

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/263245514>

Mobile device security considerations for small- and medium-sized enterprise business mobility

Article in *Information Management & Computer Security* · January 2014

DOI: 10.1108/IMCS-03-2013-0019

CITATIONS

96

READS

4,045

2 authors:



Mark A. Harris

Augusta University

28 PUBLICATIONS 849 CITATIONS

SEE PROFILE



Karen Patten

University of South Carolina

38 PUBLICATIONS 443 CITATIONS

SEE PROFILE



Mobile device security considerations for small- and medium-sized enterprise business mobility

Mobile device
security
considerations

97

Mark A. Harris and Karen P. Patten

*Integrated Information Technology, University of South Carolina,
Columbia, South Carolina, USA*

Received 8 March 2013

Revised 3 May 2013

12 July 2013

Accepted 13 July 2013

Abstract

Purpose – This paper's purpose is to identify and accentuate the dilemma faced by small- to medium-sized enterprises (SMEs) who use mobile devices as part of their mobility business strategy. While large enterprises have the resources to implement emerging security recommendations for mobile devices, such as smartphones and tablets, SMEs often lack the IT resources and capabilities needed. The SME mobile device business dilemma is to invest in more expensive maximum security technologies, invest in less expensive minimum security technologies with increased risk, or postpone the business mobility strategy in order to protect enterprise and customer data and information. This paper investigates mobile device security and the implications of security recommendations for SMEs.

Design/methodology/approach – This conceptual paper reviews mobile device security research, identifies increased security risks, and recommends security practices for SMEs.

Findings – This paper identifies emerging mobile device security risks and provides a set of minimum mobile device security recommendations practical for SMEs. However, SMEs would still have increased security risks versus large enterprises who can implement maximum mobile device security recommendations. SMEs are faced with a dilemma: embrace the mobility business strategy and adopt and invest in the necessary security technology, implement minimum precautions with increased risk, or give up their mobility business strategy.

Practical implications – This paper develops a practical list of minimum mobile device security recommendations for SMEs. It also increases the awareness of potential security risks for SMEs from mobile devices.

Originality/value – This paper expands previous research investigating SME adoption of computers, broadband internet-based services, and Wi-Fi by adding mobile devices. It describes the SME competitive advantages from adopting mobile devices for enterprise business mobility, while accentuating the increased business risks and implications for SMEs.

Keywords Small- to medium-sized enterprises, Smartphones, Small business, Computer security, Mobile business, Tablets, Security considerations, 4G wireless, Medium business

Paper type Conceptual paper

Introduction

Business mobility capabilities are becoming more critical to an enterprise's everyday business environment. Nokia defined "business mobility" as giving employees the "freedom to collaborate and transact business outside traditional workplaces and times. [Business mobility] is communications on the go, with access to the right information at the right time" (Nokia White Paper, 2006, p. 2). Employees spend more time interacting with customers and vendors and less time at their desks. Instant communications cause customers to also expect immediate responses to any requests,



Information Management &

Computer Security

Vol. 22 No. 1, 2014

pp. 97-114

© Emerald Group Publishing Limited

0968-5227

DOI 10.1108/IMCS-03-2013-0019

which require real-time customer support services. Yet, even as enterprises integrate business mobility to leverage flexibility and productivity into their business strategy, they realize that they need new policies to address people, processes, and technology implications from the mobile way of doing business. Without new policies, enterprises find themselves overwhelmed with a mish-mash of various employee-owned mobile devices (referred to as “bring your own devices (BYOD)”) and multi-vendor services. Also, as a result of the mish-mash, enterprise employees often lack systematic access to enterprise information, impeding their ability to collaborate with each other and their customers.

Mobile device technology is also changing rapidly. Mobile devices primarily include smartphones and tablets, but also include personal digital assistants (PDAs), gaming consoles, and e-readers. This paper will focus on the more popular mobile devices, smartphones and tablets. Information systems security specialists are more familiar with older technologies such as desktop computers and mobile laptops with the most-widely used Microsoft Windows operating systems. However, security experts have new concerns with the popularity of smartphones and tablets. These devices do not use the common Windows operating systems. Instead they use operating systems like Apple’s iOS and Google’s Android OS, which are much newer and less familiar. Smartphones and tablets also use different software applications than found on typical computers. This software is most often purchased through online stores controlled by the operating system’s parent (i.e. Apple and Google). These new security concerns raise issues about the security and safety of enterprise’s business, customer, and employee data and information. It also raises issues about an employee’s own personal information when employee’s use their personal devices for business.

Over the past ten years, innovative and technology-savvy small- and medium-sized enterprises (SMEs) provided their employees better broadband internet access and new mobile technology tools, which increased their productivity and improved the SMEs’ competitiveness with larger organizations (Passerini *et al.*, 2012). These new capabilities allow tech-savvy SMEs to use their smaller and less bureaucratic size to leap-frog the larger enterprises, who may adopt newer technologies at a much slower pace (Passerini *et al.*, 2012). SME managers often allow employees to use any mobile technology to get the job done. This practice comes with a price – the threat of increased security problems.

The purpose of this paper is to focus on the unique SME mobility business dilemma: invest in more expensive maximum security technologies, invest in less expensive minimum security technologies with increased risk, or postpone the business mobility strategy in order to protect enterprise and customer data and information. This paper first defines the SME and describes its importance to the economy. It explains the reasons for the new security concerns from the use of smartphones and tablets. It explores the growth and the need to provide increased security for new mobile phones and tablets as an integral part of a business mobility strategy. This paper describes preliminary recommendations, which a sophisticated large enterprise IT organization should implement. However, some of these recommendations may be very difficult for SMEs to implement because they have little or no enterprise IT security expertise, thus creating the SME dilemma. It also identifies future research questions, which address SME security awareness and capability to develop more viable security practices to minimize security threats.

SMEs technology adoption

SMEs are very important to the economies of most countries. SMEs play a major role in the USA in terms of the number of enterprises and the number of employees. According to the latest US labor statistics based on enterprise size, 99.6 percent of all enterprises had fewer than 500 employees making up 55.8 percent of the total employment (United States Department of Labor, 2005). Enterprises with one to four employees made up 54.5 percent of all enterprises, but accounted for only 5.2 percent of total employment. On the other hand, only 0.2 percent of enterprises had 1,000 or more employees, but made-up 37.4 percent of total employment (USDL, 2005). There are various definitions of SMEs. The United States Small Business Administration (SBA), Office of Advocacy, defines a small business as an independent business having fewer than 500 employees (SBA, 2011). However, for US contracting purposes, according to the USDL, businesses are considered small if they have under 100 employees and medium-sized with up to 500 employees. The SME definition differs for Europe. The 2003 European Commission for enterprise and industry defined a medium-sized business as having less than 250 employees, a small business as having less than 50 employees, and a micro business as having less than ten employees (Commission of European Communities, 2003). In Europe, SMEs comprise 99.8 percent of all enterprises.

Economic growth is impacted by SMEs in several ways. The presence of SMEs encourages large enterprises to outsource some of their activities to smaller firms thus increasing business opportunities (Audretsch, 2001). Also, each year entrepreneurs form many new small businesses. The SBA, Office of Advocacy, reported that more small businesses are started each year since 2005 than go out of business for a net increase of 1.2-1.7 percent per year (SBA, 2011).

It has commonly been assumed that SMEs are slow to adopt new technologies for a number of reasons, primarily because they lacked resources and technical knowledge. Only a small number of small businesses were bleeding or leading-edge adopters of emerging technologies according to a 2005 National Small Business Poll by the National Federation of Independent Business (NFIB) Research Foundation (Dennis, 2005). On the other hand, SMEs know the value of the internet for business success. An early study by the International Council for Small Business (ICSB) found that 35 percent used the internet for two-way communications with their customers. Plus, 39 percent had a sustained web presence (ICSB, 2008). The introduction of the internet and its resulting e-commerce capabilities enabled small businesses to compete world-wide. Broadband technologies, with its “always on” and “hi-capacity” characteristics, further increased opportunities for SMEs allowing them to “level the playing field” with the largest enterprises since they could now more easily leverage and exploit technology (Passerini *et al.*, 2012). The development of early mobile technologies began an evolution, initially for innovative small businesses who adopted these emerging technologies, resulting in the opportunity to create an even more equal competitive stage with the largest enterprises. With mobile technologies, employees spend more time interacting with customers and vendors and less time at their desks (Henri and Aurelie, 2006). Advantages for innovative SMEs who quickly adopt emerging technologies revolve around four key aspects, all of which lead to quicker decision-making (Patten and Passerini, 2007):

- (1) *Embedded technology.* SMEs are not constrained by inflexible and legacy IT infrastructures technology, which makes it easier to adopt newer technologies. Initially, early mobile technologies did not require IT staffs to implement or manage.

- (2) *Size*. Organizational size and flexibility make it easier to implement new technologies since there are fewer employees with specialized function roles to consider and train.
- (3) *Processes*. Although often informal, SME processes are usually fluid and easily adaptable to new situations. Employees generally know each other and are aware of the enterprise business goals. SME employees are also more likely to participate in planning activities and are, therefore, more supportive of new technologies.
- (4) *Workplace*. Dynamic workplaces and workforces require the latest mobility features and tools to give their employees the capability to work from anywhere, anytime. This also leads to increased employee interactions with customers, which also leads to deeper customer knowledge. This deeper customer knowledge often leads to business growth.

The rapid introduction of smartphones and tablets are once again changing the way small businesses compete. For example, these new services help SME employees increase their individual productivity at lower cost of services, which make the technologies more affordable for the small business. Industry forecasts expect that small businesses will spend more for wireless services in 2013 than they spend on wired and data services (Chaudhury *et al.*, 2011). Wireless service providers are also beginning to market to even the smallest businesses. Prior to the introduction of mobile business services, many telecommunications vendors considered small businesses the same as residential customers (Chaudhury *et al.*, 2011).

However, SMEs are just like larger enterprises in their need to effectively manage business relationships, which include the need to provide security (Romano and Fjermestad, 2007). Security breaches and threats can cost enterprises millions of dollars each year (Gordon *et al.*, 2004) and more importantly, can result in lost customers and decreased customer trust (Ponemon, 2005). SMEs cannot afford to either lose customers or decrease customer trust. SME's need to protect customer information such as customer names, SSNs, credit card numbers, telephone/cell numbers, mailing addresses and e-mail addresses just as the large enterprises do (Romano and Fjermestad, 2007).

Studies show that with evolving internet and mobile business technologies, security threats also increase. Earlier research studies documented that SME owners and managers did not understand the security risks when initially adopting computers (Bradbard *et al.*, 1990) nor did they understand the security risks with the adoption of internet-based services such as e-commerce, telecommuting, and multi-media (Spinellis *et al.*, 1999). The owners and managers also were unaware of what precautions should be taken to minimize the risks. More recently, several studies examined the awareness and actions of small business owners and home-based sales representatives concerning hi-speed internet services security risks (Johnson and Koch, 2006; Koch and Johnson, 2008). Koch and Johnson discussed how the use of increasingly complex technologies from simple dial-up internet through more sophisticated hi-speed internet and new Wi-Fi networks increased security risks and vulnerabilities. They concluded that SME owners needed to increase their vigilance and understand the increasing cost of security risks and protection.

Smartphones and tablets, with their new operating systems, pose new threats to the security and safety of enterprise information as well as customer information, especially

for SMEs who lack the finances and security infrastructure that larger enterprises may have. A smaller company, such as a doctor's office, may use smartphones, tablets, and laptop devices to improve their efficiencies, but often these same offices lack information technology specialists to properly secure these devices, plus they may be unaware of the security risks. This paper adds to the previous small business security research by exploring the SME use of smartphones and tablets and the dilemma such technologies create.

The growth of business mobility phones and devices

Smartphones now account for more than 50 percent of mobile phones in the USA and continue to sell at a brisk pace, accounting for over 75 percent of the devices sold in late 2012 (Chetan-Sharma, 2013). As of February 2013, Android accounted for 36.9 percent and Apple's iOS accounted for 27.21 percent of worldwide mobile operating systems (Statcounter, 2013). The average number of mobile devices per household was five and over 6 percent of households had 15 or more devices (Chetan-Sharma, 2013). In 2013, 50 percent of the North American workforce in medium- to large-sized businesses will use smartphones and 25 percent will use tablets (Osterman Research, 2012b).

With business mobility changing the ways people work, enterprises are becoming more aware that they require a mobility security strategy, but many have not developed one for a number of reasons (Waltz, 2011). An increasing diversity of mobile devices is appearing in the workplace due to the rapid development of the next generations of smart phones and tablet devices. Unlike the case with many other technologies, employees are driving the mobility strategy, not the enterprise IT organization. For example, employees often bring their own devices (BYOD) for both work and personal uses. An Osterman Research survey found that the use of personally owned smartphones and tablets is widespread in organizations of all sizes (Osterman Research, 2012a). Finally, the easy access to numerous mobile applications (apps) complicates the ability to develop security management policies, especially in SMEs with limited professional IT resources.

Primary security concerns

Statcounter Global Stats (2013) reports that as of February 2013, Microsoft Windows operating systems account for over 85 percent of the worldwide computers connected to over three million web sites monitored by the company. Besides security experts being more familiar with Microsoft's operating systems, end-users are also more familiar with Microsoft systems. Many end-users are familiar with the need to perform Windows updates and install antivirus and firewall software. The popularity of smartphones and tablets and the use of the newer and less familiar Apple's iOS and Google's Android OS pose new threats to information technology specialists and end-users. The next few sections discuss these new security concerns with Android and Apple iOS mobile devices with a focus on various implications for small, medium, and large enterprises.

Malware

Mobile device applications are abundant with both Apple and Android reporting about 700,000 apps available for each of their platforms at the end of 2012 (Bradshaw, 2012). It is estimated that 70 billion apps will be downloaded by 2014 (Lookout, 2013). In the fall

of 2012, Apple celebrated its 35 billionth mobile app download and Google celebrated its 25 billionth Android download (Bradshaw, 2012). With the rise of mobile apps comes the rise of malware, but Android malware is increasing at much higher rates than is Apple iOS. Malware for Android increased by 350 percent in 2012 (Trend-Micro, 2012) and now exceeds PCs for malware attacks in the USA (Mansfield-Devine, 2013). Just over 99 percent of all malware detected in 2012 was written for Android, with less than 1 percent from the other platforms (Kaspersky, 2013).

The largest problem stemming from malware is premium SMS text messaging. This type malware can send premium pay text messages in the background, without the user's knowledge. Over 78 percent of Lookout's 2012 malware detections were premium text messages that cost the average user \$9.99 a month (Lookout, 2012). TrendMicro and ESET Security also reported that SMS premium text messaging was the top malware (ESET, 2013; Trend-Micro, 2012).

Fake applications are another major malware problem for both Android and Apple. Security firm Arxan reports that all of the top 100 apps for Android and 92 of the top 100 apps for iOS have fake malware versions available as of mid-2012 (Arxan, 2012). Most fake malware applications are found on third-party application sites, which are easy access for Android users and difficult to access for iOS users.

New types of malware are also hitting the market that can affect both Android and iOS. For example, Zitmo and FakeToken are designed to intercept banking transaction authentication numbers (TANs) and embezzle bank accounts. TANs are the numbers that are sent to a user's mobile phone when they are performing banking transactions. TANs are designed to be an extra layer of security to verify the owner of the account. However, malware can intercept and redirect them elsewhere. Another new malware is PlaceRaider, an app with camera access that can take pictures and video of where the device is at any particular time (Hoffman, 2013). The phone is muted to keep it silent and the pictures and videos are sent to a server where they are reassembled into a 3D model of your house, office, etc. A malicious person can browse for objects worth stealing and sensitive data such as credit cards, checks, calendar data, and identity data (MIT-Tech-Review, 2013). While the PlaceRaider malware was originally written for the Android OS, the writers state they expect it to be adapted to other operating systems, such as Apple's iOS and Microsoft's Windows Mobile (MIT-Tech-Review, 2013). The malware can affect Android versions 2.3 and above (Android-Mag, 2013), which accounts for nearly 90 percent of the market as of January 2013 (Platform-Versions, 2013).

Mobile device platforms and markets

The Apple iOS security model is safer than the Android model primarily because of the way Apple restricts users, vendors, and manufacturers that Google does not. Apple restricts users to only installing apps from the iTunes market and there is only one assembler for its equipment. This is opposite of Google's Android platform, where users can download apps from any market and equipment comes from many vendors and is offered by many carriers. Restriction versus freedom is the fundamental difference in Apple's and Google's platforms, both of which have their advantages and disadvantages.

One major difference is application development and market submission. Applications developed for Android can be submitted and made available on the Google Play market or through third-party markets. Applications developed for iOS can

only be officially made available through Apple's App Store. Apple has a very strict vetting process for its developers and its applications. This ensures better security, but takes longer to get apps to the market. Google has a relaxed vetting process, which leads to quicker releases of apps, but less strict security. This is the primary reason for the major increase in malware in Android apps. Google has attempted to better vet their developers for the Google Play market, but their process is still inferior to Apple's (Greenberg, 2012). Google has also added malware scanning to the Google Play Market (Mansfield-Devine, 2012b). However, Google's vetting and market malware scanning does not apply to the third-party markets, which is where most of the malware is found (Arxan, 2012). Adding to the market confusion with Android is the large variation in vetting among third-party markets. While some are insecure, some have stronger vetting than Google Play and equal that of Apple, such as Amazons Appstore (Lookout, 2011; Strohmeyer, 2011).

Another major difference in Apple's iOS and Google's Android platforms are the many device manufacturers and carriers used by Google. Many manufacturers and carriers that do not follow a particular standard lead to many older versions of the Android OS still on the market (Mansfield-Devine, 2012a). Manufacturers and carriers often customize devices with installed apps and specific configurations, called bloatware, to differentiate their products from competitors. It is left up to the carrier to decide if an update to the OS is to be deployed to devices. Since the bloatware may also need updating for compatibility, many carriers choose to forgo updating. In order to get the update through official channels, a user would need to upgrade equipment, which is also an advantage to the carrier because new equipment often comes with a new contract. The result is a fragmented Android platform. As of January 2013, Jelly Bean 4.2 was the latest version of Android. However, only 1.2 percent of the devices on the market had this version (Platform-Versions, 2013). The previous version of Jelly Bean 4.1, only accounts for 9 percent of the market. The two most popular versions on the market are Ice Cream Sandwich (29.1 percent) and Gingerbread (47.6 percent). Ice Cream Sandwich was released in October 2011 and Gingerbread was released in December 2010. A fragmented OS leads to security problems. For example, the latest version of Android has malware scanning to check apps for harmful behavior when first installed, including downloaded third-party market apps. However, only 1.2 percent of the devices on the market have this capability. In contrast, Apple claimed that over 80 percent of iPhone and iPad users had the latest iOS as of June 2012 (Mansfield-Devine, 2012a).

The primary advantage iOS has over Android is security. The Apple App Store, vetting processes, limited carriers, and a single product assembler all lead to better security. However, these also lead to the primary disadvantage of iOS. People want more freedom to choose different carriers, configure their devices, and download apps from different markets. This leads to high incidences of jailbreaking, which severely increases risk. The next section discusses jailbreaking and rooting.

Jailbreaking and rooting

Jailbreaking is a term used with Apple devices. Jailbreaking a device is a process that removes the platforms restrictions, allowing users to have administrative control and install applications from any market. For frustrated iOS users, this gives them the freedom to customize their devices. Rooting is often referred to as a similar process performed on Android devices. Jailbreaking and rooting mobile devices can be thought

as upgrading from a guest account on a PC to an administrator account. It gives the user the freedom to choose instead of being restricted by the platform, vendor, or carrier.

There are a large percentage of Apple iOS devices that are jailbroken because many people like Apple products, but do not like being limited (Mansfield-Devine, 2012b). To support this statement, the new version of Apple iOS 6.1 released in January 2013 had seven million jailbreak downloads in the first four days on the market (Greenberg, 2013). Jailbreaking and rooting opens the devices to malicious software being able to more easily escalate privileges (Mansfield-Devine, 2012a). Since many of the initial restrictions were there for security purposes, jailbreaking and rooting severely jeopardizes mobile device security. Also, jailbreaking and rooting are not supported by Apple and Google, so obtaining trusted and verifiable software to perform the jailbreak or root may prove difficult.

The jailbreak and rooting security concerns for corporations are understandably high. Jailbroken and rooted devices pose tremendous threats to any organization because of the potential for malware and the potential for malware to gain escalated privileges. Because of such concerns, many IT security professionals have called for a ban of all jailbroken and rooted devices on corporate networks (ZDNet, 2013).

Wi-Fi and VPNs

Connectivity to corporate networks and the internet typically occurs either through a mobile broadband network (3G/4G) or a Wi-Fi network. As of mid-2011, 37.2 percent of US digital mobile traffic and nearly 90 percent of tablet traffic occurred via a Wi-Fi connection (Comscore, 2011). In the second quarter of 2012, over 90 percent of tablets still utilized Wi-Fi as the primary means of connecting to networks (Chetan-Sharma, 2013). This implies that, as with laptop connectivity to corporate networks and the internet, smartphone and tablet users also need to be aware of Wi-Fi security protocols and risks associated with using Wi-Fi.

Wi-Fi encryption passwords or passphrases, such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA and WPA2) are now vulnerable (Gold, 2011b). WEP and WPA have long been vulnerable, but now WPA2 is easily crackable. In 2010, Elcomsoft's Wireless Security Auditor (WSA) was released and has the ability to brute force crack as many as 103,000 WPA2 personal mode (PSK) passwords per second. Because of Wi-Fi vulnerabilities, some security experts recommend against using Wi-Fi and to instead seek wired connections (Gold, 2011b).

For companies that must use Wi-Fi, experts advise the use of 20 + character WPA2 complex passphrases when using WPA2 personal mode with a pre-shared key (Gold, 2011b). However, security is stronger when implementing a WPA2 enterprise mode radius-based virtual private network (VPN) system (Gold, 2011b). A radius server is an authentication server that works with WPA2 enterprise mode to authenticate users without the use of pre-shared keys. Instead of a pre-shared key, users can be given their own account or digital certificate that will then be authenticated by the radius server before allowing Wi-Fi access. A VPN can then be utilized to encrypt data in a secure tunnel that travels over the Wi-Fi network, thus maximizing security. VPNs can also protect Wi-Fi users from rogue access points, which can create man-in-the-middle attacks on Wi-Fi signals. This first part of this solution, the use of 20 + character passphrases in WPA2 personal mode, is practical for all enterprises and end-users.

The more secure solution may be more practical for a large enterprise than it is for smaller companies with limited or no enterprise information technology staff and with limited funds. Installing and administering a radius VPN system is not something most small to medium enterprises can accomplish without an information technology professional.

Another reason to use VPNs, whether corporate or personal, is that cellular networks are not completely safe either. In 2010, Vodafone's cellular network in Europe was hacked through a device known as a femtocell (Gold, 2011a). A femtocell is a miniature cellular base designed for localized use by homes and small businesses. The hacking used a method similar to the evil twin concept on Wi-Fi to access victim's cell phones voice and data transmissions. Other companies, such as AT&T, Sprint, and Verizon, have since launched their own femtocells. While Vodafone claims their vulnerability has been patched, the incident further strengthens the argument to use VPNs over both cellular and Wi-Fi networks.

Security recommendations

Mobile device management

Mobile device management (MDM) is software or hardware that is used to manage and secure mobile devices in the workplace, such as smart phones and tablets. This includes BYOD and corporate issued mobile devices. MDM systems can be used to secure all of the popular platforms and models of mobile devices at the same time within the same system. So no matter what device and operating system is present, a MDM solution can configure and secure it. However, the sophistication and cost of MDM solutions can vary greatly. With over 80 vendors serving the market, the choices can be daunting (Osterman Research, 2012b). Rubens (2012) states that minimum features should include password management, remote data wipe, data encryption, jailbreak/root detection, data loss prevention, remote configuration, remote OS and application updating, remote inventorying, and remote control. Among other popular features is the ability to lockdown the device's camera, bluetooth, and Wi-Fi.

Another feature that can be integrated with a MDM solution is mobile application management (MAM). Where MDM manages the physical devices, MAM services manage mobile applications, including development and deployment. Minimum MAM features include application whitelists and blacklists, enterprise application stores, application security, and data wipe by application (Rubens, 2012).

MDM solutions are primarily deployed as in-house server based solutions or as a cloud-based Software as a Service (SaaS). There is also a hardware appliance MDM solution where a piece of equipment is integrated into the existing network. All three deployment options can be managed by in-house information technology staff or by a third-party managed service provider (MSP). MSPs are companies that can perform IT duties as part of an outsourcing agreement. Osterman Research (2012a) reports that 31 percent of organizations switching to a new MDM platform said they would select a cloud-based solution and more than half of those respondents said they would choose a private cloud versus a cloud solution with databases that are shared with other companies. Osterman Research (2012a) states the primary reasons for choosing cloud-based MDM solutions are applicable to MSPs as well, such as simplified administration and maintenance, reduced and predictable costs, improved security, and the desire to not use internal IT staff to service MDM.

In 2012, one survey reported an average cost a MSP charges for MDM was \$22 per month per device (Kaseya, 2012). However, this number can be a little misleading. More than half of the respondents used a tiered/bundled service approach that also included other services, such as desktop and server support. Sixty-seven percent of the respondent's bundled services contracts were between \$1,000 and \$2,500 per month, meaning the \$22 a month average would be considerably higher for a SME without the bundled contract or economies of scale. For larger organizations with thousands of mobile devices on a cloud-based platform, the average cost can be as low as \$5 a month, depending on the services, which may not include the minimum recommended services mentioned above (Gartner, 2012). As the MDM market matures, there should be a reduction in costs to the enterprise (Gartner, 2012). If a SME can find a suitable contract with one of the many providers at a reasonable cost, this could very well be the solution to their IT mobile device business security dilemma. If a SME is too small for volume license pricing or simply cannot afford the cost of a MDM solution, the following are security recommendations they can take at minimal cost.

Recommendations for SMEs

The following list of security recommendations is considered the minimum level of security designed to deal with the potential security risks from mobile devices. Although the list is suitable for all enterprises, because many of the recommendations do not involve costly hardware, the recommendations are considered feasible for SMEs to implement. Device-oriented recommendations are concepts that should be applied to the mobile device that involve the operating system and applications that come with the device. User-oriented recommendations are concepts the user of the device should follow and management-oriented recommendations are concepts management should employ in the business.

Device-oriented recommendations

- (1) Do not jailbreak or root mobile device operating systems (FBI, 2012; US-CERT, 2011a). Doing so dramatically increases the risk of malware.
- (2) Passphrase protect all mobile devices (NIST, 2012; FBI, 2012). Requiring a passphrase makes it harder for wrong doers to access the device.
- (3) Have devices self-lock after a short time of inactivity (NIST, 2012).
- (4) Update device operating systems and applications when prompted (FBI, 2012). Updating software can help fix known vulnerabilities.
- (5) If available, encrypt data on devices, including the removable memory cards (NIST, 2012; FBI, 2012). Encrypted data is more difficult to access if compromised.

User-oriented recommendations

- (6) Install antivirus software on all Android mobile devices (FBI, 2012; US-CERT, 2011a). Antivirus is not available for iOS devices. Antivirus is an essential defense against malware.
- (7) Install software with the capability to back-up device data (US-CERT, 2011b). Many antivirus suites offer backup services.

- (8) Install data wipe software with the capability to erase data on lost or stolen devices (NIST, 2012; US-CERT, 2011a). Many of the antivirus software suites also contain features to remotely erase data and accounts on lost or stolen devices. Some even contain GPS tracking software to help find the devices.
- (9) Avoid storing usernames and passwords on the device (e.g. browser and e-mail) (Coninsync, 2013). If a device is compromised and accessible, stored usernames and passwords will make it easier for wrong doers to access data and accounts.
- (10) Do not download applications from web sites or from links within e-mails (Homeland Security, 2013; FBI, 2012). It is hard to ensure security when downloading from these sources.
- (11) On Android devices, beware of applications that request more permissions than necessary (US-CERT, 2011a; FBI, 2012). When updating applications, be wary of Android applications asking for additional and unnecessary permissions than originally needed when installed. Excessive permissions can increase security risk.
- (12) For Android, avoid untrusted third-party markets (Mylonas *et al.*, 2012; Arxan, 2012). If in question, research the market and app developers before downloading.

Management-oriented recommendations

- (13) Use 20+ character passphrases with WPA2 personal mode if WPA2 Enterprise mode with a radius server is not available (Gold, 2011b). WPA2 personal mode is vulnerable to brute force attack, so longer and more complex passphrases are essential.
- (14) Consider purchasing iOS products instead of Android devices (Mansfield-Devine, 2012b). Because of the way iOS handles software applications, the operating system is safer than the Android OS as long as the iOS device is not jailbroken. Apple has also added a few high security features to entice business users.
- (15) Provide the capability to use VPNs over all Wi-Fi connections (NIST, 2012). Personal VPNs are available from third-party companies for those that do not have corporate VPNs.
- (16) Utilize MAC address filtering on wireless access points and routers (Mitchell, 2013). This adds another layer of protection by only allowing devices with specific MAC addresses to connect.
- (17) Create a mobile device security policy (NIST, 2012; Ernst & Young, 2012). There needs to be a comprehensive policy in place that governs mobile devices so that employees know what is and is not allowed.
- (18) Educate employees (Ernst & Young, 2012). All employees should be made aware of mobile device security vulnerabilities and educated on the best practices for protection. Education is essential and should be linked to the mobile device policy.

The above list of recommendations is considered practical for SMEs, but do not maximize security. However, there are additional recommendations that may not be practical for SMEs but should be adopted by large enterprises. Enterprises should install radius-based servers with iPSec VPNs, which are much more secure than personal VPNs. All smartphones, tablets, and laptops should be connected to corporate iPSec VPN servers. These enterprises should also utilize deep packet sniffing on all packets on the VPN. While stateful packet inspection might be enough for most connections, remote VPN connections should utilize deep packet inspection. Stateful packet inspection is a technique of thoroughly inspecting the initial packets of a connection to establish the connection is trusted and then relaxing inspecting for the rest of the connection. Deep packet inspection can be set to thoroughly inspect all packets, not just the initial connection packets. Another important security aspect is data control. If users do not log into the network within a certain amount of time, the devices will delete its own data or block access to corporate e-mail (Sybase, 2011). This is good for employees that are no longer with the company, but may still have access. Large enterprises should also use two-factor authentication for laptop and tablet remote access (Kemshall, 2011). One way is to send a passcode via mobile short message service (SMS) to the users' cellular phone. The required combination of passcode and regular log-on credentials to access corporate networks increases security. Finally, large organizations should utilize the advanced features of a MDM solution, including MAM.

Discussion

Mobile device security concerns create a new business dilemma for innovative SMEs that over the last five to eight years have become early adopters of the latest technology breakthrough – mobile technologies. In the technology evolution timeline shown in Figure 1, technology has evolved from stand-alone PCs to dial up internet, then broadband internet with wireless networks, and finally, the recent introduction of smartphones and tablets. The years shown in the figure represent when the market was saturated with the technology. With the development and adoption of each of these technologies, tech-savvy SMEs were able to gradually improve their global competitiveness compared with the largest enterprises. The development and adoption of “anywhere – anytime” technologies finally give the SMEs the competitive advantage

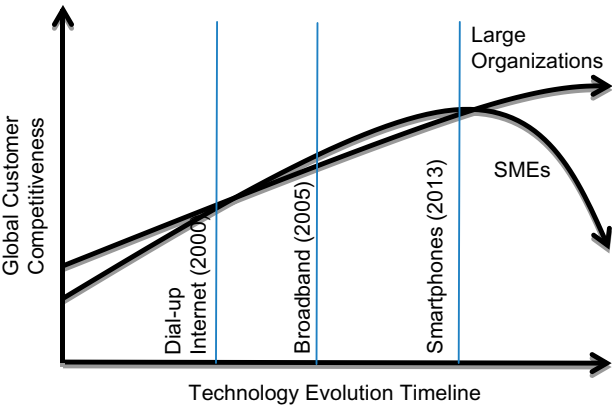


Figure 1.
SME global
competitiveness impact

over the largest competitors as discussed earlier in this paper. However, because of the new security concerns associated with smartphones and tablets, SME's global customer competitiveness will drastically decrease should they decide to forgo mobile devices because of security concerns due to the lack of resources or skills to address said security concerns. Large organizations will also decrease a little, but only temporarily as they take measures to secure their devices.

Figure 2 is a modified model showing increasing security risks from more sophisticated technologies. Koch and Johnson's (2008) original model described how security risk increases as small businesses advance through various stages of technology: stand-alone PC, dial-up internet, high speed internet, wireless network, and wide area network. The modified model maps the stages of technology introduced in the original model to the technology evolution timeline in Figure 1. It also adds a new point in the timeline where smartphones saturated the market. Another significant modification within Figure 2 is the addition of large enterprises, which allows for the comparison of cost between SMEs and large enterprise. While the cost of minimizing security risk does increase as technology gets more advanced, as depicted in the original model, there is a point where SMEs can no longer afford these costs. As described in the security review, the new risks associated with Wi-Fi and smartphones and tablets require significant information technology resources to minimize information security risk. When SMEs choose the less costly security measures, such as the use of personal VPNs versus radius server VPNs used by large enterprises, they do so with increased risk. Once a SME gets to a point where cost is prohibitive and security is not maximized, if they choose to continue to use mobile devices, risk dramatically increases. Risk also increases for large organizations, even with their superior IT resources. This risk comes from the immaturity of the mobile device market, where the technology and the security is new to everyone.

Conclusion

The biggest difference between large enterprise security and SME security is that the smaller firms have limited or no IT staff and considerably smaller IT budgets. A SME may not be able to implement VPNs with radius servers, perform deep packet sniffing, or completely control the data. The partial solution, though not optimal, is for SMEs

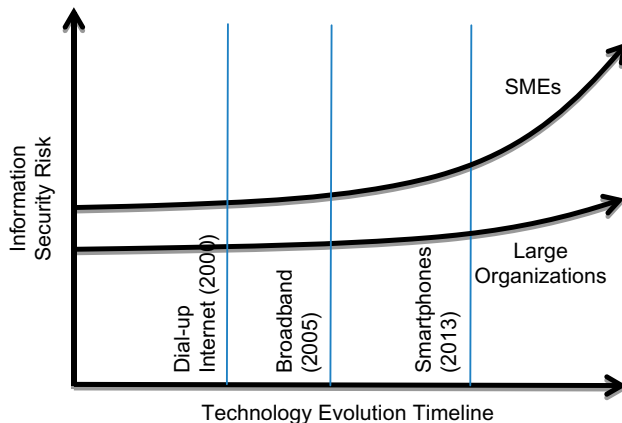


Figure 2.
SME technology
risk impact

to utilize the minimum security recommendations listed above. The security will not be as strong, which leads to the SME dilemma: embrace the mobility business strategy and adopt and invest in the necessary security technology, such as a MDM and MSP solution, take the above minimum recommended precautions with increased risk, or give up their mobility business strategy to protect enterprise and customer data and information.

This paper attempts to explain the seriousness of new security concerns created by the adoption of smartphones and tablets. Although smartphone and tablet adoption has increased the security threats for all enterprises, this paper is focused on the unique business dilemma for the SMEs. The newest “anywhere – anytime” capabilities of smartphones and tablets have finally given SMEs a global competitive advantage over the larger enterprises, but at a serious risk to the security of the SMEs’ customer and enterprise information as well as employee personal information. The paper provides several practical recommendations that can partially mitigate some of the risks. However, most SMEs are unable to implement the full set of recommendations, which are more easily obtained by larger enterprises, thus creating the dilemma.

Future research

The SME mobility strategy dilemma described above is serious. We do not know all the potential implications. However, these new technologies and the new security concerns create an opportunity for future research in several areas. How aware are SMEs to the new threats? What are the costs and implications for SMEs to invest in the new security technology solutions, such as MDM? What other security solutions might be more effective at lower costs? What IT capabilities must SMEs acquire to stay in the mobility business? We are continuing our research in this area and invite others to do so as well.

References

- Android-Mag (2013), *PlaceRaider: The “Legal” Android Trojan*, available at: www.androidmag.com/placeraider-%E2%80%99android-trojan (accessed 9 February 2013).
- Arxan (2012), *State of Security in the App Economy: Mobile Apps Under Attack*, available at: www.arxan.com/assets/1/7/state-of-security-app-economy.pdf (accessed 9 February 2013).
- Audretsch, D. (2001), “What’s new about the new economy? Sources of growth in the managed and entrepreneurial economies”, *Change*, Vol. 10 No. 1, pp. 267-315.
- Bradbard, D.A., Norris, D.R. and Kahai, P.H. (1990), “Computer security in small business: an empirical study”, *Journal of Small Business Management*, Vol. 28 No. 1, pp. 9-19.
- Bradshaw, T. (2012), *Android Apps Put Pressure on Apple*, available at: www.ft.com/cms/s/0/95338878-4daa-11e2-a0fc-00144feab49a.html (accessed 10 February 2013).
- Chaudhury, R., Covalada, A. and Ross, R. (2011), “The wireless battle for small business customers”, *Connected Planet*, available at: www.connectedplanetonline.com/3g4g/news/the-wireless-battle-for-small-business-customers-0919 (accessed 12 December 2012).
- Chetan-Sharma (2013), *Chetan Sharma: Technology and Strategy Consulting*, available at: www.chetansharma.com/index.htm (accessed 4 March 2013).
- Commission of European Communities (2003), “Commission recommendation concerning the definition of micro, small- and medium-sized enterprise adopted by the commission”, *Official Journal of the European Union*, 2003/361/EC.

- Comscore (2011), *Smartphones and Tablets Drive Nearly 7 Percent of Total US Digital Traffic*, available at: www.comscore.com/Press_Events/Press_Releases/2011/10/Smartphones_and_Tablets_Drive_Nearly_7_Percent_of_Total_U.S._Digital_Traffic (accessed 15 February 2013).
- Coninsync (2013), *Why You Should Avoid Saving Passwords on Your Smartphone?*, available at: <http://coninsync.com/why-you-should-avoid-saving-passwords-on-your-smartphone/> (accessed 17 February 2013).
- Dennis, W.J. Jr (2005), "The state of technology", *NFIB National Small Business Poll*, Vol. 5 No. 5.
- Ernst & Young (2012), *Mobile Device Security: Understanding Vulnerabilities and Managing Risks*, available at: [www.ey.com/Publication/vwLUAssets/Mobile_Device_Security/\\$FILE/Mobile-security-devices_AU1070.pdf](http://www.ey.com/Publication/vwLUAssets/Mobile_Device_Security/$FILE/Mobile-security-devices_AU1070.pdf) (accessed 2 May 2013).
- ESET (2013), *Trends for 2013*, available at: http://go.eset.com/us/resources/white-papers/Trends_for_2013_preview.pdf (accessed 7 March 2013).
- FBI (2012), *Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise*, available at: www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise (accessed 11 February 2013).
- Gartner (2012), *Magic Quadrant for Mobile Device Management Software*, available at: www.gartner.com/technology/reprints.do?id=1-1AKKJNN&ct=120518&st=sb (accessed 29 January 2013).
- Gold, S. (2011a), "Cracking cellular networks via femtocells", *Network Security*, Vol. 2011 No. 9, pp. 5-8.
- Gold, S. (2011b), "Cracking wireless networks", *Network Security*, Vol. 2011 No. 11, pp. 14-18.
- Gordon, L.A., Loeh, M.P., Lucyshyn, W. and Richardson, R. (2004), *Ninth Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, available at: www.theiia.org/iaa/download (accessed 9 February 2013).
- Greenberg, A. (2012), "Google gets serious about android security: now auto-scans app market for malware", *Forbes*, available at: www.forbes.com/sites/andygreenberg/2012/02/02/google-gets-serious-about-android-security-now-auto-scans-app-market-for-malware/ (accessed 11 February 2013).
- Greenberg, A. (2013), "Evasion is the most popular jailbreak ever: nearly seven million iOS devices hacked in four days", *Forbes*, available at: www.forbes.com/sites/andygreenberg/2013/02/08/evasion-is-the-most-popular-jailbreak-ever-nearly-seven-million-ios-devices-hacked-in-four-days/ (accessed 12 February 2013).
- Henri, I. and Aurelie, L. (2006), "Give me a mobile phone, and I will work harder: assessing the value of mobile technology in organizations – an exploratory research", *Proceedings of the International Conference on Mobile Business (ICMB'06)*, IEEE Computer Society, Copenhagen, Denmark, Paper 18, 26-27 June.
- Hoffman, D. (2013), "Exposing your personal information: there's an app [...]", *J-Net Community*, available at: <http://forums.juniper.net/t5/Security-Mobility-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058> (accessed 9 February 2013).
- Homeland Security (2013), *Cyber-Security Tips*, available at: www.dhs.gov/cybersecurity-tips (accessed 2 May 2013).
- ICSB (2008), *Results of the 2008 Dell/ICSM International Business Survey*, International Center for Small Business, available at: www.icsb.org/know_research.asp (accessed 12 December 2012).

- Johnson, D.W. and Koch, H. (2006), "Computer security risks in the internet era: are small business owners aware and proactive?", *Proceedings of the 39th Hawaii International Conference on System Sciences*, IEEE, Washington, DC.
- Kaseya (2012), *MSP Global Pricing Survey*, available at: www.kaseya.com/lps/en/lp/2012/MSPGlobalPricingSurvey_Q4.aspx (accessed 21 January 2013).
- Kaspersky (2013), *Find and Call: Leak and Spam*, available at: www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam (accessed 11 February 2013).
- Kemshall, A. (2011), "Security should not cost the world", *ChannelWeb.Co.UK*, December 22, available at: www.channelweb.co.uk/crn-uk/opinion/2134340/security-cost-earth (accessed 22 February 2012).
- Koch, H. and Johnson, D. (2008), "Are home-based sales representatives aware and proactive regarding security risks in the internet era?", *Journal of Internet Commerce*, Vol. 7 No. 3, pp. 379-402.
- Lookout (2011), *Lookout Mobile Threat Report*, available at: www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf (accessed 22 February 2012).
- Lookout (2012), *State of Mobile Security 2012*, available at: www.lookout.com/resources/reports/state-of-mobile-security-2012 (accessed 13 January 2013).
- Lookout (2013), *2013 Mobile Threat Predictions*, available at: <https://blog.lookout.com/blog/2012/12/13/2013-mobile-threat-predictions/> (accessed 11 February 2013).
- Mansfield-Devine, S. (2012a), "Android architecture: attacking the weak points", *Network Security*, Vol. 2012 No. 10, pp. 5-12.
- Mansfield-Devine, S. (2012b), "Paranoid android: just how insecure is the most popular mobile platform?", *Network Security*, Vol. 2012 No. 9, pp. 5-10.
- Mansfield-Devine, S. (2013), "Security review: the past year", *Computer Fraud & Security*, Vol. 2013 No. 1, pp. 5-11.
- Mitchell, B. (2013), *Enable MAC Address Filtering on Wireless Access Points and Routers*, available at: <http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm> (accessed 30 April 2013).
- MIT-Tech-Review (2013), "PlaceRaider: the military smartphone malware designed to steal your life", *MIT Technology Review*, available at: www.technologyreview.com/view/429394/placeraider-the-military-smartphone-malware-designed-to-steal-your-life/ (accessed 9 February 2013).
- Mylonas, A., Kastania, A. and Gritzalis, D. (2012), "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66.
- NIST (2012), *Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)*, available at: http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf (accessed 2 May 2013).
- Nokia White Paper (2006), *A Holistic Approach to Business Mobility*, Wiley, London, available at: http://dailywireless.tradepub.com/free-offer/a-holistic-approach-to-business-mobility/w_aaaa993?sr=ct&t=ct:Tele (accessed 1 March 2012).
- Osterman Research (2012a), *Achieving Rapid Payback with Mobile Device Management*, available at: www.ostermanresearch.com/whitepapers/orwp_0175.pdf (accessed 21 January 2013).
- Osterman Research (2012b), *Mobile Devices in the Enterprise: MDM Usage and Adoption Trends*, available at: www.ostermanresearch.com/whitepapers/orwp_0164.pdf (accessed 21 January 2013).
- Passerini, K., El Tarabishy, A. and Patten, K. (2012), *Information Technology for Small Business: Managing the Digital Enterprise*, Springer, New York, NY.

-
- Patten, K. and Passerini, K. (2007), "Next generation small and medium enterprises mobility strategy roadmap", *Proceedings of ISOneWorldConference, Las Vegas, NV, 11-13 April*.
- Platform-Versions (2013), *Platform Versions*, available at: <http://developer.android.com/about/dashboards/index.html> (accessed 5 February 2013).
- Ponemon, L. (2005), *Lost Customer Information: What Does a Data Breach Cost Companies?* Ponemon Institute, Tucson, AZ, available at: www.securitymanagement.com/library/Ponemon_DataStudy0106.pdf (accessed 9 February 2013).
- Romano, N.C. and Fjermestad, J. (2007), "Privacy and security in the age of electronic customer relationship management", *International Journal of Information Security and Privacy*, Vol. 1 No. 1, pp. 85-106.
- Rubens, P. (2012), *Mobile Device Management (MDM) Platform Buying Guide*, available at: www.enterprisenetworkingplanet.com/netsecur/mobile-device-management-mdm-buying-guide-1.html (accessed 21 January 2013).
- Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999), "Security requirements, risks, and recommendations for small enterprise and home-office environments", *Information Management and Computer Security*, Vol. 7 No. 3, pp. 121-128.
- Statcounter (2013), "Top 8 mobile operating systems in the United States from Jan 2012 to Jan 2013", StatCounter Global Stats, available at: <http://gs.statcounter.com/#mobile-os-US-monthly-201201-201301> (accessed 12 February 2013).
- Strohmeier, R. (2011), "Why I get apps from Amazon, not Google", *PCWorld*, available at: www.pcworld.com/article/239270/why_i_get_apps_from_amazon_not_google.html (accessed 11 February 2013).
- Sybase (2011), *Mobility Advantage: Why Secure Your Mobile Devices?*, available at: www.sybase.com/files/White_Papers/Sybase_Afaria_WhySecurity_wp.pdf (accessed 7 February 2013).
- Trend-Micro (2012), *Repeating History*, available at: www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf (accessed 9 February 2013).
- United States Small Business Administration (2013), "FAQs: advocacy small business statistics and research", Office of Advocacy, available at: www.sba.gov/faqs/faqindex.cfm?areaID=24 (accessed 9 February 2013).
- US-CERT (2011a), *Cyber Threats to Mobile Phones*, United States Computer Emergency Readiness Team, available at: www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf (accessed 9 February 2013).
- US-CERT (2011b), *Protecting Portable Devices: Physical Security*, United States Computer Emergency Readiness Team, available at: www.us-cert.gov/ncas/tips/ST04-017 (accessed 2 May 2013).
- USDL (2005), "New quarterly data from BLS on business employment dynamic by size of firm", United States Department of Labor, Bureau of Labor Statistics, Washington, DC, USDL 05-2277, December 8.
- Waltz, M. (2011), "Mobility threats", *Mobile Enterprise*, 7 March, available at: <http://mobileenterpriserise.edgl.com/top-stories/Mobility-Threats71022> (accessed 9 February 2013).
- ZDNet (2013), "Does jailbreaking or rooting devices and BYOD mix?", ZDNet, available at: www.zdnet.com/does-jailbreaking-or-rooting-devices-and-byod-mix-7000011069/ (accessed 12 February 2013).

About the authors

Mark A. Harris is an Assistant Professor in the integrated information technology program at the University of South Carolina, Columbia, SC. He has a PhD in information systems from

Virginia Commonwealth University, a MS in E-commerce and a BS in information technology from Old Dominion University. His research interests include security policy management, awareness training, human factors of security, health IT security, and mobile device security. He has authored multiple papers in well-respected refereed information systems journals and conferences. Before academia, Mark was a Senior Network Engineer for a large university, where he oversaw an expansive computer network. Mark A. Harris is the corresponding author and can be contacted at: maharris@hrsm.sc.edu

Karen P. Patten is an Assistant Professor in the integrated information technology program at the University of South Carolina, Columbia, SC. She teaches information technology project management, networking, and telecommunications. She has a BS in honors economics from Purdue University, a MS in civil engineering from the University of Minnesota, and a PhD in information systems from the New Jersey Institute of Technology. Dr Patten taught MIS, IT management, and telecommunications at the New Jersey Institute of Technology and the National Technological University. She is the author of *Data Networking Made Easy* (Aegis Publishing Group, 2000), co-author of *Information Systems for Small Business* (Springer, 2012), and has published articles in *Communications of the Association for Computing Machinery*, *Communications of the Association for Information Systems*, *Cutter IT Journal*, and the *International Journal of Computers, Systems and Signals*.

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints