Security Issues In An Emerging Information Technology Setup

Bisallah Hashim I[1], Aleshelonye abbas[2], Bello Bilkisu Mohammed [3]

[1]Computer Dept, University of Abuja, Nigeria. hbisallah@gmail.com
[2]Dept of computer Sc.. Turkish-Nile University, Abuja. yalesh200@gmail.com
[3] Dept of Computer Sc. Kaduna Polytechnic, Kaduna. candiebell2000@yahoo.com

Abstract: The theft or destruction of information or the disruption of communication resources can result in not only lost of time and revenue, but also an irreparable loss of confidence by clients and customers of an company or institutions. The ability of computer networks to remain functional continuously for their intended users has been a necessity to business. Professionals who have computer security training, who have demonstrated the ability to respond to human and organizational weaknesses by passing security certifications, and who have had instruction in cryptography, communication security, can use real-world tools to implement security for their company/institutions. This paper tends to discuss those areas in an emerging information technology setup and how they can be applied.

[Bisallah Hashim .I, Aleshelonye abbas, Bello Bilkisu Mohammed. **Security Issues In An Emerging Information Technology Setup.** *Researcher* 2016;8(8):8-11]. ISSN 1553-9865 (print); ISSN 2163-8950 (online). http://www.sciencepub.net/researcher. 2. doi:10.7537/marsrsj080816.02.

Kerwords: Networks, Data, firewall, authentication, VoIP

Introduction:

From Network to Networks

Organizations must change the way they think about network security. While network security used to have one relatively simple definition. Defending the company's data networks and Internet presence modern firms must defend several interconnected Networks.

Many organizations now have diverse networks addressing wireless communications, converged voice and data, enterprise-level network access for people outside the company (physically and/or organizationally), and network support of real-time interaction (such as chat and conferencing). These new networks have opened more potential security holes than ever. Meanwhile, potential threats have increased, with new types of viruses, hacking attacks, and other threats affecting wireless and wired networks. Organisations need to protect their diverse networks with multiple security tools, but they also need to integrate these means into a coherent system that is protected and manageable, and which does not inhibit data and voice throughput.

Building the Modern Network Infrastructure

The modern network is being pushed forward by the communications needs of modern organisations. There are several major areas in which organisations are investing. While each one of these creates new capabilities, it can also open up new security issues.

Wireless LANS (WLANs)

Capabilities: The growth of WLANs is exploding as organizations seek to enable employees to work wirelessly anywhere within a work site. This is particularly true in new offices and overseas locations where many organisations are skipping wired networks and going directly to WLANs. This growth can be seen in the worldwide sales of WLAN. WLANs can allow intruders to latch onto the signal without IT even knowing about it. They can also cause interference with other wireless networks and devices.

Converged Voice and Data/VoIP

Capabilities: By combining voice and data onto a single network infrastructure, organisations can save a great deal of money. The most notable way is by enabling voice over IP (VoIP) communications, allowing employees to make voice calls at a fraction of the cost of standard telephone calls. Convergence can also help form the technical basis for many types of useful services, including unified communication and messaging.

Issues: Converged networks place new demands on a company's infrastructure in terms of uptime, high availability, and real-time communications.

New Means of Communication

Capabilities: Just as email and Web communications quickly revolutionized business communications a few years ago and have become ubiquitous. Messaging and e-conferencing are doing so now. Messaging applications allow employees to have real-time conversations. Increasingly advanced conferencing applications allow users to not only communicate when working remotely, but also to do so in real time and to use advanced multimedia capabilities. The current wave of conferencing

applications are increasingly focused on creating shared workspaces to allow advanced collaboration.
Issues: Most organisations have not yet implemented the latest security measures such as content security and monitoring applications that keep employees from breaking laws or compromising sensitive information for Web and email usage. Web and email use are the key way viruses enter corporations. Messaging applications are almost completely uncontrolled, from a security standpoint, in most corporations.

Data Networking
Capabilities: Organisations are looking to send more data, utilize more advanced applications, and conduct more complex communications than ever before, extending these capabilities across national borders. Data networking technologies both hardware and software enable these capabilities by allowing fast, dedicated connections between branch offices.
Issues: These organizations must install content security to cover these networks while also addressing diverse technological and regulatory environments.

Notebooks PC
Capabilities: Notebooks are huge enablers of mobile productivity by allowing users to work from wherever they are located. They are especially useful in concert with other technologies, especially WLAN and VoIP.
Issues: Notebooks also open security threats because they are so easily stolen. Organisations need to make sure that the data, passwords, and wireless capabilities stored on notebooks will be useless to anyone who steals them.

Understanding the New Threat Matrix
Stronger Traditional Threats
Network security has always involved a back-and-forth battle with viruses: virus writers create new viruses, while security organizations constantly update their software to address them. Recently, however, viruses have grown worse as virus writers have combined different types of threats. For instance, one recent tactic is to put a virus inside of a Trojan, which is a program designed to sneak code past a firewall and onto a corporate network.

Meanwhile, hacking has been made easier by the common availability of tools that allow people with few technical skills to carry out relatively sophisticated hacking and denial of service attacks. Finally, spam has increased, putting further strain on corporate networks. Spam also creates an entryway for viruses.

New Threats
Organizations are using a diverse array of new technologies. However, each new technology brings a new set of potential security risks. New types of networks, particularly wireless networks, have created new points of entry for hackers and viruses. Furthermore, many organisations are trying to make wider varieties of information available to a more diverse group of users, often allowing customers and partners' deep access into their networks to facilitate communication and collaboration. Finally, new applications can create problems. This doesn't just apply to communication applications like instant messaging, but enterprise and collaborative applications that offer access to important corporate data. Not only has the possibility of security events grown worse, the implications of such events have also become increasingly grave. Notably, organisations have made more data and more important data available. Applications such as Web services and database management have allowed greater productivity and communication by unlocking data that was once locked in mainframes. Meanwhile, new legal regulations have put an onus on organisations to not lose data, especially customer data.

Holistic Security: Gathering the Ingredients
To protect their diverse networks, organisations must:
• Ensure strong security at every point
• Link these security means into a coherent system

Software
There are several important types of software that organizations need in order to address both traditional and advanced security. These include:
• **A (administration, authorization, and authentication).** This software is particularly important as organisations allow outside users such as partners, customers, or mobile employees deep access into corporate networks. A software makes sure that users who they say are partners are assigns them the proper level of access, and keeps track of their activities.
• **Business continuity.** Solutions in this area make sure that networks stay functional even in the face of physical or software problems. This means routing around problems and making sure there is no loss of important data.
• **Content security.** With huge amounts of communication coming in and out of organizations, organisations need to make sure that employees follow proper procedures to avoid both data loss and legal liability. Content security solutions should ideally cover not just Web and email communications but also emerging forms of communications, such as IM and VoIP.

• **Firewalls.** This is a traditional software area, which provides a security barrier for traffic and users trying to enter the corporate network.. Modern firewalls must provide security while allowing the fast transition of vast amounts of diverse data. They are also increasing in use for mobile networks. Meanwhile, many organisations are also using firewalls to protect data at the desktop level, especially on notebook computers used by mobile and remote employees.

• **Secure Socket Layer (SSL).** This software allows the encrypted transfer of information between a Web browser and a Web server. SSL has been established as the standard for ecommerce and has become a standard for the transmission of sensitive data.

• **Mobile security software.** Security emerged as the most prevalent and significant challenge among organisations surveyed by IDC (2003) that were adopting or considering mobile and wireless solutions. Mobile security software can be defined as software products designed or optimized to provide security specifically for mobile devices, cellular phones, PDAs, and other smart handheld devices. This security function can be in the form of encryption, authentication, authorization, access control, public key infrastructure (PKI) middleware, or firewall protection.

• **Remote device management.** As organisations become more spread out, it becomes important for IT staff to be able to manage devices centrally, assign rights, route around problems, and handle other routine tasks. This can cover all types of hardware, but is particularly important for notebook PCs, servers, security appliances, and printing/imaging devices. Other important security software areas include encryption, intrusion detection, and vulnerability assessment.

Hardware

There are three key considerations organisations need to think about when it comes to hardware: excess capacity, new types of hardware, and greater intelligence residing on devices. Capacity is probably the most pressing concern for most organisations. Servers and networks must have the ability to assure uptime and business continuity, even in the face of heavy network loads or attacks. Such capacity needs to be increased on wireless networks or in any situation in which the company relies on real-time communications.

Organisations must also work to integrate new types of devices into their network security plan. Such devices can enable significant convenience and cost savings. This is particularly true of security appliances, which can provide plug-and-play protection for branch offices. Other important devices can include IP PBXes, which enable VoIP communications, and advanced data networking hardware.

Meanwhile, organizations are enabling greater capabilities at the devices level. This includes both desktop-level security, such as desktop firewalls, and greater device-level intelligence, which enables simplified management.

Services

Services are a key resource that organizations can tap to bring the holistic security solution together. Important security services include:

• **Planning.** Many organisations have been trying to cobble together holistic security solutions. However, the best way to ensure security in a diverse network environment is to plan it from the ground up, addressing both new threats and interaction between different types of networks. Outside providers can help a company devise a network infrastructure that can allow users and information to pass freely from one network to another for instance, allowing users logged in wireless from a remote office to access data on the central network while still ensuring proper security.

• **Integration.** This is important for overall network functioning, as well as security. Many organisations are trying to build advanced communications functions directly into their networks, such as allowing employees to check email over a voice connection on a cell phone. A well-integrated system allows this to happen without opening up any new security breaches.

• **Monitoring.** Though threats come in many forms, when detected, they should all be noted and dealt with by some central authority. Given the growing complexity of diverse networks, many organisations are seeking to outsource all or part of this monitoring function to an outside provider who can utilize the latest technology in terms of detection, automated response, and other factors.

• **Management.** Organisations want networks that are capable of supporting their business needs. But for most organisations, such capabilities are not core to their business. Many will find that it is both cost effective and more secure to outsource all or part of the security management of their networks.

Conclusion

Network security used to mean protecting a single, internal network from hackers and viruses. Today, organisations must be able to deal with the following, demanding situations:

• A user laptop is stolen, but security staff can shut off functions and wireless access, and possibly even track the machine.

• An outside user picks up the signal from the corporate WLAN and tries to piggyback on it or use it to break into the network.

• A combination of high network use and a denial of service attack hits the system at the same time and it doesn't go down.

• The global network must cross national borders with different laws and technology standards yet data is still free flowing and secure. In order to do this, organisations need to create a multifaceted security system that addresses all of these types of network security across every type of network the company maintains. Wired and wireless networks must be made into a coherent and secure whole, ensuring security without burdening users with lag times and complex security procedures. IT staff, or outside providers, must have a holistic view of the entire system.

References

1. Aalbo, E. A, Issues on Networking in Today's' PC McGraw Hill Publishers Ltd, 1999 Page 110 – 2003.
2. Cooker, C.B, Internet Networking McGraw Hill Publishers Ltd, 2004 Page 5 – 69.
3. Salchi M.K, Your Security Your Network Pakalcha Communication Inc. India, 2004.

8/16/2016