Selected Readings in Cybersecurity

Selected Readings in Cybersecurity

Edited by

Young B. Choi

Cambridge
Scholars
Publishing

Selected Readings in Cybersecurity

Edited by Young B. Choi

This book first published 2018

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-5275-1641-5
ISBN (13): 978-1-5275-1641-0

To My Family with Love.

TABLE OF CONTENTS

Part One: Humans and Information Security

Part Two: Security Systems Design and Development

Part Three: Security Systems Management and Testing

Part Four: Applications of Information Security Technologies

Part Five: Outstanding Cybersecurity Technology Development Trends

FOREWORD

Cybersecurity is becoming an increasingly important topic in our daily conversations today. In this respect, I have been thinking about writing a book about this crucial topic based on my long experience of working in computer networking and telecommunications security and management in industry, research, and academia internationally. I wanted to present a diverse spectrum of Cybersecurity topics in a clear and organized way.

This book is a collection of papers highlighting the current state of the art of Cybersecurity. It introduces significant viewpoints in Cybersecurity in the following five sections: Humans and Information Security, Security Systems Design and Development, Security Systems Management and Testing, Applications of Information Security Technologies, and Outstanding Cybersecurity Technology Development Trends.

This book is mainly for practitioners of the Cybersecurity industry and college faculty/students in the disciplines of Cybersecurity, Information Systems, Information Technology, and Computer Science, etc. as a Cybersecurity primer or textbook.

Each section is composed of relevant subtopics in modular chapters; hence, a set of relevant sections and subtopics with specific papers can be selected flexibly and reviewed based on each reader's customized requirements. Each chapter explains various topics of Cybersecurity using plentiful and up to date articles as references to help a reader in further investigative research.

I have added a set of acronyms used in the papers and indexed frequently used important Cybersecurity related terminologies at the end of the book.

I hope this book can be an excellent, succinct, and handy guide to exploring the discipline of Cybersecurity – to assist in your studies or business as a useful reference.

Please let me know if you find any errors or have suggestions to improve the quality of the book by sending your e-mail to ychoi@regent.edu.

Finally, I thank all the dedicated article contributors who made the publication of this book possible.

August 22, 2018
Young B. Choi, Ph.D.
Regent University, Virginia Beach, Virginia

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The author would like to thank the following article contributors: Jaymee Arputham, John Briggs, Michelle T. Carroll, Dakota Cecil, Brandon Clark, Chad Clukey, Derrick C. David, Zariah Dawson, Sara J. Forkey, Bryan J. Garcia, Randal J. Gooddine Jr., Roy Griffin, Augusta Hayward, Zechariah Heinsius, Shawn Henriquez, Arthur B. Hernandez, David Hiatt, Nathan Hunter, Shady M. Khella, Kenneth LaCroix, Jason Maurer, Michael Molleda, Alphonso Price, Brandon Richard, Christopher M. Sershon, Edward J. Shockley III, Raymond R. Sheldon, Stephen J. Tipton, Eric Vollman, Daniel J. White, and Jillian Yang.

I want to express my sincere thanks to the faculty, staff, and students of the Department of Engineering & Computer Science, the College of Arts & Sciences, and Regent University for their support and encouragement.

The author especially wants to express his special thanks to his student Mr. Shady M. Khella for his excellent editorial work and article contribution and Mr. Chris Cartwright for his thorough proofreading work. Without their dedicated help, the publication work would have been extremely challenging for me. Ms. Helen Edwards of Cambridge Scholars Publishing helped me from the beginning to the end regarding this book publication with wonderful professionalism and kindness. The author wants to express his sincere thanks to her.

The author also wants to say a word of appreciation to the world-renowned Emographer Huh Hwe-Tae for the generous donation of his two beautiful and creative artwork images from his recent series 'Feast of Enumeration' as the front cover of this book. (http://www.moosan.net/)

The author wants to express his deepest appreciation to his academic advisors Dr. Jae-Nyun Park, Professor Emeritus of Sookmyung Women's University; Dr. Gil-Chang Kim, Professor Emeritus of KAIST; and Dr. Jonathan C. Oh and Dr. Adrian Tang, Professors Emeriti of the University of Missouri–Kansas City. They guided and inspired me during my global academic journey. Without their wonderful teaching and guidance, I couldn't have written this book today.

Finally, the author wants to give warm thanks from the bottom of his heart to his beloved parents who sacrificed their whole lives with love for their eight daughters and sons and his five uncles and many other relatives. He wants to dedicate this book to them and his beloved brothers and sisters as a small token of recognition for their warm-hearted, positive encouragement during his long academic journey.

PART ONE

HUMANS AND INFORMATION SECURITY

CHAPTER ONE

HUMAN FACTORS IN INFORMATION SECURITY

ALPHONSO PRICE AND YOUNG B. CHOI

Abstract

We will look at some crucial issues concerning insider threats to information security from employees who may unwillingly play a crucial role in causing significant accidents to an organization's information systems. In a computer security system, no matter how flawlessly designed and implemented, there will be human error involved.

We will address some appropriate technical measures to implement in protecting an organization's information systems and consider ways of designing and creating strong security policies for all staff members. We will briefly cover personality traits, individual differences, mental abilities, and behavior risks. We will also focus on the training and education level and information security awareness among company employees and staff members.

Keywords: Human factors, information security, computer security, insider threats, information systems protection.

Insider Threats

Many organizations have historically tried to develop techniques to safeguard corporate data from data breaches and any other occurrences where information taken without proper authorization. "While many businesses have focused on improving their protections against external cyber-attacks, far fewer have adequate internal protection in place to guard against malicious actions by their own staff" (Groenfeldt, 2014). It is hard enough for organizations to come up with a game plan to try to stop cyber-attacks and hackers from breaching their firewalls, gaining access to their networks, and stealing vital information. The financial strain that placed on many of these corporations is overwhelming.

The majority of society thinks threats to many businesses come from malicious hackers who are prowling the wires looking for a way in. Businesses will direct the majority of their focus on trying to keep the enemy out, while the enemy is in fact an insider: an employee, staff member, or a contractor that has been granted access company networks and is thus in a position to become an even more significant threat to the corporation. "Late 2013, Vodafone Germany confirmed that an attacker with insider knowledge had stolen the personal data of two million of its customers from a server located in Germany. Customer name and address and date-of-birth information and some bank account details were taken." In this case, Vodafone identified the perpetrator as an insider with knowledge of its most sensitive internal systems. Vodafone claims to have up-to-date and well-maintained security systems, but still fell victim to what the company described as "a highly complex attack that was conducted with inside knowledge of its most secure internal systems" (Groenfeldt 2014).

Employees of corporations who have access to highly sensitive and classified data have the most significant opportunity to cause harm, whether it is accidental or malicious. They are the trusted employees, staff members, and contractors given access to all sorts of information, information they are required to protect and not misuse. "Organizations must balance the need to access information for conducting business with protecting this information from unauthorized misuse by trusted personnel. Unauthorized access to sensitive information is routinely considered as an external threat" (Info security, 2012). In addition, there is the notion that accidents happen which can lead to an accidental breach, misplaced classified data, or vital information compromised.

"The insider threat takes two forms: accidental and malicious, and both can compromise corporate assets, including its information" (Info security, 2012). Then there are the unintentional threats "such as walking away from a workstation without locking a session, not securing passwords, or misuse of system procedures due to improper training, which can lead more serious compromises" (Info security 2012). Accidental threats are not rare in the workplace: they can happen at anytime and anywhere. A recent survey of Defense Department IT professionals found that 55 percent said careless and untrained insiders are the greatest source of threats to their agencies' IT security. Moreover, while 66 percent said malicious insider threats could be as damaging or more than external attacks, 56 percent also said the damage done by *careless* insiders could be just as bad as that caused by malicious insiders (McCaney, 2015). Accident and carelessness is pretty much the cause of most data breaches that occur on the part of an employee of that organization or contractor, which caused a rise in this phenomenon. “The FBI this week issued a warning to companies about a rise in hacking by current and former employees. Insider threats, both intentional and accidental, were cited by more than 70 percent of information security managers as their biggest concern in an April survey.” (Strohm, & Robertson, 2014).

Having careless and untrained employees can be considered a significant threat to organizations; some workers may be naive or susceptible to social engineering attacks or victimized by other employees who may have been reprimanded, passed over for a promotion, or terminated. These individuals could quite quickly become targets of malicious software and hacking techniques inflicted on them by disgruntled employees. To distinguish them from the targets, some of these “hackers” may even use their co-worker’s compromised computers as a launch pad to attack unprotected systems further and cause harm and financial damage to the organization. “The most costly data breaches are usually those that are created by a malicious insider. These people normally have access to things external hackers generally don’t have access to.” (Strohm, & Robertson, 2014).

Having to deal with colleagues who display malicious intent creates a toxic work environment, thus making it difficult for employees to perform their assigned tasks; it can be hard to prove to supervisors and upper management sometimes what is going on. “Nearly two-thirds (64%) believe malicious insider threats to be as damaging as or more damaging than malicious external threats, such as terrorist attacks or hacks by foreign governments. Further, 57 percent believe breaches caused by accidental or careless insiders to be as damaging as or more damaging than those caused by malicious insiders.” (Darkreading, 2015).

Malicious insiders come in all shapes, sizes, and colors, but there are many ways of detecting these callous frauds. Let us look at some ways a malicious insider can be detected, non-technical and technical: “**The not-so model employee”** – This individual has consistently been the first in and last out of the office recently. There is much work to do and this individual is pulling long hours. If there is not a project due soon, this could be an indicator that the individual is working on a little *extra-curricular* malicious work (Khimji, 2015). Then there is **“The Ironman streak”** – An individual who has not taken a vacation in a long time may not have had the opportunity to share his or her work with others. If they are keeping their work to themselves without collaborating or having others review it, there is a chance that their project is of that *extra-curricular* malicious nature (Khimji, 2015).

These are the types of threats most co-workers and executive staff would have a hard time detecting, let alone suspecting that there was a threat from inside coming from one of their own. Many organizations are mindful of the numerous external threats that continually try to attack from outside. Fortunately, these organizations are stepping up their efforts in combating this increase in illegal activity. Many have put in place typical countermeasures such as Intrusion Detection Systems (IDS), antivirus software, and firewalls, which are all directed at these unwanted threats. However, these countermeasures offer little to counter that unsuspected more significant threat, which is that malicious insider who has no morals or ethics and who will stop at nothing in trying to sabotage the organization.

The unintentional threat has become an increasing problem for many organizations. Let us look at the definition of what an Unintentional Insider Threat (UIT). "An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems." (Cert Team, 2013).

For example, about a year ago, spear phishers from China infiltrated the *New York Times* website in the hope of gaining access to names and sources that Times reporters had used in a story. A year earlier, Google pulled more than 22 malicious Android apps from the market after the apps where found infected with malware. This year, security blogger Brian Krebs reported, "The breach at Target Corp. that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation. The Target breach spear phishing attack is an example of social engineering and illustrates how an unintentional threat can cause harm to any organization." (Mundie, 2014). It is not easy to know the details of an organization can stop these threats or mitigate the risks posed by these individuals. We certainly hope the right kind of technical and non-technical combination are utilize in thwarting this unusual behavior. "Security awareness training needs to be updated on a constant basis and implemented throughout the organization; this should be something that is mandatory. Employees and contractors should be required to sit through some form of training. There are unintentional threats that are uncontrollable due to certain circumstances. Some can include the employees tricked into providing classified information, hardware and software failure in which equipment may not work correctly. Human errors are known as mistakes that employees may make by leaving their accounts open or losing company provided laptops, and the most destructive unintentional threat to them all is natural disasters like hurricanes, tornadoes, and blizzards" (Karabat, & Karabat, 2012).

Computer Security Systems

"When it comes to computer security, the problems most companies experience can be traced to the living units that interface with their systems. Otherwise known as humans, and with humans come errors." (Berr, 2015). Human operator error has been the cause of many failures and loss of data in numerous IT departments of major corporations. It seems as though either computer security is not strong enough or personnel using the computers are not adequately qualified. "Only 54% of companies offer some form of cybersecurity training, with the format most often being new employee orientation or some kind of annual refresher course" (Berr, 2015). "These mistakes have cost corporations millions in finances, corporate unpredictability, and communications paths have been disrupted; "heavily regulated fields including healthcare, finance, and pharmaceuticals incurred breach costs that were 70% higher than other industries" (Infosecurity, 2013).

Investing in infrastructures that can handle human errors should be near the top of the priority list, but recently, the media has been discussing data breaches possibly been caused by human error, inadvertent data dumps, and transfers. "Together, human errors and system problems account for 64% of data breaches in the global study, while prior research shows that 62% of employees think it is acceptable to transfer corporate data outside the company – and the majority never deletes the data, leaving it vulnerable to leaks." (Infosecurity, 2013). Having strong computer security defense on your computers, networks, and maybe even your smartphone should help protect against accidental or unauthorized access from anyone. There are vast number of threats to computer security that can cause serious damage. Unfortunately, most of these threats come from human error. "The Trojan is one of the most complicated threats among them all. Most of the popular banking threats come from the Trojan family, such as Zeus and SpyEye." (Martino, 2013). "A Trojan has the ability to hide from antivirus detection and steal important banking data to compromise your bank account." (Martino, 2013).

"Looking back 10 years in technology, a virus is something that was really popular. A virus is a malicious program that replicates itself and aims only to destroy a computer. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly if at all." (Martino, 2013). "Worms, one of the most harmless threats are programs designed only to spread. They do not alter your system to cause you to have a nightmare with your computer, but can spread from one computer to another computer within a network or even the Internet" (Martino, 2013). "Spyware is a Malware which is designed to spy on the victim's computer. If infected with it, your daily activity or certain activity may have spyware, and it will find a way to contact the host of this malware. Mostly, the use of this spyware is to know what your daily activity is so that the attacker can make use of your information." (Martino, 2013). "Scareware is something that plants into your system and immediately informs you that you have hundreds of infections which you don't have. The idea here is to trick you into purchasing a bogus anti-malware that claims to remove those threats." (Martino, 2013). "A keylogger is something that keeps a record of every keystroke you made on your keyboard, stealing login credentials." (Martino, 2013). These are just a handful of threats listed.

Information Systems Protection

It seems as though an organization's information systems are either probed or under attack on a constant basis. Unfortunately, there are many computer systems with theoretical and actual weaknesses. The three most important aspects of computer security are Confidentiality, Integrity, and Availability, and these three addresses security in computing. The evolution in the computer industry along with the advancing changes of the internet mean only one thing: the need for new and improved security measures implemented, and policies amended to reflect the latest changes.

There are a couple of ways companies can utilize security measures to "help prevent and respond to insider's intentional or inadvertent disclosure of confidential company information" (Tonsager, 2013). Look at the five privacy and data security measures that can protect your company from unauthorized access and possible theft.

1. "*Internal Privacy and Data Security Principles*: By specifying how the company collects, uses, discloses, and protects the personal data of its customers and employees, internal privacy and data security policies can help companies identify who needs access to confidential data, how this data should be secured, and procedures for effectively deleting or destroying data once it is no longer needed by the

company." (Tonsager, 2013).

2. "*Internet Access and Use Policies*: Many companies implemented employee policies in the 90s governing how employees may access and use the internet and the company's computer networks. However, these policies should be updated as new technologies that may increase the disclosure of confidential company information, such as peer-to-peer programs and third-party mobile applications, emerge." (Tonsager, 2013).
3. "*Social Media Policies*: Social media policies typically govern how employees may use social media for work purposes, and, in some cases, set forth guidelines for employee use of personal social media accounts as well. While these policies help to remind employees that they should be cautious when using social media to avoid the disclosure of confidential or proprietary company information, employers need to ensure that these policies are consistent with federal labor laws and state laws restricting an employer's ability to request access to an employee's personal online accounts." (Tonsager, 2013).
4. "*Robust Protections in Service Provider Agreements*: Confidentiality clauses and nondisclosure agreements with service providers are common and important. However, robust privacy and data security provisions can provide additional protection and mitigate the risk of a breach, especially where the service provider will handle your customer's personal information." (Tonsager, 2013).
5. "*Bring Your Own Device ('BYOD') Policies*: Employers increasingly are allowing employees to use their smartphones, tablets, and other devices to access work e-mail accounts and the employer's computer network. While both employers and employees can benefit from this approach, companies need to make sure that their bring-your-own-device policies provide employees adequate notice and allow employers to implement appropriate data security measures, such as remote wiping tools." (Tonsager, 2013).

Individual Personalities

Do organizations do enough when it comes to background checks on newly hired individuals? Is there enough being done to ensure individuals who have chosen the IT field have the right personality traits like teamwork, drive, dedication, assertiveness, and optimism – to name a few? "A successful team of IT professionals represents a necessary piece of building a successful enterprise. Selecting the right candidates for IT positions includes identifying those who possess the personality traits that provide IT professionals with a robust framework for success within the field." (Long, 2015). IT professionals must have the right chemistry to work with one another to accomplish the tasks assigned.

"IT professionals should possess a desire for continual learning and achievement within the field of IT. Other personality traits you should look for in an IT professional include dependability and the ability to adapt to a changing work environment, such as the need to come in on weekends to address critical systems issues." (Long, 2015). Having the necessary characteristics to deal with customers on a daily basis justifies the need for IT personnel to pass thorough background check. Customer service is a big part of the IT field, and these staff are going to speak to and deal with people who come from all over the world with various backgrounds, and who may have an above average social status.

Training and Education

When someone is trying to establish themselves in the IT field, he or she must consider the copious amount of hours and training that is involved in qualifying in one of many IT certifications offered in the professional IT field. "Training today's cyber professionals requires the use of a broad range of venues to prepare this personnel to operate in a technically challenging environment." (Welsh, 2014). The technical environment is continuously changing, requiring schools to update their training material and to enhance learning objectives continuously. Security awareness is a critical issue and topic.

Several employees are not receiving the proper training on this subject and when adequate training is not sufficient, mistakes will occur. "Security awareness training is a formal process for educating employees about corporate policies and procedures for working with IT. A good security awareness program should educate employees about corporate policies and procedures for working with IT. Employees should receive information about whom to contact if they discover a security threat and be taught that data as a valuable corporate asset. Regular training is particularly necessary for organizations with high turnover rates and those that rely heavily on contract or temporary staff." (Rouse, 2015). Responsibilities for making sure employees are trained rest on the shoulders of the CSO (Chief Security Officer), who is responsible for the company's information systems. "A CSO is the highest-level executive directly responsible for an organization's entire security function. Increasingly, CSOs are not only responsible for their organizations' physical security needs but also their digital or electronic security requirements, including computer networks.

Originally a title used to designate the person most responsible for IT security, the new CSO executive looks at all threats and institutes appropriate security programs." (Guerra, 2015). Therefore, as the CSO, training is critical, and all staff, employees, and contractors should receive the proper training that they are required to receive.

Conclusion

We have described some crucial issues regarding insider threats to information security, protection of information systems and computer security systems, individual personalities, education, and training. Information security systems will forever require human interaction, and the employees and staff members who manage these systems sometimes unknowing and unwillingly play a crucial role in causing significant accidents because of human error or malicious intent. One thing for sure is that personality characteristics, individual differences, mental abilities, and behaviors are an essential part of having the necessary skills in becoming an IT professional.

References

Berr, J. (2015). *Computer Security's Weak Link: Humans*. Retrieved from http://www.cbsnews.com/news/the-human-element-and-computer-security/

Cert Team. (2013). *Unintentional Insider Threats: A Foundation Study*. Retrieved from http://www.sei.cmu.edu/reports/13tn022.pdf

Darkreading. (2015). *Ed Survey Results: Insider Threats*. Retrieved from http://www.darkreading.com/vulnerabilities---threats/ed-survey-results-insider-threats/d/d-id/1318850

Groenfeldt, T. (2014). *Insiders Pose a Serious Threat To Corporate Information*. Retrieved from http://www.forbes.com/sites/tomgroenfeldt/2014/05/08/insiders-pose-a-serious-threat-to-corporate-information/

Guerra, T. (20145). *Roles & Responsibilities of a Chief Security Officer*. Retrieved from http://webcache.googleusercontent.com/search?q=cache:BSdr0uSSMkgJ:work.chron.com/roles-responsibilities-chief-security-officer-19479.html+&cd=4&hl=en&ct=clnk&gl=us

Info security. (2012). *The Good, the Bad, and the Ugly Insider Threats*. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-good-the-bad-and-the-ugly-insider-threats/

—. (2013). *Human Error and System Glitches Drive Nearly Two-Thirds of Data Breaches*. Retrieved from http://www.infosecurity-magazine.com/news/human-error-and-system-glitches-drive-nearly-two/

Karabat, B. Ç., & Karabat, C. (2012). Increasing awareness of insider information security threats in human resource department. *International Journal of Business and Management Studies, Yıl*, *4*.

Khimji, I. (2015). *The Malicious Insider.* Retrieved from http://www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/

Long, N. (2015). *Personalities That Do Well in the IT Industry.* Retrieved from http://smallbusiness.chron.com/personalities-well-industry-10591.html

Martino. (2013). *28 Types of Computer Security Threats and Risks*. Retrieved from http://forums.iobit.com/forum/iobit-security-software/ iobit-security-softwares-general-discussions/other-security-discussions/15251-28-types-of-computer-security-threats-and-risks

McCaney, K. (2015). *The Accidental Hackers: Insiders Pose the Top Threat to DOD Networks.* Retrieved from http://defensesystems.com/articles/ 2015/01/29/dod-insider-threats-it-security-survey.aspx

Mundie, D. (2014). *Unintentional Insider Threat and Social Engineering.* Retrieved from http://blog.sei.cmu.edu/post.cfm/unintentional-insider-threat-social-engineering-090

Rouse, M. (2015). *Security Awareness Training*. Retrieved from http://searchconsumerization.techtarget.com/definition/security-awareness-training

Strohm, C., & Robertson, J. (2014). *Companies' Worst Hacking Threat May Be Their Own Workers*. Retrieved from http://www.bloomberg.com/ news/articles/2014-09-26/companies-worst-hacking-threat-may-be-their-own-workers

Tonsager, L. (2013). *5 Privacy and Data Security Measures That Can Protect Your Company Against Trade Secret Theft*. Retrieved from http://www.insideprivacy.com/data-security/5-privacy-and-data-security-measures-that-can-protect-your-company-against-trade-secret-theft/

Welsh, W. (2014). *Cyber Warriors: the Next Generation*. Retrieved from http://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx

CHAPTER TWO

SECURING BYOD NETWORKS: INHERENT VULNERABILITIES AND EMERGING FEASIBLE TECHNOLOGIES

ARTHUR B. HERNANDEZ
AND YOUNG B. CHOI

Securing BYOD Networks

The popularity of BYOD or "bring your own device" networking for enterprises is on the rise. From 2013 to 2014, there was a 46% increase in companies who planned to support BYOD functions in 2014, or 84% of all companies polled (Clarke, 2013). However, most of these companies intended only to implement a Mobile Device Management (MDM) system. While MDM systems are designed to manage smartphones and tablet devices remotely, according to Clarke (2013), an MDM system will not be enough to secure one's network.

This paper will discuss BYOD networking, how it is accomplished, and technological solutions that are utilized for this purpose and will evaluate some of these security technologies. It will also address inherent vulnerabilities present in BYOD networking.

Keywords: BYOD, BYOD network, MDM, MAUP, SecSDLC, VPN

Background

Before iOS and Android devices became so popular, the majority of employees privileged enough to enjoy a mobile device were issued with a laptop or a Blackberry device, or both. Laptops could be easily managed through VPNs, firewalls, and other commonplace security architecture. To use Blackberry devices with one's network back in the day only required that the organization deploy a BlackBerry Enterprise Server (BES), which allowed network managers to control which devices connected to the network and what activities they could perform. The BES allowed the employees to synchronize their work calendar, contacts, and email with their mobile device and limited access to specific applications and work files outside of the office. Network managers were satisfied with this configuration as BES servers supported “AES and Triple DES encryption to protect and ensure the integrity of wireless data that is transmitted between the BlackBerry Enterprise Server components and devices” (Blackberry, 2014, para. 2). Employees were satisfied because they didn’t know how much better it could get.

Alas, the age of tablets and consumer-oriented smartphones is upon us, each ripe with its unique vulnerabilities and threats waiting to spread to our network like a virulent STD. Worst of all, the employees themselves purchase and own these devices. Ever since we crawled with our first PCs at home, we knew that employees are our most significant threat; and now they have so much more power for ill. And so, we with hands tied behind our back are asked by our management to secure the insecure and protect those that do not want to be protected. So, really…nothing has changed.

Defining an Enterprise MDM Policy or MAUP

The first step in implementing a BYOD network is to plan for how it will affect your network and how you can curtail any increased risk. Thus, one should define an enterprise-wide mobile device management (MDM) policy, also known as a mobile device acceptable use policy (MAUP). This policy can then be incorporated into your organization’s written information security program as an issue-specific add-in.

According to Speed, Nykamp, Anderson, Nampalli, and Heiser (2013), a MAUP “is a formal agreement between an organization and the employees…[that] document[s] acceptable rules for mobile device usage…[and] review[s] any penalties that could be applied resulting from the rule violation from incorrect use of mobile devices” (Appendix D, para. 4). The MAUP should incorporate the concepts of the security systems development life cycle (SecSDLC) including defining the procedures for implementing the BYOD network; the people who will manage this implementation; eligibility criteria to include one’s device(s); hardware and software requirements necessary to implement the MDM policy; and what data will be accessible and in what ways (Whitman, & Mattord, 2012).

Also, as with other issue-specific security policies, it should include at a minimum: 1) a statement of purpose and the scope of the policy; 2) the philosophy of the organization concerning the implementation of the MDM policy; 3) fair and reasonable use as it applies to data owned by the company versus devices owned by the employees with liability defined on both sides; 4) unauthorized or prohibited use, including context, and repercussions for such actions; 5) employer monitoring, if applicable; 6) device management (software updates, antivirus, back up procedures, and MDM agent requirements); 7) physical security requirements and repercussions; 8) a statement about the importance of following the policy including any applicable legal or ethical regulations which are applicable; 9) the responsibilities of device owners, network managers, and organizational leadership, and policy enforcers if they are separate; 9) the policy review schedule; and 10) applicable limitations of liability or disclaimers (Appendix A contains a MAUP template) (Whitman, & Mattord, 2012).

According to Midgley (2013), an effective MDM policy is built on three key pillars. Together these pillars "offer comprehensive visibility and control over all IT endpoints, anywhere, anytime" (Ch. 6, para. 8). These pillars include: 1) framing the organization's mobility needs; 2) defining the organization's security policy; and 3) offering and implementing device management and support solutions (2013). Midgley (2013) continued that by incorporating these three pillars into one's MAUP, the organization would reap the following benefits: 1) reducing risk and cost associated with risk levels; 2) defining a clear roadmap for the technological roll-out of the BYOD network topology; and 3) enabling increased employee productivity, potentially making new services and processes possible, and/or make existing services or processes more efficient.

Choosing an MDM Solution

Network World reviewed six of the most popular MDM solutions (Figure 1 below).

Each of these six systems supports different types of devices which include Android, iOS, BlackBerry, Windows, and a variety of other MAC products. They support servers being placed in the Cloud or on the premises of the organization. They range in price. Network World did not rank any product higher than the others but pointed out that they all have their strengths and weaknesses and would be chosen based on the needs of the network in which they would be installed.

Some additional features of these MDM systems are offering a secure container, device control, app control, and file control. Creating a secure container overcomes the inherent weaknesses present in Android operating systems, in that these devices offer no intrinsic encryption or automatic