ROAD WARRIORS AND INFORMATION SYSTEMS SECURITY: RISKS AND RECOMMENDATIONS

Warren Fisher, Stephen F. Austin State University
Charlotte Allen, Stephen F. Austin State University

ABSTRACT

Information systems are threatened by “road warriors” and other employees whose computer and other electronic devices are used outside the organization. Devices can be lost, compromised, or misused; communications can be intercepted and organizational systems can be penetrated, especially when the compromised devices are brought back inside the organization. The increasing use of “cloud computing” and “BYOD” (Bring your own device) add to those risks. Specific threats are discussed along with recommendations for reducing the likelihood of problems.

INTRODUCTION

It is widely known that information systems are an important part of most organizations and an essential part of many. It is also widely known that systems connected to the Internet are at risk of penetration by hackers, including competitors, criminals, foreign governments, and others—see Fisher, Tinsley, & Strader (2010) for a discussion of the threats and recommended non-technical precautions (technical precautions are beyond the scope of this paper and are best left to information security professionals). Unfortunately, even organizations with state-of-the-art security installed on their information systems are at risk from their own employees, particularly “road warriors” and other employees whose computers and other electronic devices are used outside the protection of the organization’s security systems. The risk is especially great when systems are accessed from outside the organization as well as when employees use devices outside the organization—exposing them to the risk of malware—and subsequently bring them back inside the organization’s system. The situation is made worse if employees violate company information security policies. Doing so is an especially great temptation for road warriors (D’Arcy & Devaraj, 2012), since higher security often requires increased time and effort to use devices and systems.

Hackers and malware have long been associated with networks and desktop or laptop computers. Unfortunately, the surging popularity of smartphones and tablet computers has captured the hackers’ attention. Mobile threats are growing rapidly, with the fastest growth in attacks on Google’s Android devices (Drew, 2012). One reason revealed in a recent study is that many Android devices have known and longstanding vulnerabilities that have not been patched (repaired by update). Older devices are at an especially great risk because manufacturers and/or phone carriers stop sending out updates too soon (Constantin, 2012). Once a device (whether computer, phone, etc.) is compromised, both the data on that device and the systems the device can access are at risk.

One current trend that adds risk is the increased reliance on the Internet through “cloud computing.” Although that term has many definitions (Geelan, 2009), this study focuses on the
situation in which application software and/or its associated data are “in the cloud,” i.e., on the Internet, physically away from the using person or organization. This results in both a loss of control and an increased exposure to Internet risks. “BYOD” (bring your own device) is another trend that adds risk. As reported by Burt (2011), some employees prefer to work with a smartphone, tablet, or other device that they already own and are comfortable with using. Businesses are also attracted to this paradigm because it puts the equipment purchase burden on the employee. The problem is how to maintain security on devices that the organization does not control. Older devices (especially older Android devices) are particularly problematic, since security updates may be unavailable (Constantin, 2012). The following sections address the threats posed by road warriors and other employees who use their device(s) outside the organization. Recommendations for reducing the risk of harm from the various threats are also provided.

RISKS POSED BY ROAD WARRIORS

Nearly everyone uses computers and/or other electronic devices in their work. Sometimes, a device is physically taken outside the organization to facilitate the employee’s work while travelling or at home. The term “road warrior” is often applied to employees who spend an especially large percentage of their work time travelling. Such employees have in fact long been early adopters of information technology. From the time of the first generation “portable” computers to the latest and greatest smartphone of today, the traveling business person has used technology to keep in touch with colleagues and clients. Many road warriors also utilize their business devices for personal purposes, such as to keep in touch with family and friends while away from home. Multiple devices are becoming the norm, with many people carrying a smartphone (or two), a tablet computer, and/or a laptop computer. A recent study of over 6000 guests by Four Points Sheraton Hotel chain found that over half of business guests carried three or four devices with them, with a smartphone being the most popular, followed by tablets and then laptops (Ragan, 2012).

If a device contains sensitive information (which it often would), a major concern is that information on or transmitted to or from the device might fall into the wrong hands (competitors, thieves, news organizations, foreign governments, etc.). This can happen accidentally, such as when the employee leaves a cell phone in a cab or a tablet computer in the airport security screening area. That happens often: in 2011, over 8,000 mobile devices were left behind at the seven largest airports in the U.S. (Ragan, 2012). A device might also be stolen from an employee’s vehicle, motel room, or home, and the thief might be looking for more than just a few dollars at the nearest pawn shop. Further, it might not be necessary to steal a device to compromise data. A data thief might merely access the device while it is left unattended. And, if a device is used for non-secure communications, electronic eavesdroppers may obtain sensitive information. Tablets are of special concern in this regard, since it is more likely that the road warrior is accessing confidential information than if they are just checking their email on a smartphone (Cox, 2012). Another risk is that information could be displayed on screen under circumstances in which it can be seen by unapproved persons (e.g., over-the-shoulder).

Of necessity, road warriors often use their device(s) to connect to the Internet from hotels, airports, and other non-secure locations. Several problems can result: (1) If the location’s Internet connection is not secure, communications may be intercepted; (2) Hackers can setup “ad hoc” networks that are similar to those of a legitimate location’s network and fool the traveler
into accessing the bogus network; and (3) the ability of a device to setup a wireless “hot spot” may be convenient but may allow other less secure devices to access it. Regardless of where a device is used, infection by malware (including spyware) may occur if the user is careless about web sites visited, software installed, e-mail attachments opened, etc. Even for careful users, part of the problem with any device that connects to the Internet is the risk that a hacker will exploit an un-patched vulnerability (Fisher et al., 2010; Riley & Vance, 2011).

Riley & Vance (2011) and Panton et al. (2014) report that “zero day” exploits (those that no one but the creator knows about) are bought and sold, so even users with up-to-date devices are at risk. A hacker that gains control of a device can plant a “keystroke logger” program on it to extract passwords, then take control of the device, extract any data or documents on it, and use it to log into systems the user accesses. Note that this type of attack may be successful even if the organization’s system requires secure access (e.g., virtual private network (VPN)), since the hacker can probably do anything with the device that the user could do.

Another danger from malware-infected devices is that a user could accidentally or intentionally bring the infected device back into the organization and connect to a sensitive system. Often, protection of sensitive systems is focused on the Internet connection and firewall, so malware on an internally-connected device might easily slip in. Even a system not connected to the Internet at all could be compromised in this manner. Stealthy malware might just collect information from such a system, then await an opportunity to transmit it to the hacker when the device is again removed from the organization.

If an employee collects data or creates documents while travelling, damage to or loss of the device could result in loss of irreplaceable information. The use of cloud-based applications or back-up storage may help but then bring its own problems. Persons traveling between countries may face (usually temporarily) device confiscation and snooping by government employees. U.S. Customs officials have the authority and sometimes seize devices being brought into the U.S. including those owned by U.S. citizens; other countries operate with similar procedures (Bector, 2009). Further, a device “inspected” by a government--or even by an organization--could be returned with malware installed. Just using a device in a non-secure area can result in data being compromised. Connecting to the Internet at a customer’s site could allow their system to penetrate the road warrior’s system, possibly compromising product costs or other sensitive information that a sales person needs but that the company does not want the customer to see. Nakashima and Wan (2011) report that problems are particularly serious in China where smartphone contents can be downloaded in seconds, and networks (and the Internet) are widely monitored by government agents. They also report that malware has been remotely installed in smartphones and later used to infect servers in the U.S.

Eddy (2010) reports a disturbing trend among road warriors: use of business and/or personal devices for personal purposes while travelling on business. The author reports that younger workers are especially likely to update social network accounts, “tweet” about their travels, and/or randomly surf the web. This activity is problematic in at least two different ways: (1) The traveler’s location and activities can be identified, which could let a client or supplier know where the person has been thus identifying potential clients or new business locations and (2) Social networks are common targets (McMillan, 2011) since few users ever read the end license agreements, and malware can easily be installed. Another issue with accessing web sites other than the organization’s systems is that many sites store “cookies” that can contain sensitive information, and other sites can potentially access that information. Lanois (2011) reports a particularly troubling related issue: cookies based on the Adobe Flash player are not controlled.
by the user’s browser privacy settings, and flash cookies can even reconstruct cookies that the user has deleted.

CLOUD COMPUTING ISSUES

The use of cloud computing is exploding. A 2011 survey showed that 45 percent of multinational corporations used some form of cloud computing services (up from 24 percent in 2010), and many more were planning to adopt cloud computing over the next five years (Lanois, 2011). More recent surveys indicate continuation of the trend (Cohen, 2013). A major attraction of cloud computing is that the organization does not have to maintain the hardware and software that it uses, thereby saving time and money. And, because systems are accessed over the Internet, employees can access them from anywhere. Data security for a road warrior can actually be better than the traditional method of carrying data and documents on a laptop: loss or damage of a device that accesses a cloud system does not necessarily cause a serious problem, since the data and documents are not located on the device (Blyth, 2011). However, cloud computing usually requires that the employee connect to the Internet to do meaningful work. Doing so is always risky and sometimes (especially at hotels/motels and other non-secure hotspots) is very risky (Fisher et al., 2010). Loss of a device that is not secure (e.g., no access password, an easily-defeated password, or unencrypted storage) could allow the thief to get into cloud-based systems just as easily as getting into systems located on the device if the cloud-based systems are set up for automatic login or have saved passwords.

When a road warrior uses a cloud-based system, he or she is logging into a system that is not controlled by the company. The cloud provider (particularly free services) may have less-than-optimal security and/or may collect and distribute information about users. Problematic practices may be disclosed only in the fine print of a hard-to-read end user license agreement (EULA). The provider’s employees have no loyalty to the road warrior’s organization and may be tempted to profit at their expense. The reduction of company resources required to set up and run cloud-based systems may be at least partly offset by an increase in company resources needed to ensure that the provider’s security is adequate (and possibly more resources to fix issues if the security is breached). If the road warrior depends on a cloud site to do a presentation or to access information needed for a meeting with clients or customers, there is the risk that the site or the local Internet connection could be very slow or even fail completely. For example, the Prezi presentation site became virtually unusable for several days in early November, 2012 (“Website Temporarily Down,” 2012).

BRING YOUR OWN DEVICE (BYOD) ISSUES

One of the alarming trends for IT security professionals is the popularity of BYOD (Bring Your Own Device). Some recent reports indicate that BYOD is a rapidly growing trend that is here to stay (Rhodes, 2012). Supporting that theory, Burt (2011) reported a study showing that over 40% of the devices used by employees in 2011 were owned by the employees (not the company), up 10% over the previous year. Others (Cox, 2012) find that, although organizational use of tablet devices like iPads is growing rapidly, some firms are choosing to deploy only company-owned devices in order to maintain greater control. The problem is that mobile devices are risky under ideal conditions, and having to control multiple brands and models of non-owned devices—each of which normally requires a different installation of basic anti-virus, firewalls,
VPN, and other security software—makes the situation much more difficult for the organization’s IT staff (Rhodes, 2012). BYOD is particularly troubling for accounting firms and others that store confidential customer data on their systems. If an employee downloads confidential data to a personal device and that device is subsequently lost, stolen, or compromised, the firm could face liability and regulatory consequences in addition to serious reputational damage (Drew, 2012). There are also negatives for the employee as reported by Rhodes (2012). The company will probably require that mobile device management (MDM) software be installed, and that could result in personal files (like pictures of a new baby) being wiped if the device is temporarily misplaced. Note that this could also cause the employee to delay reporting a missing device, thereby adding to the risk that company data or systems could be compromised. Rhodes (2012) also reports that MDM software often logs GPS locations, so employees may be surprised to find that the boss knows where lunch hours are spent. Finally, the employee who uses his or her own device for work is probably going to expect to retain personal usage rights. Failing to read the fine print in a new application or cloud service EULA could expose the user and organization to risk.

RECOMMENDATIONS

The next section of this paper will discuss in detail recommendations on how to deal with specific security issues that arise with road warriors. We will discuss physical and electronic security, tactics to deal with attacks from inside the organization, and travel in risky locations. We will further address strategies for security in cloud computing and BYOD situations followed by a discussion of the importance of multi-factor authentication and VPN (Virtual Private Network) use along with other general security guidelines.

Physical Security

One of the first things a road warrior should do is ensure the physical protection of his or her device(s). Road Warriors (and other technology users) like that newer devices are becoming smaller and lighter in weight, but that makes it easier for a thief to steal or for the device to be misplaced. Suggestions from Piscitello (2012) and Pash (2009) include:

1. If possible, use a security cable on the device.
2. Install “alarm” software that will set off an alarm if the device is moved, unplugged, etc.
3. Link the device to another device easily carried with you, such as Bluetooth key fob attachments. These vary in capabilities ranging from locking down a device when out of range to sounding an alarm. Drew (2012) provides further discussion of the “leashing” software used for this purpose.
4. Require appropriate security at employee residences if devices are kept or used there.

Electronic Security

It is typically not possible to completely eliminate the chances of a device falling into the wrong hands. Consequently, precautions must be taken that will protect the organization’s data and systems in case that happens. The following three features are recommended at a minimum, and devices lacking one or more of these should be avoided (Piscitello, 2012; Whitwam, 2012):

1. Set a passcode, boot password, or the equivalent for the device. That is, the device should be completely unusable unless and until the proper passcode is entered. Obviously, the passcode should
be strong, i.e., hard to guess (an Internet search of “strong password” will reveal many sources for advice), and the device should be set to require the passcode after a relatively short idle period. For even stronger protection, use a device with “multi-factor authentication” as described below. Also, more secure devices like the iPad automatically encrypt all data if a passcode is set (Mogull, 2011).

2. Encrypt all sensitive data and documents with a passcode that is different from that for the device. Even if the device is passcode-protected, there is the possibility that the passcode could be guessed or that the device’s memory or hard drive could be removed and accessed. Encrypting the data and documents with a different passcode provides a second layer of protection in case the device is penetrated. Encryption is available in most operating systems, in some applications, and from third-party software.

3. Activate remote wiping on each device. Most modern portable devices have the capability of being wiped (erased) remotely in case of loss or theft, but the feature is often turned off by default. Apple iCloud and Google Sync users automatically have this capability (“Find My iPhone,” 2014; “Remote Wipe,” 2012).

Protect Against Inside Attacks

Another high priority should be protecting the organization’s systems from compromised devices. Obviously, systems connected to the Internet should have appropriate security precautions (firewall, etc.) to protect from outside attacks. It is at least as important to have policies in place that protect from inside attacks, especially from devices that have been used outside and brought back inside. Because such a device might have been compromised, it should not be allowed to connect to an internal system unless and until cleared by company security experts. Even a flash drive or CD can contain malware that attempts to install itself when inserted into a computer, so those items should also be inspected carefully before use. In fact, it has been recently reported that USB device code can be hacked in a manner that allows, for example, a flash drive to function as a keyboard to type malicious commands or install malicious software (“BadUSB,” 2014). Obviously, that means that all users should avoid connecting unknown USB devices to their computer regardless of where the computer is located.

Travel in Risky Locations

For employees traveling to risky locations (where the risk that a device might be confiscated, compromised, or have communications intercepted is high), it may help to issue a device specifically set up for high security (see other recommendations) and the ability to access only information absolutely necessary for the trip. The authors of this paper have been told that some organizations issue a device with newly-formatted memory before such a trip and reformat the memory upon return. The logic is that use of a device in a high-risk area creates a significant likelihood of malware infection regardless of precautions. This would be especially true if a device were taken out of the user’s control, such as for “inspection” by an organization or government. In any case where the device is outside the user’s control for any period of time, it would be safest to assume that it has been compromised and act accordingly.

Nakashima & Wan (2011) report that some travelers keep information on flash drives and only access it from off-line computers. Those authors also report that a particular security expert recommends buying a new device before each trip, then never using it again. While a bit extreme, that action would protect against hidden malware that might survive memory reformating as well as use of the device identifying information to track the user. Other suggestions from those authors include leaving devices behind altogether or removing the batteries from a device when in an especially sensitive situation. The latter tactic has the
advantage of ensuring that no GPS data are produced by the device during the sensitive time frame.

Cloud Computing

Greater control is usually had by not using cloud systems. In situations where the advantages of cloud computing outweigh the disadvantages, it makes a lot of sense to look for external validation that the vendor site has state-of-the-art security. As reported by Julisch & Hall (2010), it is good to look for SAS 70 (“SAS 70 Overview,” 2012) and/or ISO 27001 (“ISO 27001 Security,” 2012) certification. However, Ristov, Gusev, and Kostoska (2012) report that the popular ISO 27001:2005 certification fails to address certain threats and vulnerabilities. Those authors propose extensions to the certification that, if adopted, should lead to higher security in certified cloud providers. Other recommendations for ensuring cloud vendor security are provided by Drew (2012).

One way to have some of the advantages of a cloud system while still retaining control is to use a “private” cloud. That is, the system is set up for and used only by the road warrior’s organization, as opposed to the “public” cloud systems that simultaneously serve many customers. As indicated by Schultz (2011), some organizations choose to have both public and private cloud systems depending on the security needs of each.

As noted above, cloud systems suffer from the risk that the Internet or the cloud site could temporarily be very slow or even fail. Consequently, if a road warrior is planning to make a presentation or conduct business that requires access to a cloud-based system, it would be wise to have a “plan 2,” i.e., an alternate means of carrying out the tasks. For example, an online presentation can usually be saved to a computer or flash drive, and even a paper copy might be better than nothing. Similarly, data normally accessed via cloud computing might be saved on a device, and transactions could be stored temporarily for entry later. Of course, security appropriate to the value of the data should be used.

BYOD

We agree with Walters (2012) of US-CERT (United States Computer Emergency Readiness Team) and Piscitello (2012) that security is better if personal and business data/systems are kept completely separate. If the firm does decide to embrace BYOD, employees using personally-owned devices should of course be instructed to use the same precautions as for company-owned devices. These additional steps are particularly important for BYOD:

1. Require that each device be set up for security proportional to the value of information stored on, accessed, and/or transmitted by the device, such as lock codes, restricted application access, encryption, etc. (Drew, 2012; Piscitello, 2012).
2. Require that employees sign agreements authorizing remote erasure of their device should it be lost, stolen, or misplaced, and have included in the agreement a timeframe in which the loss must be reported before major penalties kick in for the employee. This is particularly important if the device has access to sensitive organization systems (Drew, 2012).
3. Subject each device to vulnerability scanning to identify common problems (Piscitello, 2012).
4. Require that different passwords be used for personal use (e.g., banking; social networking) and for access to organizational systems.
5. It may be desirable to allow only company-owned (secure) devices to access more sensitive systems.
Multi-Factor Authentication

Devices and systems that contain sensitive information may not be adequately protected by a single password. Even if a password is strong, the possibility exists for it to be seen while being typed or be recorded by keystroke logger malware. Better security is had with “multi-factor authentication,” also called “multi-step verification” (previously known as two-factor authentication or verification). Awareness of this process is increasing as both Google and Facebook are offering the service to their users. The best multi-factor authentication systems require the user to present at least two of the following three kinds of authentication (“Multi-factor authentication,” 2014):

1. Something the user knows (such as a password or PIN).
2. Something the user has (such as credit card, USB plug-in device, or specific computer).
3. Something the user is (biometric characteristic, e.g., fingerprint, retina pattern, etc.).

An ATM machine, for example, requires both the ATM card and a PIN. Some banks require that a specific device be registered with the server, and additional authentication is required if the user attempts to access the site from an unregistered device. With Gmail and many other sites, the additional authentication is in the form of sending a PIN to the user by a means other than the Internet, such as by cell phone (“About 2-step verification,” 2014). Less secure methods (but still better than a single password) often have the user provide an additional piece of information after logging in, such as a PIN or the answer to a security question.

Restrict User Privileges

Because users can accidentally or intentionally take actions that compromise security, steps should be taken to limit their ability to do so. One way is by requiring that employees only access company systems using a computer or other device that implements “least privilege security.” Many devices and all major computer operating systems have the ability to create user accounts that are limited in functionality. A separate “administrator” account is used to set user limits and perform functions that are not allowed for users. One typical limitation is on the ability to install software, thereby preventing the user from accidentally or intentionally installing malware or an application that compromises the device’s security. Least privilege security is discussed in depth by Smith (2010). Although a bit more complicated than just setting up non-administrator accounts, functions can also be limited on iOS (iPhone; iPad) and Android devices (Bohon, 2011; “Deploying,” 2012; “Device Administration,” 2014).

Require Use of VPNs or a Travel Router

Communications between the user and organization systems (whether those systems are internal or cloud-based) will be much more secure if via VPN than if by ordinary Internet connections (Walters, 2012). Since the quality of VPN software can vary, the product selected should be consistent with the security needed for the particular system. Some systems connect through the organization’s VPN for all Internet access, thereby allowing greater control than if the user connects directly to the Internet. One of the problems with that arrangement is that the organization’s VPN must then be high enough capacity for all of the users’ Internet needs, which can be a problem with high-bandwidth sites like Netflix and Youtube. Some organizations limit
access to non-essential high-bandwidth sites to preserve system performance under this setup (Neff, 2012). One way to greatly improve the security of hotel/motel and other low-security systems is to connect through a “travel router”: a portable device that creates a “private, secure, wireless network with a robust firewall” (Brown, 2014). That is, the travel router connects to the low security Internet access system, creates a secure wireless network for the user(s), and puts a quality firewall between the secure network and the Internet in much the same way that a normal router would.

Motivate Security Policy Compliance

It does not help to have information security policies if employees do not follow them. As reported by Puhakainen and Siponen (2010), training—when done properly—does improve employee compliance with security policies. D’Arcy and Devaraj (2012) also report that employees may be less likely to misuse technology if there are formal sanctions, e.g., risk of discipline or termination. Those authors report that informal sanctions are even more effective than are formal sanctions. Specifically, employees who anticipate social and self-disapproval upon policy violation are less likely to do so. Training, therefore, should focus both on what to do/not do and on the consequences of non-compliance.

Recommendations from US-CERT

The following recommendations from US-CERT are useful for all computers but are especially important for mobile devices (“Security Tip,” 2010):

1. Do not allow applications and sites to save passwords. Saving passwords allows anyone accessing a device to access to all of the accounts and systems the device can access.
2. Store especially sensitive data separately from devices that use it, such as on an encrypted flash drive attached to a key ring.
3. Install and maintain anti-malware, antivirus, and firewall software.
4. Backup important information to a secure location. Note that this is important even if the primary storage is cloud-based, since the possibility always exists that information could be accidentally or intentionally damaged, or that the cloud provider could have a storage malfunction. Off-line, non-erasable media like CD-ROM or DVD-ROM are recommended for the best protection, and sensitive information should be encrypted in case the backup falls into the wrong hands.

US-CERT (United States Computer Emergency Readiness Team) is a government-sponsored site devoted to improving cybersecurity (“US-CERT,” 2014). The site provides numerous recommendations, many of which are easily readable by managers and users, and some of which are cited herein. More thorough and technical information is available from the Carnegie Mellon University Software Engineering Institute CERT® site (“The CERT Program,” 2014), which helped create US-CERT and works closely with it. Organization IT security personnel should visit the sites (http://www.us-cert.gov/ and http://www.cert.org/) periodically and ensure that the recommendations found on them are followed. Apple® mobile device security information is available from “Deploying iPhone and iPad Security” (2012) while the “Android Tips” site (2014) provides some guidance for Android devices.
Getting Back to Work

Finally, if a device is lost, stolen, or confiscated, the user faces another problem besides compromised data: “How will I be able to work?” The same is true if a device merely fails. Cloud computing would seem to be an advantage in this case, since another device could be purchased, therefore making systems quickly available again. However, a new system would probably not come set up for a reasonable level of security, thereby allowing it to easily be compromised. A better solution would be to have more than one device, so an alternate can be used if the primary device is not available. This is probably one reason why so many road warriors carry multiple devices as reported by Ragan (2012).

CONCLUSION

The concepts discussed herein are applicable to organizations that have employees who access company information systems while located physically outside the organization. The systems may be located on a device carried by the employee, but it is increasingly common to use a device that connects to organizational systems by network (particularly the Internet). Such systems may be located within the organization’s control but are increasingly cloud-based. So-called “road warriors” rely heavily on using systems in this manner. Road warriors and their electronic devices raise many threats to information system security. A lost or damaged device may result in loss of valuable information that is not stored anywhere else. Systems and their data can be compromised by access to a device or system by an unauthorized person as well as by the monitoring of unsecure communications. Threats may be physical, such as when a device is stolen, confiscated by authorities, or accessed without permission. Electronic risks include hacker attacks and malware infections. Internal systems that are otherwise secure can be penetrated when a compromised device is brought inside the organization and connected to them.

The increasing use of cloud computing brings both advantages and disadvantages. Although cloud storage may prevent device loss or failure from causing data loss, there are risks associated with depending on the Internet to do meaningful work and with having critical systems located outside of the organization’s control. The fact that cloud systems can be used from anywhere means that they can be compromised from anywhere. Additional risk comes from the growth of BYOD. Allowing employees to use their own devices means that IT staff will have more device types to worry about. The employees will also expect to use their devices for personal purposes, which will increase exposure to malware and other risks. In addition, company secrets can be compromised by inappropriate use of social media even if the device being used is secure.

Recommendations are provided herein that should minimize the impact of the stated risks. Actual implementation of some of these recommendations will require the skills of professional IT staff. Others (like setting a device passcode) are simple enough for anyone to do. The choice of which precautions to implement should take into account both the degree of risk for the particular user (such as whether a device is used in an especially dangerous location) and the value of the respective system and/or information.

Finally, it should be noted that no set of precautions can completely eliminate the risk to systems used and/or accessed by road warriors. Accidents and mechanical failure can happen, users can be careless, determined criminals can find a way to steal devices, and “zero-day” vulnerabilities apply to every device that connects to systems by network. Care should be taken
to balance the benefit of using systems away from the organization against the risk. As discussed by Fisher et al. (2010), some systems may be too sensitive to risk their use or access from outside the organization’s control.

REFERENCES


