Vulnerability of IT Infrastructures: Internal and External Threats

Sylvester Ngoma
Ph.D. Candidate
Information Technology Educator

March 04, 2012
Introduction

The pervasive and complex nature of security threats to Information Technology (IT) continues to be a major concern for modern organizations and businesses. IT infrastructures, which have become the cornerstone of organizational management, are highly vulnerable to potential attacks and sabotage. IT vulnerabilities may be attributable to internal and external sources (McNamara, 1998; Yeh and Chang, 2007). As Colwill (2010) notes, these sources can be intentional or accidental.

IT threats are multilayered. They involve a number of components including operating systems, networks, computer systems, wireless technologies, software applications, the Intranet, the Internet, and other threat vectors. In broad terms, IT threats can be grouped into various categories. Yeh and Chang (2007) identified seven major categories: software, hardware, data, network, physical, personnel, and administration. The magnitude of the threats to these distinct layers has spurred heightened attention to the issue of IT/IS security in recent years (Whitman, 2003). It is evident that lack of security undermines the stability of IT/IS systems with dire consequences in many cases.

This paper examines various forms of IT threats. It is organized as follows. It begins with an exploration of the nature of IT infrastructures to provide a context for IT security threats. This section provides a brief overview of IT infrastructures and delineates the scope of IT. A critical review of IT vulnerabilities follows this nomenclature portion. It assesses critical security issues that pose real threats to interconnected IT assets and reviews existing countermeasures. Finally, a few recommendations are suggested for improving IT security management in organizations. The paper concludes with strategic guidelines for safeguarding IT infrastructures.
Nature of Information Technology

Information Technology, abbreviated to IT, has been defined in various ways in the literature. IT is an umbrella term which covers a myriad of interrelated components including hardware, software, and telecommunication networks (Ward and Peppard, 2002, p. 3). It is worth noting that this definition encompasses the tangible and intangible nature of IT. Ruiz-Mercader, Merono-Cerdan, and Sabater-Sanchez (2005, p. 17) expand this characterization to include the Internet, electronics, and the resulting technologies. Hence, IT can be regarded as a platform that can enhance the processing, management, and transmission of knowledge and information.

In this respect, IT is different from IS, which covers a much wider field. Although the term IT has been used interchangeably with ICT in the European Union (Ward and Peppard, 2002), it appears that IT and ICT are two distinct entities. Equating both concepts may be misleading because ICT encompasses a wide-ranging set of technologies and services including the computing industry, electronic data processing and related services, telecommunication and services, the Internet, and related services; and audio visual equipment and services (Torero and von Braun, 2006, p. 3). IT is concerned with computer systems and related services, software, networks and ancillary equipment, telecommunications and related resources and services. A robust and efficient security is central for IT to perform its role of facilitating acquisition, storage, processing, movement, management, and manipulation of data.

Arguably, scholars have differed slightly on their characterizations of the concept IT. However, there is substantial convergence of three main components: computer systems, networks, and telecommunications (Ward and Peppard, 2002; Ruiz-Mercader et al., 2005). Research has shown that IT/IS has become a critically important tool to the success of
organizations (Zhain, Kassim, Mokhtar, 2003, p. 69). In PK-12 schools, these three systems have become essential pedagogical and management tools. Many schools rely heavily on computer-based and telecommunication-based systems. As such, there are several security hazards inherent in these systems. These risks include—but are not limited to—piracy of server content, modification or destruction of data, hardware vandalism, software piracy, and network sabotage.

**Vulnerability Analysis of IT Infrastructure**

Vulnerability as a concept and as a process has been defined as a weakness that can be exploited to gain access to data (Liu and Cheng, 2009). Vulnerability refers to a deficiency or a security hole. There is a general consensus that computer systems and networks are inherently imbued with a number of weaknesses that may compromise their security. Weaknesses take various forms: architectural, procedural, and structural. Programming errors, network errors, operation errors, compatibility errors, and configuration errors are some examples of vulnerabilities. It is supremely useful to identify sources of the vulnerabilities. Ramarkrishnan and Sekar (2002) argue that vulnerabilities stem from interactions among several system components such as operating system, file system, sever processor, and content.

There is ample evidence that IT systems are facing serious security challenges. The nature of the threat has evolved, and with it, the sources, the perpetrators, the intent, and the consequence (Yeh and Chang, 2007). From the fear of forced access to physical entities hosting computer systems to unauthorized remote access to IT assets (Loch, Carr, and Warkentin, 1992), the changes in techniques and tools have been markedly innovative. Given the diversity of attack tools currently used, there has been a drastic increase in the number of security vulnerabilities. Computer Emergency Response Team Coordination Center (CERT/CC) has noted that security vulnerabilities have increased exponentially from 171 to 7,236 between 1995 and 2007.
Consistent with this escalation, the nature of threats has mutated as well. Yeh and Chang (2007, p. 480) identified four main treats: interception, interruption, modification, and fabrication. These threats affect industries in a variety of ways. In addition to interception and modification, there are other threats including disclosure, and destruction of data (Loch et al, 1992); and exposure of information to unauthorized individuals, and destruction of hardware, software and/or information (Workman, Bommer, and Straub, 2008). Other standard threats include natural accidents, man-made accidents, losses/wastes, malfunctions, erroneous actions, and crimes (Ekenberg, Oberoi, and Orci, 1995). These threats may originate from internal and external sources.

Regarding internal attacks, McNamara (1998) lists the following insider threats: theft of proprietary information, accidental or non-malicious breaches, sabotage, fraud, viruses, and eavesdropping/snooping. These attacks can be premeditated, deliberate or malevolent. Magklaras and Furnell (2002) contend that there are four main categories of insider threat: (1) Possible intentional, (2) potential accidental threat, (3) suspicious and (4) harmless. It should be noted that threats posed by a malicious insider may be exponentially far greater than that posed by an outsider (Colwill, 2010, p. 187). Taking advantage of their internal system knowledge (Liu and Cheng, 2009), malicious insiders may attempt to perform harmful actions. Of all the security issues, the 2010-2011 Computer Crime and Security Survey found malware infection to be the most commonly reported attack. 67.1 per cent of respondents to survey questions reported instances of malware infection. To mitigate the insider threat, Colwill (2010, p. 193) suggests a four-point approach combining (1) encryption, (2) access control, (3) minimum privilege, and (4) monitoring, auditing and reporting.
IT assets are vulnerable to external threats as well. Outsider attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network (Liu and Cheng, 2009). Lacey et al. (2011) provide an updated profile of sophisticated outside attacks which can compromise the security of Mobile Ad-hoc Network (MANET). They include eavesdropping, routing table overflow, routing cache poisoning, routing maintenance, data forwarding, wormhole, sinkhole, byzantine, selfish nodes, external denial of service, internal denial of service, spoofing, Sybil, badmouthing, and flattering. Outsider attackers may range from hackers to cyberterrorists or from petty thieves to professional criminals.

Global connectivity exacerbates security vulnerability because it allows remote access. Alhazmi and Malaiya (2007) argued that highly interconnected computer systems pose security challenges to the architecture of operating systems (OS). Today’s IT infrastructure is more vulnerable to attacks due to connected networks. Therefore, there is urgent need for advanced detection capabilities. Connectivity opens up a computer system or a network system to multiple points of attacks for espionage and other threats.

In other words, highly connected networks make the threats worse. By way of illustration, NCWISE—the Student Information System used in more than 1000 public and charter schools in North Carolina—exemplifies the perils of IT connectivity and centralization. All the schools utilize a centralized portal to retrieve NCWISE—a program that is central to school administration and management. Although there have not been any reported instances of system intrusion, malicious insiders or outsiders may gain access to district’s data and may destroy or alter student academic records.

In today’s IT environment, cyberattacks present enormous security challenges to organizations due to their complexity and sophistication. Increasingly, spams, Trojan horses,
logic bombs, computer viruses, worms, spyware, pharming, sniffing, phishing, and other types of malware pose real security threats. Through electronic mail, instant messaging (IM), Voice Over Internet Protocol (VoIP), and other programs, these attacks can seriously damage the integrity of data. Attacks are becoming increasingly coordinated and automated. Furthermore, they can target multiple systems at once. Research has identified a wide spectrum of sources which generate these cyberattacks. Sources include terrorists, criminal groups, foreign intelligence services, spyware/malware authors, hackers, insider threat, botnet operators, phishers, and spammers (Gao, 2005, p. 13). In today’s world, a cyberterrorist can cripple vital IT resources.

Flaws in network topologies, software design, and systems administration may account for the vulnerabilities of IT environments to this type of attacks. Attackers may take advantage of bugs, defects, and flaws in software configuration (Liu and Cheng, 2009). Thus, it is important that organizations recognize the nature of cybersecurity threats and take necessary measures to safeguard IT assets. Equally important, it is crucial to recognize legal consequences of security breaches. This can help curb security attacks.

Netspionage—espionage made possible by interconnected networks—is another example of a commonplace cyberattack to information security (Kovacich, 2000). Through netspionage, attackers may access highly sensitive information. For defense purposes, this practice has increasingly been gaining preeminence in recent years. Kovacich (2000) explains that some netspionage acts may be ethical and legitimate; unethical but legal, unethical and illegal.

Moreover, Kovacich (2000) describes in detail three types of espionage that occur in cyberspace: (1) competitive intelligence espionage, (2) industrial espionage, and (3) economic espionage. Competitive intelligence (CI) espionage refers to the gathering of highly sensitive information or knowledge about a competitor. Its main goal is to help organizations or
governments gain a competitive edge. Economic espionage (EE) differs from CI in that it is about the collection of sensitive economic information. Finally, industrial espionage (IE) allows individuals or organizations to obtain such protected information as trade secrets, engineering processes, and other key documents.

The motives driving these practices as well as other IT sabotage may range from personal predispositions, unmet expectations, stressful events, ignored rule violations, and lack of physical and electronic access controls (Band et al, 2006). The sheer thrill of spying, sniffing or hacking may also drive certain attacks. However, certain attacks are motivated by personal predispositions.

In a case study about espionage and IT sabotage, for example, Band et al. (2006) from CERT point out that a former disgruntled Air Force analyst wanted to sell classified documents to Iraq, Libya, and China. This insider attack may have been driven by a mix of personality problems and resentment towards employer. The 1996-2002 Insider Threat Study conducted by CERT and the U.S. Secret Service revealed that 92% of all sabotage attacks by insider attackers happened as a direct result of a stressful situation in the company (Band et al., 2006). This finding is significant because it emphasizes the frequency of internal attackers.

Financial motivation may also account for the occurrence of these harmful actions. Kovacich (2000) recounts an industrial espionage case involving Hitachi and IBM in the 1980’s. Hitachi enticed an IBM employee into selling business sensitive documents about a new computer system. Without the intervention of the Federal Bureau of Investigation (FBI), this transaction would have gone through. Because of the financial impact and the severity of the damage these acts may cause, the United States Congress approved the Economic Espionage Act of 1996 to deter both espionage and other IT sabotage acts. Although there has been a
significant decrease in the annual cost of information theft fraud from $56 billion in 2002 to $37 billion in 2010, according to the 2011 Javelin Strategy & Research Report, much work still needs to be done to secure IT infrastructures in the United States. McNamara (1998) points out that the annual loss in 1998 was only $136 million, according to a CSI/FBI Computer Crime Survey.

**Peer-to-Peer Applications**

By default, open peer-to-peer (P2P) networks are vulnerable to security threats (Vlachos, Androutsellis-Theotokis, and Spinellis, 2004). P2P applications including VOIP, instant messaging, videoconferencing sharing, and open source file sharing (Waklawsky, 2006) are another source of IT security threat in an organization. Architecturally, P2P networks are vulnerable to attacks. Through file-sharing, networks may be exposed to malicious worms, unknown viruses, and other types of malware. P2P applications support illegal file sharing, and are open to a variety of worms (Vlachos et al., 2003). Hence, they are highly vulnerable.

Given these vulnerabilities, the Charlotte-Mecklenburg school (CMS) district limits access to P2P-based social media websites. Access to such websites as LinkedIn, Vimeo, Dailymotion, Instagram, Flickr, Orkut, and Youtube are only granted to school faculty. It is my view that such restrictions rob students of an opportunity to experience collaborative learning opportunities. Although books can be accessed through the Kindle feature on cell phones, for example, cell phones cannot be used as instructional tools in the classroom in many schools. This raises the question of the problematic of IT integration into educational curricula. Quality multimedia products and rich features from social media can bring true experiences to the reach of students. Unfortunately, school-safe social media such as Schooltube and Teachertube have not been adopted by a large portion of teachers and students. It would be rewarding to see
schools use social media specifically designed for schools, and which enjoy massive popularity among students.

Some attempts have been made to integrate effective IT networking tools into PK-12 education with Glogster (a digital poster publishing tool), Moodle (a learning management system), Mixbook (a customizable photo book publisher), BlackBoard (a collaborative learning platform), and Edmodo (a collaborative teaching-learning tool). Other tools such as Yammer allow teachers to collaborate in the virtual world. However, we are still far from popular and secure networking media that can allow students opportunities to self-publish, co-create IT reality, and network with other students around the world. Facebook, Twitter, and Myspace were not created primarily for schools.

Because of the ubiquitous nature of the threat inherent in P2P applications, Banic (2007) suggests a unified solution integrating security and acceleration components. The security components include intrusion prevention systems (IPS), firewalls, remote access and access control products. Wide Area Network (WAN) optimization solutions other application front ends account for acceleration solutions.

**Wireless Technologies**

Furthermore, certain wireless systems such as Bluetooth and Wi-Fi are susceptible to attacks (Hoppe, Kitz, and Dittmann, 2010). Their interfaces predispose them to potentially detrimental threats. An intruder may gain access remotely to unsecure wireless devices (mobile wireless phone, wireless laptop, Personal Digital Assistant, SMS, MMS, LAN, VPN, and WAN) through a shared medium, and exploit the vulnerabilities to alter or destroy important data. Selective jamming is one type of external attack that threatens the integrity of wireless networks (Proano and Lazos, 2011). There is a host of anti-jamming initiatives to combat jamming attacks.
including channel surfing strategy, spatial retreats strategy, and jamming-resistant MAC protocol (Chen and Leneutre, 2011); and SPREAD system, RFReact, and internal adversary model (Proano and Lazos, 2011). Simply stated, these researchers recommend fighting jamming with jamming.

Security Countermeasures

As noted earlier, IT threats are multi-dimensional by nature. They can occur at the network and the application levels (McNamara, 1998); the browser level; the server level; the TCP/IP level; the cloud level; and the hardware level. For example, Microsoft Vista was so littered with security holes that many organizations including the Charlotte-Mecklenburg Schools (CMS) never adopted it. Until recently, Windows XP was used in all CMS schools. In 2010, Windows 7 replaced Window XP.

To prevent unauthorized interception or unauthorized modification of information, a number of security countermeasures must be in place. A security countermeasure is designed to deter an attack or minimize potential costs. Workman et al. (2008, p. 2800) listed a few countermeasures such as virus scanners, firewalls, security patches, password change control systems, and a range of other technologies. Furthermore, encryptions, virus detection and prevention programs, and physical and virtual honeypots are other tools used to secure IT systems.

Encryptions

Encryptions offer a protection mechanism for IT environments. They help protect information from theft. However, they are not immune from attacks. DSA and RSA private keys may be intercepted and decrypted to allow access to protected information. Encryptions are embedded with their own vulnerabilities. Ultimately, who encrypts and who decrypts affects the
integrity, availability, and confidentiality of information. Shao, Liu, and Zao (2011) suggest a PRE scheme model which fosters proxy re-encryption of the private key to by-pass security challenges. For secured communication through mobile networks, Siponen and Oinas-Kukkonen (2007) recommend the use of symmetric algorithms—DES, IDEA, RC2, RC5, and Blowfish—and asymmetric cryptographic techniques—communication without sharing a secret key.

As has been noted above, no countermeasure is inherently perfect. However, each does guarantee a certain degree of protection or defense. The choice of a set of countermeasures depends upon the security policy and guidelines of an organization. Unfortunately, research has shown that there is a gap between security awareness and execution of security plans (Colwill, 2010).

Detection and Prevention Programs

For about three decades, a number of detection programs have been utilized to prevent attacks to IT infrastructures before they occur. These programs are designed to identify security breaches (Sobh, 2005). Thus, their main goal is to spot intrusions on a computer or in a network. With varying degree of success, programs such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Collaborative Intrusion Detection Systems (CIDS), and Network Intrusion Detection and Prevention Systems (NIDS) monitor computers and networks for unauthorized activities. Zhou, Leckie, Karunasekera (2010) posit that these attacks are often coordinated and encompass large-scale stealthy scans, worm outbreaks and distributed denial-of-service (DDoS) attacks. There are wireless IDS specifically designed for wireless networks such as wireless sensor networks (Chen, Hsieh, and Huang, 2010).

Clearly, detection programs do not guarantee full protection to such IT systems as network topologies, web content management systems (WCMS), and computer systems. These
programs focus primarily on finding configuration errors (Ramakrishnan and Sekar, 2002). Other solutions have been tried and tested: measuring the vulnerability density (Alhazmi, Malaiya, and Ray, 2006), using such tools as COPS and SATAN (Ramakrishnan and Sekar, 2002), and using $\beta$-disruptor to evaluate the vulnerability of a network (Dinh et al, 2010). Ultimately, any security solution that only targets logic errors or errors in system design has been found ineffective. Passive monitoring with IDS and IPS programs has not proven to be successful to mitigate attacks in all situations. Consequently, other more comprehensive and integrated approaches have been applied.

**Honeypots**

As indicated above, intrusion detection programs have their own limitations. It has been reported that honeypots are above traditional IDSs and IPSs (Artail, Safa, Sraj, Kuwatly, and Al-Masri, 2006). Honeypots are systems designed to monitor networks from unknown attacks. Subsequently, they protect networks and computer systems from intruders. There are two types of honeypots: physical and virtual (Artail et al., 2006). Despite the advent of smarter honeypots such as SweetBait, Vern Paxson’s Bro, Argos, Honeycomb, LaBrea, AutoGraph, EarlyBird, and Honeystat which can generate automated signatures (Portokalidis and Bos, 2006), honeypots still are not the magic wand solution to IT security. Both high-interaction and low-interaction honeypots cannot warn network administrators about every unauthorized activity on the network but do not always provide accurate information about sources of security threats. Honeypots can be fooled or circumvented.

In summary, the main goal of the protection measures discussed above is to safeguard IT infrastructures. It should be noted that consequences of failure to secure IT assets may be incalculable. For example, a breach to the security of a server of a major banking company
website may be costly. Credit card numbers as well as other demographic and financial information may be in peril. In education, there have been reported cases of students tempering with grades after gaining access to student information systems. Smart classrooms, which are filled with IT-supported systems, may be an easy target for attacks. Similarly, other IT-powered systems including remotely controlled systems—lighting, security cameras, heating and cooling systems—in a house or a business, smart mobile phones, digital entertainment systems, nuclear plants, and electrical power grids—‘smart grids’ as they often known—may succumb to inside and outside attacks. The vulnerability of these systems explains why organizations are increasingly prompt to invest significant resources in IT security.

**Recommendations**

With the ever-increasing emergence of security threats, a host of possible solutions have been attempted to minimize security risks. There is general recognition that a one-size-fits-all solution to security threats does not exist. Changes must begin with a clear vision of enhancing access controls, legislation, system monitoring, threat analysis capabilities, system and network configuration, and education about security risks. An integrated and hybrid solution has been adopted as a preferred approach for this paper.

**Access Controls: A Biometric Approach**

One such solution for access controls that has received much attention in the last two decades is biometrical authentication. Biometrical authentication is a fairly convenient way to authenticate an IT user. As such, biometrics deals with authentication and identification of information or individuals. Sipponen and Oinas-Kukkonen (2007, p. 65) surveyed some common authentication techniques including Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Access Matrix. The effectiveness of
each technique varies. However, the authors believe that they play a significant part in securing access to data.

Architecturally, Sukhai (2005, p. 125) suggests four important components of a biometric access control system: (1) Proper identification, (2) authentication, (3) authorization and (4) accountability. Bhargav-Spantzel et al. (2007, p. 534) propose a biometric system with two subprocesses: registration (also refers to as enrollment) and authentication. A system with three components—enrollment, authentication, and identification—appears to be more efficient. Sipponen and Oinas-Kukkonen (2007, p. 61) recommend a biometrical authentication model that addresses four security issues: (1) access, (2) secure communication, (3) security management, and (4) secure IS. Fundamentally, such a model offers more guarantee of security.

There are several challenges associated with biometric systems. Passwords and tokens can be lost, shared, forgotten, and observed. Moreover, privacy concerns may cause apprehension about the use of biometric technologies. Since biometrical authentication focuses on physiological characteristics, health concerns about such biometric techniques as iris scan and retina scan may negatively influence a user’s decision. Another notable drawback is the colossal cost of biometrical authentication technologies. An efficient authentication system should minimize health risks; it should be affordable, automated, and user-friendly. It should also allow system administrators to conduct forensic investigation if crimes are perpetrated. Finally, biometric solutions may hide biometric data collected through biometric systems (Bhargav-Spantzel et al., 2007) but they cannot prevent misuse of the data, which may lead to legal actions.

*Legislation*
Because of the financial impact and the severity of the damage attacks cause, a number of countries have adopted some form of Data Protection or Privacy Act (Ward and Peppard, 2002, p. 74). In the United States, the federal government and states have introduced a number of legislation. In 1996, the Congress approved the Economic Espionage Act to deter espionage acts. Other legislation includes Health Insurance Portability and Accountability Act (HIPAA), U.S. state data breach notification law, Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI-DSS), International privacy or security laws, Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), Health Information Technology for Economic and Clinical Health Act (HITECH Act), Payment Card Industry Payment Application Standard (CSI/Computer Crime and Security Survey Report, 2011), USA Patriot Act, Children's Online Privacy Protection Act (COPPA), Digital Millennium Copyright Act, and California Database Security Breach Act. Although these laws may not guarantee full protection of data integrity or privacy, efforts should be made to adopt universally accepted legislation to protect intellectual property, privacy rights, and data integrity.

Other countries have implemented a number of privacy and data protection laws as well. The United Kingdom Parliament enacted the UK Data Protection Act in 1998 in an attempt to improve the protection of personal information in the United Kingdom. The Australian Government has its own version of the Privacy Act. How these laws are being reinforced and what effects they have on crime prevention are open to debate.

In this globalized IT world, neither legislation above-mentioned applies to all countries. Jurisdictions are restricted to geographical spaces. Yet, the Internet, for example, is a borderless technology. Copyrights of intellectual property will continue to be infringed upon until all countries or a vast majority of countries agree on a set of laws that should govern the Internet. To
Vulnerability of IT Infrastructures

protect IT infrastructures and IT users worldwide, it is suggested here that the world adopts a set of laws that can govern all Internet users. Additionally, an international Internet governing body—much like the International Criminal Court—needs to be put in place to handle severe cases of espionage and IT attacks. Such a governing body may decide what, how, and why information must be protected (Jones, 2009). The legislation must also specify the nature of sanctions that might apply in case of violation.

System configuration

System configuration has been listed as a factor that causes security risks. Traditional system designs and network topologies have exposed a number of security holes. In many cases, new IT-based systems are integrated into legacy systems. Analog and digital systems may coexist, especially in education. Schools are known to be late adopters of information technologies (Barrett, 1999, p. 4). Closed-circuit televisions in Charlotte-Mecklenburg schools are often faced with the duality of analog-digital infrastructure coexistence.

As indicated earlier, there are different approaches for managing security of IT-based infrastructure. Some commonly used measures include anti-spyware scanning programs, firewalls, filtering software programs, anti-virus scanning programs, security awareness training, multifactor authentication, and encryptions of wireless network transmissions (Colwill, 2010). Lacey et al. (2011) proposed a ‘multilayer’ security approach called RIPsec framework which allows detection of attacks and improved network performance. This approach is reported to effectively mitigate 12 of 15 attacks listed under outsider attacks. These security strategies have not been effective in securing full protection of the IT infrastructure. Figure 1 provides an illustration of an actual attack. It goes without saying that this vicious attack would have had severe consequences if the system was not properly protected.
Let us consider software design. By virtue of the multiplicity of manufacturing sources—cloud computing vendors, open source software, in-house developers, ERP providers, packaged software providers, and IT services firms (Hoffer, George, and Valacich, 2011, p. 32); software design is bound to have security flaws. Coordinated efforts may help eliminate vulnerabilities. Core beliefs about software development life cycle, software engineering, and the von Neumann architecture need to challenged and revisited. Hence, Research Into Secure Operating Systems (RISOS) studies to investigate security flaws in operating systems are encouraged in this paper. Similarly, academic inquiry into more efficient data storage and data processing systems should be promoted.

Standard software development techniques—Rapid Prototyping, Joint Application Development (JAD), Computer-Aided Software Engineering (CASE), Rapid Application Development (RAD), Rational Unified Process (RUP), Reusable Components, Service Oriented
Vulnerability of IT Infrastructures

Architecture (SOA), and eXtreme Programming (Hoffer, George, and Valacich, 2011)—have not produced many software products with long-lasting life span. Driven by commercial interests, software developers tend to manufacture software programs that have a short life span. Furthermore, the internationalization of software design coupled with outsourcing only complicates the matter in that approaches in software development vary from one country to another. Software programs are constantly changing. A variety of versions of Photoshop or Dreamweaver makes the case. Thus, changes should focus on the life span of software programs.

Network topologies may account for network security vulnerabilities. To safeguard a network system, it is essential to consider two dimensions: supervision and protection (Ganame, Bourgeois, Bidou, and Spies, 2008). With an increasing push towards virtualization, cloud computing, and wireless communication, traditional network topologies—bus, mesh, ring, star, and tree—may become cumbersome and ineffective to guarantee the security of a network. Neither topology is inherently perfect in today’s IT environment. Therefore, a hybrid combination of these configurations may prove to be more efficient.

Education

Essentially, no non-technical measure to IT security threat is more important than education, training and awareness (Colwill, 2010). Every organization must have a comprehensive and integrated IT security education program. Education programs should target key security issues: sources of attacks, profile of attackers, system controls, system configuration, access controls, and threat awareness. It is important to raise awareness of employees, employers, and every system user about certain threat vectors: removable compact flash, smart media, memory stick, disk reader, and hard drives. These media may carry harmful viruses. The security of documents in the cloud or of open source programs is another area of
focus. The main goal is to develop an organizational culture based on vulnerability awareness, empowerment, engagement, and performance.

**Conclusion**

This paper has examined several aspects of IT security. It addressed different layers of IT vulnerability and proposed needed changes and recommendations to improve the security of the IT infrastructure of an organization. It is suggested that a holistic approach encompassing biometric authentication as an access control mechanism, efficient system configuration, legal protection of data and privacy, and education and awareness is fundamental to IT security.

As Alhazmi, Malaiya, and Ray (2006, p. 223) noted, undiscovered vulnerabilities pose more threat than discovered vulnerabilities. Having a comprehensive IT/IS security strategic plan is not enough; it must be fully implemented. Therefore, bridging the knowing-doing gap is central to the success of IT security management. Security must be a prominent component of any strategic information systems plan.
References


