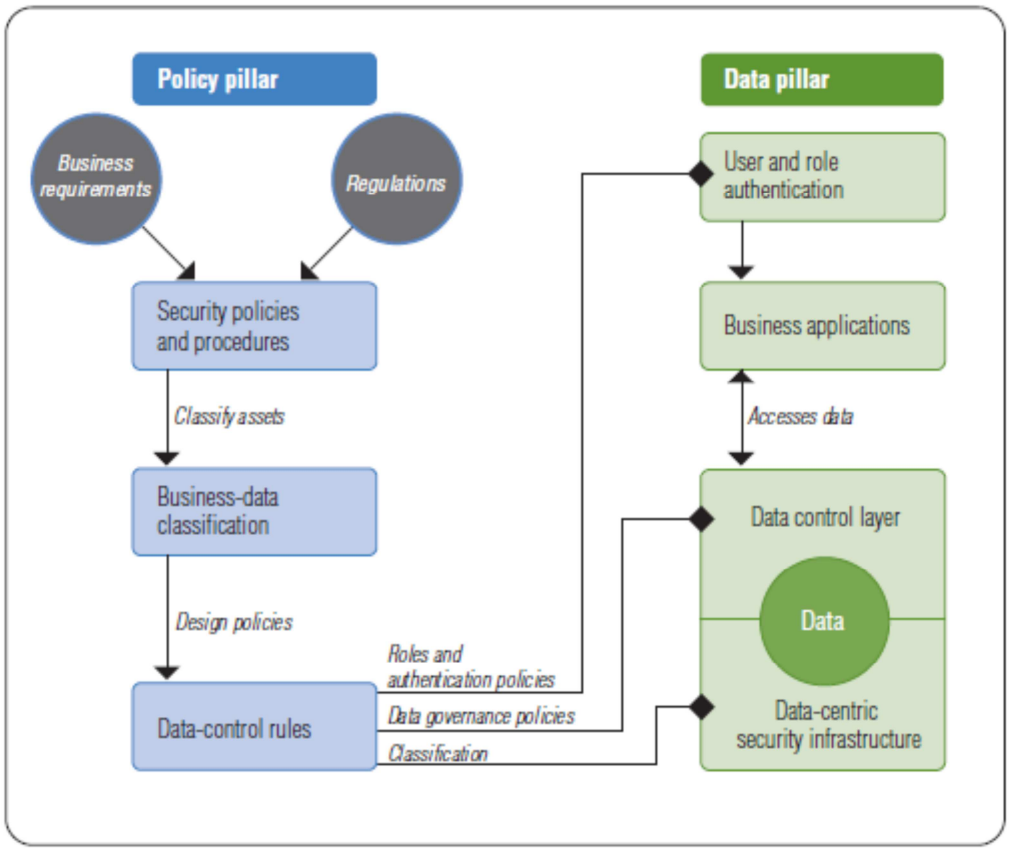


Figure 2-9: The Components of DCSM (Bilger *et al.*, 2006).

The data pillar is comprised of the data control layer that controls access to the data and allows actions on the data. The policies and the DCR are interpreted and implemented at the

data control layer using the security services in the IT infrastructure as illustrated in Figure 2-10 (Grandison *et al.*, 2007).

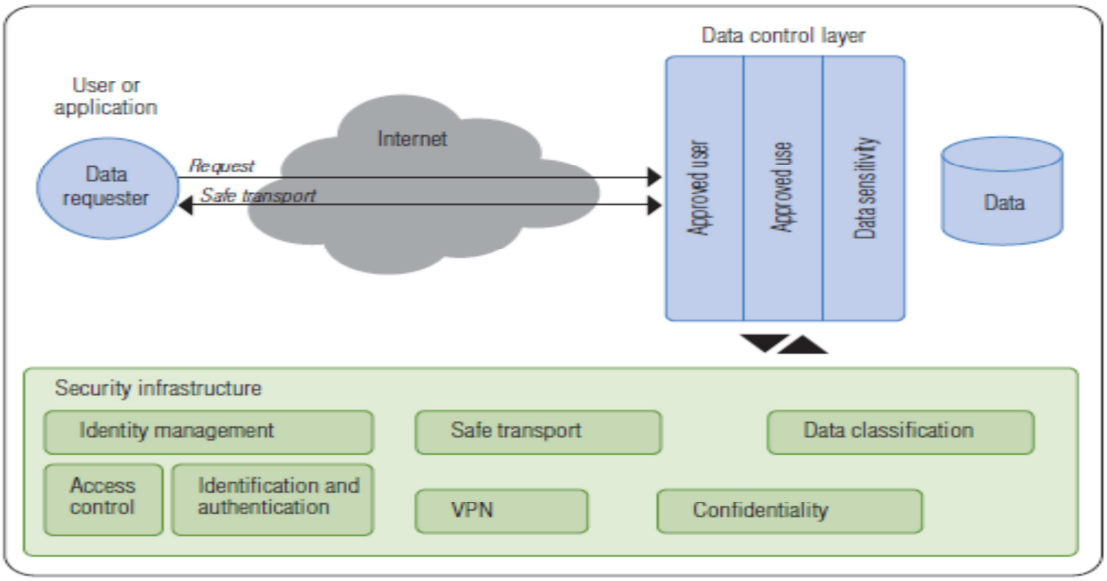


Figure 2-10: Logical Deployment of DCSM (Bilger *et al.*, 2006)

The request to access corporate data from a mobile user is sent to the data control layer, which forwards the request to the security infrastructure. The security infrastructure responds with a service, as defined in the data control policies, which fulfils the request. For example, a request to access a document that has been classified, according to BDC, as confidential, will require the security infrastructure to respond with a service that employs tunnelled VPN connection to deliver the document securely to the mobile device.

2.4.4 De-perimeterisation

The Jericho Forum is an intercontinental group of bodies committed to evolving the solutions relating to de-perimeterisation. The de-perimeterisation term was initially invented by Jon Measham, and subsequently became a term used by the Jericho Forum of which the United Kingdom's Royal Mail was a founding member (Wikipedia 2011). The Jericho Forum believes that the threats faced by today's networks have become so immense and diverse that the only viable strategy is to protect the information itself, rather than protecting the infrastructure (Jericho Forum, 2007). This belief is consistent with data-centric security model.

Figure 2-11 illustrates changes in business practices that have led to increased connectivity over time, leading to a distributed, globalised, and disaggregated business environment that compels more open access to corporate sensitive data.

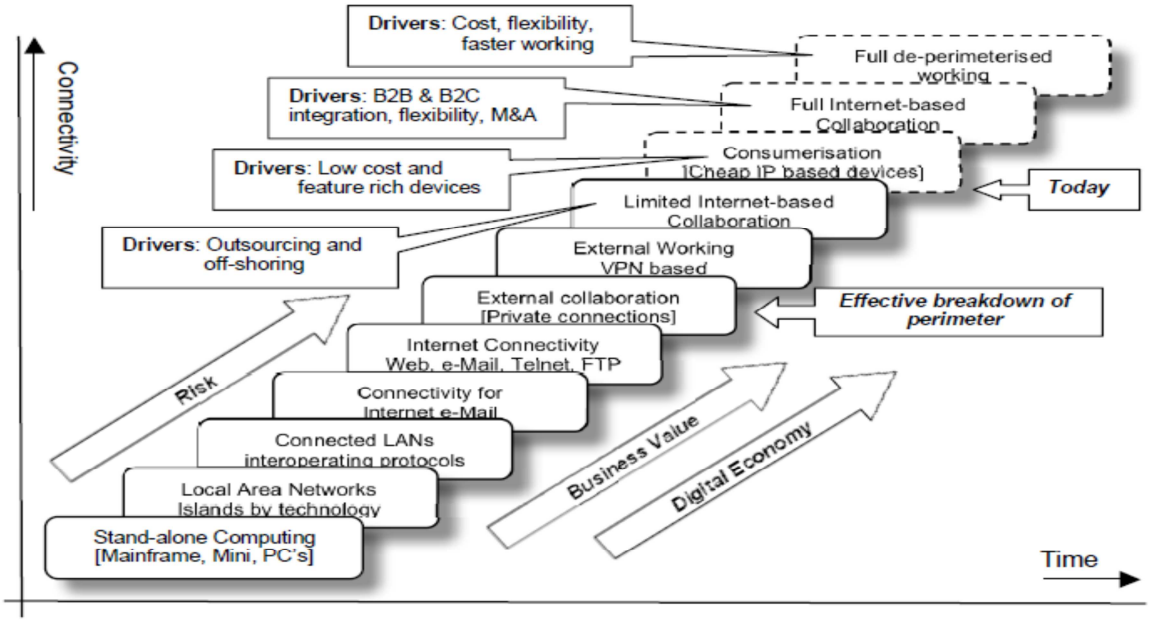


Figure 2-11: Changes in Business Practice Leading to De-perimeterisation (Jericho Forum, 2007))

This further demonstrates that the traditional perimeter-based security approaches are incapable of coping with modern business drivers, consequently leading to an urgent need to deploy data-centric approaches and new approaches to infrastructure architecture in order to support these modern business drivers while ensuring that information is safeguarded in the manner that the business dictates (Stamp, Whiteley, Koetzle & Rasmussen, 2005).

The traditional infrastructure-based security model controlled access to the organisation's infrastructure (i.e. connectivity, storage, and computing resources) in a tightly controlled closed perimeter. Connectivity (bandwidth and network access), storage, and computing resources are declining in scarcity and have become less expensive, leading to an increased requirement to support these resources in a cloud or outsourced environment, thus changing what was then a tightly closed perimeter into a porous one (Jerbic, Keck & Satola, 2007). The security no longer has full control of the significant portion of traffic that passes through it due to a large amount of connectivity that happens outside the enterprise (business partners, customers, and mobile employees). Furthermore, these tightly controlled perimeters are now being bypassed by new technologies that tunnel through these perimeters and sometimes encapsulate protocols within allowed web protocols.

While some scholars believe that the perimeter is diminishing, some believe that they are changing to perimeters without any specific shape (Jerbic *et al.*, 2007). They traverse across traditional business boundaries and assume new shape to accommodate the new business requirements of protecting information from wherever it is, to wherever it is going.

Figure 2-12 illustrates both the conventional security model as well as the de-perimeterised security model.

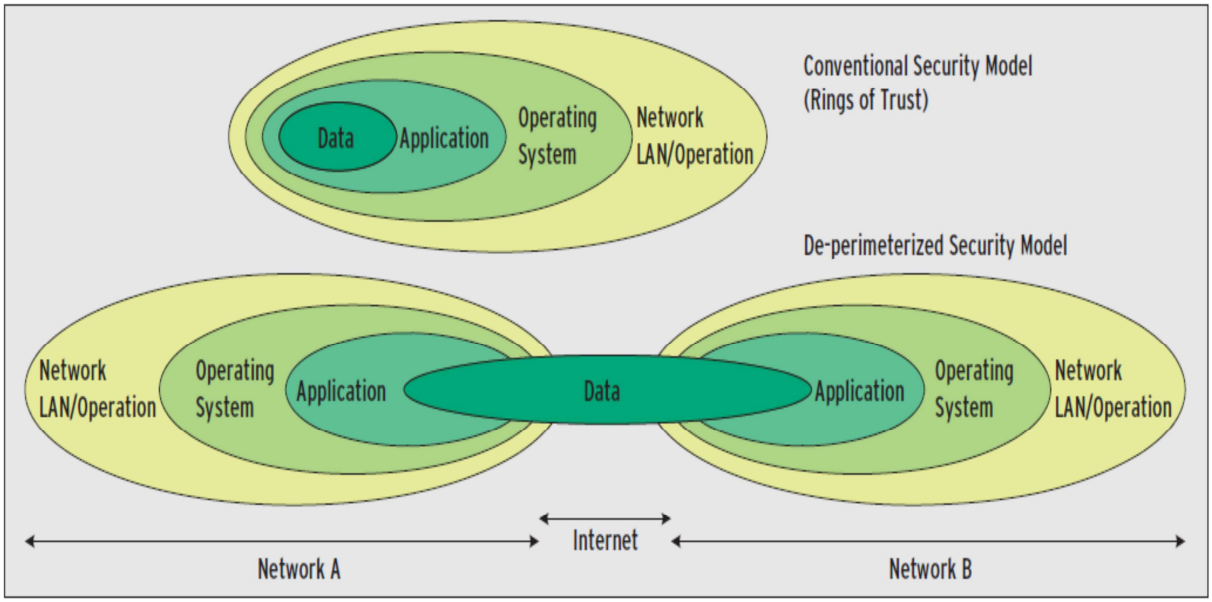


Figure 2-12: De-perimeterisation Illustrated (Fritsch, 2008)

The conventional security model shows data being protected using layers of clearly defined perimeters or rings of trust. The ring that is situated further to the data has a lower security level than the ring closer to the core. The de-perimeterised security model, on the other hand, shows data existing independently of the layered perimeters. In this model the data does not depend on any application, operating system, or network to provide security. Rather, the security is embedded on the data itself.

The Jericho Forum suggests that organisations will move into four stages before conducting their business in a fully de-perimeterised environment (Cummings, 2004).

2.4.5 Discussion of the Models

The second objective of this research is to examine the existing data-centric security models and understand how the models can be applied to mitigate mobile device risks. According to Mogull (2008b), the realisation of data-centric security can be achieved once the following sets of principles have been fulfilled and tied to overall research objectives:

1. Information (data) must be self-describing and defending.
2. Policies and controls must account for business context.
3. Data must be protected as it moves from structured to unstructured, in and out of applications, and changing business context.

4. Policies must work consistently through the different defensive layers and technologies implemented.

The four models are examined against these principles as shown in Table 2-2.

Table 2-2: Comparison of the Models against the Principles

	Principle One	**Principle Two**	**Principle Three**	**Principle Four**
TecSec Information-centric security model	Fulfilled: Data classified using HIPPA requirements that in turn determine the level of protection required.	Fulfilled: the policies and controls implemented to protect medical information are driven by business requirements.	Partial: Data protection mechanisms proposed by TecSec are only applicable to this business context. It cannot be determined if they will remain applicable should the business context change.	Fulfilled: TecSec made use of security domains that are subjected to similar policies and architecture.
Security Oriented Security Architecture	Partially: the data is not self-describing and defending, but the services that render access to data.	Fulfilled: the need to develop this architecture is driven by the changing business requirements.	Fulfilled: using Service View, Identity View and Message View	Fulfilled: Security Oriented Security Architecture makes use of consistent security policies within the various views.
IBM Data-centric security model	Fulfilled: Data is encapsulated with data control rules that describe or determine how data will be protected, and what type of security services will be used to protect data.	Fulfilled: IBM DCSM makes use of business requirements and organisational roles to derive the access control policies, which are in turn applied directly to the data. The policies used therefore account to business context.	Fulfilled: Since IBM DCSM creates a container around the actual data with access rules and business context, the data remains protected regardless of where it is situated.	Fulfilled: The data-handling policies applied onto the actual data are derived from business requirements, and these in turn result in security technology requirements. Consequently, the policies remain consistent through the different layers of technology.
De-perimeterisation	Fulfilled: Security is embedded in the actual data.	Fulfilled: Refer to Figure 2-11	Fulfilled. Since security is embedded in the actual data, the data remains protected regardless of where it is situated.	Fulfilled: In this model, data exists independently of the various defensive layers because it is embedded in the actual data and therefore remains consistent.

It is evident from these four models that the data-centric security concept cannot be implemented without the support of existing traditional perimeter-focused security controls.

The four models somehow agree that the content of the data should be examined based on its attributes and business requirements in order to determine what data is stored where, and how it is flowing into and out of the network. That is, data should be classified based on business requirements. Data classification remains a core requirement on all models.

Data encryption follows from data classification. The TecSec Incorporated information-centric security model assumes that all medical information is sensitive and should be encrypted. Likewise, the IBM DCSM and de-perimeterisation security model proposes that data should be encrypted, in storage, and during transit, so much so, that Jericho Forum even went further to publish a Technology paper establishing the need to have secure products, services and protocols to secure communication of information leaving a trusted environment. This paper was entitled "(The need for) inherently secure communication" (Jericho Forum, 2008a).

De-perimeterisation and TecSec Incorporated information-centric security model alludes to trust model or 'rings of trust'. De-perimeterisation suggests that data exists independent of 'rings of trust', while the TecSec Incorporated information-centric security model proposes that information and access to information should be clearly segregated between security domains based on their level of trust. Despite these variances, the applied policies remain consistent through the various rings of trust, domains or layers.

The SOS model focuses more on software security than on actual data or information. This model is, however, relevant to this research because of its decentralised approach in securing SOA.

A clear observation from the models discussed is that they ***do*** highlight a problem where traditional approaches to architecting security solutions aimed at securing organisational boundaries and the network are divergent to the future business needs of most organisations. The future business needs in this case refer to the organisation's ability to adopt mobile devices and various other channels to conduct business. The models ***do not***, in completeness, suggest a technical solution or toolsets to mitigate the risks associated with the adoption of mobile devices to satisfy the future business needs. While the TecSec model suggested the use of Field Programmable Gate Array and Constructive Key Management, no evidence was found if these were successfully implemented. Likewise, the framework that was proposed by the Jericho Forum (for de-perimeterisation) to enable architected business-driven solutions to be developed and delivered, suggested the following technologies:

- endpoint security;
- secure communications; and
- secure data (DRM).

However, no evidence has been provided showing that these technologies are adequate to protect an organisation against today's mobile device threats.

The successes and failures inherent in existing implementations of data-centric security models must be highlighted prior to the proposal of a utopian architecture framework for mitigating risks borne by mobile devices.

In this section, the research objective of examining existing data-centric security models to understand if they are adequate in address mobile device risks was met. The subsequent sections describe in detail the three technologies used for the implementation of data-centric security model.

2.5 Enterprise Digital Rights Management

Digital Rights Management (DRM) is a class of access control technologies used to protect or limit the use of multimedia assets (such as video, audio, and picture) and devices after they have been sold to the consumer. DRM technologies provide control to the seller of digital content or a device after it has been sold or given to a consumer (Yu & Chiueh, 2004).

This technique is also used to manage access to sensitive documents, emails, computer-aided designs, and other digital assets within the Enterprise- hence the name Enterprise Digital Rights Management (EDRM). Enterprise DRM is often referred to in other similar terms such as Enterprise Rights Management, Information Rights Management, Enterprise Digital Rights Management, Document Rights Management, and Intelligent Rights Management. In this study, we consider all these terms to represent the same technology group.

EDRM protects sensitive information from unauthorised access by persistently controlling access to information and usage thereof. It ensures that the enterprise's digital assets are used aptly by employees, customers, and partners throughout their lifecycles. Information Rights Management makes use of granulated, user-based access rights to digital data objects regardless of where and when the access occurs (Smallworld, 2005). For example, a mobile employee might be able to read an email attachment from his Tablet but not forward the attachment to another recipient. A freelancer might be able to read a document but not print it (Howitt, 2010).

Any Enterprise Digital Rights Management solution falls within one or more of the following categories.

2.5.1 Document Repository Solutions

A majority of Enterprise Digital Rights Management toolsets fall within this category. This is better understood by first describing the function of a document repository solution.

An Electronic Document Management system (EDMS) is a form of a document repository solution that allows users at distantly situated information systems to manage documents and other media. Components of the system include public data network, a publication facility, a remote storage facility and a document manager computer (Cullen & Peairs, 1999). The system is capable of keeping track of the different versions of documents modified by different users, versions which include electronic documents, images, email messages, and other computer files, as well as scanned paper documents.

Paper documents are captured using scanned images and fed onto EDMS. The user is then prompted to provide details for the appropriate storage of the documents. EDMS can also store documents that are already in digital format provided the user gives the required details to store the documents. This metadata assists in the correct filing and tracking of documents. Additional metadata is compiled by EDMS to allow users to locate documents quickly by keyword searches. Correct indexing, then, is essential in ensuring timely retrieval of documents.

EDMS solutions pose two security challenges: 1) the first challenge is that once the document is retrieved from the repository, it can be sent to any recipient at any location, without any restrictions or traceability (Abatan, 2010); 2) another security challenge is that the documents cannot be protected using an encryption tool while inside the Electronic Document Management System because the contents of EDMS cannot be indexed when encrypted, and consequently searching becomes impossible (Abatan, 2010).

These challenges are both resolved by an Enterprise DRM document repository solution because this solution protects the documents as soon as they are retrieved from the repository. This is a client-server based solution, components of which are illustrated in Figure 2-13.

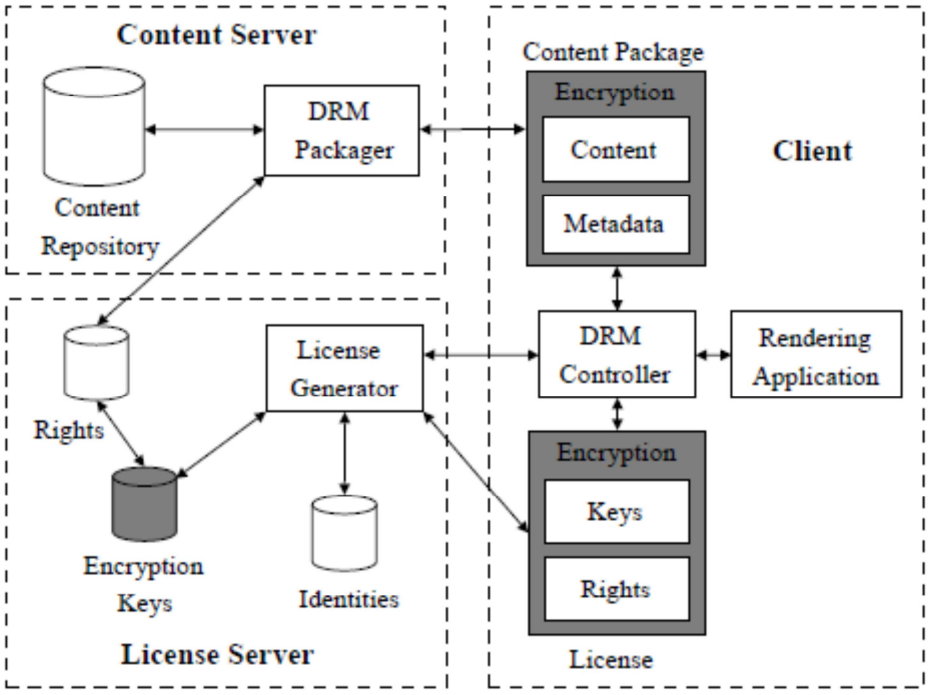


Figure 2-13: Architecture Representation of E-DRM

The *content server* stores the protected content files in a content repository, commonly referred to as file server, document repository, or database system. *The DRM Packager* is responsible for encoding and wrapping the confidential content and related metadata, and creating the rights specifications for the content as soon as it leaves the repository (Yu & Chiueh, 2004).

A client cannot access a document inside the repository without a valid licence. These licenses, generated by a *license generator* on the license server, contain information about the identification and rights specifications of the content to which the rights apply, and the identity of the user or device that wants to exercise rights to content (Yu & Chiueh, 2004). These rights specifications and encryption keys used for authenticating the user and for decrypting content are kept in isolated databases on the license server. The additional database on the license server contains user identities (usernames, biometric information, or digital certificates) for users that exercise rights to protected content.

Communication between the client and the license server happens at the *DRM Controller*, and the content is decoded and presented to the client by the *rendering application*.

The above-mentioned components of an Enterprise DRM document repository solution are not necessarily detached. For instance, Windows Rights Management System does not store the protected files in a content repository, and does not store rights specifications on the license server. The rights policies are attached to the document and travel with the document

wherever it is stored. The rights policies can be changed at any instance, regardless of where the document is located (Arnab & Hutchinson, 2005).

An Enterprise DRM document repository solution can also safeguard protected files within the following systems as enumerated by (Abatan, 2010):

- Enterprise Resource Planning Systems (e.g. SAP);
- Electronic Document Management System (e.g. Documentum);
- Knowledge Management Systems (e.g. Lotus Notes);
- Groupware systems (e.g. ProjectPlace); and
- Product Data Management (PDM) systems which serve as a central knowledge repository for process and product history.

2.5.2 Document Exchange Solutions

The document exchange solutions are designed to be used both inside and outside the corporate infrastructure. The objective of this solution is to enable an organisation to send sensitive documents to their partners while ensuring that the confidentiality and integrity of the document is preserved. Various forms of authentication ranging from email authentication to web based authentication are used to grant access to documents protected using E-DRM.

The rights policies are packaged together with the files, with restrictions of who can open the files and for what purpose (e.g. print, view, save, edit and copy). The file author is notified through email as soon as the file recipient opens the file. The rights to the file can be revoked at any time, regardless of whether the file is in transit, is in use, or is at rest. The file recipient first needs to download the E-DRM client software in order to open and read the protected file, the user will then authenticate to the E-DRM server before downloading the actual content.

2.5.3 File Server Solutions

This solution is used to protect documents stored inside the file server by applying security policies to specific folders in the file server. The file inherits the security policies of the folder as soon as the folder is dragged or saved into the folder protected by E-DRM. The policy determines who can read, save, edit, or view the file, and can be applied differently to each folder.

The files saved or dragged into the folder protected by E-DRM are also automatically encrypted in addition to the inherited policies. This is different from normal file encryption in that the security policy is attached to the file permanently whether the file is in use, at rest or

in motion; whereas with normal file encryption once the file is decrypted it can be used and distributed without any further controls (Abatan, 2010). Furthermore, the E-DRM solution keeps an audit log of who has accessed the file and for what purpose.

2.5.4 Print Solutions

Print solution is geared for organisations that want to avoid leaks via printed documents. When documents protected using this feature are printed, they get the watermark effect over the document itself, along with the username of the person who printed the document, thus putting the onus of protection responsibility onto the person who printed the document. This can be used in conjunction with other Enterprise Rights products such as document repository solutions (Abatan, 2010).

2.5.5 Mobile Device Solutions

The Enterprise DRM Mobile Device Solution recognises how mobile devices like BlackBerry and iPhone, as well as Symbian, Windows and Android based smartphones are becoming essential business tools extending well beyond voice communication. This solution extends the enterprise rights that exist inside the corporate infrastructure to the mobile device used outside the corporate infrastructure. That is, if you have “read only” rights to a particular document, then the same “read only” rights will be extended to the mobile device. The goal of this solution is to protect confidential information on mobile devices, information which can be protected while it exists either in file or email form.

2.5.6 Web Solutions

This particular solution is geared towards protecting information copied from websites. That is, it can prevent screen dumps from ERP, or Knowledge based websites.

2.5.7 Desktop Solutions

This solution automatically encrypts files at the moment of file creation. Only the pre-designated person can use the file, and that pre-designated person cannot use the file beyond his or her permission. This is policy defined at the point of file creation, and policy is downloaded during logon. The policy, however, can be changed at PC-level to grant other users access to the file as defined by the Administrator. The difference between this and encryption is that the policy is attached to the file and is maintained while an authorised person is using the file. Other capabilities include ability to work offline and it is advised for only short periods.

2.5.8 Key Selection Criteria for Enterprise Digital Rights Management

Forrester Research Inc. conducted research in 2010 on the eight key enterprise digital rights management vendor products (Hill & Jaquith, 2010). Figure 2-14 lists these eight key enterprise digital rights management vendor products and presents summary of the results against the evaluation criteria. A comparison between the selection criteria used by Forrester Research and that used by Gartner in a report titled "Key Selection Criteria for Enterprise Digital Rights Management" (Quellet & Wagner, 2010) makes it evident that the following selection criteria appear to be prevalent on both reports, as shown in Table 2-3.

Table 2-3: Selection Criteria for Enterprise Digital Rights Management

Selection Criteria	Description
Policy creation and Management	The criterion defines the extent of protection or restriction that the E-DRM solution can have on the documents or class of information where the policy is applied.
Third Party Product Integration	The criterion measures the extent to which E-DRM integrates with context-aware DLP, email and message archiving applications, document and content management systems.
Usage Tracking (Auditing)	The criterion assesses the degree to which each Vendor: • Supports logging of basic document open, paste, copy, and cut events. • Supports logging of policy creation and modification events • Captures user session times.
Mobile Device Support	The criterion measures the extent to which the E-DRM can support various mobile devices and operating systems.
Usability and Portability	The criterion measures the extent of usability to external parties. For instance, the third part should be able to access the protected document without having the E-DRM client installed; and without access to the centralised key servers.

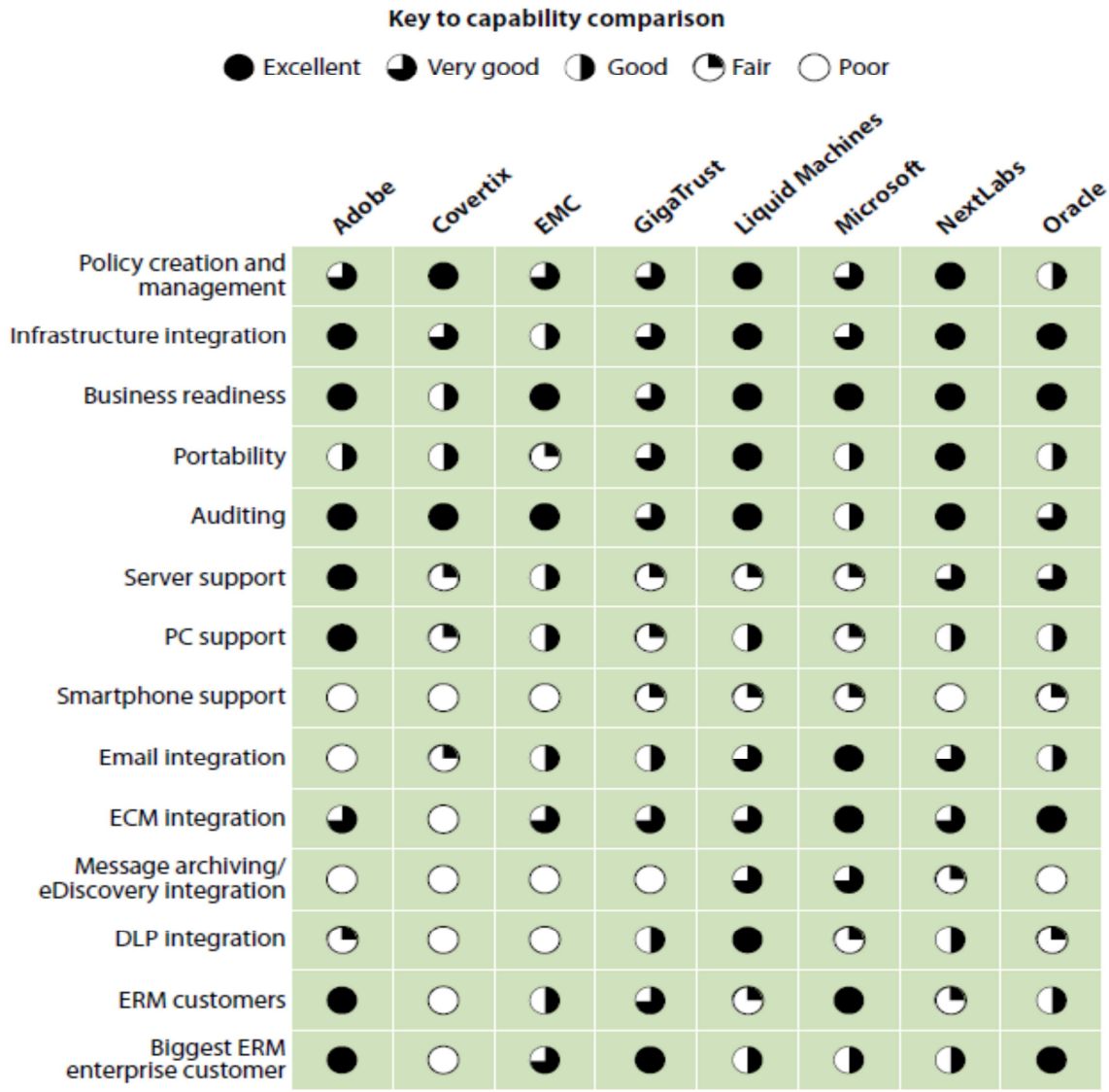


Figure 2-14: Summary of Evaluated E-DRM Products (Hill & Jaquith, 2010)

2.5.9 Case studies: Enterprise Digital Rights Management

This section presents and discusses case studies from three organisations that have experienced the implementation of Enterprise Digital Rights Management and are therefore considered subject matter experts. The case studies are chosen to align to the research objective of analysing the shortcomings of data-centric security technologies (E-DRM) in a real world scenario. Furthermore, the case studies are chosen to align to the problem statement of whether or not data-centric security technologies are implemented to address the business requirements and to enforce the correct level of protection necessary to result in both effective and cost-efficient controls. A brief description of each organisation is given, followed by a description of the case study pertaining to the particular organisation. The three case studies are compared to identify commonalities and the various strengths and weakness of each are discussed.

The organisations will first be introduced to provide a context for its expertise on the subject of Enterprise Digital Rights Management. The case studies will then be described and evaluated to identify commonalities between them. Finally, the strengths and weaknesses of some of the case studies will then be discussed to determine the desirable attributes that will be included in the proposed new model.

The case studies are drawn from a diverse selection of organisations using different Enterprise Digital Rights Management toolsets. The three organisations under consideration are as follows:

- Versace;
- Amkor Technologies; and
- Microsoft.

2.5.10 Case Study One: Versace

Versace is an international extravagance goods and chattels enterprise famous for its designing, manufacturing, and licensing of clothing, accessories, and other items under Gianni Versace Couture, Versace Jeans Couture, Versus and Versace Signature brands (Versace, 2011).

The protection of Versace's Intellectual property is deemed a high priority by Versace Group. There is a continuous flow of official design documentation between the Milan headquarters, various offices, retailers and ateliers worldwide, and conserving the secrecy of these documents is essential at all times (Versace, 2011).

Versace Group's business requirement is a solution that restricts and controls the use and access of Intellectual property and minimise risk of data leakage. Furthermore, the solution should restrict and control the use of and access to Versace's Intellectual property and minimising risk of data leakage (Versace, 2011).

An Enterprise Digital Rights Management solution known as Boole Server was implemented to address this specific business requirement. The machines belonging to staff at the Milan headquarters were installed with E-DRM desktop client, with an implementation of a web client for simple access through an internet browser for all other worldwide locations and partners (Versace, 2011). The design documents were encrypted both in storage and in transit using 2048 bit encryption mechanism deployed with the E-DRM solution. The sharing of design images such as sketches, drawings, and preview material for advertising campaigns is protected using identification watermarks in order to restrict unauthorised access or

transmission and to track potential leakages to their origin. The E-DRM solution provides an auditing system that allows real-time tracking of user activity on each and every image and protected document.

2.5.11 Case Study Two: Amkor Technologies

Amkor Technology is one of the largest suppliers of contract semiconductor assembly and test services headquartered in Chandler, USA. Founded in 1968, Amkor initiated the outsourcing of integrated circuit assembly and test and is now a strategic manufacturing partner for more than 200 of the world's leading semiconductor companies and electronics original equipment manufacturers (OEMs) (Brook-Bilson, 2012).With operations that encompass production facilities, product development centres, and sales facilities across Asia, Europe, and the United States, Amkor assembles and tests around 7% of the world's semiconductors (Brook-Bilson, 2012).

Historically at Amkor, documents were handled in person on paper. Employees would often hand carry designated reports to an automotive customer across the globe, present the information for audit purposes, and then take the paper away when leaving. However, travel became expensive, telephone calls were unmonitored, and e-mails difficult to control. Stakeholders were hesitant to share sensitive information because they lacked confidence in the exchange process, a barrier that impeded the collaborative workflows essential to electronics manufacturing. In addition, audit trails were weak. Increasingly, Amkor recognised the need to implement a more secure digital document exchange process to help prevent loss, make business more cost-effective, and enhance collaboration (Brook-Bilson, 2012).

Amkor's business requirement was to protect its Intellectual property in two ways: 1) first, the firm is entrusted with specifications from its customers and vendors that require that their information not be breached; and 2) Amkor undoubtedly must protect its own proprietary patents from Industrial Competitors.

An E-DRM solution was implemented to address these specific business requirements. The implementation was rolled out in a phased approach using Adobe LiveCycle Rights Management System following a successful proof of concept and eight months pilot implementation. The specification sheets are uploaded in Word, Excel and PowerPoint. Then E-DRM was used to apply the needed controls to the document: adding watermarks, setting expiration dates for opening, password-protecting files, disabling printing and other restrictions (Brook-Bilson, 2012). Authentication is required on download. Downloaded

documents remain on a user's hard drive, eventually becoming disabled upon the expiration date set by the E-DRM solution. The E-DRM auditing capability allows Amkor to have a view of document activities and enables monitoring of each recipient's IP address. If a document is opened outside the normal IP address range, Amkor receives a notification.

2.5.12 Case Study Three: Microsoft Corporation

Microsoft Corporation, an international company with head offices in Redmond, Washington, USA is involved in the development, production, licensing and support of a wide range of products and services related to computing. The company is, today, the world's largest software producer by degree of revenues (Microsoft Corporation, 2009).

Microsoft workforces depend on Microsoft Office Outlook e-mail messaging and collaboration client to communicate with internal and external stakeholders. Microsoft workforces also depend on Microsoft Office applications to record, share and present organisational ideas and other confidential information.

Microsoft's business requirement was to develop a solution to safeguard the contents of its business e-mail messages and documents, without impacting on productivity.

Microsoft Corporation implemented Active Directory Rights Management System (AD RMS) to address this specific business requirement. AD RMS, combined with Microsoft Office, enables Microsoft employees to add usage restrictions to their e-mail messages and documents. The rights control the usage of the email message and document and are applied directly to the protected data object which is encrypted and can only be decrypted through a use-license from the AD RMS. Internally licensed right-protected content is accessible from outside the corporate network boundary through publishing the internal AD RMS servers using Microsoft Internet Security and Acceleration (ISA) Server reverse proxying capabilities. This option was chosen over placing an AD RMS server in a demilitarised zone. (Microsoft Corporation, 2009). A valid Windows authentication is required by the AD RMS server before a use-license is issued to enable an external user to open a protected document.

2.5.13 Analysis of case studies

There is a noticeable commonality between all three case studies: as an initial step, the three case studies make clear that an organisation must first understand the organisation's current strategy, operational model, and business requirements prior to the implementation of E-DRM. In all three case studies, E-DRM was installed in reaction to, and specifically to address existing business requirements. That common business requirement is to share

documents and information outside organisation boundaries, but only in particular manners and with certain people. It is evident from these case studies that the implementation of E-DRMS is based on business requirements, technical demands and the constituency the enterprise wishes to support.

The strength of the Amkor case study is the level of planning and preliminary work prior to E-DRM deployment. The implementation was rolled out in a phased approach using Adobe LiveCycle Rights Management System following a successful proof of concept (POC) and eight months pilot implementation. The POC ensures that vendor claims regarding features, functions, seamlessness, integration with existing systems and user experiences all meet the stated goals of the deployment. E-DRM integrates with existing productivity applications, such as office suites, document management systems, and legal compliance systems. These capabilities often require organisations to carefully rethink the way they handle and process confidential information; therefore the POC will often buy organisations time to review and rethink existing workflows (Hill & Jaquith, 2010; Quellet & Wagner, 2010).

In alignment to the problem statement, the case studies reveal that E-DRM toolsets are implemented to address existing business requirements and to enforce the correct level of protection necessary to result in both effective and cost-efficient controls; however, the case studies do not reveal the shortcomings of E-DRM. The next section outlines the shortcomings of E-DRM as per the objectives of the research.

2.5.14 Shortcomings of Enterprise Digital Rights Management

E-DRM toolsets have been available since as early as 1997; however, their market penetration still remains fragile (Smallworld, 2005; Quellet, 2010). Table 2-4 represents adoption plans across a range of various data security technologies based on a survey conducted by Forrester in North America and Europe in late 2009. According to Table 2-4, only 10% of organisations in Europe and North America reported using E-DRM, while 40% of the organisations showed no interest in adopting the technology. This lack of market adoption is largely attributed to its high cost of implementation, application rigidity, and integration limitations (Hill & Jaquith, 2010).

Cost: The cost per user license ranges from $40 to hundreds of dollars (Penn, 2010), a huge difference when compared to other data security technologies, such as antivirus products where costs are typically much less expensive.

Table 2-4: Promising Adoption Plans Across a Range of Data Security Technologies

	Implemented, not Expanding	Expanding Implementation	Planning to implement in next 12 months	Planning to implement in a year or more	Interested, but no plans	Not Interested	Don't know
Database Encryption	15%	3%	4%	5%	24%	44%	5%
Email Encryption	14%	4%	7%	6%	34%	32%	4%
Centralised Key Management Solution	11%	2%	6%	5%	29%	40%	7%
Enterprise Digital Rights Management	10%	1%	4%	5%	32%	40%	7%
Network Storage Encryption	9%	2%	6%	7%	33%	38%	6%
Database Vulnerability Assessment,Montoring and Auditing	8%	3%	4%	7%	36%	37%	6%
Data Leak Prevention	8%	2%	6%	7%	40%	30%	7%

Source: (Penn, 2010)

Integration limitations: There is a high prevalence of security toolsets that can be used as a substitution for E-DRM, or that can offer a significant subset of E-DRM-like capabilities that may be better suited to perform a given task of protecting sensitive digital assets. These include but not limited to, content-aware data loss prevention (DLP), email encryption, identity and access management (IAM), watermarking, and contractual limitations. The lack of integration of E-DRM with the aforementioned toolsets has exacerbated the lack of E-DRM popularity. Figure 2-14 shows that Liquid Machine is the only vendor that can fully integrate with content-aware DLP.

Application rigidity: Enterprise processes and workflows are designed in such a way that they can be updated easily to accommodate organisational changes; they are therefore adaptable, fluid, and flexible. Implementing an EDRM framework can dramatically reduce this flexibility (Hill & Jaquith, 2010).

E-DRM toolsets are often used in highly specialised areas such as the ones described in the above-mentioned case studies, as well as other legal and client communication arenas. Consequently, E-DRM deployments have been departmentalised and very few Enterprisewide deployments have been reported (Hill & Jaquith, 2010). They focus on the needs of specific business unit within an organisation and in most cases those business units reside outside of IT Security; this significantly reduces the need to integrate them with other security technologies such as DLP, content management, and IAM. Furthermore, the high costs of specialised plug-ins have retarded E-DRM market growth (Hill & Jaquith, 2010).

Another considerable factor in E-DRM lagging behind other security products is the lack of legislations and regulations that compel organisations to implement E-DRM in order to comply with such legislations (Hill & Jaquith, 2010).

2.6 Virtualised Desktop Infrastructure

Virtual desktop infrastructure refers to the hosting of a desktop operating system and applications within a virtual machine running on a hosted, centralised or remote server (Kroeker, 2009). This technology separates the programmes, applications, processes, and data from the physical machine using client-server model, where the technology could either be server-based or client-based (Petrović & Fertalj, 2009).

In a server-based virtualisation technology, the server runs multiple virtual machines instances and the user accesses the virtual machine by using a thin VDI client or simply through a web interface (Miller & Pegah, 2007). This permits the end-user to execute operating system and applications from a mobile device or thin client which exceeds the user hardware's ability to run. Furthermore, the information resides on the server and not on the client so that when the mobile device is lost, the information remains safe (Miller & Pegah, 2007).

In a client-based technology, since all the resources are hosted on the client, it is mostly implemented in situations where a user needs to work offline or when the user is exposed to inadequate bandwidth (Petrović & Fertalj, 2009).

2.6.1 Implementation Drivers for Virtualised Desktop Infrastructure

Virtualisation technology was first implemented in enterprises in the 1960s when IBM programmer, Jim Rymarczyk, was involved in the first mainframe Virtualisation project (Hand, 2012). This concept went unobserved for almost two decades until VMware revived this concept and soon extended to servers, storage and desktops. The driver towards virtualisation technology in general was never security, but cost: saving money, stretching the useful life of computing resources and increasing efficiency in provisioning infrastructure. The same applies with the driver towards the adoption of virtualised desktop infrastructure. It's about the total cost of ownership of the desktops, and not necessarily security (Zacharopoulos, Karatzas & Leon, 2012).

However, since virtual desktop infrastructure delivers centralised control and management of desktops to any mobile device, the explosive growth of mobile devices in the workplace not only spikes the demand for virtualised desktops, but appends security as another driver or key

factor towards the decision to implement virtual desktop infrastructure.Virtualised desktop infrastructure has the capability to present applications and desktops hosted in datacentre to any device thereby supporting the concept of BYOD and consumerisation of IT as described in Section 2.3.2 (Bourne, 2012). In a study conducted by Citrix in October, 2011, a majority of the surveyed organisations cited improved information security as one of the benefits of implementing virtualised desktops (Citrix, 2011). The other benefits are displayed in Figure 2-15 and Figure 2-16.

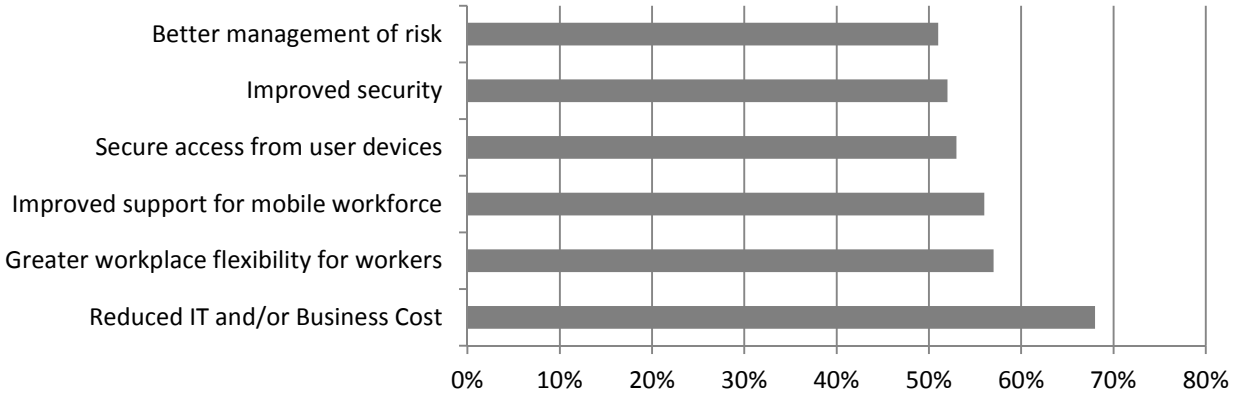


Figure 2-15: Perceived Benefits of Desktop Virtualisation (Citrix, 2011)

The other driver towards improved information security is the VDI's ability to centrally update and patch applications on distributed mobile devices in a timely fashion. This benefit is vital because a majority of exploits compromise known vulnerabilities where a patch has already been made available (Cosgrove, 2011).

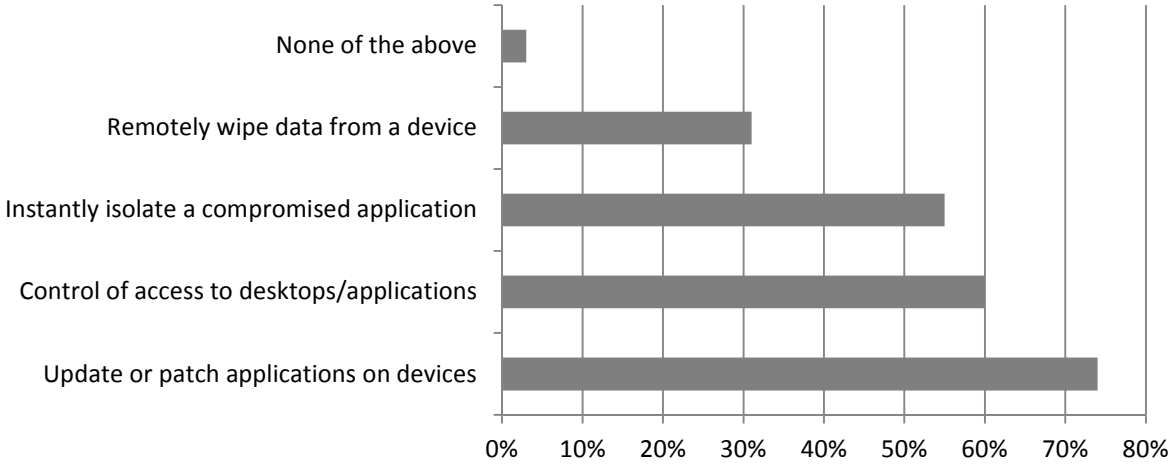


Figure 2-16: Security Benefits Delivered by Virtualisation through Centralized Desktop Management (Citrix, 2011)

Virtualised desktop Infrastructure can employ similar capabilities as that of E-DRM toolsets in that, through configured policies, information loss can be prevented by restricting the ability of users to save, print, copy, and otherwise distribute data (Petrović & Fertalj, 2009).

The centralised management of applications prevents users from installing their own applications, and thus prevents organisations from litigations caused by users installing unauthorised applications. An organisation is legally responsible for licensing any software application that is installed in its systems. So if a user installs an unauthorised application, the organisation is responsible for ensuring that the application is licensed (Posey, 2012).

User installed applications also increase the chances of malware infections and support costs (Posey, 2012). An unauthorised application might replace dynamic-link library (DLL) files and affect the way applications share code and other resources to perform application programme tasks. Furthermore, unauthorised applications can make registry changes that cause problems with other applications. The service desk technicians might not immediately spot these problems because they are initially unaware of the unauthorised application's existence.

2.6.2 Shortcomings of Virtual Desktop Infrastructure

Offline capability is at the core of VDI shortcomings (Phadmanabhan, 2010). There are many instances where users find themselves without Internet access and therefore unable to access the virtualised desktops residing on the data-centre. While this shortcoming can be alleviated by implementing a client-based virtualisation technology, this is, however, a less-secure option.

The protruding characteristic of VDI is the capability of consolidating computing resources into a data centre where they can be centrally managed. This characteristic neglects the risk of a single point of failure to such an environment (Phadmanabhan, 2010). If the servers in the data centre go down, all the virtualised desktops go down. This shortcoming can be alleviated with redundancy; however, this could increase complexity of the solution (Petrović & Fertalj, 2009). On the other hand, IT needs to ensure that adequate computing resources are available during peak hours by predicting the amount of resources to over-provision. In most cases, this over-provisioning is not adequate to accommodate peak capacity.

Moore's Law states that "Over the history of computing hardware, the number of transistors on integrated circuits doubles approximately every two years" (Moore, 1965). This trend can be similarly applied to virtualised desktops running at the data-centre as depicted in Table 2-5.

Table 2-5: Moore's Law Applied to Virtual Desktops in a Data centre

Year	VM's per Server	VM's per Rack	Estimated Cost per user
2012	70	1120	$400
2014	150	2400	$330
2016	300	4800	$260
2018	600	9600	$150

Source: (Phadmanabhan, 2010)

The above trend implies that as the servers become better and increasingly cost-effective; the cost of VDI will also drop. However, this prediction is only true in an ideal environment where the hosted applications remain the same. In a real-world situation, applications expand and continue to consume additional bandwidth, and thus negate savings from Moore's Law (Phadmanabhan, 2010).

VDI supports the concepts of consumerisation of IT and bring your own device (BYOD); however, there are still some problems with regards to management of mobile devices. A majority of organisations use VMware View client (with Persona Management for User Profile) to provide mobile employees with desktop access on iPads, Smartphones, and other personal devices. According to a survey conducted by VIBriefing on behalf of Virsto, 50% of the survey respondents use VMware View, followed by Citrix XenDesktops (Virsto, 2012).

It is evident from the number of problems related to VMware View posted on the VMware Community Forum[3]that VMware View is still unstable and that many IT Professionals find the Persona Management feature not mature enough. As a result, they turn to other third party products for managing user profiles at an additional cost (Wood, 2012). Companies often use Remote Desktop Protocol (RDP) or VDI to deliver Microsoft applications to mobile devices. But this isn't ideal because virtual desktops typically don't conform to most tablet and smartphone screens Furthermore, it is difficult to diagnose and troubleshoot problems with virtual desktops on any given platform.

VDI licenses are complex and difficult to manage and enforce. Many vendors have not overhauled their licensing rules to accommodate mobile devices (Botehlo, 2012; Bourne, 2012). For instance, up until July 1, 2010, Windows Client Software Assurance (SA) customers had to buy a separate license to access their Windows operating system in a virtual desktop infrastructure (VDI) environment (Botehlo, 2010). The same initiative now allows

[3]http://communities.vmware.com

non-Windows clients such as thin-clients to access virtualised desktops through Virtual Desktop Access licensing.

Virtualised desktops on mobile devices also comes with human challenges in that IT needs to educate the virtual desktop users, dictate the correct hardware to use and ensure that VDI policies are enforced (Wood, 2012).

There are VDI vendors like Citrix and Ceedo that support user installed applications. This creates a problem in resource consumption since virtualised desktops co-exist in a finite pool of hardware resources. Authorised applications are tested to ensure that they do not consume excessive CPU cycles, disk I/O or network bandwidth. An unauthorised application can disturb this gentle balance of hardware provisioning that is in place (Posey, 2012).

A survey conducted by VIBriefing on behalf of Virsto found that despite the large number of VDI projects initiated amongst medium-to-large IT organisations, VDI implementations still fail due to cost, performance and user-complaints (Greenfield, 2012). Figure 2-17 shows probable reasons for failure of launching VDI amongst 46% of the survey respondents.

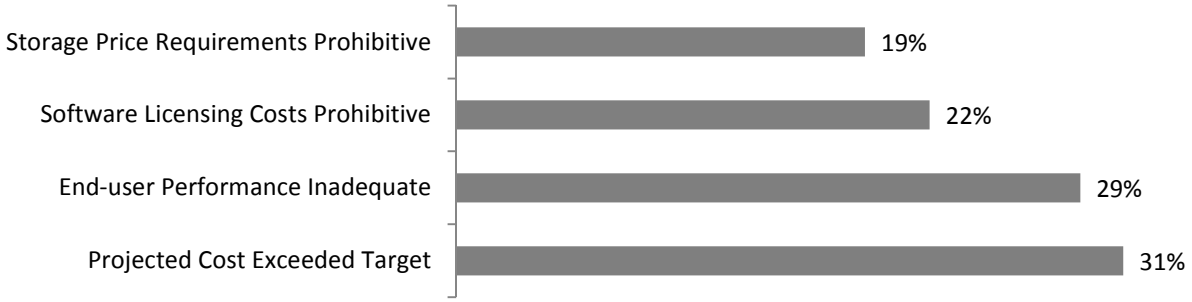


Figure 2-17: Reasons for Failure to Launch VDI (Virsto, 2012)

2.7 Mobile Device Management

Mobile Device Management (MDM) refers to technologies that are an emerging solution for centrally managing and securing both corporate-issued and personally-owned mobile devices by enterprise users. Additionally, the term is used to describe a system or solution for securing, monitoring, managing and supporting mobile devices deployed across mobile operators, service providers and enterprises (Mobile Device Management, 2011; Whatis.com, 2006). The MDM technologies cover mobile devices such as smartphones and tablets from various manufacturers yet often exclude laptops because the security controls available for laptops today are different from those available for smartphones, tablets, and other mobile device types (Souppaya & Karen, 2012). MDM software relies on over-the-air programming (OTA) to distribute updates; configuration and policy settings to a fleet of

mobile devices in a form of Binary SMS message (Gascón, Bielsa, Genicio & Yarza, 2011). These technologies emerged as a response to the implementation drivers described in Section 2.3, as well as the realisation that mobile devices require additional protection as their nature exposes them to a higher threat landscape than desktops and laptops (mostly used within the corporate infrastructure). Worldwide, there are less than 100 vendors providing MDM technologies while the market is quickly evolving with an expected increase in capability and maturity in the next few years (Redman, Girard & Wallin, 2011).

Table 2-6 lists the important security capabilities of MDM solutions that are a differentiator for leading MDM vendors. The list is drawn from the evaluation done by (Redman, Girard & Basso, 2012) and (Kane & Gray, 2012) on the top MDM vendor products.

Table 2-6: Key Security Capabilities of MDM

MDM Capability	Description
Enforced Password	Enforces strong password policy.
Selective Wipe	In an event of a device getting lost or stolen, the MDM solution deletes corporate information only and leaves personal data untouched.
Jailbreak/rooted Detection	Capability to detect Jailbroken and Rooted devices and prohibit them from connecting to corporate network.
Audit trail/Logging	Capability to capture and store events.
Application Verification	Capability to verify the origin of the downloaded application using integrity check.
Encryption	Capability to encrypt stored information on a file-level, OS-level, and device level.
Secure Connection	Capability to integrate with VPN solutions and to manage Certificates.
Application Whitelisting	Capability to allow only approved corporate applications to execute on the device.

2.7.1 Current State of Mobile Device Management

BlackBerry Enterprise Services has set a gold standard in the management and security of mobile devices, and Blackberry mobile devices are still the most supported enterprise devices (Kane & Gray, 2012). Figure 2-6 depicts the prominence of Blackberry as compared to other mobile vendors, especially in South Africa. A mobile device management product provided by a phone manufacturer, such as BlackBerry Enterprise Services, may always have more robust support for its native phones than third party products (Souppaya & Karen, 2012). Despite this, there are still a number of MDM vendors that do not support BlackBerry integration (Redman, Girard & Wallin, 2011). Most companies implement MDM solutions to

gain control of the new device types that are connecting to the network, that is, Android and iOS devices. As a result, MDM vendors focus on supporting these devices only with plans to support other platforms at a later stage (Kane & Gray, 2011). The level of security applied to these new platforms has not reached the level of security that has been traditionally applied to BlackBerry. Vendors and companies alike are aware of the security concerns with Android and iOS platforms, consequently companies deliver only basic services (e.g. email, calendar, contacts) to their employees, while vendors offer basic security features (e.g. remote wipe, device lock) with plans to add more functionality as these platforms and MDM solutions mature (Kane & Gray, 2011) .

Allowing IT to support heterogeneous device platforms has cost-savings implications. Currently the employees have to contact their service provider for support when their device breaks instead of contacting IT, thus reducing the amount of time spent supporting these devices.

IT Support staff are not only faced with the challenge of supporting multi-platform mobile devices, but different mobile applications as well. Many IT departments and IT service providers have responded to this challenge by segmenting their workforce and assigning a different service level support (e.g. Platinum, Silver, Gold, and Bronze support) to each various segment (Kane & Gray, 2011). For instance, the segment that uses tablets may have access to different service level support and applications that compare to segments that use workstations, while segments that use corporate-issued devices may enjoy a greater level of support (platinum) than the segment that brings their own devices.

2.7.2 Shortcomings of Mobile Device Management

The Mobile Device Management is currently only focusing on the management of mobile devices and their security, while ignoring the growing pool of mobile applications (Kane & Gray, 2011). Companies have a desire to deliver their own applications as well as device-specific applications (e.g. iTunes) to smartphones and tablets and to be able to manage those applications from a unified portal. The application management capabilities of MDM solutions, especially those supporting Android and iOS, cannot meet organisational application management requirements (Kane & Gray, 2011). As a result, organisations are forced to look at third party tools (such as Apperian, AppCentral, and Partnerpedia) to manage more than just calendar, email, and contacts.

2.8 Summary

In this chapter we expanded on the challenges and drivers introduced in Chapter 1, reviewed related work on the key models that were designed for a data-centric model, and visited the three case studies describing the technologies implemented to successfully achieve a data-centric security model. The research objective of analysing the shortcomings of each technology in an effort to identify gaps was also achieved.

The introduction of mobile devices extends organisational information to mobile devices and consequently presents numerous risks surrounding corporate information. Related work on pre-existing models highlights a number of concepts that could be useful in mitigating current threats brought about by mobile devices. Given these risks, the drivers towards the implementation of information-security controls are inevitable.

An analysis on these controls reveals a few general issues:

1. None of the evaluated technologies have the *combined* ability to do cross-organisational authentication, policy enforcement, data leakage protection and federated identity management.
2. Based on the evaluation of E-DRM vendor products conducted by (Hill & Jaquith, 2010), E-DRM has very strong information protection capabilities; however, this capability is not yet widely extended to mobile devices.
3. VDI proved to be adequate in protecting information outside the corporate infrastructure; however, its implementation results in too many shortcomings, as described in Section 2.7.2.
4. MDM toolsets possess strong information protection capabilities; however, they lack granulated, user-based access rights to information found in E-DRM.

The next chapter proposes an ideal data-centric security model intending to minimise the above-mentioned gaps using existing technology.

Chapter 3 : Architecture Model for Data-centric Security

3.1 Introduction

This chapter introduces the architecture framework required to implement data-centric security in a utopian environment. The environment is described as utopian since the research proposes a model that can be implemented in an ideal environment. An architecture framework is a consistent set of principles, policies, capabilities and standards that establishes the direction and vision for the development and operation of the organisation's business information systems so as to ensure alignment with and support for the business requirements (Lynas, 2012). This architecture model does not take into account the organisation's operating regimen or culture, management style, management standards, and management processes because all these will change over time. However, it attempts to resolve the piecemeal technology implementations described in Chapter 2.

The chapter begins by presenting the utopian architecture framework, which then broken down and explained (in subsequent sections) according to its architecture layers.

3.2 Utopian Reference Architecture Framework

The utopian reference architecture framework is fundamentally based on Sherwood Applied Business Security Architecture (SABSA) Framework. As shown in Table 3-1, SABSA follows closely to the work done by John Zachman and both models identify similar architecture layers (Zachman, 1987). However the two models were developed independently of each other (Sherwood, Clark & Lynas, 2005). SABSA is chosen as the base reference architecture, because like the Zachman framework, it takes into consideration the business requirements as well as the strategy. However, SABSA is more adapted to security. The Zachman framework was originally designed for Enterprise Architecture (Zachman, 1987), whereas SABSA leverages on Zachman's Enterprise Architecture segmentation into an identical multi-dimensional matrix that systematically describes and defines risks and threats within the paradigm of information security architecture. Furthermore SABSA ensures that any technological security element can be justified by reference to a risk-prioritised business requirement. For the reason that SABSA is built to drive complex design solutions (Sherwood, Clark& Lynas, 2005); an assumption is made that a data-centric security solution designed to mitigate risks that mobile devices bring to corporate information is complex, and that SABSA will offer a framework within which this complexity is broken into apparent simplicity.

Table 3-1: Mapping SABSA to Zachman Framework

SABSA	Zachman Framework
Contextual Security Architecture	Scope (Contextual) – Planner
Conceptual Security Architecture	Business Model (Conceptual) – Owner
Logical Security Architecture	System Model (Logical) – Designer
Physical Security Architecture	Technology Model (Physical) – Builder
Component Security Architecture	Detailed Representations (Out-of-Context) - Subcontractor
Operational Security Architecture	Functioning Enterprise

Source: (Zachman, 1987)

Table 3-2 shows the SABSA matrix that formulates foundation of this proposed utopian data-centric architecture framework.

The Trust model concept introduced by Tsang *et al.* (2004) in Section 2.4.1 is enhanced using SABSA's security domain concept. Likewise, the "Who? Knew What? And When? Approach" proposed by Tsang *et al.* (2004) is expanded by the SABSA framework through the introduction of three additional questions --"Why, How, and Where" -- as illustrated in Table 3-2. That is, while the TecSec Incorporated Data-centric Security Model poses three questions (Who?, What?, and When?), the SABSA framework poses six questions instead (What?, Why?, How?, Who?, Where? and When?).

Table 3-2: SABSA Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tool & Standards	Process Tools & Standards	Personnel Management Tool& Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Service Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

Source: (Lynas, 2012)

The proposed utopian model suggests a similar notion offered by Bilger *et al.* (2006) on IBM DCSM of applying the access control policies to the actual data, where the access policies are in turn driven by business requirements and defined using organisational roles. The proposed utopian model, however, expands the only single layer proposed by Bilger *et al.* (2006) called

the Data Control Layer into multiple layers, as shown in Table 3-3, in order to provide clear architecture views where each control lies.

Table 3-3: SABSA Architecture Views

Business View	Contextual Architecture
Architect's View	Conceptual Architecture
Designer's View	Logical Architecture
Builder's View	Physical Architecture
Tradesman's View	Component Architecture
Service Manager's View	Operational Architecture

Source: (Lynas, 2012)

The utopian architecture framework is illustrated in Figure 3-1 and each architecture layer is explained in the subsequent sections.

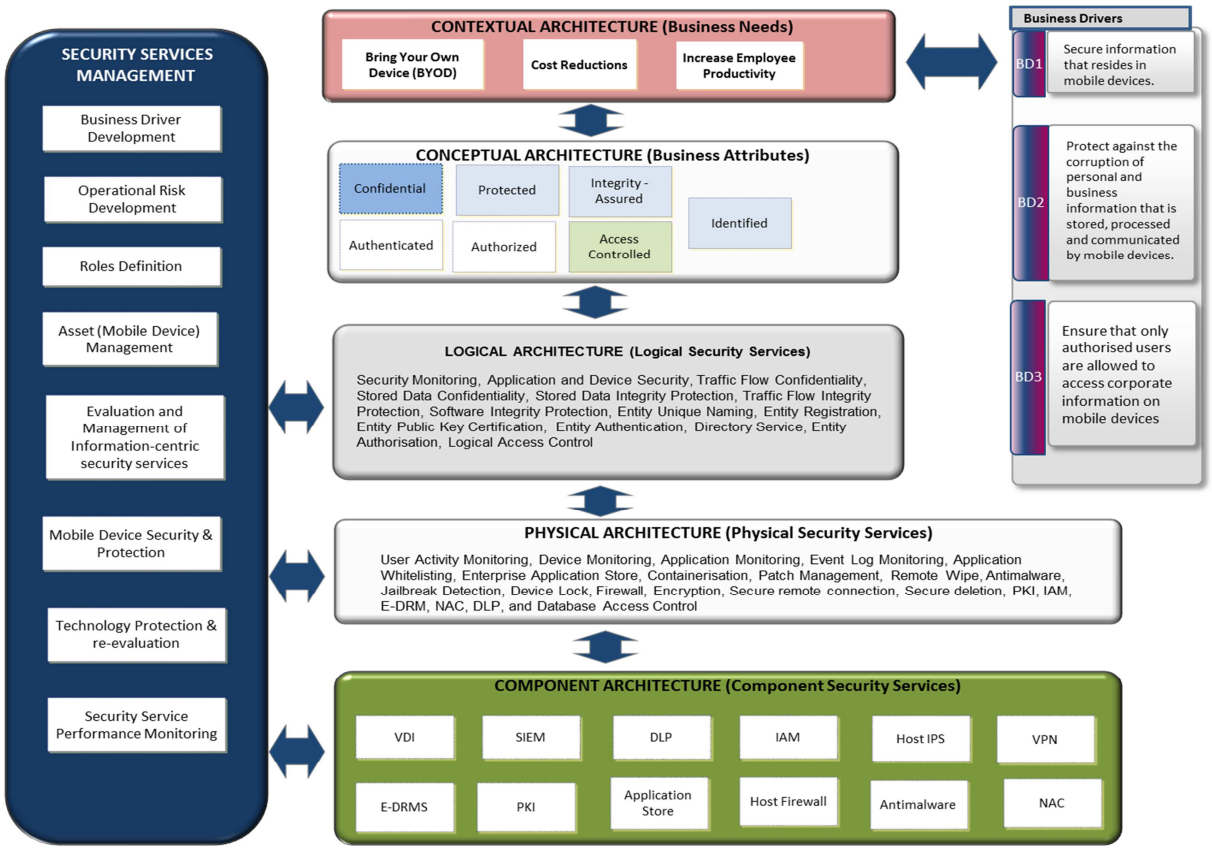


Figure 3-1: Utopian Reference Architecture Framework Based on SABSA

3.3 Contextual Architecture

The contextual architecture captures and presents the full set of requirements for the scope of the assignment. The drivers for data-centric security model are described in Section 2.3. The full set of business requirements is contextualised into business security context as shown in

Table 3-4, where BD1, BD2, and BD3 represent the three summarised high-level business drivers for security. This is a fundamental step in ensuring that the resultant reference architecture framework does not only address the business requirements, but also addresses the business requirements for security.

Table 3-4: Contextual Architecture for Data-centric Security

Business Requirements	Business Drivers for Security
Allow employees to bring their own devices to reduce cost of corporate issued devices (BYOD). Increase employee productivity by allowing employees to use their personal device to work from anywhere.	**BD1**– Secure corporate information that resides in mobile devices. **BD2**– Protect against the deliberate, accidental or negligent corruption of personal and business information that is stored, processed and communicated by mobile devices. **BD3**– Ensure that only authorised users are allowed to access corporate information on mobile devices.

The business drivers for security focus on protecting information stored on mobile devices and information that is accessed and processed through mobile devices. The business drivers for security ensure that the business drivers are met. BYOD has the business requirement of reducing the capital expenditure (CAPEX) costs associated with user ownership of the device. Another business driver for mobile computing is the increase in user productivity due to easy access to work, even while commuting. A study conducted by (Kalkbrener & McCampbell, 2011) showed that mobile devices increased productivity by 62.5 percent of the time.

3.4 Conceptual Architecture

In this architecture layer, the organisation determines the strategy for treating risks associated with mobile devices and establishes a strategy for meeting the controls and enablement objectives.

An Attribute is a conceptual abstraction of a real business requirement confirmed as part of the business contextual architecture (Sherwood, Clark & Lynas, 2005). Attributes conceptualise the business requirements and measure performance in a way that is applicable to relevant stakeholders, providing a link between the requirements and the technology

design. Each business driver for security described in Table 3-4 is mapped to its supporting attribute as shown and explained in Table 3-5.

Table 3-5: Drivers to Attributes Mapping

Business Driver	Supporting Attribute	Attribute Definition
BD1– Secure corporate information that resides in mobile devices.	• Protected • Confidential	**Protected:** The user's information and access privileges should be protected against abuse by other users or by intruders. **Confidential**: The confidentiality of corporate information in accordance with mobile security policy
BD2– Protect against the deliberate, accidental or negligent corruption of personal and business information that is stored, processed and communicated by mobile devices.	• Integrity-assured	**Integrity-assured:** The integrity of information should be protected to ensure that it has not suffered unauthorised modification, duplication or deletion.
BD3– Ensure that only authorised users are allowed to access corporate information on mobile devices.	• Identified • Access-controlled • Authenticated • Authorised	**Identified:** Each entity that will be granted access to system resources and each object that is itself a system resource should be uniquely identifiable such that there can never be confusion as to which entity or object is being referenced. **Access-controlled**: Access to information and functions within the mobile devices should be controlled in accordance with the authorised privileges of the party requesting the access. **Authenticated**: Every party claiming a unique identity should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity. **Authorised:** The system should allow only those actions that have been explicitly authorised.

The attributes are chosen from the original SABSA Business Attributes Taxonomy developed by (Sherwood, Clark& Lynas, 2005) that focuses specifically on ICT systems and their environments. See APPENDIX A.

The seven attributes outlined in Table 3-5 are selected because of their relevance to data-centric security based on the risks that mobile devices bear to corporate information.

Although **Identified** generally forms part of **Authenticated**, this research aims to emphasise the important distinction between identification and identity as per research done by (Roussos, Peterson& Patel, 2003) in a mobile business environment. The success of mobile business infrastructure is dependent on the pivotal shift from identification to identity; the concept of identification is static whereas identity is dynamic and governed by trust (Roussos, Peterson& Patel, 2003). This research focuses on Identity and its dynamic characteristic of transitioning (Roussos, Peterson & Patel, 2003):

- from one device to another device;
- from one location to another location; and
- from one context to another context (time, date, location).

A risk analysis is performed on each of the seven attributes to assess the negative impact (threat) or positive impact (opportunity) it has on business. This impact-based approach to explain the business risks is preferred because it uses language that is well understood by business. The threat-based approach is not ideal since technical threats are not well understood by stakeholders. A negative impact is expressed as the reduction in attribute performance or a failure to attribute performance target, whereas a positive impact is expressed as an increase in attribute performance. Attribute targets determine the risk threshold for acceptable risk, that is, failure to meet the attribute performance target represents an unacceptable outcome. Meeting the attribute target is the same as meeting the business objective. A second performance target is assigned as shown in Figure 3-2 to detect early warnings that are signalled when the second key risk indicator threshold (KRI threshold 2) is exceeded.

These key risk indicators are then employed to create measurable approaches and metrics to each attribute and displayed in a form of a dynamic risk dashboard as shown in Figure 3-3.

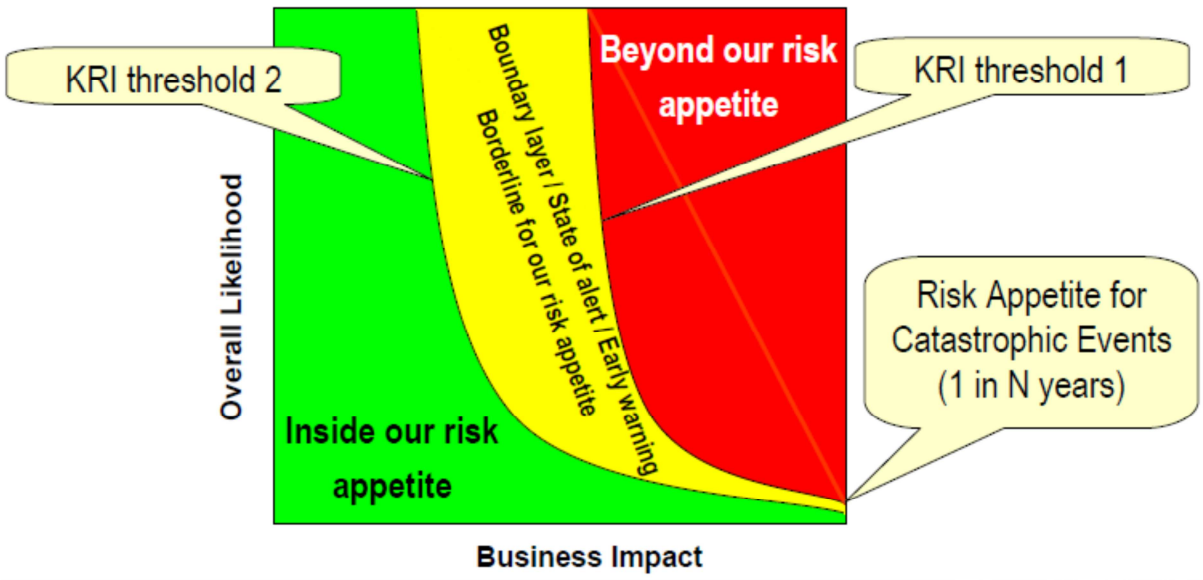


Figure 3-2: SABSA Risk Appetite Threshold (Lynas, 2012)

A traffic light reporting of red colour means that the identified attribute has exceeded the organisation's risk appetite and requires urgent attention.

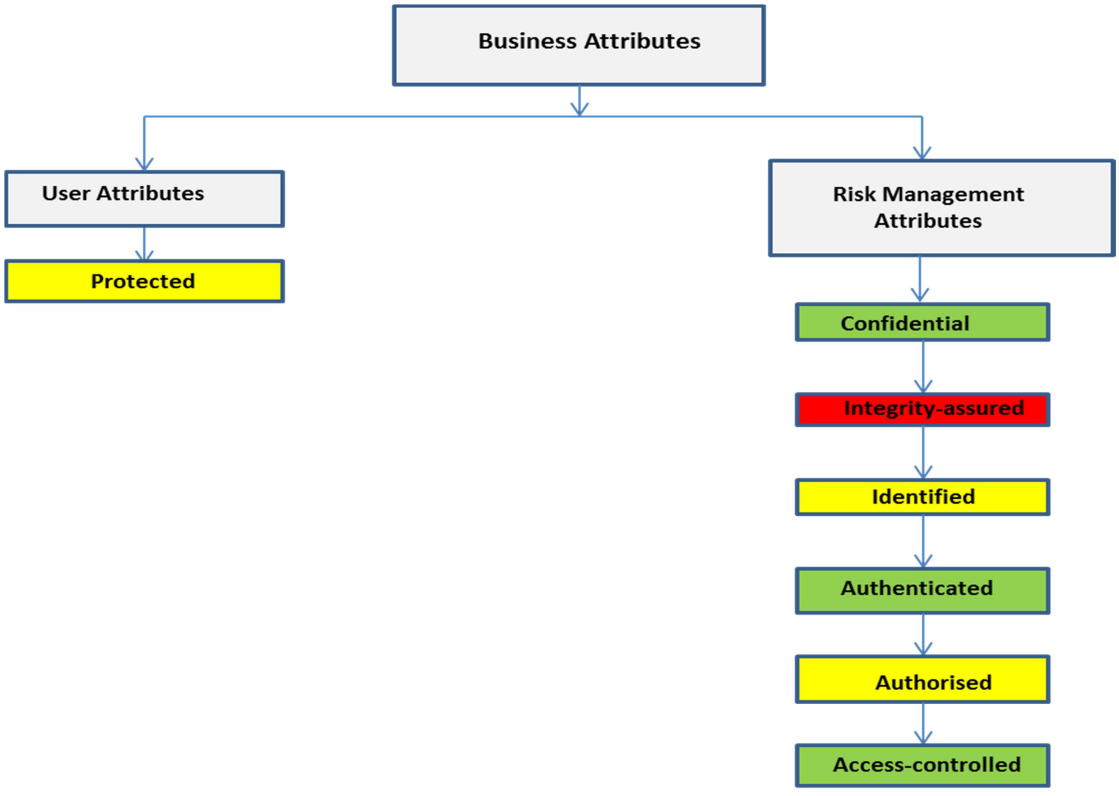


Figure 3-3: Dynamic Risk Dashboard

3.5 Logical Architecture

The logical architecture layer provides a designer's view of the ICT Systems. In this layer, a mobile security policy is developed based on the business requirements specified in the contextual layer. The operational risks and opportunities are assessed prior to the development

of a mobile security (Lynas, 2012). The mobile security policy translates the business requirements for security into logical services that can be applied, monitored and measured. The logical services specified in the security policy do not make any particular reference to the physical mechanisms that will deliver the service. A security policy exists on different architecture layers and thus SABSA adopts a hierarchically layered security policy architecture approach, where each layer is derived from the previous layer with traceability, as shown in Figure 3-4.

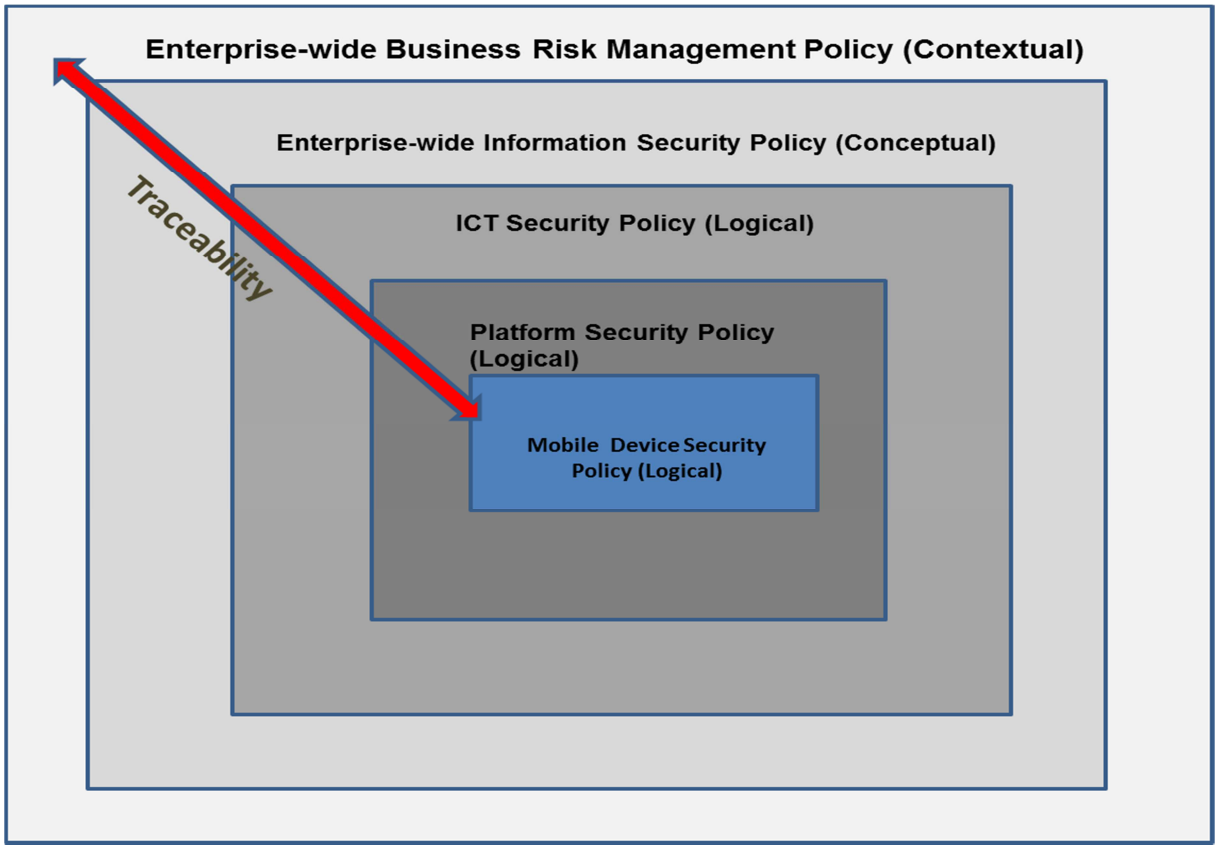


Figure 3-4: Inter-domain Policy Relationship (Lynas, 2012)

On top of the hierarchy, the Enterprise-wide business risk management policy and Enterprise-wide Information Security Policy provide directives to the business to manage the risks and opportunities associated with sharing information outside the corporate infrastructure, according to defined business risk appetite and using standard risk management methods. The ICT Security Policy mandates the IT department to comply with Enterprise-wide Information Security Policy and to manage information risks and opportunities according to defined appetites and using standard methods. The Platform Security Policy mandates the IT department to manage risks associated with each platform, in compliance with ICT Security Policy, and to deploy relevant platform security services. The Mobile Security Policy ensures

that risks to a particular mobile device platform are mitigated in compliance with Platform Security Policy, and by deploying relevant mobile device security services.

The defined policies clearly distinguish the usage of employee-owned devices and corporate-issued devices and aim to recognise the evolution of the mobile endpoint market. Recognising the evolution of the endpoint market ensures that the developed policies are technology and device agnostic. Organisations that insist on developing device-specific policies often fail to keep up with the rapidly evolving mobile endpoint market, resulting in the device-specific policy being completely outdated at the time of publishing (Disabato & Berenbaum, 2012).

Once the policies are defined, the logical security services required to deliver on the above-mentioned attributes are defined. For each attribute, a list of security services is defined as shown in Table 3-6.

Table 3-6: Logical Security Services to Deliver the Required Attributes

Attribute	***Protected***	***Confidential***	***Integrity-Assured***	***Identified***	***Authenticated***	***Authorised***	***Access-Controlled***
Logical Security Service	Security Monitoring Application Security Device Security	Traffic Flow Confidentiality Stored Data Confidentiality	Stored Data Integrity Protection Traffic Flow Integrity Protection Software Integrity Protection	Entity Unique Naming Entity Registration Entity Public Key Certification	Entity Authentication	Directory Services Entity Authorisation	Logical Access Control

The rationale behind the selection of each security service is articulated for each attribute:

Protected

- **Security Monitoring**: refers to constant monitoring of access to information by mobile devices to ensure that information remains protected (e.g. Mobile Security Intelligence)
- **Application Security**: deals with security services that build protection in the application layer. In this architecture layer, these services are specified on the high level within the mobile device security policy, or separately within software development lifecycle (SDLC) policy.
- **Device Security**: refers to services that ensure the protection of the actual device, for instance, to locate, lock, and wipe information on the mobile device in an event theft or loss.

Confidential

- **Traffic Flow Confidentiality:** refers to security services put in place to ensure that the traffic flowing between the mobile device and the corporate network is protected and information remains confidential.
- **Stored Data Confidentiality:** refers to security services put in place to ensure that information stored on the mobile device is protected and remains confidential (e.g. using encryption).

Integrity-assured

- **Stored Data Integrity Protection:** refers to security services put in place to detect malicious modifications of key files stored on mobile devices (Sivathanu, Wright& Zadok, 2005).
- **Software Integrity Protection:** refers to security services put in place to detect changes in program code on downloaded software due to code manipulation, virus infections, or otherwise (e.g. MD5, SHA-1).
- **Traffic Flow Integrity Protection:** refers to security services put in place to provide data origin authentication and connectionless integrity, such as Encapsulation Security Payload (ESP) protocol, or Secure Socket Layer (SSL) (Kent, 2005).

Identified

- **Entity Unique Naming:** refers to security service that ensures that both the user and the device can be uniquely identified within the Certificate Authority (CA) domain.
- **Entity Registration:** refers to security service that binds the entity to its public key through a registration process done by the Registration Authority (RA) to ensure non-repudiation (Corella, 2004).
- **Entity Public Key Certification:** refers to the process of issuing identity certificates and binding of public key to the entity through digital signatures (Canetti, 2004).

Authenticated

- **Entity Authentication:** refers to the process of determining, confirming or verifying the attribute of an entity to whom or what it is declared to be (Needham & Schroeder, 1978). The entity could be a device, application or user.

Authorised

- **Directory Services:** refers to a shared central information repository that stores, organises, and manages access to resources or objects on the directory server (Carter, 2003).
- **Entity Authorisation:** refers to the process of defining access control rules for authenticated entities in order to determine whether to grant or deny access requests (Ashley, Vandenwauver& Siebenlist, 2000). Access is authorised during the definition of access policies or access control rules and the access policies are enforced through denying and approving of access requests.

Access-controlled

- **Logical Access Control:** refers to mechanisms that regulate access to information systems resources based on what the identity is authorised to access.

3.6 Physical Architecture

The physical architecture layer provides the Builder's view of the ICT systems. On this layer, the physical security mechanisms that deliver the logical security services (specified in Logical Architecture) are defined. The actual security practices and procedures are derived from the security policies developed in the logical architecture layer, with traceability. Security Policy Documentation exists on each architecture layer as illustrated in Figure 3-5.

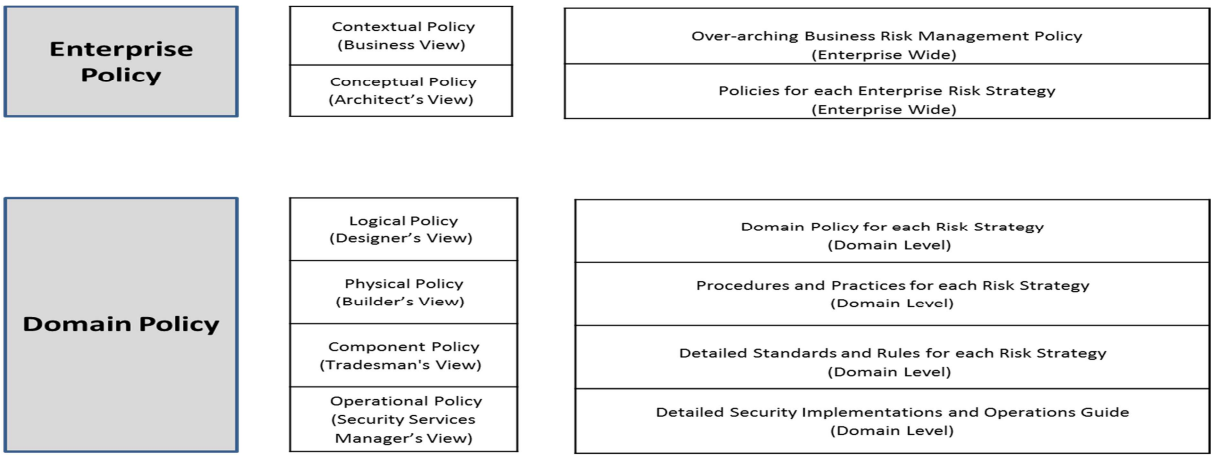


Figure 3-5: SABSA Policy Architecture Framework (Sherwood, Clark & Lynas, 2005)

The high-level architecture layers deal with enterprise wide security policies and the lower-level architecture layers focus on security policies pertaining to a specific security domain (Sherwood *et al.*, 2005). A detailed description of a domain is provided in Section 2.4.3. The domain-level polices are created by the individual domain owners that act as Policy Authorities with clear ownership of the risk in that domain (Sherwood, Clark& Lynas, 2005).

These domain-level policies also define how a domain interacts with other domains. In the physical architecture layer, the security procedures and practices outline the actual physical mechanisms required to deliver on the attributes as depicted in Table 3-7.

Table 3-7: Physical Security Services to Deliver the Required Attributes

Attribute	***Protected***	***Confidential***	***Integrity-Assured***	***Identified***	***Authenticated***	***Authorised***	***Access-Controlled***
Physical Security Service	User Activity Monitoring Device Monitoring Application Monitoring Event Log Monitoring Application Whitelisting Enterprise Application Store Containerisation Patch Management Remote wipe Antimalware Jailbreak/Rooted Detection Device Lock Firewall	Data Encryption (Field-level, File-level, and Application-level) Message Content Encryption Secure Remote Connection Secure Deletion	Public Key Infrastructure Checksumming Hashing	Digital Certificates	Digital Certificates	Identity and Access Management	Information Rights Management Database Access Control Network Access Control Identity and Access Management DLP Data Classification and Reclasification

Each attribute has a selection of logical security services required to deliver on the attribute; likewise, the logical security services in turn have its own physical security mechanisms. That is, the physical security mechanisms implemented in this layer are derived from the Logical security architecture layer. While the ownership of the device is considered on the logical architecture layer during the development of the mobile device security policy, the decision whether to implement selective wipe or total wipe is taken on the physical security architecture layer. This decision is influenced by privacy laws within that Country. If the device is employee-owned, privacy regulations may dictate the enterprise not to issue the remote wipe command on the premise that the data resident on the mobile device is owned by the employee and should therefore be left intact (Glazer, 2012). The physical security

mechanisms for the logical security services required to deliver on the protected attribute are listed and explained in Table 3-8.

Table 3-8: Mapping of Logical Service to Physical Mechanisms – Protected

Logical Security Service (Designer's View)	Physical Security Mechanisms (Builder's View)	Brief Description of Physical Security Mechanism
Security Monitoring	User Activity Monitoring	A mechanism that provides IT with real-time visibility into the users that access the corporate network as well as user behaviour.
	Device Monitoring	A mechanism that provides real-time visibility into the devices (device type, operating system, model, etc.) that access the corporate network, as well as device usage patterns. This enables the generation of an inventory list of all mobile devices in order to block any mobile devices that are unauthorised to access the network.
	Event Log Monitoring	A mechanism for appending event messages to event logs, in real-time, as soon as they are emitted by the log client in order to perform event correlation or to analyse the events at a later stage (Vaarandi & Tehnikaülikool, 2005). Event correlation is a real-time event processing task that assigns new meaning to a set of events taking place within a predefined time interval (Jakobson & Weissman, 1995)
Application Security	Application Monitoring	A mechanism that provides visibility into the variety of applications running on employee devices.
	Application Whitelisting	A mechanism to prevent users from executing applications that are untrusted or unapproved (e.g. affect employee productivity) or do not meet regulatory compliance (Huh, Lyle, Namiluko& Martin, 2011).
	Enterprise Application Store	A mechanism to provision applications through an internal enterprise self-service model where IT maintains security and administrative control of what applications a user can request (Polte, 2012). Prohibited applications are placed on the application quarantine and access is monitored (Basson & Redman, 2011).
	Containerisation	A set of mechanisms that isolate personal content from corporate content on the mobile device through granular control and policy enforcement (Basson & Redman, 2011). The policy also prevents the export of application data from the container, and prohibits copying pasting, thereby enforcing data leakage prevention (Basson & Redman, 2011).
	Patch Management	A mechanism to remove or prevent a threat's ability to compromise vulnerability in an asset by installing a piece of software code to update the application product (White, 2007).
Device Security	Remote wipe: Selective wipe and total wipe	Selective wipe refers to the mechanism to remotely delete corporate data while leaving

		personal data untouched (Kane & Gray, 2012). Total wipe, commonly known as hard wipe, refers to mechanisms to remotely delete all the data on the mobile device with no chances to recover the data after deletion (Basson & Redman, 2011)
	Jailbreak/Root Detection	Refers to mechanisms that allows for the detection of Jailbroken and Rooted devices (Basson & Redman, 2011)
	Device Lock	A mechanism to lock the device after a certain time of inactivity (Basson & Redman, 2011).
	Antimalware Software	Refers to software used to detect and eradicate malware.
	Firewall	Refers to a packet filtering application that monitors ingress and egress over-the-air or wired TCP/IP traffic and denies or allows traffic based on predefined or custom filters (Qiu, Zhou& Bao, 2004).

Infrastructure-centric security forms a foundation for this proposed reference architecture model. This means that an implementation of mobile security architecture requires some basic level of security such as firewall, patch management or NAC. An infrastructure with inadequate level of security will yield weak mobile security architecture. The physical security mechanisms for the logical security services required to deliver on the confidential attribute are listed and explained in Table 3-9.

Table 3-9: Mapping of Logical Services to Physical Mechanisms – Confidential

Logical Security Service (Designer's View)	Physical Security Mechanisms (Builder's View)	Brief Description of Physical Security Mechanism
Stored Data Confidentiality	Data Encryption (Field-level, File-level, and Application-level)	A mechanism that renders the device hard disk or selected folders and files unreadable in an event of device theft or loss.
	Secure Deletion	Mechanism to delete data on storage media by either using software or by physically destroying media (Gutmann, 1996).
Traffic Flow Confidentiality	Message Content Encryption	A mechanism that secures the delivery of sensitive electronic communication to its destination through encryption.
	Secure Remote Connection	A mechanism to enable a secure encrypted tunnel between the device and the corporate asset or application.

The physical security mechanisms for the logical security services required to deliver on the Integrity-assured attribute are listed and explained in Table 3-10.

Table 3-10: Mapping of Logical Services to Physical Mechanisms – Integrity-Assured

Logical Security Service (Designer's View)	Physical Security Mechanisms (Builder's View)	Brief Description of Physical Security Mechanism
Stored Data Integrity Protection	Checksumming	Checksumming refers to a mechanism for conducting data integrity check by computing a checksum value for disk data and comparing the stored value and newly computed value in order to verify that the data that is read has not been altered (Sivathanu *et al.*, 2005). Host Intrusion Detection Systems (e.g. Tripwire) also use checksums to detect unauthorised modification or replacement of key binary files by custom malware (Sivathanu *et al.*, 2005).
Traffic Flow Integrity Protection	Public Key Infrastructure	A mechanism for enforcing integrity, confidentiality, authentication and non-repudiation through the distribution and use of public keys and digital certificates (Corella, 2004).
Software Integrity Protection	Hashing	A mechanism for verifying application integrity and ensuring that the downloaded application has not been modified. Hashing functions like MD5 and SHA-1 are widely adopted because of their randomness and collision resistant features (Sivathanu *et al.*, 2005).

The physical security mechanisms for the logical security services required to deliver on the **Identified** and **Authenticated** attributes are the identity certificates or digital certificates. Following a successful registration of user with the CA domain and binding of the unique user identity to the public key, the certificate for the device is generated. The same certificate is used to authenticate the user and the device to other internal corporate resources such as VPN servers and email servers such that when the certificate is revoked, the device immediately losses access to the corporate resources. The certificate information (distinguished name) is stored in a Directory Service such as Identity and Access Management tool that maps the certificate with the user object on the Directory structure.

In this utopian model, the Identity and Access Management (IAM) solution acts as the physical security mechanism for the logical service required to deliver on the **Authorised** as well as the **Access-controlled** attribute. IAM is defined in Table 3-11. In addition to acting as a data and retrieval for user identities, the IAM determines what the mobile identity can perform (authorise) within the enterprise (McQuaide, 2003). Furthermore, since the Data-centric security model requires information to be protected throughout its lifecycle, the IAM manages mobile identities throughout their life cycle, until termination. The physical security mechanisms for the logical security services required to deliver on the Access-controlled

attribute refer to mechanisms that apply the access-control policies or access rights to the actual data – See Table 3-8.

Table 3-11: Mapping of Logical Services to Physical Mechanisms – Access-controlled

Logical Security Service (Designer's View)	Physical Security Mechanisms (Builder's View)	Brief Description of Physical Security Mechanism
Logical Access Control	Information Rights Management	Refer to Section 2.5
	Database Access Control	Refers to mechanisms that regulate access to database for a user, server or group of users.
	Network Access Control	A mechanism restricting access to network resources on condition that the device is configured to meet organisational security policies.
	Identity and Access Management	Refers to security services for managing digital identities, their authentication, as well as how they are authorised into corporate systems (Witty, Allan, Enck& Wagner, 2003).
	Data Leakage Protection	Refers to security services that enable content-aware and context-aware security policies to control access to sensitive data on devices, and to control unauthorised dissemination of corporate information through containerisation (Lawton, 2008b). See Table 3-8 for definition of containerisation.
	Data Classification and Reclassification	Refers to framework for classification of information based on its level of sensitivity as well as its value within the organisation as stipulated in the organisation's information security policy (Markiewicz, 2011). This assists in developing standard security controls for controlling access to classified data. Reclassification is performed on an ongoing basis to reassess the assigned classification to ensure that it is still consistent with the changes in legal and contractual obligations as well as changes in data usage and significance within the organisation (Markiewicz, 2011)

In this architecture phase, the logical descriptions that were defined in the Logical Architecture layer were turned into technology models (physical elements) that are used in the construction of the data-centric solution. Each physical security mechanism that forms part of the overall solution requires specialised skills and specific products to construct the planned

solution. The implementation of the solution entails integrating these skills and products as described in the component architecture layer.

3.7 Component Architecture

The component architecture layer provides the Tradesman's view of the ICT systems. It is in this layer that the physical mechanisms described in the Physical Layer are integrated in the construction process by a team of subject matter experts equivalent to Tradesmen. These Tradesmen work with specialised products and systems components that maybe hardware components or software components; hence, Component Architecture Layer.

This section starts by listing the ICT security components required to deliver on the seven attributes. Each component is then discussed to explain the rationale behind its selection as well as its relevance to the corresponding physical mechanisms in order to ensure traceability. Table 3-12 lists the ICT security components required to deliver on the seven attributes.

Table 3-12: Component Security Services to Deliver the Required Attributes

Attribute	***Protected***	***Confidential***	***Integrity-Assured***	***Identified***	***Authenticated***	***Authorised***	***Access-controlled***
Component Security Service	SIEM VDI Enterprise Application Store MDM Patch Management tools Antimalware tools Host Firewall	E-DRM SSL/TLS and S/MIME VPN Shredding/Physical Destruction/Degaussing; Crypto Shredding WPA	PKI tools Host IPS MD5/SHA-1 MDM Mobile Application Tunnel	Digital Certificates	Digital Certificates	IAM tools	E-DRM Database Access Control tools Network Access Control tools IAM tools DLP

The utopian model proposes an architecture model where Mobile Device Management is the core technology towards mitigating the risks associated with mobile devices in the Enterprise. MDM integrates with other technologies, as shown by the dotted lines in Figure 3-6. The model depicted in Figure 3-6 proposes a defence in depth strategy where layers of security controls are placed between users and enterprise information. This strategy, with its origins in Military, suggests multiple layers of defence mechanisms between the adversary and the target (information) with each mechanism offering a distinctive impediment to the adversary (Luddy, 2010).

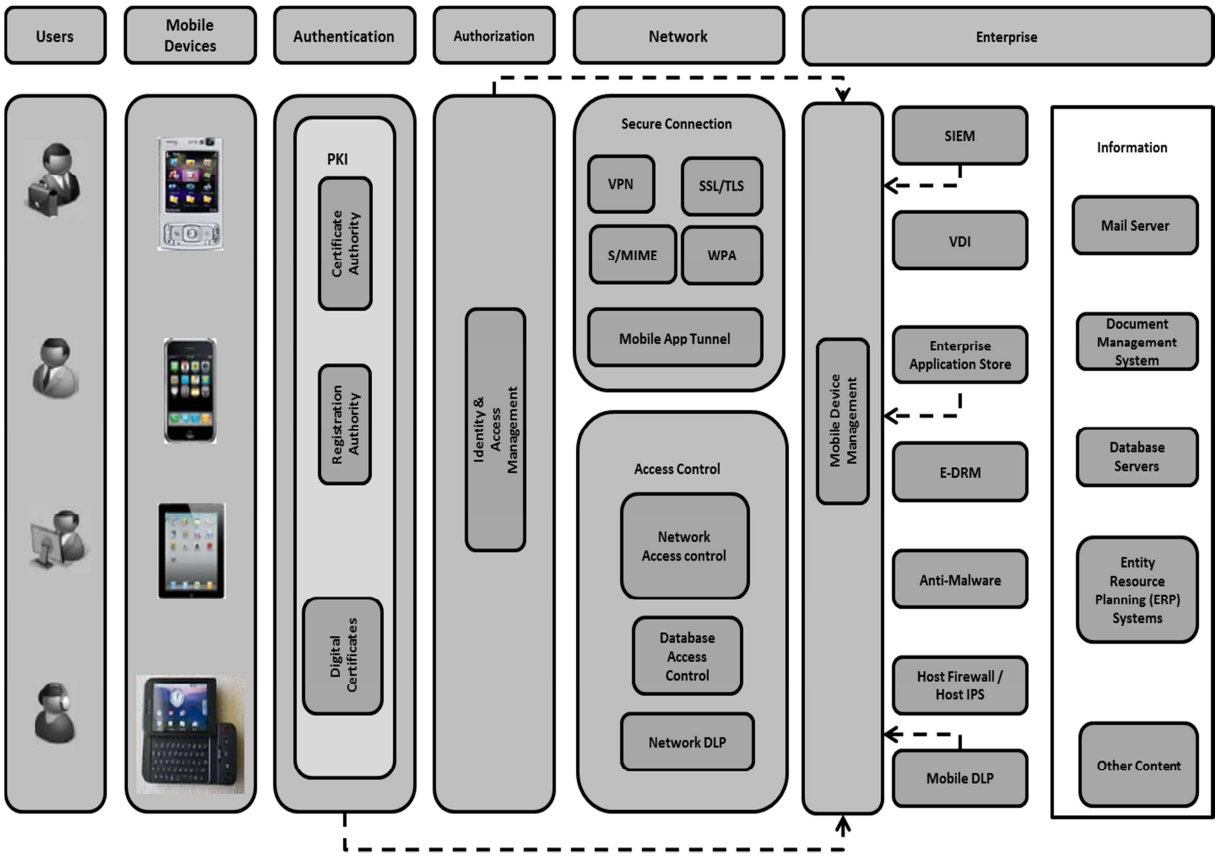


Figure 3-6: Mobile Security Architecture in a Utopian Environment

The integration of MDM with other technologies avoids a situation of implementing multiple isolated security technologies that have little or no inter-operability with one another. All MDM components (that is, the MDM Gateway and MDM server and database containing user information), are housed inside the enterprise and not on the DMZ where they could potentially be exposed to external threats.

The utopian mobile security architecture proposes public key infrastructure as opposed to a secret key technique. The latter technique requires a secret key to be shared (in an out-of-band fashion) between the mobile device and the network provider prior to any cryptographic operations taking place (Dankers, Garefalakis, Schaffelhofer & Wright, 2002). This approach is only ideal in an environment where there is already a pre-established relationship between the two entities, and is not ideal in a dynamic environment where one of the entities (a mobile device) changes all the time or is previously unknown to the other entity (Dankers, Garefalakis, Schaffelhofer & Wright, 2002). Furthermore, the secret key technique presents additional challenges with regards to the management and administration of secret keys in a large scale enterprise deployment, and this has a negative effect on the scalability of the solution. The number of secret keys is proportional to the square of the number of entities. That is, for each pair of entities, you need to generate and administer a unique secret key.

Therefore, for a group of *n* entities, *n(n-1)/2* keys are required, thus complicating key management of the solution (Dankers, Garefalakis, Schaffelhofer & Wright, 2002). Encryption on the device and file level is performed MDM using similar key management techniques.

Leveraging PKI for authenticating mobile devices, a mobile device generates the public/private key pair and communicates the public key to the CA. The CA signs the public key and issues a X.509 digital certificate to the mobile device (Dankers, Garefalakis, Schaffelhofer & Wright, 2002). This approach is ideal because the generation of X.509 digital certificates is only required for identity and authentication purposes. Likewise, this approach addresses the ubiquity of mobile devices, both corporate issued and employee owned devices. Integrating PKI solution with Mobile Device Management allows mobile devices that use the Network Device Enrolment Services (NDES), such as iPads to enrol for device certificates (Jaquith, 2010a). NDES uses the Simple Certificate Enrolment Protocol (SCEP) and MDM acts as SCEP server (Jaquith, 2010a). In this setup, the mobile device generates the public/private key pair and sends the request to the NDES/SCEP server (MDM) to request for device certificate from the CA (Amerk, 2012). The CA in turn issues the X.509 certificate to the device via the Network Device Enrolment Service. This approach is not chosen for the utopian model because of the vulnerabilities described by Diodati (2012) and Orlando, Manion & Shorter (2012), and the fact that a number of mobile devices have not adopted SCEP. The certification enrolment procedure proposed by this utopian model is illustrated in Figure 3-7. Upon device enrolment with MDM, MDM generates the public/private key pair and sends the certificate request to the CA using either Microsoft Active directory Certification Service, Generic SCEP, or any other pre-defined credentials. The CA issues the certificate in response to the certification service request (CSR) file provided by the device.

MDM then generates a configuration profile for the device and attaches the certificate it received from the CA to the profile. By so doing, the configuration profile is digitally signed to avoid tampering, where the only means of removing the configuration profile is to wipe the device to factory default (Jaquith, 2010a). In Step-4, MDM sends the configuration profile and the certificate to the device. With this approach, it is not mandatory to enable SCEP but it can be used for communication between internal CA's if required. This authentication obeys NIST 800-63 Level-3 Authentication requirements described by Burr, Dodson & Polk (2006).

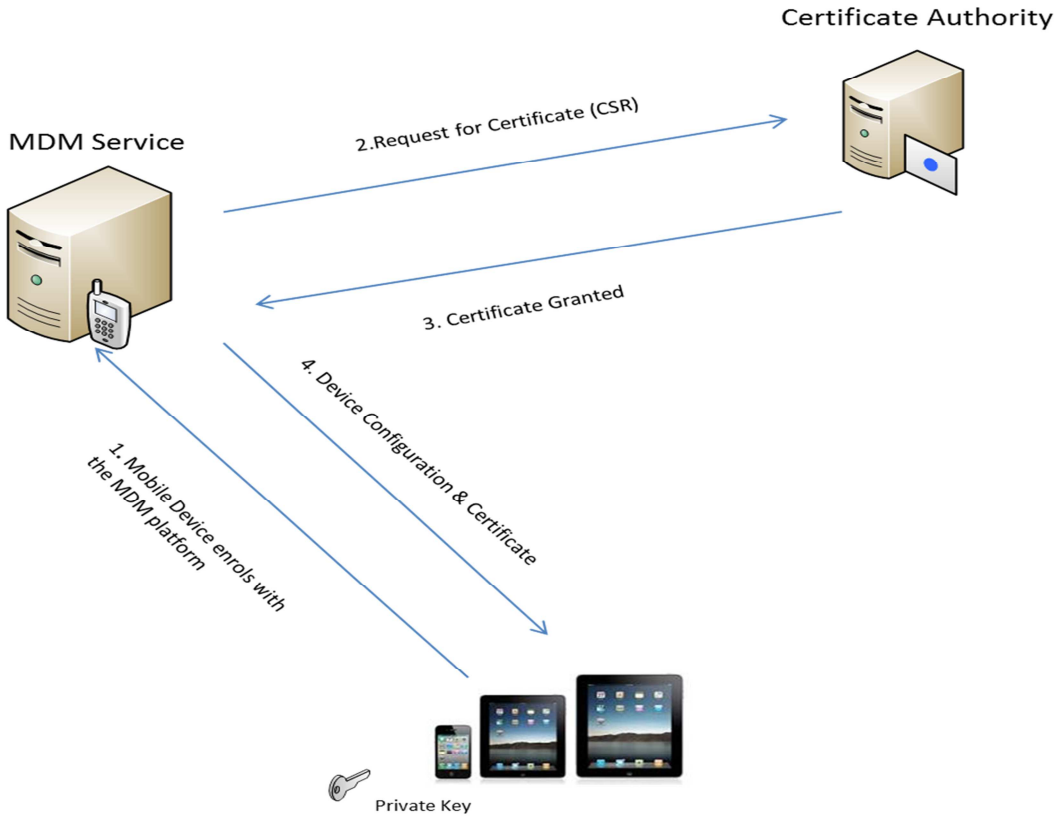


Figure 3-7: Certification Enrolment Steps in a Utopian Model

This utopian model does not propose NIST 800-63 Level-4 Authentication because this level requires the use of Smartcards and Secure Elements which, at the time of this research, are not supported by other mobile device vendors such as Apple Inc.; only the BlackBerry vendor (Research In Motion) provides smartcard readers that can pair the mobile device to the workstation to offer two-factor, smartcard authentication (Jaquith, 2010a). Furthermore, a number of mobile devices do not have a suitable card reader to accept the standard sized smartcards, thus rendering the procedure of interfacing the device to the reader, relatively burdensome

In this model, a VPN solution is proposed in addition to PKI to authenticate certain remote users to access corporate resources. Since VPN authentication is also certificate-based, the VPN server keeps its own certificate key pair that may differ from the one stored on the trusted CA. It is therefore imperative that the trusted CA list is regularly updated to ensure that all the existing certificates are synchronised, and to ensure that a VPN user can connect to corporate network with a certificate that is not tied to the trusted CA (Diodati, 2011).

Certificate-based authentication for email is proposed to mitigate the risk posed by email applications when storing user credentials on the mobile device email client. These credentials are required to access the back-end email server and can be easily retrieved in an event that

the mobile device gets compromised. Digital certificates eliminate the storage of user credentials within the email client, thus reducing the risk of unauthorised access to the mobile device and consequent information loss. Using this approach, user credentials are stored on the directory service such as Active Directory or IAM, instead of storing them on the mobile device itself.

The functionality of existing IAM is broadened to support the mobile platform. In this model, IAM is used as the first entry point to authorise, control, and audit access of digital identities to the back-end applications and information. The PKI ensures that, through the use of digital certificates, all the digital identities are sufficiently trustworthy and that the IAM knows in advance all the identities that are likely to request authorisation to the managed corporate resources such as emails. Integrating IAM with MDM enables the ability to automatically detect connecting devices based on operating system and device type (e.g. Netbook). Since mobility of workforce results in unpredictable changes in user location, as well as the time and the device from which the workforce accesses corporate resources; the IAM assumes a context-centric access model where access is granted based on context information such as location, device type and time (Corrad, Montanari & Tibaldi, 2004). In the same analogy that a Role-Based Access Control (RBAC) model grants the digital identity access to a resource based on properties, context-centric access model grants access based on context (McDaniel, 2003). If the digital identity is subjected to a certain context, then access permissions mapped to that particular context are assigned (Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M. & Abowd, G. D., 2001).

Security Information and Event Management (SIEM) provides Security Information Management (SIM) and Security Event Management (SEM). SIEM is predominantly implemented to provide log management, compliance reporting, real-time monitoring, alerting, correlated intelligence, incident management as well as forensic analysis (Nicolett & Kavanagh, 2011). Integrating MDM and SIEM extends these functionalities into mobile devices, thereby building intelligence on mobile device usage as well as mobile workforce behaviour. SIEM receives real-time events from other security technologies such as Antimalware, Host IPS, and Host Firewall and sends these events to the MDM to gain full visibility of the mobile network traffic. Furthermore, the SIEM can collect unique logs such as mobile device ID, Geographical Positioning System (GPS) logs, as well as Jailbreak information that could be analysed to create traffic and activity patterns that provide useful input for threat and fraud mitigation purposes (Wang, 2012).

An enterprise application store allows enterprises to develop and deploy applications to mobile devices in a secure and organised manner. Integrating enterprise application stores with MDM allows IT administrators to set policies for application usage and allows IT administrators to provision applications to users based on their roles (Gray, 2012). The utopian model proposes virtualised desktop infrastructure for application whitelisting and patch management in conjunction with offering these capabilities using MDM. MDM provides an added layer of application security through a dedicated encrypted tunnel called "Mobile App Tunnel" between application client on a mobile device and the actual application sitting on the Application store (Zenprise, 2012). In this model VPN is reserved for back-end legacy applications that were not originally designed to be accessed remotely by mobile devices.

Data Leakage Protection is based on policies that monitor and protect data based on its content (content-aware) as well as its context (context-aware). The data could be in storage (at rest), in transit or in use (Mogull, 2008a). DLP tracks data at rest and prevents the leaking of sensitive data as it flourishes to mobile devices. Endpoint DLP continues to provide protection of data on mobile devices, even when data has left the confines of the corporate infrastructure (Mogull, 2008a). The protection of data in use is achieved through E-DRM's policies. The integration of DLP with MDM allows for an even more robust set of policies that significantly reduce data loss. MDM toolsets provide containers that separate corporate data from personal data within a single mobile device (Basson & Redman, 2011). DLP policies are then defined to prevent the export of data from one container to another container (Basson & Redman, 2011).

E-DRM encrypts data within database tables and cells and acts as a database access control tool by assigning authorisation levels to database tables and cells. Access rights are assigned to emails leaving the mail server, as well as to documents leaving the document management systems and enterprise resource planning toolsets. E-DRM audits access to documents and any changes made to policies or rights.

3.8 Operational Architecture

The operational architecture layer provides the service manager's view of the ICT system. This layer acts as a departure point for those who were responsible for architecting, designing, and building the solution, and an entry point for the team responsible for day-to-day operations of the solution hence, operations layer. This is analogous to a facilities manager or service manager of a building responsible for its day-to-day maintenance.

The security services management architecture exists on each layer of the SABSA architecture model and its tasks are interpreted in detail on each of the five layers. Table 3-8 shows some of the operational activities that are implied by each layer of this utopian model.

Table 3-13: Security Services Management Architecture

SABSA Layer	Operational Activities
Contextual Layer	Business Driver Development
Conceptual Layer	Developing operational risk management Objectives through risk assessment, Roles Definition.
Logical Layer	Mobile Device (Asset) Management, Mobile Security Policy Management, Evaluation & Management of Data-centric security service
Physical Layer	Device Security and Protection
Component Layer	Technology Protection & Re-evaluation, Security Service Performance Monitoring

(Sherwood *et al*., 2005)

3.9 Summary

In this chapter we defined an outreach architecture model for mitigating the risks that mobile devices bring to corporate information, a model which is cognisant of the business requirements and harmoniously integrates the piecemeal technologies into a seamless whole. The model takes a layered approach where the business requirements are defined in the top layer, with a new level of abstraction developed on each lower layer until the very lowest layer (component architecture), where the selection of technologies and products is made. Finally, the operational aspects of the solution are addressed in the operational architecture layer. The complete diagram of all the architecture layers and their relationship is illustrated in Figure 3-1.

The next chapter presents a qualitative study to test this utopian model in a real environment. The study is conducted on various organisations to ultimately test whether or not adequate attention is paid to business requirements when implementing technologies to mitigate risks that mobile devices bring to corporate information.

Chapter 4 : Research Methodology

Broadly speaking, the goal of this research is to derive a practical data-centric model that can be applied in a real-life environment to protect corporate information on mobile devices. The derived model is based on the outcome of the qualitative study that is presented in this Chapter. That is, the practicality of implementing the utopian model will be assessed through the qualitative study comprised of a survey and a series of expert in-depth reviews leading to the refinement of the utopian model. The refined model is presented in Chapter 5.

The qualitative study is conducted to examine and support the pre-existing theory described in the previous Chapters. It details the survey responses, case studies and interviews used for evaluating the technologies that have been implemented by organisation to protect information outside the corporate infrastructure.

This Chapter begins by describing the research approach, data collection method, the series of interviews and questionnaire used in the survey. The method of analysis is then described before the presentation and actual analysis of the results. The Chapter concludes by summarising the findings from the qualitative study.

4.1 Research Approach

The shortcomings in the technologies that have been implemented by organisations to adopt the data-centric security model as posed in Chapter 2 reveal a need for further investigation into the implementations of these technologies in the real world. Hence a qualitative research approach based on questionnaires, case studies, and interviews from specialist practitioners was chosen to meet the research objectives set out in Chapter 1.

4.2 Data Collection Methods

Introductory letters printed on Rhodes University letter-head were collected and sent to the targeted population before the actual data collection started as a means of seeking consent for the study. This preliminary gesture is vital given the sensitive nature of the data being gathered. Refer to APPENDIX B for a sample consent letter.

The researcher collected data by administering an initial questionnaire and through conducting an iterative process of data collection and data analysis leading up to a model. Ethics clearance relating to the content of the questionnaire was obtained from Rhodes University. The primary objective of the questionnaire was to get a sense of the number of organisations that have adopted or are in the stages of adopting the data-centric security model. Expert in-depth reviews were conducted with various companies probing detailed

questions specific to each technology (Mobile Device Management Questionnaire, Virtual Desktop Infrastructure Questionnaire and Enterprise Digital Rights Management Questionnaire) in line with research objectives. The intended outcome of these expert in-depth reviews was to get a view of whether the implemented technologies adequately addressed the business requirements for security and the risks that mobile devices bear to corporate information.

4.2.1 Questionnaire

The questionnaire consisting of approximately 16 questions divided into two sections 'A', and 'B', used structured questions, Section 'A' consisted of three questions seeking to answer the first research question. Section 'B' consisted of five questions to test the hypothesis.

The first few questions were generated to receive some demographic data about the participants. This determines the importance of the topic in relation to the function of the participants, the industry in which their company is working, and the size of the company.

The duration of the survey was approximately two months (19 March 2012 to 10 May 2012). The survey was developed using an online survey tool called SurveyGizmo and shared over the Internet (LinkedIn). The survey participants were sourced by sending the link to the survey to all the people connected to the researcher on LinkedIn (249 people). Out of the population of 249, only 68 responded, yielding a return rate of 27%.

The survey containing simple closed ended questions was completed in full by 55 participants, with thirteen participants partially completing the survey. The responses from uncompleted surveys were taken into consideration during data analysis. Table 4-1 states the exact questions from the pilot questionnaire, excluding the demographic questions (refer to APPENDIX C for a complete questionnaire).

4.3 Method of Analysis

The responses from the questionnaire survey were analysed using SurveyGizmo to yield visual representation in the form of graphs and tables. The detailed descriptive responses from expert in-depth reviews were presented in chronological order. Analysis is conducted through the identification of themes.

Table 4-1: Questionnaire

Section	Research Question / Hypotheses	Investigative question
A	What accounts for the inconsistency between data-centric security controls and business objectives?	**Policy** - does a security policy or strategy document exist for mobile devices?
		Awareness training - does the enterprise have an awareness programme in place that addresses the importance of securing the mobile devices physically and logically?
		Usage - what is the mobile device normally used for? (i.e. is it used for accessing emails or for accessing corporate resources within the enterprise?)
B	The technologies used to protect information outside the corporate infrastructure do not implement the correct level of protection that can result in controls that effectively address the business requirements.	**Data classification** - does a data classification policy exist? Is data classified and labelled according to its sensitivity?
		Encryption - is data labelled as sensitive properly secured while in transit or at rest?
		Secure transmission - do mobile device users connect to the enterprise network via a secure connection?
		Antivirus updates - does the enterprise update the mobile device antivirus software to prevent perpetuation of malware?
		Asset Management- is there an asset management process in place for tracking mobile devices?
		Installed technologies - has the enterprise installed any of the following technologies to address the proliferation of mobile devices: • Mobile Device Management • Virtual Desktop Infrastructure • Enterprise Digital Rights Management.

4.4 Presentation and Analysis of Questionnaire Survey

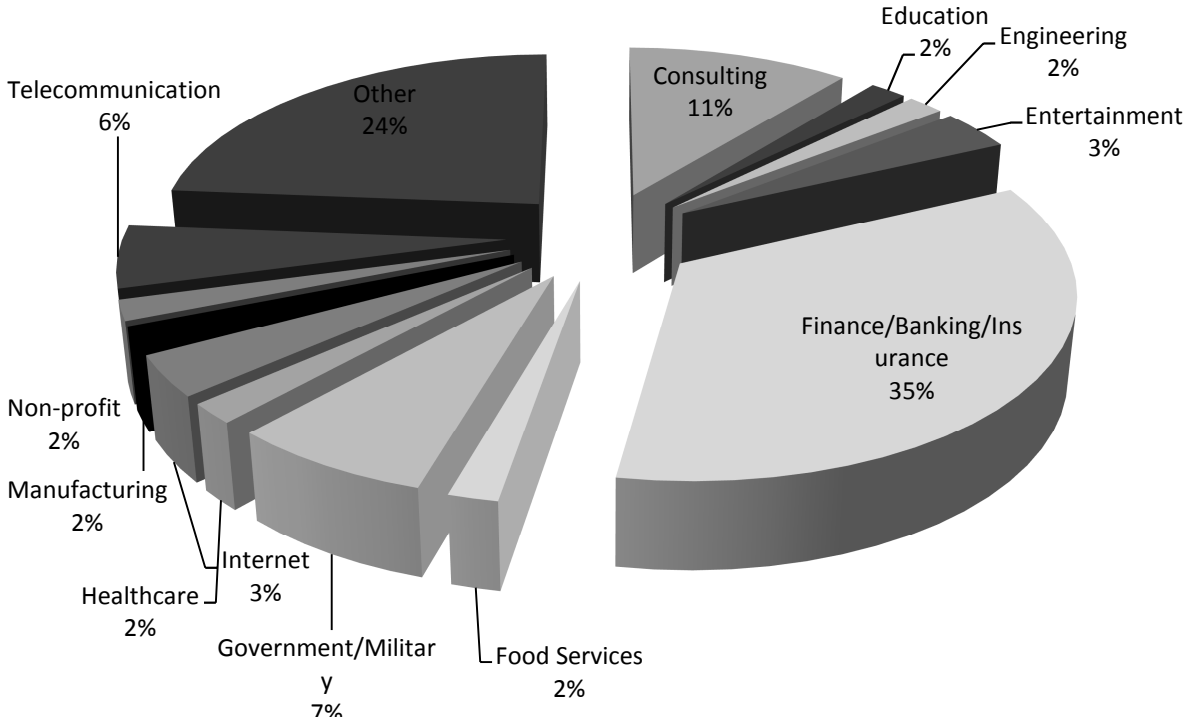
Questionnaire survey results show that Mobile Device Management has the largest footprint (45%) when compared to other technologies as shown in Table 4-2.

Table 4-2: Technology Distribution Landscape

	Implemented	NOT Implemented	Total Responses
Mobile Device Management	30	4	34
Virtual Desktop Infrastructure	23	2	25
Information Rights Management	15	2	17

N=55

Figure 4-1, a majority of the respondents (34%) are from the Banking or Financial sector, with only a few (2% each) from Manufacturing, Education, Food Services, and Engineering industry verticals.



N=55

Figure 4-1: Respondents by Industry Vertical

The large percentages (69%) of the respondents are in a management position, including Managers, Vice Presidents, Top Level Executives, and Directors. The results in Table 4-3

represent balanced views and opinions of people in both management and non-management levels.

Table 4-3: Job Title of Participants

Job Title	Number of Participants
Top Level Executive	1
Vice President	3
Director	7
Manager	27
Professional	16
Support Personnel	1

N=55

The largest implementations of MDM toolsets exists on smartphones (77.1%), with the least implementations seen on laptops, as shown in Table 4-4.

Table 4-4: Technology Distribution per Platform

	Smartphones	Tablets	Laptops	Total Responses
Mobile Device Management	25	11	17	52
Virtual Desktop Infrastructure	3	3	21	32
Information Rights Management	2	1	11	14

N=55

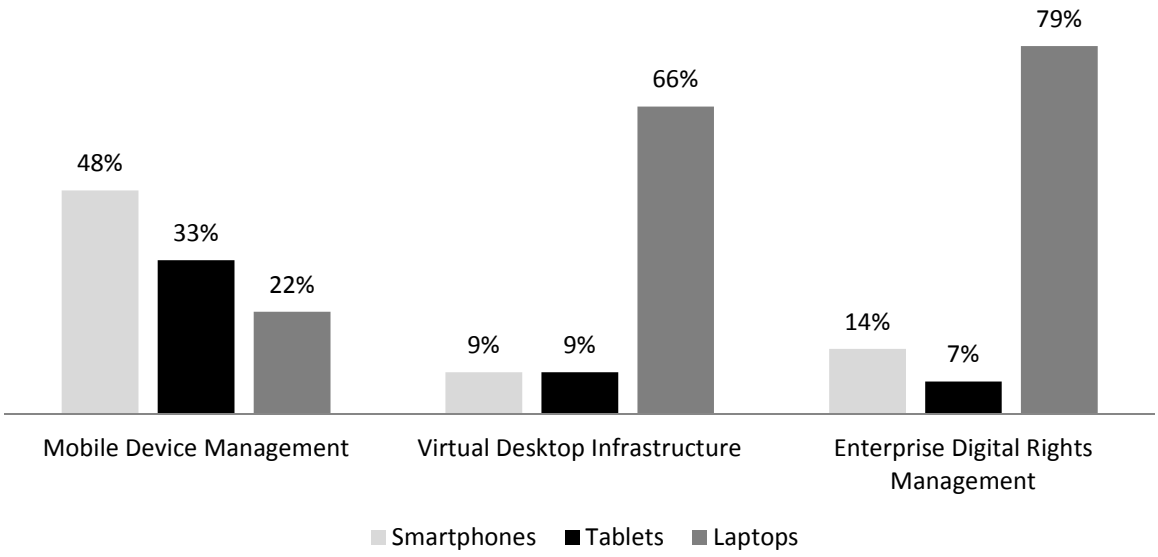
Virtualised desktops are prominent on laptops (66%) and less prominent on tablets (9%) and smartphones (9%). Only 16% of the respondents were either not sure whether VDI is installed in their organisations or indicated that it was not installed.

There are only a few implementations of MDM on tablets (21%) as compared to laptops (33%) and Smartphones (48%). This could be attributed to the fact that there are fewer tablets at this point within organisations as compared to laptops and smartphones.

A large percentage (79%) of respondents that indicated having implemented E-DRM in their organisations have installed it on laptops, with only a small percentage (7%) having installed it on tablets and smartphones (14%) compared to laptops.

N=55

Figure 4-2 depicts the graphical representation of the above-mentioned technologies, distributed per device platform.



N=55

Figure 4-2: Technology Distribution per Device Platform

While VDI possesses strong security capabilities in terms of application whitelisting, patch management, encryption (through VPN) and controlled access to corporate resources, the survey results show that its deployment is protuberant only in the desktop environment, and still lacking in the smartphone and tablet circles.

The number of employee-owned tablets and smartphones outweighs the number of those that are corporate-issued.

Table 4-5: Corporate –issued Devices vs. Employee-owned Devices

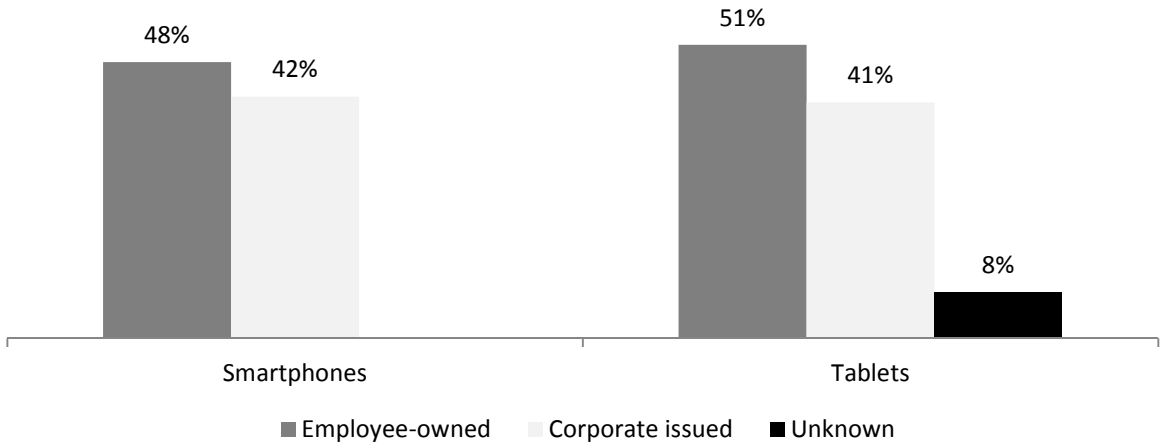
	Employee Owned	**Corporate Liable**	**Total Responses received from Survey**
Smartphones	33	29	69
Tablets	30	24	59

N=55

Tablets carry the largest percentage (51%) of the devices that are owned by employees, followed by Smartphones at 48%, attributable to the fact that only a few organisations are willing to provide their employees with tablets, and the few employees who enjoy this privilege are in management ranks.

Only 42% of smartphones are owned by the companies, and only 41% of tablets belong to companies. The remaining 8% of respondents (see N=55

Figure 4-3) could not indicate whether their tablets are corporate-liable or owned by themselves personally.



N=55

Figure 4-3: Corporate vs. Employee-Owned Devices

There were 128 responses (from 55 participants) to this particular question, an indication of an increasing number of employees who carry separate devices for both work and personal use. This could also be accredited to the fact that some employees own a personal device before they are issued with a corporate device.

The traditional controls for tracking the lifecycle of IT equipment (e.g. asset management) have not fully cascaded into smartphones and tablets. Most organisations have not included smartphones and tablets into their asset management system.

Only 22 of the 42 respondents (53.7%) indicated having included tablets in their asset management system. This trend is consistent with the fact that tablet adoption is fresher on the market in comparison to laptops and smartphones. Furthermore, since asset management provides organisations with a method of keeping track of which devices have been provided to which users, organisations have not realised the requirement to track tablets and

smartphones because their ownership is widely held by employees rather than with corporates themselves.

Antivirus software deployments are not particularly prevalent on tablets and smartphones.

Table 4-6: Antivirus Deployment on Mobile Devices

	Antivirus Installed	Antivirus Not Installed
Smartphones	22	33
Tablets	23	32

N=55

As shown in Table 4-6, there are still more smartphones (60%) and tablets (58.2%) that do not have Antivirus installed compared to those that do have Antivirus installed.

Most organisations (74.6% of the 55 respondents) already have a policy document for mobile devices. This is an indication that organisations are starting to formalise their mobility strategy by developing corporate policies to support employees who bring their own smartphones and tablets to work and use them for work activities.

Likewise, 65.5% of the respondents already have a data classification policy document, and only 56% admitted having actually classified its data according to its sensitivity.

Though 89% of employees use mobile devices to access corporate emails, about 56% admitted to using mobile devices to access corporate documents as well. Some of the documents that are accessed using mobile devices are sensitive in nature.

An awareness programme that addresses the importance of securing mobile devices was indicated by only in 32 of the 55 respondents, as shown in Table 4-7.

Table 4-7: Awareness Program for Mobile Devices

	Number of Respondents
Awareness Program Exists	32
Awareness Program Does Not Exist	23

N=55

4.5 Expert In-depth Review on Virtual Desktop Infrastructure

In identifying the specialist practitioners to be interviewed for VDI; the LinkedIn social media application was used to send messages to approximately 50 members of a group called “Virtual Desktop Infrastructure”, and two participants responded. The interview questions

(see APPENDIX-E) were then sent via email to two organisations that accepted the consent to conduct study. The participants were:

- one of the largest financial services group in South Africa; and
- a multinational company manufacturing network devices, headquartered in San Jose, USA.

The adoption of virtualised desktop infrastructure in the organisations that were interviewed was largely influenced by cost (i.e. lower total cost of ownership of desktops). The network devices company also highlighted the concept of "Work-your-Way" as an additional contributing factor towards adoption of VDI. "Work-your-Way" refers to the new style of work where employers are required to provide employees with increasingly flexible options for where and what device to use for work (Cisco Systems, 2012). Today's VDI do not only support virtualised desktops, but voice and video or tele-presence as well, thus allowing mobile employees to use any device (smartphone or tablet for example) to collaborate with internal workforce.

The expert in-depth review revealed that the secondary driver towards implementation of VDI is to have the capability of restricting applications that can run on mobile devices through application whitelisting. Application whitelisting is the inverse of blacklisting, referring to a technique of accepting only applications that are on the allowed list and denying any other applications.

The other benefit comes from the functionality of VDI as some form of a patch management toolset. The VDI instances are patched on a regular basis to ensure that supported operating systems and applications remain up to date. However, the interviewed financial organisation alluded to the fact that its applications estate is very diverse and complex, resulting in a lack of patch management coverage in some of the supported applications. VDI proved to be useful in patching known and supported applications.

The connection channels between the various device types and the back-end virtual server is usually encrypted using VPN's. One of the organisations has installed VDI only on desktops, while the other organisation extended the implementation to iPads and iPhones due to the fact that iPads and iPhones already have supported VPN clients.

Both the interviewed organisations agreed having classified the VDI instances in terms of criticality. The critical desktop instances are segregated from the normal desktop instances. Standards are put in place to ensure that virtual switches, VLAN's, routing protocols, and

other networking components are configured according to best practice to ensure that no traffic can leak from a VLAN that is hosting critical virtual desktops to another due to misconfigurations.

A client component is usually installed on desktops to initiate or execute the VDI session. The network device company uses Citrix XenDesktops client for both desktops and mobile devices, while the financial institution has installed VMware view client only on desktops because the VDI implementation is not extended to mobile devices. Authentication is required to execute the client component.

The network device company expressed a need to move towards a client-less, browser-based VDI access using HTML-5 Remote Desktop Protocol (RDP) client such as Ericom Access now. This removes the need to install Flash, Silverlight, ActiveX or any other underlying technology on the desktop and mobile device. The VDI sessions run entirely on a browser that has Websocket and HTML-5 support such as Internet Explorer, Chromebooks, Safari, Firefox, Google Chrome, and Chromebox. The other drive towards HTML-5 RDP is that in the event of a disaster, users can be redeployed promptly and securely without additional infrastructure thus enabling disaster recovery and business continuity.

4.6 Expert In-depth Review on Mobile Device Management

In identifying the specialist practitioners to be interviewed for MDM; consent letters were sent to the 68 respondents identified during the initial survey, with only one participant responding. A message was then posted on LinkedIn group called “BYOD: Bring Your Own Device” inviting 2,937 members of the group to participate in the study, and three members responded. This low response rate from the group members could be attributed to a number of issues, with time being a primary factor. While most respondents usually do not have time to spare to respond to relatively long interview questions, others still regard interviews as being a bother. The interview questions (see APPENDIX D) were then sent via email to three organisations that accepted the consent to conduct study. The participant organisations were the following:

- an information assurance and systems security engineering company based in Melbourne, Florida, USA;
- a large IT outsourcer in South Africa with offices based in Midrand, South Africa; and
- one of the four largest Banks in South Africa.

The interview questions consisted of both closed and open-ended questions, and divided into four sections:

1. introductory questions;
2. inventory related questions;
3. application related questions; and
4. technology specific questions.

The adoption of MDM toolsets into the organisations that were interviewed was led by the proliferation of mobile devices in the workplace. Executive managers started bringing their own iPads and the organisations then issued corporate-owned iPads to senior and middle managers. The infusion of mobile devices started becoming unmanageable and IT implemented MDM toolsets in attempting to catch up and to manage the mobile workforce.

None of the organisations interviewed have implemented MDM for more than two years; the least recent implementation was completed less than six months from the date of survey (15 October 2012). Two out of the three respondents (67%) chose to install Airwatch following a rigorous proof of concept; the other organisation chose to install Good Technology MDM. The two organisations admitted that the choice of Vendor (Airwatch) was influenced by Airwatch's ranking in the MDM market space. In addition to Airwatch' s position in the Leaders Quadrant of Gartner's 2012 MDM Magic Quadrant (Mobile Device Management, 2011; Redman, 2012), Airwatch received Frost & Sullivan's 2012 North American Customer Value Enhancement Award in Mobile Device Management (Espinoza, 2012).

The interviewed organisations rely on mobile device management toolsets to collect information such as make and model of diverse mobile device as well as applications deployed on those mobile devices. The mobile device management toolset was also found useful in identifying the versions of the mobile applications and for deploying application and operating system updates.

The interviewed financial organisation uses the network discovery features of the existing vulnerability management toolset (QualysGuard) to discover and prioritise all network devices, including mobile devices.

Organisations found it relatively easy to detect browser and operating system versions, but beyond well-known and finite models (such as iPhones), Android variants number in the

thousands. The organisations rely on databases such as GSM Arena[4] to keep up with the plethora of Android devices. This is usually automated, semi-automated and unstructured; as a result the organisations do not know, with absolute precision, the exact type of devices that access their network, including those that access via VPN. The Financial institution does, however, maintain a list of all the devices that should connect to the network including its brand (i.e. only iPhone, Blackberry, and iPads are managed through MDM toolsets). This institution has installed Network Access Control in addition to MDM to prevent certain devices from connecting to the network if they do not comply with the security, privacy, and data protection policies. Furthermore, the financial institution has restricted their end-users from using personal applications while connected on the internal network. The other two organisations were quite flexible in their approach and allowed their employees to use their personal applications. With the latter approach, the organisations accepted the risks that personal applications might pose (e.g. viruses) on the corporate network and assets.

The mobile device management service is an insourced service amongst all the surveyed organisations.

The organisations found it very easy to manage large-scale deployments of mobile devices, using their existing MDM solutions because the enrolment of a device and configuration of policies is done easily over the air.

Only one of the interviewed organisations did not have a mobile device management policy in place. The remaining two organisations performed a gap analysis on the existing security policies to see if they cover mobile devices. The financial organisation followed the gap analysis with a risk analysis. It was realised by both organisations that, given the prevalent state of the situation, there was a need to develop a separate policy for mobile device management, instead of merely modifying existing policies.

All interviewed organisations found MDM very useful in detecting Jailbroken and Rooted devices. When MDM detects a Jailbroken device or a device that is running a blacklisted application, it immediately blocks that particular device from accessing network resources. Likewise; within the interviewed organisations, MDM has been configured to block devices that have not accessed the network for certain number of days. Figure 4-4 shows a screenshot from MDM management console, where the right hand side depicts a graph that keeps track of the date when the device was last seen on the network. Both organisations configured this feature in order to restrict devices that have out-of-date MDM policy access to the network.

[4] http://www.gsmarena.com

These devices are sent to a quarantine folder and updated, before being granted access to the corporate resources.

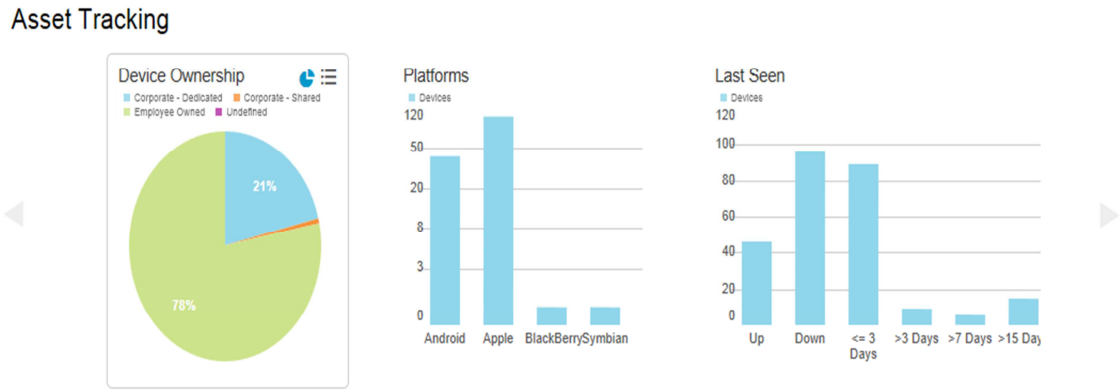


Figure 4-4: Screenshot from MDM toolset (Surveyed Respondent)

All three organisations have configured MDM to distinguish corporate-owned devices from personal devices. Selective remote wipe is also configured on all three organisations, and passwords are used as the primary means of authentication.

4.7 Expert In-depth Review on Enterprise Digital Rights Management

In identifying the specialist practitioners to be interviewed for E-DRM; the interview questions (see APPENDIX-F) were sent via email to two organisations that accepted the consent to conduct study through a group called “Information Rights Management” on LinkedIn. The interview questions were sent to the following specialist practitioners:

- Seclore Technologies –a security software company providing information security solutions in the areas of information usage control, information rights management, and IT security outsourcing. The company, based in Mumbai, India, develops the IRM product called Seclore FileSecure, and also uses it internally to secure its intellectual properties. It has more than 2 million users Worldwide.
- Wipro Limited –a multinational outsourcer headquartered in Bangalore, Karnataka, India.

The interview questions consisted of 25 questions structured as follows:

- seven introductory closed-ended questions;
- twelve open-ended questions relating to handling of files and documents; and
- six open questions relating to the functionality of the technology.

Wipro Limited only responded to the twelve open-ended questions; and some of the responses are taken into consideration during analysis.

Seclore Technologies has a number of clients that have been using their E-DRM product for more than three years. Their IRM products go a very long way in protecting information residing in documents and emails, however, the IRM technologies in general are still lacking in protection of information residing in web sites. For instance, their product cannot prevent someone from capturing screen dumps from web based applications like Enterprise Resource Planning (ERP) applications. Wipro Limited uses Microsoft Rights Management Services and has also attested to a similar issue.

Seclore FileSecure has strong encryption capabilities, so much so that it encrypts database tables and cells; it even goes so far as to define authorisation levels (reading and editing) on database tables and cells. Data classification policy exists on most of Seclore Technologies' clients, however, it is not always enforced, making it difficult to choose which files or database fields to encrypt and which ones to leave behind. Consequently, all files and documents are encrypted, irrespective of their file sensitivity or classification level.

File sharing and document management systems like Microsoft SharePoint and IBM FileNet provide a granular level of access control governing who can access a particular file or document. However, these controls do not extend to mobile devices once the documents have been downloaded. Seclore admitted that its E-DRM product (FileSecure) does extend this scope and reach of security policies defined in file and sharing document management systems to desktops. Furthermore, Seclore FileSecure provides extension mechanism and Application Programming Interfaces which extend the scope and reach of security policies defined within ERP applications (e.g. SAP), Knowledge Management Systems (e.g. Lotus Notes), Groupware Systems (e.g. ProjectPlane), and Product Data Management systems. Wipro Limited, on the other hand, confirmed that its E-DRM extends its security scope only to Microsoft Office documents stored on Microsoft SharePoint. SharePoint technologies can store AD-RMS protected documents, and since Wipro Limited uses AD-RMS in Windows 2008 and Office SharePoint Server 2007, documents encrypted using AD-RMS are visible to SharePoint and can be tagged or indexed.

At Wipro Limited, the document owner assigns rights to a document created using an AD-RMS enabled application such as Microsoft Office Enterprise. Likewise, email senders use Office Outlook to apply rights to email messages as well as to the unprotected Office Word, Office Excel, or Office PowerPoint document attachments that might be included. The

Seclore clients use a similar approach; however, the document owner assigns rights to any document, irrespective of whether it was created using Microsoft Office Enterprise, and irrespective of the email application client used. The rights of the file remain with the file throughout its lifecycle and cannot be copied to another file unless the other file is also protected. Both toolsets offer the capability to expire the rights on any specific date in order to revoke access rights remotely. Document expiration does not destroy the document, it only expires the right to open the document. In addition to revoking access through expiration, Seclore FileSecure provides remote control to every piece of information which is shared within and outside of the organisation thereby providing the capability to remotely revoke access rights as long as the remote device is online. Offline machines validate the expiry date against local machine's internal clock, and online machines validate the expiry date against a remote time (NTP) server.

Seclore FileSecure protected files open only after successful authentication, and Seclore FileSecure client must be installed on the device. Once a user authenticates, the decryption key and policy information is downloaded onto the local computer and allows the file to open with restricted access. The decryption key is only valid for that particular session, that is, when a user closes the protected data file and reopens it again, another authentication is required (either single sign-on or stored session) in order to download the decryption key to open the protected file. Protected documents can also be accessed in offline mode when the document owner has provided the rights to access the document in offline mode, and when the document was opened before in online mode. All activities on the document are logged and stored in a central audit trail repository in order to assist with forensic investigation and to ensure compliance reporting to regulatory requirements such as ISO27001, Sarbanes Oxley Act (SOX), HIPPA, GLBA, and PCI-DSS. These activity logs can be configured in different formats, using a report builder, to satisfy various regulatory reporting requirements.

At Wipro Limited, on the other hand, AD-RMS also relies on operating system user authentication to validate the user's identity, before the user is issued with a licence. AD-RMS protected files open only to a user that possesses a valid end use licence (EUL) issued by AD-RMS server. This licence is used to decrypt the contents of the file and to enforce the specific usage restrictions assigned to the file. End use licences can be cached and reused to open a protected file in offline mode. For instance, Microsoft Word appends the use licence to the WORD document allowing the document to re-open from any machine where the user has an active account without having to consult with AD-RMS server, until the licence expires. Likewise, the document can also be created either in offline or online mode when the device

that is used to create the document possesses a unique valid publishing licence issued by the AD-RMS server. Each successful and failed attempt to access a protected document is logged for user tracking, and to assist with forensic investigations. This AD-RMS optional feature allows activity logs to be sent to a log database using Microsoft Message Queuing (MSMQ) Services. The MSMQ service ensures that the logs are cached internally, in an event of a log database being unavailable, and replicated to the log database when the log database becomes available.

None of E-DRM toolsets used in either organisation have the capability to protect documents in printed format, thus avoiding information leaking through printed documents. For instance, the E-DRM toolset can add watermark effects on the printed document as well as the credentials of the person that printed the document, thereby enforcing the person that printed the document to protect it (Cheung & Chiu, 2003). When interviewed, Seclore Technologies mentioned that protecting documents in printed format does not add value because the printed documents can be scanned back into electronic format, and watermarks can be removed, in that way allowing the previously protected printed document to be stored unprotected.

Wipro Limited indicated that their E-DRM only recognises Windows-based mobile devices and does not recognise mobile devices like BlackBerry, iPhone, iPad, PlayBook, Symbian, and Android based mobile devices. The rights that can be assigned to email messages on outlook mobile are only limited to “Do not forward”. Office Mobile can only read IRM protected documents and does not allow for the creation of protected documents. Seclore Technologies confirmed that a number of their clients are using its Seclore FileSecure applications for iOS devices (Seclore FileSecure Lite) to access rights protected documents and emails from iOS devices. The iOS devices are only restricted to view the protected file and cannot access the contents of the protected document devoid of authenticating and uploading the protected file to a cloud based viewer owned by Seclore (Seclore FileSecure WebConnect).

The implementation challenges faced by most of Seclore Technologies’ clients are largely attributed to the lack of knowledge or information about E-DRM within IT teams, as well as lack of awareness on the need for protecting information among business users. Overcoming these challenges involves educating both IT personnel *and* business users. Seclore Technologies also shared some experiences from E-DRM deployments from clients at various industry verticals (Gupta, 2012). At a multinational IT company, Seclore Technologies went beyond training personnel and worked with users to create confidence. At a manufacturing

organisation, a champion for the E-DRM cause was identified from business. Although the organisation had a strong information security team, not all of the business users were security savvy. Leveraging on the support of the head of the business, educating other business users and the IT team became a seamless effort. In another client, an Indian power company, the existing knowledge portal was used to distribute information about E-DRM.

4.8 Limitations of the Study

The research has limitations with respect to the generality of the findings. The expert in-depth reviews were conducted on relatively fewer participants (a total of seven participants) compared to the questionnaire survey, thus it may be uncertain whether the findings from the expert in-depth reviews may generalise to other organisations. It was also difficult to make systematic comparison on some of the survey responses due to widely differing, and sometimes subjective responses. Despite this, analysis on the survey responses provided insight on how the technologies are used to mitigate risks from mobile devices, and how these technologies are used to address business requirements for security.

4.9 Summary

The questionnaire survey results support the literature review in that the organisations do allow mobile devices (either personal or corporate-issued) to access their network, as well as other corporate resources such as emails, contacts, web applications and documents.

The survey results do, to some extent, answer the research question posed in Section 1.3. There is some level of inconsistency between the data-centric security controls and the business objectives. This inconsistency is instigated by the fact that organisations implement the information security controls on a very reactive and tactical basis. The organisations identified the business requirements of mobility such as employee productivity and cost reductions. To address these business requirements, the organisations identified technologies to implement as point solutions, without regard to the broader implication. Consequently, the implemented technologies exist in isolation, with no evidence of integration and inter-operability.

The qualitative study results show that information protection is not the primary objective in why the interviewed organisations chose to implement the data-centric security technologies. For instance, the organisations that implemented virtualised desktops were largely driven by the business objective of reducing the total cost of ownership of desktops. Similarly, organisations that implemented mobile device management toolsets did so in trying to catch up with the proliferation of mobile devices and to respond to the concept of ‘bring your own

device' (BYOD). This is a strong indication that security is often the *last* aspect to be considered when implementing solutions to address specific business requirements. Furthermore, the implemented solutions only address the business requirements, and not the business requirements for security. In Table 3-4, we listed the business drivers for security for each business driver in order to ensure that security is not considered lastly when designing the solution.

In-depth analyses on the survey results highlight general issues with regards to implementing the utopian architecture model in a real world:

- E-DRM is not popular in the smartphone and tablet circles and requires a great deal of user awareness.
- MDM relies heavily on passwords and PIN to authenticate mobile devices and digital certificates are still not widely used.
- NAC has been considered by one of the organisations to assist in conjunction with MDM in preventing certain devices from connecting to the network if they do not comply with the organisation's security, privacy, and data protection policies.

In the next chapter, we propose a refined data-centric security model based on the above-mentioned findings as well as additional literature.

Chapter 5 : The New Proposed Mobile Architecture Framework

5.1 Introduction

The layered utopian architecture model presented in Chapter 3 is revisited with the intention of refining the utopian architecture model to arrive at an immensely practical architecture model. The refined model is practical in a sense that it maximises financial, operational and business benefits while mitigating the risks that mobile devices bring to corporate data. A similar approach as the one used in Chapter 3 is followed; that is, no changes are made to the business drivers, business drivers for security, attributes, or the architecture layers. The only alterations are made to the security mechanisms required to deliver on the required attributes. The chapter opens by describing the modifications to the utopian architecture model as well as the rationale behind the modifications. A new model is then architected based on the modifications.

5.2 Modifications towards a Utopian Architecture Reference Framework

The process for modifying the utopian architecture model begins by reviewing the mobile security architecture illustrated in Figure 3-6. The security mechanisms or technologies defined in this utopian mobile security architecture are reviewed to determine their pragmatism in the current real-world scenario. The derived model is designed in such a way that it can be customised to fulfil the requirements of any specific use case. The use case defines how the mobile device will be used to accomplish certain tasks within the organisation and how confidential information and applications should be accessed (Maiwald & Blum, 2012).

While it is not desirable to store sensitive information on the mobile device, a specific use case may require sensitive information to be stored on the mobile device so that it can be easily accessed in offline mode. Another use case may require certain applications to cache information locally to achieve better user experience. That said, the use case impacts on the choice of security mechanisms to employed and ultimately in the derived architecture model. Therefore, the proposed practical model should cater for multiple use cases.

In the new model, it is proposed that the following technologies are reviewed and modified, with justifications thereof:

- public key infrastructure;
- identity and access management;
- application store;

- virtual desktop infrastructure;
- host firewall & antimalware; and
- mobile data leakage protection; and

5.2.1 Public Key Infrastructure

The new model does not propose the use of X.509 certificates to authenticate mobile devices primarily because of scalability, usability and the overhead required to manage multiple certificates from different mobile device vendors (Diodati, 2011). In Chapter 3, it was proposed that the trusted CA list needs to be regularly updated to ensure that all the existing certificates are synchronised, and to ensure that a VPN user can connect to corporate network with a certificate that is not tied to the trusted CA. While this is possible on mobile device platforms such as iOS and BlackBerry, this centralised management capability is not supported on Android-based operating systems (Diodati, 2011). Consequently, an organisation needs to procure or manage additional VPN solutions for Android-based devices, each with its own trusted CA list.

The use of X.509 certificates to authenticate mobile devices is also dependent on the capability of the mobile device operating system to integrate with PKI. A mobile device operating system's cryptographic API is responsible for allowing the mobile device to use digital certificates and associated private keys. While BlackBerry and iOS display strong integration capabilities with PKI, Android is lacking (Diodati, 2011).

Furthermore, PKI cannot be used on its own to provide authentication for mobile devices. PKI requires the capabilities of MDM to provide enhanced scalability and OTA management of digital certificates and mobile identities.

In light of this, the new model proposes the use of one-time-password (OTP) authentication system. This authentication system uses a secret key to generate a sequence of one-time passcodes such that when a user authenticates using the generated passcode, the passcode never travels through the network, thereby preventing 'replay attacks' (Haller, Metz, Nesser & Straw, 1996). A replay attack occurs when an attacker intercepts a network connection and eavesdrops to capture login credentials to use them at a later stage. Traditionally, OTP authentication systems were implemented on hardware that is commonly known as OTP tokens. In recent years, the software-based OTP authentication systems became popular due to the proliferation of smartphones and the need for organisation to improve usability and reduce the costs borne by OTP tokens (Diodati, 2010). The new model proposes the use of software-based OTP systems because they are much easier to deploy when compared to

X.509 certificates (Diodati, 2011). Software-based OTP systems can be easily deployed to consumers and 3rd parties using a self-service application; deployment to internal users can be done using MDM. The passcode that is generated by the software OTP is used in conjunction with the credentials stored on the IAM to provide two-factor authentication. The OTP authentication service validates the OTP and the IAM validates the credentials as illustrated in Figure 5-1.

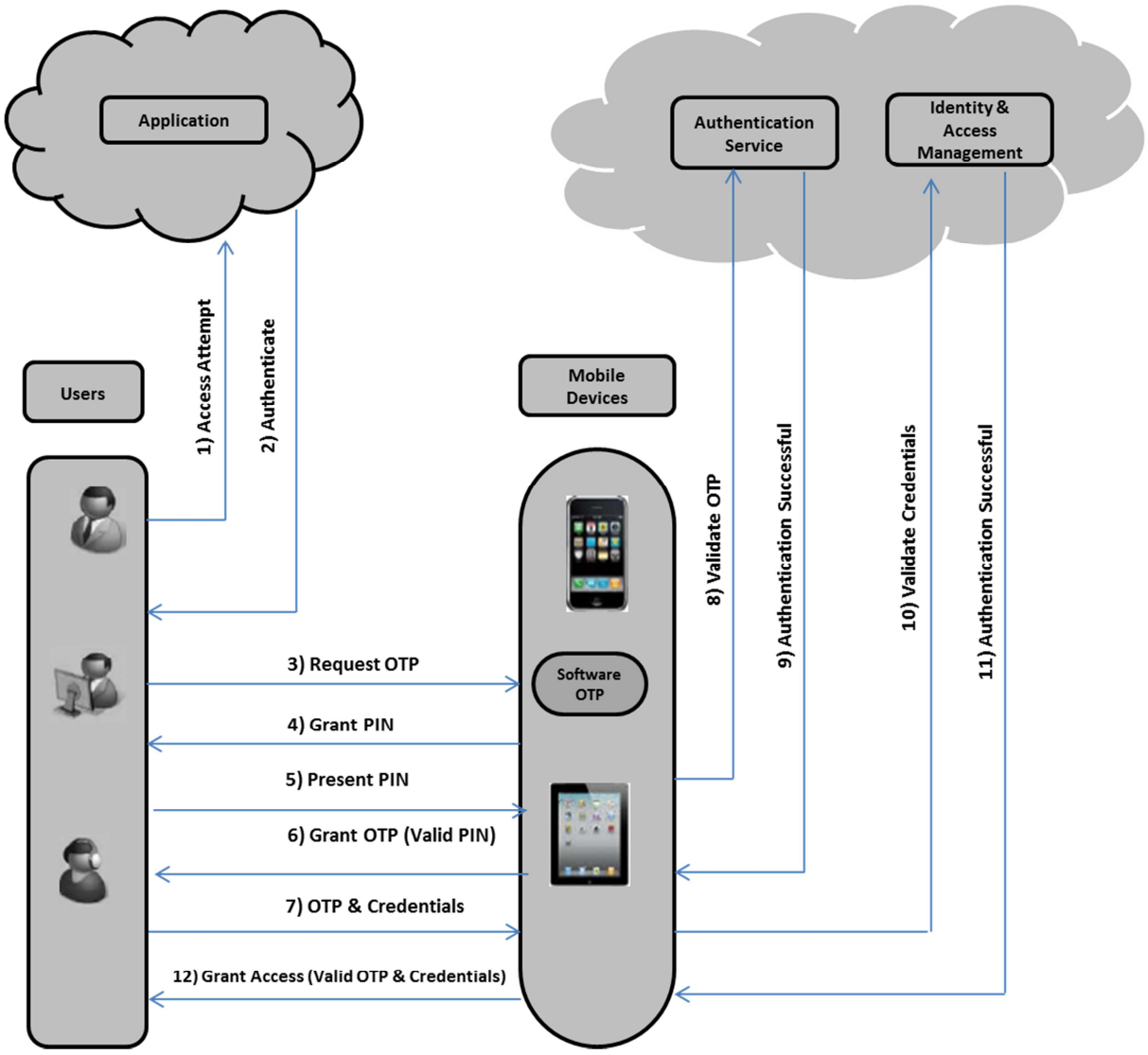


Figure 5-1: OTP Authentication Process

Figure 5-1 illustrates the process steps required to successfully authenticate using OTP in the proposed mobile architecture model. When the mobile user attempts to access an application on the cloud (Step 1), the application responds by requesting authentication (Step 2). The mobile user then requests the OTP from the software-based OTP client running on the mobile

device (Step 3). The mobile user only gets successfully authenticated once a valid OTP and valid credentials have been presented to the mobile device.

5.2.2 Identity and Access Management

In the traditional non-mobile setting, the authorisation decision is made by an external authorisation layer situated within the organisational infrastructure, and not by the endpoint device itself (Glazer, 2012). A similar scenario should be followed within a mobile architecture environment. While the utopian architecture model illustrated in Figure 3-6 defines IAM at the middleware layer, the practical model proposes to implement this layer in the Cloud as shown in Figure 5-1. This approach is chosen to ease the bottleneck between the IAM middleware layer and the back-end from increased mobile traffic volumes. This approach saves the organisations from constantly planning for the capacity required to accommodate the increase in mobile traffic volumes.

IAM solution is proposed instead of a simple directory service such as Active Directory because of the scalability of the IAM technology proportionate to mobile device usage. Mobile devices are now implementing new technologies such as secure element and near field communication for higher levels of identity verification and authentication (Reveilhac & Pasquet, 2009). IAM technology is better positioned to leverage on these improved authentication methods to authorise access to corporate applications and data. However, at the time of this research, IAM had not developed optimised capabilities to fully accommodate these improved authentication methods and the relationship between IAM and mobile computing is still standing apart (Glazer, 2012).

Similar to the IAM solution proposed in the utopian model, the derived model employs context-based IAM solution. As explained in Section 2.3.4, mobile devices generate new data that previously never existed through embedded sensors and applications. The IAM solution uses this contextual information to build known trends on contexts such as geolocation, nearby devices, mobile identities; to strengthen its authorisation decision and to effectively associate the mobile user to the mobile device (Glazer, 2012). There are, however, privacy concerns that organisations need to address when leveraging this solution. For instance, enabling geolocation reveals private information about the mobile user such as the location from which the user authenticated, and this may not be widely accepted on employee-owned mobile devices.

5.2.3 Application Store

Developing an in-house application store and infrastructure requires new costly investments that are prone to failure (Wang, 2012). William Mitt Romney, Republican Party nominee for President of United States in 2012, initiated the Orca Project that eventually became a significant case study in enterprise mobility due to failures relating to mobile application deployments (Habberman & Burns, 2012). The project was aimed at identifying voters, from a pre-existing list, that had not yet casted their votes, and to send them customised targeted messages to remind them to go and vote; and to dispatch local volunteers to push the voters to the ballot boxes (Habberman & Burns, 2012). The project failed fundamentally because of lack of beta testing and lack of user application support, amongst other things (Steele, 2012). To avoid such failures, organisations need to leverage on existing 3rd party applications (in the Cloud), and other pre-existing applications first, before developing new ones in-house.

Currently there are two prominent techniques for Mobile Application Management (MAM): 1) Software Development Kit (SDK); and 2) Application Wrapping. Application wrapping refers to the addition and modification of application binaries in order to enhance security features of the application (Madden, 2012). The derived architecture model proposes a concept of dynamic application deployment. This concept allows organisations to either make use of application wrapping to repackage 3rd party applications' binary code to add supplementary security features such as encryption and geofencing; or to use Software Development kits for the development of new rich mobile applications in order to add security features to an application at the time of code creation. Cloud-delivered applications consist of application programming interfaces (API) that can be customised by SDK to add security features such as single sign-on (SSO) – written on access management languages like OAuth, OpenID, or SAML (Dudney & Adamson, 2009). In this model, OAuth is used due to its strength in providing authentication and session management for rich mobile applications (Diodati, 2011). Furthermore, OAuth has a larger life span in a sense that a user is not required to re-authenticate for each session, and it can be used for multiple sessions.

Hosting applications in the cloud brings a cost-saving in that organisations no longer need to spend funds in upgrading the DMZ and VPN gateways due to an increase in bandwidth caused by mobile device traffic (Wang, 2012).

Instead of building all the security functions into the application, some of the functions are moved into the middleware layer to allow other applications to benefit from the same security

features. The security functions that could be moved to the middleware layer are described by Wang (2012) as follows:

- session management;
- secure communication;
- access monitoring;
- logging;
- interface consolidation; and
- access and credential management.

The practical model proposes that organisations adopt a layered approach when delivering mobile applications to mobile devices. The management of mobile devices should be based on the applications that the devices run as well as the risk that they pose to the organisation (Gray, 2012). As illustrated in Figure 5-2, the practical model proposes that organisations adopt a strategy where fully managed corporate-owned devices are provisioned a full-suite of corporate applications, while the partially managed employee-owned devices are provisioned basic applications such as emails, virtual applications, and VPN-enabled browsers. Partially managed devices do not necessarily have to be on the MDM toolsets, but can access corporate mail via Microsoft ActiveSync because most mobile devices support the Exchange ActiveSync (EAS) protocol. Despite the strength of EAS, it is proposed for partially-managed because it is not deemed strong enough for heterogeneous environments with knowledgeable users (Maiwald & Blum, 2012).

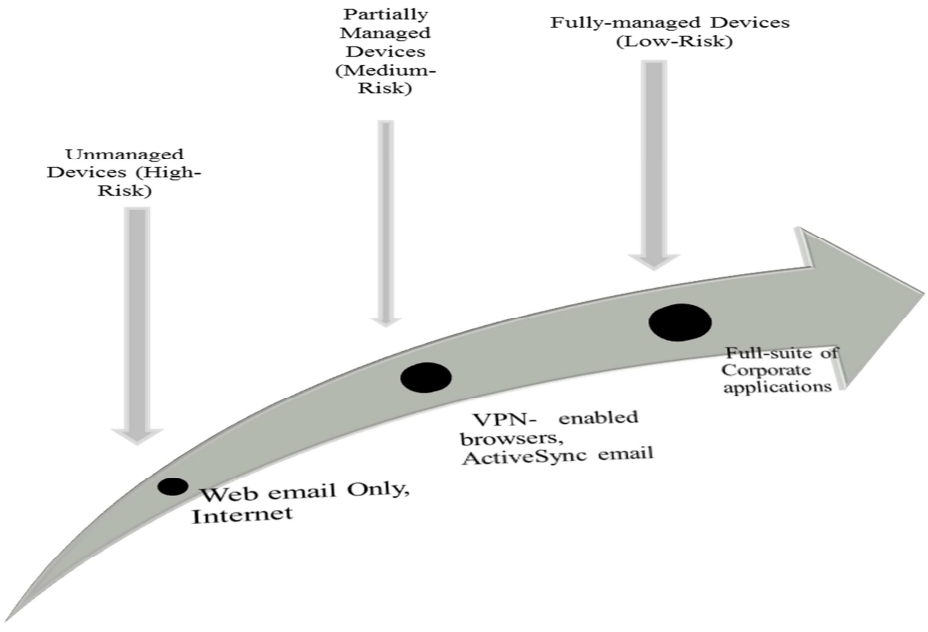


Figure 5-2: Increasing Device Support Commensurate to Risk

Unmanaged devices are configured with default security policies that provide lax user restrictions. Unmanaged devices are usually owned by employees. Partially managed devices are configured with a certain degree of security policies that provide limited user restrictions and the user typically has full or partial administrative privileges on the mobile device endpoint (Maiwald & Blum, 2012). Fully-managed devices are configured with firm security policies allowing restrictive access only to authorised users. Users are not granted administrative privileges on the mobile device endpoint and any violations to the policies is detected and reported in real-time (Maiwald & Blum, 2012). These devices are owned by the organisation, not the employee, and any changes to the mobile device configuration follow the change control process.

5.2.4 Virtualised Desktop Infrastructure

In Section 4.3 the surveyed network device company expressed a need to move towards a client-less, browser-based VDI access using HTML-5 Remote Desktop Protocol (RDP). The proposed practical model will not employ HTML-5 browser-based VDI access due to its lack of standardization as well as lack of browser vendor support. While browsers such as Internet Explorer, Google Chrome, Apple Safari, Opera, and Firefox claim full HTML-5 support, this is hardly true (Hammond, Rymer& Kroll, 2010). For instance, Internet Explorer does not support the <canvas> tag, while other browsers do (Hammond, Rymer & Kroll, 2010). In addition to this partial HTML-5 support, HTML-5 is still in draft specification and has not become fully approved by World Wide Web Consortium (W3C) standard, resulting in various unpredictable behaviours[5] when browsers execute HTML-5 code (Hammond, Rymer & Kroll, 2010). Furthermore, developing in HTML-5 presents some cost implications in that organisations need to upgrade their current infrastructure to support newer protocols such as Websocket communication protocol that are currently being developed by W3C (Gray, 2012).

Since an HTML-5 browser-based VDI is a web application, it means that its data can be cached on the mobile device endpoint for offline processing (Disabato & Berenbaum, 2012). Web applications are known for not being able to adequately protect data in offline mode, and in online mode, web applications are predisposed to attacks such as cross-site scripting and cross-site request forgery (Disabato & Berenbaum, 2012).

Given these current challenges, the proposed practical model uses client-based VDI and VPN enabled browsers to render virtual desktops and applications (particularly legacy applications) to any mobile platform. Through virtualisation, traditional Windows desktop operating

[5]These various unpredictable behaviours can be seen on MIX10: The Next Web Now (http://live.visitmix.com/MIX10/Sessions/KEY02)

systems such as Windows XP and Windows 7 can be easily accessed using RDP – without leaving traces of data on the mobile device endpoint (Disabato & Berenbaum, 2012). VDI will also complement MDM in whitelisting applications and for deploying patches.

5.2.5 Host Firewall and Antimalware

In Section 2.3.1, we observed that most of malware in the mobile device space are caused by unsigned applications targeting the Android platform. Threats relating to Jailbreaking and Rooting exploit the operating system's mechanisms of validating the integrity of code, rather than being malware threats that directly infect the operating system. Other mobile device platforms like Apple and Blackberry employ code-signing systems and sandboxing, reducing their susceptibility to mobile malware. The use of application wrapping and SDK, coupled with the aforementioned security functionalities, reduces the risk of malware infection for the foreseeable future (Jaquith, 2010b). The practical model proposes the use of such compensating controls, including MDM's Jailbreak and rooted detection capabilities, instead of implementing host firewall and antimalware on diverse mobile device types. Installing antimalware on mobile devices is not only security overkill, but it significantly reduces mobile device battery life by about 50%, thus rendering it less desirable (Jaquith, 2010a). Installing host firewall is also a waste of money since there are fewer listening ports on mobile devices as compared to personal computers (Jaquith, 2010b). Security software vendors like McAfee and Kaspersky report on mobile malware, as described in Section 2.3.1 of the Literature Review, in an exaggerated fashion so as to scare mobile device users and increase sales (Jaquith, 2010b) . Mobile devices have a smaller attack surface compared to traditional computers. Even the most appalling attacks on the iOS have their origins from traditional PC's. For instance, there was Jonathan Zdziarski's "lunchtime attack" that exploits the iPhone's buffer overflow vulnerability when it is in recovery mode in order to disable the passcode and access the iPhone's content in unencrypted form (Jaquith, 2010a; Zdziarski, 2012). This attack has its origins from the well-publicised "cold boot" attack[6] and it exploits all software-based full-disk encryption products when the machine is in its pre-boot state by closing the power supply to a pre-booted device and accessing the contents of RAM (Halderman *et al.*, 2009).

Application control or application whitelisting is an additional compensating control that is proposed because it limits the applications that can be deployed to the mobile device endpoint, thereby significantly reducing malicious code that can execute on the mobile

[6] A video demonstration of this attack is available on http://www.engadget.com/2008/02/21/cold-boot-disk-encryption-attack-is-shockingly-effective

device. This approach, however, may restrict user flexibility and may lead to an employee finding other measures to bypass these restrictions (Maiwald & Blum, 2012).

5.2.6 Mobile Data Leakage Protection

Agent-based mobile DLP solutions are not necessary for mobile devices because most of the information on mobile devices is already mirrored on corporate servers (Jaquith, 2010a). A useful axiom for mobile device architecture is to store as minimal data as possible on the mobile device itself (Disabato & Berenbaum, 2012). Since most of the information leaking through mobile devices occurs on emails (employees sending sensitive documents to their Gmail accounts), and through applications such as Dropbox; it is still necessary to install DLP on the email gateway, as well as web DLP, and network DLP; and not necessarily on the mobile device endpoint. As mobile devices continue to proliferate, MDM vendors will add DLP functionalities onto the MDM solutions, and organisations should wait until this happens, instead of procuring standalone Mobile DLP toolsets.

Only 56% of the organisations that were surveyed in this research have actually enforced their data classification policies and classified their information according to its sensitivity levels (e.g. secret, confidential, and public), a clear indication that most of the organisations have not done this crucial preliminary exercise required to achieve a successful DLP implementation. This implies that most organisations do not define restrictions on information based on classification level when information is stored or in usage. This results in a common misconception that all information residing on the mobile device needs to be secured, while in reality, only sensitive information needs to be secured. In the absence of data classification policies, the practical model proposes that organisations default to “low-medium-high” information classification levels, whereby restrictions are also defined on the mobile devices used to access that information. For instance, information that has a default classification of high can only be accessed using a ‘low-risk’ mobile device.

The practical model proposes the use of containers (containerisation) for protection against information leakage. Since containerisation separates personal data from enterprise data within the mobile device endpoint, information leaking from enterprise container to non-enterprise container is protected using an MDM solution that supports containerisation (Maiwald & Blum, 2012; Disabato & Berenbaum, 2012).

5.4 Use Cases

There are two elements that the Researcher believes they should be evaluated prior to the development of the derived mobile security architecture model:

1. Usage of mobile device: A use case may require the mobile device endpoint to store and process sensitive information or applications on the actual device itself due to certain requirements such as a requirement for offline access, or a requirement for caching information locally to enhance user experience on web applications (Maiwald & Blum, 2012).
2. Type of security controls: The type of security controls implemented to mitigate the risks that mobile devices bear to the corporate information are largely dependent on the level of risk associated with unauthorised disclosure of sensitive corporate information or unauthorised access to sensitive corporate application via mobile devices (Maiwald & Blum, 2012). A use case may optimise the security controls if the level of risk is very high, while another use case may chose not to implement any security controls and accept the associated level (low) of risk. A risk is deemed not appropriate to accept if a mobile device that is not owned by the corporate is used to access high-risk applications or is used to store sensitive information (Maiwald & Blum, 2012).

The logic for implementing these elements is illustrated in Figure 5-3.

The logic begins by establishing whether the use case will require sensitive information to be stored on the device. While some use cases may determine that there is no need for sensitive information to be stored on mobile devices, the proposed model suggests that a potential for sensitive information to be accessed using mobile devices still exists and therefore each mobile device should be subjected to a policy compliance and configuration verification process. The likelihood of accessing or storing sensitive information on mobile devices requires some level of policy compliance verification and health check to mitigate the risk. Various mechanisms are used for policy compliance verification and health check such as making use of NAC to allow or deny mobile device access into the enterprise network based on the mobile device's health status. Other mechanisms include the installation of a suitable agent on the mobile device to verify endpoint configuration (Maiwald & Blum, 2012). Once the organisation has determined that additional security controls are required following the policy compliance verification

and health check step, appropriate security controls will be implemented based on the risk level.

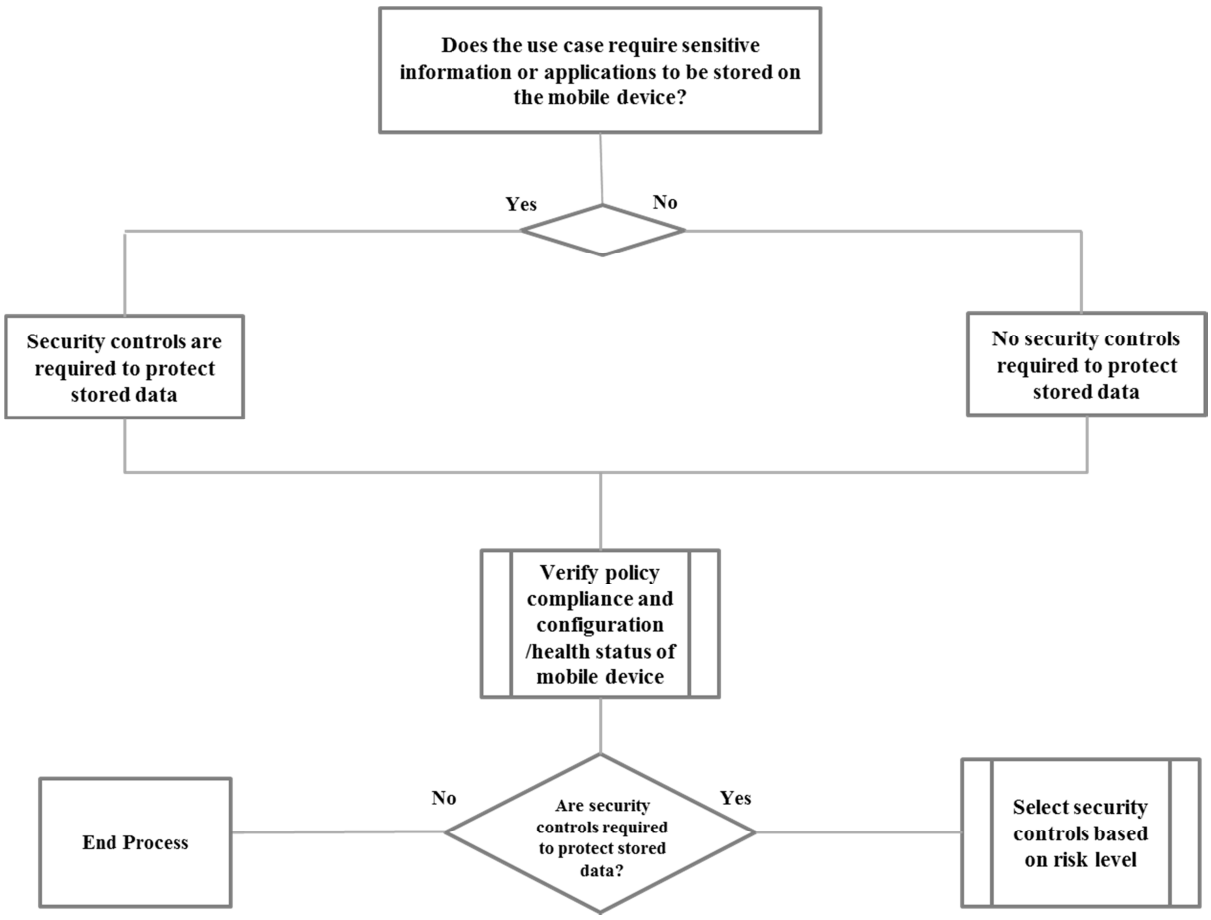


Figure 5-3: Logic for Implementing Use Case Elements

If the risk level is high in that the mobile device is used to access high-risk applications and sensitive information, then the mobile device should be fully-managed. The concept of fully-managed is explained in Section 5.2.3. Likewise, if the risk level is medium, then the device should be partially managed.

5.5 The Derived Mobile Security Architecture Model

The practical mobile security architecture model that is based on the modifications presented in the previous sections is illustrated in Figure 5-4. The implementation of the security controls illustrated in the model depends largely on the use case for the mobile device endpoint, and the security controls presented in the architecture model might not therefore be used in its entirety. Other factors that influence the type of controls to be used are cost, impact on user experience and impact on other solutions and use cases. As much as the architecture model can be customised to align with a specific use case, organisations should also adapt their policies and approaches to align with their predetermined use cases.

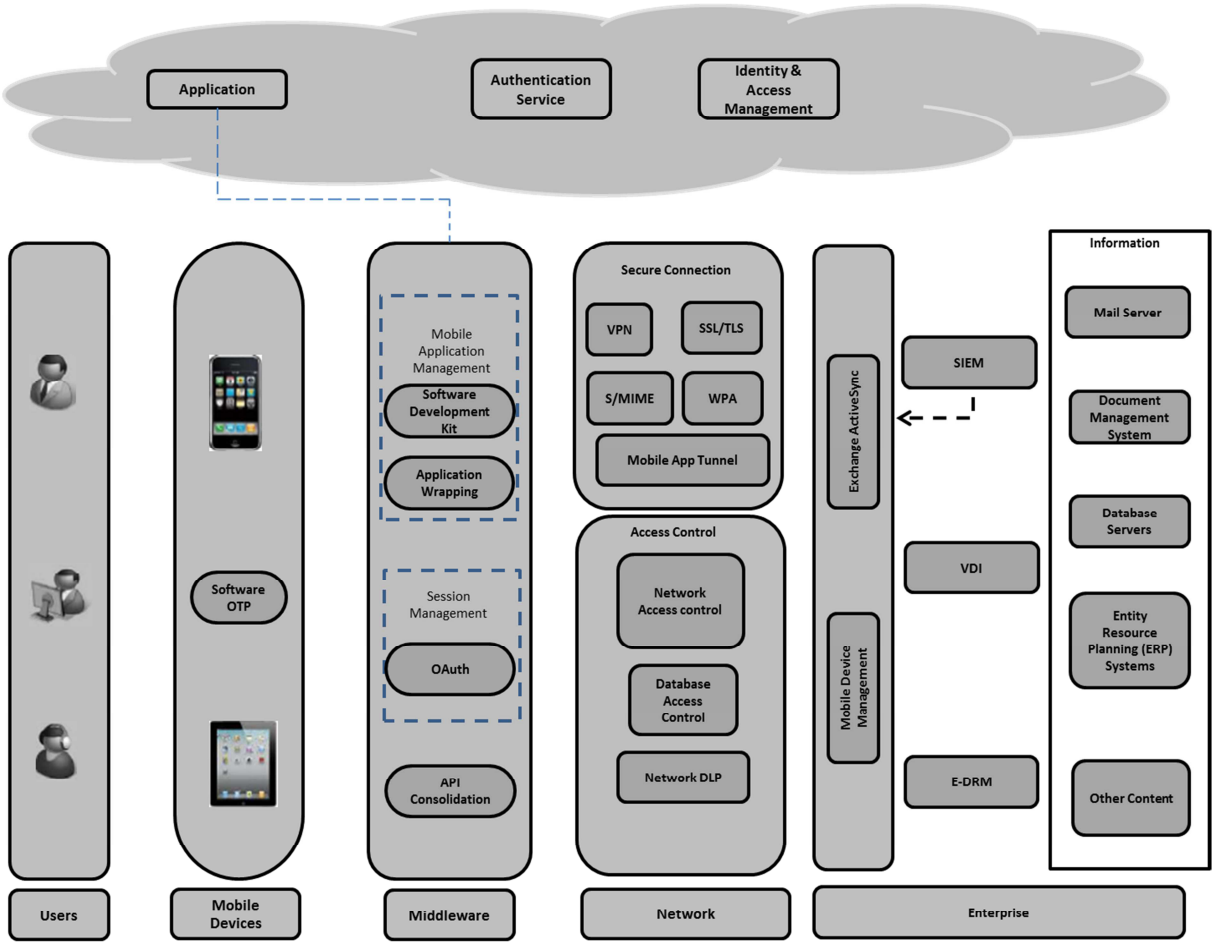


Figure 5-4: Derived Mobile Security Architecture Model

This derived architecture model uses defence-in-depth by implementing various layers of security mechanisms to restrict access to corporate information and applications. The first layer is the user. Once the user successfully authenticates using the mobile device, the user is subjected to various security mechanisms that determine whether the user will be granted access to corporate information and applications via controlled processes. The proposed model combines middleware, network, application and information architectures to allow mobile devices to gain secure access to corporate information; irrespective of mobile device type, its ownership, or where it is located. As described in Section 5.2.3, access to enterprise applications is managed by the middleware layer. The network layer consists of infrastructure-centric security mechanisms to enable secure connection and to control access to the enterprise. The cloud-based security mechanisms consist of OTP authentication services and IAM. A layer of on-premise security mechanisms such as MDM and Exchange ActiveSync is implemented as another defence-in-depth layer prior to the information layer.

5.3 Dependencies and Constraints

The technologies required to develop a practical mobile architecture model have a strong dependence on the type of mobile device. Mobile devices vary in their capabilities and

maturity. This phenomenon was explained in Section 3.7, that the handling of authentication certificates differs from one mobile device to another, and that currently only the BlackBerry vendor (Research In Motion) provides smartcard readers that can pair the mobile device to the workstation to offer two-factor, smartcard authentication (Jaquith, 2010a). The choice of authentication mechanism is influenced by the type of device used.

Furthermore, the technologies required to develop a practical mobile architecture model have a strong dependence on adequate connectivity to allow communication between mobile devices and the back-end infrastructure. However, situations of inadequate connectivity such as lack of cellular coverage and lack of Wi-Fi signal are inevitable (Glazer, 2012). It is therefore imperative that this constraint be taken into consideration when selecting the component security mechanisms for this practical model. While some security mechanism such as authentication and authorisation can either take place locally on the mobile device or on an external service, it is always advisable to ensure that none of the security mechanisms are executed on the mobile device. An alternative is to allow the system to employ a specific security mechanism in an adaptive manner based on some risk calculation to use connectivity sparingly (Glazer, 2012). For instance, some portions of a mobile application might be configured not to request authentication while the more sensitive data and application functions are configured to authenticate to an external authentication service.

Finally, the type of security controls that can be implemented on the mobile device endpoint are constrained by device ownership – whether the device is owned by the organisation or owned by employee. The security controls implemented on a device that is owned by the employee can be removed without the permission of the organisation because the employee has administrator privileges on the device. Likewise, the employee can sell the mobile device containing organisation information without the consent of the organisation, and without providing the organisation an opportunity to erase that sensitive information (Maiwald & Blum, 2012).

5.5 Summary

In this chapter, the utopian architecture model that was initially presented in Chapter 3 is modified to derive a mobile security architecture model that can be implemented in a real-world environment. The proposed mobile security architecture model leverages on cloud computing and goes beyond MDM toolsets to provide a broader perspective in addressing business, technical and organisational requirements. The model makes use of use cases to ensure that conflicting architecture requirements are adequately analysed. Conflicting

architecture requirements refer to a situation where the mobile architecture implements controls that are in conflict with each other and that have inadvertent outcomes such as unmet business requirements or poor user experience. The proposed model ensures that the implemented controls are (directly or indirectly) correlated to user and business requirements, and that the implemented controls are commensurate to the risk. In the next chapter, brief summaries and conclusions are drawn from each of the previous chapters.

Chapter 6 : Conclusion

6.1 Introduction

This chapter summarises the work presented for this research and describes how the research objectives were met and how the research questions were answered. The chapter closes by considering future work that warrants further research.

6.2 Brief Summary of Research Objectives

The five objectives outlined in Section1.3 are reiterated as follows:

1) to understand the drivers for the implementation of data-centric security controls;

2) to examine the data-centric security approach and understand how it can be used to mitigate risks that mobile devices bring to corporate information;

3) to analyse the strengths and shortcomings for each technology in an effort to identify gaps in technologies used to implement this model; and

4) to propose a reference architecture framework that will address the identified gaps and ensure an effective implementation of the data-centric security model that is aligned with business objectives.

All the above-mentioned objectives were met. The first objective is addressed in Section 2.3 where the fundamental elements that are believed to be the drivers towards a data-centric security approach are described. These drivers, or elements, are positioned as risks that mobile devices bring to bear on corporate information. The second objective is addressed in Section 2.4 by reviewing related work where the data-centric security concept is applied. Related work conclusively highlighted the need for using the data-centric approach in mitigating the risks that mobile devices bring to corporate information. The third objective is addressed in the remainder of Chapter 2, by reviewing literature pertaining to VDI, MDM, and E-DRM and identifying shortcomings inherent in each of these technologies. These shortcomings, or gaps, are then addressed in greater detail in Chapter 3, from which a reference architecture framework that minimises these identified gaps is proposed. The fourth objective is therefore addressed in both Chapter 3 and Chapter 5.

6.3 Summarised response to the Research Question

The question that this research answers is whether or not current technology implementations designed to mitigate risks from mobile devices, actually address business requirements. This

research question, answered through a qualitative study described in Chapter 4, determined some level of inconsistency between the data-centric security controls and business requirements. As described in detail in Section 4.7, this inconsistency is instigated by the fact that organisations implement the information security controls on a very reactive and tactical basis. The mobile security architecture models proposed in this research allow organisations to bridge this gap between information security controls and the objectives of the business strategy, in particular by using SABSA as the underpinning framework. The proposed models take into account both general business requirements as well as specific business requirements for security, and relate security controls and security services directly to business requirements – a relationship that is too often concealed by presenting security controls and security services as the *only* solutions to the problem.

To mitigate the risks derived from mobile devices to corporate information, we require a framework that adopts data-centric security concepts of protecting information (rather than the device) throughout the entire lifecycle of this information. To this end, a model for achieving these objectives has been presented.

6.4 Future Work

- Future work should focus on viewing security as an integral part of information management to ensure that information is protected throughout its entire lifecycle. Information Lifecycle Management is also a discipline that lacks academic literature.
- Integrating Mobile Device Management toolsets with Public Key Infrastructure provides a certain level of cryptographically secure means of authenticating mobile identities. However, at the time of this research, the avenues of integrating MDM solutions with Identity and Access Management to provide mechanisms for authorising these mobile identifies to perform specific actions within the enterprise has not yet been widely explored.
- The native standards and protocols that already exist to provide certificate-based authorisation in a PKI environment (e.g. SPKI/SDSI) have not been widely adopted (Thompson, Essiari & Mudumbai, 2003). Certificate based authorisation of mobile identities is certainly an area that could branch off into significant research of its own.
- Since mobile computing requires personal information to co-exist with corporate information on the same mobile device, segregation of corporate information from personal information is vital. Currently segregation can only be achieved using MDM systems or 3rd party toolsets such as Apple's Boot Camp or AT&T's Toggle through authentication, encryption and virtualisation (Disabato & Berenbaum, 2012). Future

work should focus on developing segregation capabilities natively within the mobile operating system. Likewise, data loss prevention capabilities should be built directly into the operating system, restricting information flow between the segregated environments.

- Lastly, the merging of digital identity credentials stored on smart ID cards with the new technologies being built into mobile devices generate numerous opportunities for research around the areas of allowing organisations to store their employee's digital identities on NFC-enabled mobile device's secure elements to provide secure access to corporate resources. At the time of this research, NFC-enabled mobile devices are still a rare breed, with absolutely no NFC-enabled mobile devices from Apple, and only a few devices supported by BlackBerry and Android (Diodati, 2011). According to (Glazer, 2012), approximately 50% of mobile devices will be NFC-enabled only in 2015. This presents an additional area for future research and development in building optimised capabilities for IAM toolsets to manage NFC-enabled devices once the smart card management systems and other authentication services have fully matured.

6.5 Final Word

While the previous section recommends a number of future technology improvements for mobile security, the real controls for mitigating risks that mobile devices bring to organisations will not be completely from technology. Instead, they will only be fully realised with better management of people *and* processes – better business processes, and much more user awareness and training. These risks will be mitigated using policies, procedures and a well-behaved user base – in addition to the technologies that are aligned to business requirements.

This research presents a different approach to mitigating mobile device risks, one that drives security controls from a business requirements perspective, thereby allowing business people to realise an inherent benefit or Return on Investment (ROI) from information security in general.

As much as tradesmen might bring their own tools to a construction site, employees will continue bringing their own mobile devices to the workplace. With the growing trends such as BYOD, consumerisation of IT and "externalisation of IT" (e.g. cloud computing), organisations will continue introducing and interacting with unmanaged mobile devices that are not under their ownership. Organisations will have to extend their existing security strategies used for traditional workstations to mobile devices. The risks that mobile devices

bear on an organisation's information will not be fully mitigated, but organisations must seek to strike a balance between the risks and the benefits that mobile devices bring to organisations – sometimes the risk of not using mobile devices and taking advantage of its benefits outweighs the risk highlighted in this research. A comprehensive approach is essential in dealing with mobile device risks, one that focuses on protecting the information – and data-centric security approach – rather than the device itself.

References

Abatan, P. (2010). *Enterprise Digital Rights Management*. Retrieved March 18, 2012, from http://enterprisedrm.tumblr.com/

Amerk. (2012). *Connecting iPads to an enterprise wireless 802.1x network using certificates and network device enrolment services (NDES).* Retrieved June 24, 2012, from http://blogs.technet.com/b/pki/archive/2012/02/27/ndes-and-ipads.aspx

Amitay, D. (2011). *Big brother removed from app store*. Retrieved November 18, 2012, from http://danielamitay.com/blog/

Andress, A. (2003). *Surviving security: How to integrate people, process, and technology.* (2nd edn). Florida, USA: Auerbach Publications. ISBN-10: 0849320429

Arnab, A.& Hutchinson, A. (2005). Requirement analysis of enterprise DRM systems. *Information Security for South Africa (ISSA) 2005.* Retrieved April 21, 2011, from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/024_Article.pdf

Ashley, P., Vandenwauver, M.& Siebenlist, F. (2000). Applying authorization to intranets: Architectures, issues and APIs. *Computer Communications, 23* (17), 1613-1620.

Ask, J. (2011). *Augmented Reality: Emerging tools to explore*. Forrester Research, Inc. December 22, 2011.

Barker, E., Barker, W., Burr, W., Polk, W. & Smid, M. (2011). Recommendations for key management - part 1: General (revision 3). *NIST Special Publication 800-57,* 27-47.

Bilger, M., O'Connor, L., Schunter, M., Swimmer, M.& Zunic, N. (2006). Data Centric Security: Enabling Business Objectives to Drive Security. White paper (December 2006), Retrieved February 18, 2011, from http://whitepapers.techrepublic.com./abstract.aspx

Blasing, T., Batyuk, L., Schmidt, A. D., Camtepe, S. A.& Albayrak, S. (2010). An Android application sandbox system for suspicious software detection. *5th International Conference on Malicious and Unwanted Software (MALWARE), 19-20 Oct. 2010,* 55-62, doi: 10.1109/MALWARE.2010.5665792.

Boehmer, W. (2008). Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001. *SECURWARE'08: Proceedings of Second*

IEEE International Conference on Emerging Security Information, Systems and Technologies, 25 - 31 Aug 2008, 224-231, doi: 10.1109/SECURWARE.2008.7.

Botehlo, B. (2010). It's official: Microsoft overhauls its VDI licensing strategy. Retrieved March 25, 2011, from http://searchvirtualdesktop.techtarget.com/news/1505627/Its-official-Microsoft-overhauls-VDI-licensing-strategy

Botehlo, B. (2012). Microsoft licensing rules for BYOD not set; beware of snags. Retrieved August 4, 2012, from http://searchenterprisedesktop.techtarget.com/news/2240114591/Microsoft-licensing-rules-for-BYOD-not-set-beware-of-snags

Bourne, V. (2012). *Workshifting: a global market research report.* Retrieved September 8, 2012, from http://www.citrix.com/site/resources/dynamic/salesdocs/Citrix_Workshifting_Index_Whitepaper_FINAL.pdf

Brook-Bilson, R. (2012). *Amkor technologies case study*. San Jose, CA: Adobe Systems, Inc. Retrieved July 18, 2012, from http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/customer-success/pdfs/amkor-case-study.pdf

Bu, Z. (2012). *McAfee threat report: Second quarter 2012.* McAfee Inc. Retrieved November 30, 2012, from http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q2-2012.pdf

Burr, W. E., Dodson, D. F.& Polk, W. T. (2006). Electronic authentication guideline.*NIST Special Publication, 800*- 63. Retrieved March 12, 2012, from http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf

Canetti, R. (2004). Universally composable signature, certification, and authentication. *Proceedings of 17th IEEE Computer Security Foundations Workshop, 28 - 30 June 2004*, 219-233, doi: 10.1109/CSFW.2004.1310743.

Carter, G. (2009). *LDAP system administration*. Cambridge: O'Reilly Media, 11-29.

Chansanchai, A. (2011). *Malware infects more than 50 android apps*. Retrieved August 13, 2012, from http://www.nbcnews.com/id/41867328/ns/technology_and_science-security

Cheung, S.& Chiu, D. K. W. (2003). A watermarking infrastructure for enterprise document management.*Proceedings of the 36th Annual Hawaii International Conference on System Sciences,* 10 -15, doi: 10.1109/HICSS.2003.1174246

Chittaranjan, G., Blom, J.& Gatica-Perez, D. (2012). Mining large-scale smartphone data for personality studies. *Personal and Ubiquitous Computing*, 1-18. Retrieved January 11, 2013, from http://publications.idiap.ch/downloads/papers/2011/Chittaranjan_PUC_2012.pdf

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R.& Molina, J. (2009). Controling data in the cloud: Outsourcing computation without outsourcing computation. *CCSW'09: Proceedings of the 2009 ACM Workshop on Cloud Computing Security,* 85-90, doi:10.1145/1655008.1655020.

Cisco Systems. (2012). *Mobile collaboration in the public sector: Work your way*. San Jose, USA: Cisco Systems, Inc. Retrieved August 16, 2012, from http://www.cisco.com/web/strategy/docs/gov/next_gen_mobile_collab_whitepaper.pdf

Citrix. (2011). *Desktop virtualisation and security: A global market research report.* Retrieved May 29, 2012, from http://www.citrix.com/site/resources/dynamic/additional/Security_Index_Whitepaper.pdf

Corella, F. (2004). *Public Key Infrastructure*. US Patent No. 1,117,206. Washington, DC: U.S. Patent and Trademark Office. Retrieved September 10, 2012, from http://www.freepatentsonline.com/EP1117206.html

Corrad, A., Montanari, R.& Tibaldi, D. (2004). Context-based access control management in ubiquitous environments. *Proceedings of third IEEE International Symposium on Network Computing and Applications, 2004 (NCA 2004), 30 Aug - 1 Sept 2004,* 253-260, doi: 10.1109/NCA.2004.1347784.

Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M.& Abowd, G. D. (2001). Securing context-aware applications using environment roles. *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies,* 10-20, doi10.1145/373256.373258.

Cullen, J.& Peairs, M. (1999). *Document Management System.* U.S. Patent No. 5,893,908. Washington, DC: U.S. Patent and Trademark Office.

Dankers, J., Garefalakis, T., Schaffelhofer, R.& Wright, T. (2002). Public key infrastructure in mobile systems. *Electronics & Communication Engineering Journal, 14*(5), 180-190.

Dr Macenstein. (2008). *Is aurora feint the iPhone's first spyware?* Retrieved August 4, 2011, from http://web.archive.org/web/20080724140502/http://macenstein.com/default/archives/1523

Dudney, B.& Adamson, C. (2009). *iPhone SDK development*. Cambridge: O'Reilly Media, 14-62.

Eagle, N., Pentland, A. S.& Lazer, D. (2009). Inferring friendship network structure by using mobile phone data. *Proceedings of the National Academy of Sciences, 106*(36), 15274-15278.

Edwards, C. (2011). Calling Dr. Jekyll. *Engineering & Technology, 6*(3), 56-59.

Elisabeth Howitt. (2010). *Why enterprise rights management matters: How to keep corporate data from walking out the door.* Retrieved November 8, 2011, from http://www.computerworld.com/s/article/9175850/Why_enterprise_rights_management_matters_How_to_keep_corporate_data_from_walking_out_the_door

Engler, T. (2011). *Severity of vulnerabilities is worrying (translated).* Heise Online. Retrieved September 11, 2011, from http://www.heise.de/preisvergleich/?fs=schaerfegrad%20der%20schwachstellen%20ist%20besorgniserregend

Enzer, G. (2011). *Sophos reveals lax mobile device password use*. Retrieved August 10, 2011, from http://www.itp.net/585754-sophos-re

Espinoza, M. (2012). *Frost & Sullivan applauds AirWatch's comprehensive customer-focused MDM platform.* Retrieved December 3, 2012, from http://www.frost.com/prod/servlet/press-release.pag?Src=RSS&docid=265644249

Farrow, R. (2009). *iPhone hack, take two.* Retrieved January 14, 2011, from http://rikfarrow.com/iphone-take-2.html

Felt, A. P., Finifter, M., Chin, E., Hanna, S.& Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices,* 3-14.

Ferrer, M. (2012). *Economies of scale: A perspective on cross-platform vulnerabilities.* Retrieved January 6, 2013, from http://blogs.technet.com/b/mmpc/archive/2012/07/31/economies-of-scale-a-perspective-on-cross-platform-vulnerabilities.aspx

Fischer, D. (2012). *The rise of cross-platform malware*. Retrieved August 24, 2012, from http://threatpost.com/en_us/blogs/rise-cross-platform-malware-082412

Freeman, E. H. (2007). Holistic information security: ISO 27001 and due care. *Information Systems Security, 16(5),* 291-294, doi: 10.1080/10658980701746478

Friedman, L. (2012). *LinkedIn privacy issues: Possible password breach; iOS app data leak.* Retrieved June 6, 2012, from http://www.macworld.com/article/1167113/linkedin_privacy_issues_possible_password_breach_ios_app_data_leak.html

Fritsch, J. (2008). *No Borders - De-perimeterization and life after the firewall*. Retrieved March 18, 2011, from http://nnc3.com/LinuxMag/Magazine/Archive/2008/89/060-063_deperiment/article.html

Gartner, *Managing the Next Generation of Client Computing.* Cosgrove, T. February 8, 2011.

Gartner, *Critical capabilities for mobile device management*. Basson, M.& Redman, P. August 8, 2012.

Gartner, *On the verge: Strong authentication as a service*. Diodati, M. June 15, 2010.

Gartner, *The evolving intersection of mobile computing and authentication*. Diodati, M.. December 22, 2011

Gartner Press Release, *"Mobile device certificate enrolment: Are you vulnerable?"*. Diodati, M. July 2, 2012. http://blogs.gartner.com/mark-diodati/2012/07/02/mobile-device-certificate-enrollment-are-you-vulnerable/

Gartner, *Key elements of a mobile architecture*. Disabato, M.& Berenbaum, J. October 16, 2012

Gartner, *Decision point for identity and access management in mobility projects*. Glazer, I. August 3, 2012

Gartner, *Decision point for mobile endpoint security*. Maiwald, E.& Blum, D. July 10, 2012

Gartner, *Magic Quadrant for Security Information and Event Management*. Nicolett, M.& Kavanagh, K. M. June 2, 2009

Gartner, Symposium/ITExpo Presentation, *"Gartner says consumerisation will be the most significant trend affecting IT During the next 10 years"*. Pettey, C. 17 - 21 October, 2005

Gartner, *Getting Your Organisation Ready to Deploy Enterprise Digital Rights Management*.Quellet, E.August 3, 2010

Gartner, *Key Selection Criteria for Enterprise Digital Rights Management Solutions*. Quellet, E.& Wagner, R. June 29, 2010

Gartner, *Forecast: PC installed base, worldwide, 2006 - 2015*. Raphael Vasquez & George Shiffler.March 24, 2011

Gartner, *Magic Quadrant for Mobile Device Management Software*. Redman, P. , Girard, J.& Basso, M. May 17, 2012

Gartner, *Magic Quadrant for Mobile Device Management Software*. Redman, P., Girard, J.& Wallin, L. April 13, 2011

Gartner, *Identity and Access Management Defined*. Witty, R., Allan, A., Enck, J.& Wagner, R. November 4, 2003

Gartner, *Three crucial security hurdles to overcome when shifting from enterprise-owned devices to BYOD*. Zumerle, D. December 4, 2012

Gascón, D., Bielsa, A., Genicio, F.& Yarza, M. (2011). *Over the air programming with 802.15.4 and ZigBee - OTA*.Libellium. Retrieved March 30, 2012, from http://www.libelium.com/over_the_air_programming_OTA_802.15.4_ZigBee

Gill, N. (2011). *Credant survey finds consumers left thousands of laptops and smartphones at airports across the United States*. Schwartz Communication. Retrieved July 13, 2011, from http://www.credant.com/news-a-events/press-releases/238-credant-survey-finds-consumers-left-thousands-of-laptops-and-smart-phones-at-airports-across-the-united-states.html

Gonzalez, M. C., Hidalgo, C. A.& Barabasi, A. L. (2008). Understanding individual human mobility patterns. *Nature, 453*(7196), 779-782.

Goodin, D. (2009). *Backdoor in top iPhone games stole user data, suit claims*. The Register. Retrieved November 8, 2009, from http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/

Grandison, T., Bilger, M., T., O'Connor, L., Graf, M., Swimmer, M., Schunter, M., Wespi, A. &Zunic, N. (2007). Elevating the discussion on security management: The data centric paradigm. *Second IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM 2007), 21 - 21 May 2007*, 84 - 93, doi: 10.1109/BDIM.2007.375015.

Gray, B. (2012). *Define a roadmap for mobile security and operations.* Forrester Research, Inc. May 16, 2012.

Graziano, D. (2012). *Android is under attack: New malware threats tripled in Q2 2012.* Retrieved December 12, 2012, from http://bgr.com/2012/08/17/android-malware-q2-2012-study/

Greenfield, D. (2012).*Will the iPad and android tablet save business continuity?* Network World. Retrieved March 24, 2012, from http://www.networkworld.com/community/blog/will-ipad-and-android-tablets-save-business-continuity

Gupta, A., Kuppili, P., Akella, A.& Barford, P. (2009). An empirical study of malware evolution. *First International Communication Systems and Networks and Workshops,(COMSNETS),* 1-10.

Gupta, V. (2012). *Tips to overcome information rights management implementation challenges.* Retrieved November 22, 2012 from http://www.seclore.com/Tips%20to%20overcome%20information%20rights%20management%20implementation%20challenges.pdf

Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. *Proceedings of the Sixth USENIX Security Symposium,* San Jose, CA, *14*, 77-90.

Habberman, M.& Burns, A. (2012). R*omney's fail whale: ORCA the vote-tracker left team flying blind*. Retrieved November 8, 2012 from http://www.politico.com/blogs/burns-haberman/2012/11/romneys-fail-whale-orca-the-votetracker-149098.html

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., Feldman, J. A., Appelbaum, J.& Felten, E. W. (2009). Lest we remember: Cold-boot attacks on encryption keys. *Communications of the ACM, 52*(5), 91-98, doi: 10.1145/1506409.1506429

Haller, N., Metz, C., Nesser, P.& Straw, M. (1996). A one-time password system. *Internet Standard, RFC1938*. Retrieved February 16, 2011, from http://www.hjp.at/doc/rfc/rfc2289.html

Hammond, J., Rymer, J.& Kroll, A. (2010).*Does HTML-5 herald the end of RIA plug-in's? not really*. Forrester Research, Inc. April 21, 2010.

Hand, J. (2012).*Virtualisation history.*VMBlog. Retrieved February 3, 2012, from http://vmblog.com/archive/2012/02/02/virtualization-history-has-an-impact-on-windows-server-backup.aspx

Hill, B. W.& Jacquith, A. (2010). *Markert overview: Enterprise Rights Management.* Forrester Research, Inc. June 3, 2010.

Hoffman, D. (2006). *An Data-centric approach to information security.*Virtualisation. Retrieved March 23, 2011, from http://virtualization.sys-con.com/node/171199

Huh, J. H., Lyle, J., Namiluko, C.& Martin, A. (2011). Managing application whitelists in trusted distributed systems. *Future Generation Computer Systems, 27*(2), 211-226.

Husson, T. (2011). *Mobile Augmented Reality.* Forrester Research Inc. January 4, 2011

ISACA. (2010). Securing mobile devices. *ISACA Emerging Technology Whitepapers.* Retrieved May 16, 2010, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx

ITWeb Surveys.(2012). *Mobile security survey.* Retrieved September 16, 2012, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=56485&Itemid=2801

Jakobson, G.& Weissman, M. (1995). Real-time telecommunication network management: Extending event correlation with temporal constraints. *Proceedings of the Fourth International Symposium on Integrated Network Management IV,* 290-301.

Jaquith, A. (2010a). *Apple's iPhone and iPad: Secure enough for business?* Retrieved January 8, 2013, from http://www.utahta.wikispaces.net/file/view/apples_iphone_and_ipad_secure_enough_for.pdf

Jaquith, A. (2010b). *The mobile security theat is overblown: The complete post*. Retrieved April 8, 2010, from http://blogs.forrester.com/andrew_jaquith/10-04-07-mobile_security_threat_overblown_complete_post

Jeff, B. (2012). *Absinthe 2.0 proves jailbreaking is as popular as ever*. Retrieved May, 28, 2012, from http://www.idownloadblog.com/2012/05/28/absinthe-2-0-proves-jailbreaking-is-as-popular-as-ever/

Jerbic, M., Keck, R.& Satola, D. (2007). Information security strategy: A framework for Data-centric security governance. *The Open Group Forum, Business Law Section.* 1-16. Retrieved August 2, 2011, from https://www2.opengroup.org/ogsys/catalog/w075

Jericho Forum.(2007). Business rationale for de-perimeterisation. *Jericho Forum - White Paper.* Retrieved February 11, 2011, from https://www2.opengroup.org/ogsys/catalog/W127

Jericho Forum. (2008a). (The need for) inherently secure communications. *Jericho Forum - Technology Paper,*1-6.

Jericho Forum. (2008b). Framework for Secure Orientated Collaboration Architectures (O-SCOA). *The Open Group Forum - Technical Guides.* Retrieved September 30, 2012, from https://www2.opengroup.org/ogsys/catalog/G127

Joanne Cummings. (2004). *Security in a world without borders*. Retrieved November 4, 2011, from http://www.networkworld.com/buzz/2004/092704perimeter.html.

Kalkbrener, J.& McCampbell, A. (2011). The advent of smartphones: A study on the effect of handheld electronics on Personal and professional productivity. *Journal of Applied Global Research, 4*(8), 1-9.

Kane, C.& Gray, B. (2011). *10 lessons from the early adopters of mobile device management solutions*. Forrester Research, Inc. September 19, 2011.

Kane, C.& Gray, B. (2012). *Market overview: On-premises mobile device management solutions.* Forrester Research, Inc. February 22, 2012.

Kent, S. (2005). *IP encapsulating security payload (ESP)*. Retrieved May 15, 2012, from http://tools.ietf.org/html/rfc4303.html

Kindervarg, J. (2012). *Control and protect information in the era of big data.* Forrester Research, Inc. July 12, 2012.

Kirk L Kroeker. (2009). The evolution of virtualization. *Communications of the ACM - being Human in the Digital Age, 52*(3), 18-20.

Kravets, D. (2009). *iPhonejailbreaking could crash cellphone towers, apple claims.* Retrieved February, 20, 2010, from http://www.wired.com/threatlevel/2009/07/jailbreak/

Laurila, J. K., Gatica-Perez, D., Aad, I., Blom, J., Bornet, O., Do, T. M. T., Dousse, O., Eberle, J.& Miettinen, M. (2012). The mobile data challenge: Big data for mobile computing research. *Mobile Data Challenge by Nokia Workshop, in Conjunction with Int. Conf. on Pervasive Computing, Newcastle, UK.* Retrieved December 29, 2012, from http://research.nokia.com/files/public/MDC2012_Overview_LaurilaGaticaPerezEtAl.pdf

Lawton, G. (2008a). Is it finally time to worry about mobile malware? *Computer, 41*(5), 12-14, doi: 10.1109/MC.2008.159.

Lawton, G. (2008b). New technology prevents data leakage. *Computer, 41(9),* 14-17, doi: 10.1109/MC.2008.394.

Lewis, B. (2011). *Stewardship not ownership, its time for IT to give up control*. Retrieved March 29, 2011, from http://www.infoworld.com/t/it-management/stewardship-not-ownership-its-time-it-give-control-085

Loebenberger, D.&Wielputz, R. (2006). Evolution! from creeper to storm. *Presentation for the Seminar on "Malware",* 1-7.

Luddy, D. (2010). *Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments*. Fort Meade, MD 20755-6737: National Security Agency. Retrieved May 19, 2012, from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Lynas, D. (2012). SABSA security strategy and planning - foundation module F1.Unpublished manuscript.

Madden, J. (2012). *App "wrapping" with mocana mobile app protection*. ConsumerizeIT. Retrieved June 8, 2012, from http://www.consumerizeit.com/blogs/consumerization/archive/2012/06/08/app-wrapping-with-mocana-mobile-app-protection.aspx

Magaudda, P. (2010). Hacking practices and their relevance for consumer studies: The example of the 'Jailbreaking'of the iPhone. *Consumers, Commodities & Consumption, 12(1).*Retrieved February 12, 2011, from http://csrn.camden.rutgers.edu/newsletters/12-1/magaudda.htm

Mann, C. (2002). *Interview with Bruce Schneier*. *The Atlantic News, interview*. Homeland Insecurity. Retrieved April 10, 2012 from http://www.theatlantic.com/past/docs/issues/2002/09/mann.htm

Markiewicz, D. (2011). *Guidelines to data classification.* Retrieved December 15, 2012, from http://www.cmu.edu/iso/governance/guidelines/data-classification.html

Marko, K. (2008). A data-centric security model: Data protection is the ideal supplement to traditional infrastructure security. *Processor Editorial Articles, 30*(26), 25.

McDaniel, P. (2003). On context in authorization policy. *In Symposium on Access Control Models and Technologies: Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies,2(3),* 80-89.

McFadzean, E., Ezingeard, J. N.& Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660.

McQuaide, B. (2003). Identity and access management. *Information Systems Control Journal, 4*, 35-38.

Microsoft Corporation. (2009). *Deploying Active Directory Rights Management Services at Microsoft.* Retrieved May 27, 2012, from http://blogs.msdn.com/b/tonytri/archive/2009/09/23/new-content-deploying-active-directory-rights-management-services-at-microsoft.aspx

Miller, C. (2011). Mobile attacks and defenses. *Security & Privacy, IEEE, 9(4), 68-70,* doi: 10.1109/MSP.2011.85.

Miller, C.& Mulliner, C. (2009). Fuzzing the phone in your phone. *Black Hat Security Conference USA 2009, 25 July - 30 July 2009.* Retrieved July 25, 2011, from http://coffee.mulliner.net/security/sms/feed/smsfuzz_26c3.pdf

Miller, K.& Pegah, M. (2007). Virtualization: Virtually at the desktop. *Proceedings of the 35th Annual ACM Special Interest Group on University and College Computing Services (SIGUCCS) Fall Conference,* 255-260, doi: 10.1145/1294046.1294107.

Mobile Device Management. (2011). *Mobile device management overview.* Retrieved November 13, 2011, from http://www.mobiledevicemanagement.org/mobile-device-management-overview

Mogull, R. (2008a). *Best practices for endpoint data loss prevention*. Securosis, L.L.C. Retrieved January 5, 2013, from https://securosis.com/assets/library/reports/BestPracticesforEndpointDLP.pdf

Mogull, R. (2008b). *Principles of Data-centric security.* Retrieved October 18, 2011, from https://securosis.com/blog/principles-of-Data-centric-security

Moore, G. (1965). Cramming more components into integrated circuits. *Reprinted from Electronics, 38*(8), *April 19,1965, 114, Solid-State Circuits Newsletter (IEEE), 11(5), 33-35,* doi: 10.1109/N-SSC.2006.4785860.

Moren, D. (2009). *Retrievable iPhone numbers mean potential privacy issues*. Retrieved September 29, 2011, from http://www.macworld.com/article/1143047/phone_hole.html

Mukhopadhyay, S., Clark, B.& Tariq, T. (2012). *Mobile Jailbreaking cheat sheet.* Retrieved November, 18, 2012, from https://www.owasp.org/index.php/Mobile_Jailbreaking_Cheat_Sheet

Needham, R. M.& Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM, 21(12), 993-999,* doi: 10.1145/359657.359659.

Neuman, B. C. (1991). Protection and security issues for future systems. *Workshop on Operating Systems of the 90s and Beyond, Springer-Verlag Lecture Notes in Computer Science, 563,* 184-201.

Nosseir, S. (2010). *Data sprawl: Content aware identity and access management to the rescue*. Retrieved October 29, 2011, from

http://community.ca.com/blogs/iam/archive/2010/10/28/data-sprawl-content-aware-identity-and-access-management-to-the-rescue.aspx

Orlando, A., Manion, A.& Shorter, T. (2012). *Vulnerability note VU#971035: Simple certificate enrollment protocol (SCEP) does not strongly authenticate certificate requests.* CERT Vulnerability Notes Database. Retrieved October 16,2012, from http://www.kb.cert.org/vuls/id/971035

Pelino, M. (2010). *Managing Mobile Complexity.* Forrester Research Inc. October 28, 2010.

Pelino, M. (2012). *Benchmarking your enterprise mobile device operations initiatives and plans.* Forrester Research, Inc. October 10, 2012.

Penn, J. (2010). *The state of SMB IT security and emerging trends: 2009 to 2010.* Forrester Research, Inc. January 25, 2010.

Peterson, G. (2005). Service oriented security architecture. *Information Security Bulletin, 10,* 325 - 330.

Petrović, T.& Fertalj, K. (2009). Demystifying desktop virtualization. *Proceedings of the 9th World Scientific and Engineering Academy and Society International Conference on Applied Computer Science*, WSEAS, 241-246.

Phadmanabhan, P. (2010). *VDI post on madden: Good observation, different conclusions.* MokaFive Blog. Retrieved June 25, 2010, from http://blog.mokafive.com/2010/06/vdi-post-on-madden-nice-try.html

Polte, M. (2012). *Are enterprise app stores the future?* Retrieved October 13, 2012, from http://www.networkworld.com/news/tech/2012/101212-enterprise-app-stores-263336.html

Posey, B. M. (2012). *Application whitelisting for virtual desktops*. Retrieved January 30, 2012, from http://searchvirtualdesktop.techtarget.com/tip/Application-whitelisting-for-virtual-desktops

Protalinski, E. (2012) *Charlie Miller: 'difficult to write exploits for android 4.1'*. ZDNet. Retrieved July 18, 2012, from http://www.zdnet.com/charlie-miller-difficult-to-write-exploits-for-android-4-1-7000001073/

Qiu, Y., Zhou, J.& Bao, F. (2004). Mobile personal firewall. *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2004. PIMRC, 5 - 8 Sept 2004, 4*, 2866-2870, doi: 10.1109/PIMRC.2004.1368844.

Rash, W. (2012). *Dropbox password breach highlights cloud security weaknesses*. Retrieved August 3, 2012, from http://www.eweek.com/c/a/Security/Dropbox-Password-Breach-Highlights-Cloud-Security-Weaknesses-266215/

Reveilhac, M.& Pasquet, M. (2009). Promising secure element alternatives for NFC technology. *First International Workshop on Near Field Communication, 2009. NFC'09, 24 - 24 Feb 2009,7*5-80, doi: 10.1109/NFC.2009.14.

Robert Smallworld. (2005). *Enterprise Rights Management heats up.* Retrieved November 13, 2011, from http://www.kmworld.com/Articles/Editorial/Feature/Enterprise-rights-management-heats-up-14320.aspx

Rosewarne, C. (2011). *2011 SA Information Security Thermometer Report*. Retrieved November 19, 2011, from http://www.wolfpackrisk.com/research/sa-information-security-thermometer-survey-2011/

Roussos, G., Peterson, D.& Patel, U. (2003). Mobile Identity Management: An enacted view. *International Journal of Electronic Commerce, 8*(1), 81-100.

Sadun, E. (2009). *iPhone dev: Retrieving user phone numbers.* Retrieved June 27, 2011, from http://arstechnica.com/apple/2009/01/iphone-dev-user-phone-numbers/

Schadler, T. (2010). *A fact-based approach to workforce technology needs assessment.* Forrester Research, Inc. September 27, 2010.

Schadler, T.& Bernoff, J. (2010). *The HERO index: Finding empowered employees.* Forrester Research, Inc. July 22, 2010.

Schadler, T., Gray, B.& Wang, C. P. (2012). *Charter a mobility council with seven tasks.* Forrester Research, Inc. May 7, 2010.

Shacham, H., Page, M., Pfaff, B., Goh, E. J., Modadugu, N.& Boneh, D. (2004). On the effectiveness of address-space randomization. *Proceedings of the 11th Association for Computing Machinery conference on Computer and communications security*. ACM.298-307, doi: 10.1145/1030083.1030124.

Sherman, C. (2012). *Survey employees to target mobility improvement*. Forrester Research, Inc. April 25, 2012.

Sherwood, J., Clark, A.& Lynas, D. (2005). Enterprise security architecture. *Computer Security Journal, 21*(4), 24.

Sivathanu, G., Wright, C. P.& Zadok, E. (2005). Ensuring data integrity in storage: Techniques and applications. *Proceedings of the 2005 Association for Computing Machinery Workshop on Storage Security and Survivability.* ACM.26-36.

Smith, C. (2003). Understanding concepts in the defence in depth strategy. *Proceedings of IEEE 37th Annual International Carhanan Conference on Security Technology, 2003.14-16 Oct. 2003,* 8 - 16, doi: 10.1109/CCST.2003.1297528.

Souppaya, M.& Karen, S. (2012). *Guidelines for managing and securing mobile devices in the enterprise (Draft). NIST Special Publication 800-124*, 2-15.

Stamp, P.,Whiteley, R., Koetzle, L.,& Rasmussen, M. (2005). *Jericho forum looks to bring network walls tumbling down.* Retrieved October 12, 2011, from http://www.cio.com/article/220590/Jericho_Forum_Looks_to_Bring_Network_Walls_Tumbling_Down

Steele, C. (2012). *How not to deploy Mobile App, by Mitt Romney*. ConsumerizeIT. Retrieved November 9, 2012, from http://www.consumerizeit.com/blogs/consumerization/archive/2012/11/09/how-not-to-deploy-a-mobile-app-by-mitt-romney.aspx

Thea. (2008). *"Data sprawl" - not just an IT problem*. OHSAS 18001 Expert. Retrieved November 12, 2012, from http://ohsas18001expert.com/2008/07/21/data-sprawl-not-just-an-it-problem/

Thompson, M. R., Essiari, A.& Mudumbai, S. (2003). Certificate-based authorization policy in a PKI environment. *ACM Transactions on Information and System Security (TISSEC), 6*(4), 566-588, doi: 10.1145/950191.950196/

Tippett, T. (2006). *The fourth generation of malware*. CIO Update. Retrieved February 23, 2012, from http://www.cioupdate.com/trends/article.php/3598621/The-Fourth-Generation-of-Malware.htm

Töyssy, S.& Helenius, M. (2006). About malicious software in smartphones [Electronic Version]. *Journal in Computer Virology. Springler-Verlag, 2*(2), 109-119, doi: 10.1007/s11416-006-0022-0.

Tsang, W., Scheidt, E.& Burkardsmaier, K. (2004). *Final report: Navy STTR - information centric security*. Vienna: Office of Naval Research. Retrieved December 12, 2009, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA421985

Vaarandi, R.& Tehnikaülikool, T. (2005). *Tools and techniques for event log analysis*. Doctoral Dissertation. Tallinn University of Technology.

Vance, A. (2010, January). If your password is 123456, just make it HackMe. *New York Times.* Retrieved February, 18, 2010, from http://www.nytimes.com/2010/01/21/technology/21password.html?_r=0

Versace, S. (2011).*Versace case study.* Retrieved June 12, 2012, from www.booleserver.com

Virsto. (2012). *Virsto VDI survey: Ready for VDI lift off?* Retrieved August 8, 2012, from http://virsto.com/blog/infographic-vdi-research-findings-virsto-2012

Von Roessing, R., Gallego, R., Anderson, K., Dudunetz, C., Pironti, J.& Wood, P. (2012). Securing mobile devices using COBIT 5 for information security.19-22.

Wang, C. P. (2012). *Prepare for anywhere, anytime, any device engagement with A stateless mobile architecture*. Forrester Research, Inc. June 29, 2012

Wang, P., González, M. C., Hidalgo, C. A.& Barabási, A. L. (2009). Understanding the spreading patterns of mobile phone viruses. *Science, 324*(5930), 1071-1076.

Websense® ThreatSeeker®. (2012). *Benefits of your blackberry ID in this attached malware*. Retrieved November 28, 2012, from http://community.websense.com/blogs/securitylabs/archive/2012/08/22/benefits-of-your-blackberry-id-in-this-attached-malware.aspx

Whatis.com. (2006).*What is mobile device management?* Retrieved November 13, 2011, from www.whatis.com

White, D. S. D. (2007). *Limiting vulnerability exposure through effective patch management: Threat mitigation through vulnerability remediation*. Master's thesis. Rhodes University.

Whitehouse, O. (2010). *An analysis of Address Space Randomization on Windows Vista*. Retrieved February 6, 2011, from http://www.symantec.com/avcenter/reference/Address_Space_Layout_Randomization.pdf

Wood, A. (2012, November). *Using desktop virtualisation for BYOD security and management.* Retrieved November 8, 2012, from http://searchvirtualdesktop.techtarget.com/tip/Using-desktop-virtualization-for-BYOD-security-and-management

Yu, Y.& Chiueh, T. C. (2004). Display-only file server: A solution against information theft due to insider attack. *Proceedings of the 4th Association for Computing Machinery workshop on Digital Rights Management* (ACM), 31 - 39, doi: 10.1145/1029146.1029154

Zacharopoulos, N., Karatzas, N.& Leon, P. (2012). *Virtualization Desktop infrastructure (VDI).* Retrieved November 28, 2012, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Desktop-Infrastructure-VDI.aspx

Zdziarski, J. (2012). *Hacking and securing iOS applications: Stealing data, hijacking software, and how to prevent it.* Cambridge: O'Reilly Media.

Zenprise, I. (2012). *The ten "must haves" for secure mobile device management.* Retrieved December 21, 2012, from http://www.zenprise.com/resources/whitepapers

APPENDIX A

SABSA Attributes Taxonomy

Source: (Sherwood, Clark& Lynas, 2005).

APPENDIX B

Sample Consent Letter

RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

COMPUTER SCIENCE DEPARTMENT

Tel: +27 46 603 8291

Fax: +27 46 636 1915

PO Box 94, Grahamstown, 6140

Simphiwe Hector Mayisela

Sir/Madam

This letter serves as a preliminary gesture to obtain consent to conduct an Interview for a Masters' research thesis in Information Security at Rhodes University, South Africa.

The Interview seeks to get information on the implementation and application of Information Rights Management at Wipro Limited.

It is anticipated that I will require an hour of your time in order to conduct the interview.

If you have any further queries, please contact me (Simphiwe.Mayisela@T-Systems.co.za) or my supervisor, Dr Barry Irwin (b.irwin@ru.ac.za).

Appended to this letter is the list of questions that will be used during the interview.

Your assistance will be greatly appreciated.

Yours in service,

Simphiwe Mayisela (Mr).

APPENDIX C

Questionnaire

1. Do you wish to be sent the results of the Survey as well as the Research Thesis?

2. On which Industry does your organisation belong?

3. What is the size of your organisation?

4. On which of the following ranks does your job title fit?

5. Has your organisation implemented any of the following technologies? (Select one or more from the list below):

- Mobile Device Management (MDM)
- Virtual Desktop Infrastructure (VDI)
- Enterprise Digital Rights Manager

6. On which of the following platforms has the above-mentioned Technology been implemented?

	Smartphones	Tablets	Laptops
Mobile Device Management			
Virtual Desktop Infrastructure			
Enterprise Digital Management			

7. Are the following mobile devices employee-owned or corporate-owned?

	Employee owned	Corporate owned
Smartphones		
Tablets		

8. Is there an asset management process in place for tracking the following Corporate issued devices?

	Yes	No
Laptops		
Tablets		
Smartphones		

9. Does a Policy document exist for mobile devices?

10. Does a Data Classification Policy exist?

11. Is data classified and labelled according to its sensitivity?

12. Is data labelled as sensitive properly secured while at rest or in transit? (Please select the one that is applicable):

- Sensitive Data only encrypted at rest
- Sensitive Data only encrypted during transit
- Sensitive Data encrypted both at rest and during transit
- Sensitive Data is NOT encrypted

13. Does your organisation have an Awareness program addressing the importance of securing mobile devices?

14. Is Anti-Virus installed on mobile devices?

- Antivirus installed on Smartphones?
- Antivirus installed on Tablets?

15. For which of the following functions do you use your mobile device for?

- Accessing emails
- Accessing documents (resources) from corporate network

16. Please provide the email address where you wish to be sent the results of the survey as well as the Research Thesis:

APPENDIX D

Interview Questions - Mobile Device Management

Introductory questions:

1. Does your organisation make use of an MDM solution and if so which product(s) are used?
2. How long has the MDM solution been in place?
3. What led to the adoption of MDM toolsets within your organisation? Did the proliferation of mobile devices force your organisation to accept and support mobile devices even though traditionally they were slower to change and support new technologies? Please elaborate.
4. Was a gap analysis performed to see if the existing security policies cover mobile devices?
5. Did you modify existing policies to address mobile device security risks, or did you need to create a separate mobile device policy and/or policies?

Inventory related questions:

6. How does your organisation know the versions of operating systems the users are running on their mobile devices?
7. Does your organisation know exactly all the mobile devices that connect to your corporate network, including those that connect via VPN? How do you inventory these devices?
8. How do you prevent certain devices from connecting to the network if they do not comply with your security, privacy, and data protection policies? What technology toolsets (other than MDM) have you considered to assist in this space?
9. How does IT support such a diverse inventory of mobile devices? Is the support provided internally or is it outsourced to the Vendor(s). If outsourced, does a service level agreement (SLA) exist will the Vendor(s)?

Application related questions:

10. Does your organisation allow employees to run their personal applications on mobile devices while on the corporate network?

11. How do you ensure that the personal applications on mobile devices cannot harm (e.g. viruses) the corporate network and assets?
12. How does IT provide updates or security patches to all mobile applications? How do you manage patches on open source applications (e.g. Android, and android-based applications)?
13. What means do you put in place to ensure that users do not connect to the corporate network using a jail-broken mobile device?

<u>Technology specific questions</u> (please respond with a short answer):

14. Does your MDM solution require password after device unlocked?
15. Does your MDM solution detect if device is jailbroken?
16. Does your MDM differentiate between Company-Liable (CL) and Personal-Liable (PL) devices?
17. How does your MDM solution remove corporate data after deprovisioning (after the employee has left the organisation)?
18. Is your MDM solution capable of deploying OS updates?
19. Does your MDM solution protect profiles with a password?
20. Does your MDM solution Audit administrative user account activity (add user/delete user/wipe device)?
21. Does your MDM solution have the capability to remotely wipe data from a lost or stolen device? Is selective wipe possible?
22. Does your MDM send an alert when the MDM agent is uninstalled from the device?
23. Does your MDM solution restrict access to email, VPN, and Wi-Fi when blacklisted applications are installed? Or if the device is jailbroken?
24. Does your MDM solution Restrict access to email, VPN and Wi-Fi if device has not checked in X days?
25. Does your MDM lock account after invalid attempts?

APPENDIX-E

Interview Questions - Virtual Desktop Infrastructure

1. Was the adoption of VDI within your organisation motivated by cost (lower total cost of ownership (TCO) of workstations) or by security? Please explain.
2. Is VDI deployed on mobile devices (iPads, Smartphones, etc) within your organisations?
3. How does your organisation collect information on diverse mobile device types (make and model), as well as applications deployed in them?
4. Is VDI used to restrict applications that can be run on mobile devices (application whitelisting)?
5. Is VDI used to deploy patches to *supported* OS and applications?
6. Is VDI used to deploy patches to *non-supported* OS and applications?
7. Is the connection channels between the various device types and the back-end virtual server encrypted?
8. Are the virtual desktops classified in terms of criticality? Are the critical desktops segregated from the normal desktops?
9. Does your organisation have standards to govern how the virtual switches, VLAN's, routing protocols, and other networking components should be configured?
10. Is there a client component on your mobile device or workstation that you need to execute to start your VDI session (e.g. VMware View)? Is authentication required to execute the client component?
11. Has VDI made it easier for your organisation to comply with laws and regulations such as the U.S. Sarbanes–Oxley Act of 2002 and the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996, which require back up of certain data?

APPENDIX-F

Interview Questions - Enterprise Digital Rights Management

1. Does your Enterprise DRM solution protect files immediately when they are checked in and out of your document repository or file server?
2. When the contents are copied and pasted to another file, do the security features of the original file get inherited by the new file?
3. Does your Enterprise DRM solution protect documents located in the following information systems (mention those that are applicable):
    a. Enterprise Resource Planning Systems e.g SAP
    b. Knowledge Management Systems e.g. Lotus Notes
    c. Electronic Document Management System e.g. Documentum
    d. Groupware systems e.g. ProjectPlace
    e. Product Data Management (PDM) systems
    f. Other, please specify
4. Is your Enterprise DRM solution able to package the files sent via email with your own security policy in which you define who can open a file and for what purpose, e.g. view, print, save, edit, etc?
5. If yes, do you get a notification via email whenever a recipient opens the file?
6. Does your Enterprise DRM have the capability of further protecting printed documents thus avoiding leaks via printed documents? For instance, can a printed document get the watermark effect over the document itself, as well as the username of the person who printed the document, thus making the person who printed the document obliged to protect the document?
7. Does your Enterprise DRM recognise mobile devices like BlackBerry and iPhone, as well as Symbian, Windows and Android based smartphones? That is, can the enterprise rights (e.g. read, write, print, etc.) that the document has inside the corporate infrastructure be extended to mobile devices, both in file format and in email?

8. Does your Enterprise DRM able to protect information copied from websites. For example you can prevent screen dumps from ERP, or Knowledge based websites?

9. Does your Enterprise DRM encrypt files in accordance with its sensitivity or data classification level?

10. How does your Enterprise DRM authenticate users?

11. Does your Enterprise DRM encrypt database tables and cells?

12. Does your Enterprise DRM define authorisation levels (for reading, editing, etc.) on database tables and cells?