Cyber risk management for wireless communication in organization

Darul Mutakin[*], Mohd Toriq Khan Mohd Niyaz Khan[**], Jamaludin Ibrahim[**]

[*] darul_mutakin@yahoo.com, [**] mohdtoriqkhan@hotmail.com, [***] jamal55@gmail.com

Department of Information Systems, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia

Abstract- This paper will discuss the current cyber threats in organization wireless network since it is a trend nowadays to implement wireless network in an organization. Despite the benefits that wireless technology can provide to organization, it also can bring potential cyber threats which are done in a form of sophisticated and diverse attacking mechanisms that will jeopardize the organization reputation. The BYOD initiative in organization has brought significant cyber risk and threats into the organization because of tremendous possession of mobile and portable devices by employees which can also utilized during work. The organization wireless network is accessible by the employees but at the mean time they bring potential cyber threats to the organization's wireless network due to negligence of security policy on their devices, lack of security awareness, differences in device's technology, inappropriate network configuration and advance attacking techniques. In this paper, some recommendation will be provided to readers in dealing with wireless cyber risk and threats in order to come out with sufficient cyber risk management plan for an organization.

Index Terms- wireless network, cyber threats, security, WLAN, BYOD.

I. INTRODUCTION

We live in the information era where access to information is changing rapidly where portable and mobile technologies have become a commodity in our daily life. The proliferation of these technologies and devices has brought great benefits and opportunities but their use also exposes us to significant risks. Information systems and communication become more complex because the increase number of individuals, organizations and business get networked. The complexity triggers new cyber threats and attacking methods to surface.

Information technology (IT) has been utilized extensively today, not forgetting organizations. IT can be used as leverage for achieving various goals [1]; it also can be used as a weapon for mass destruction in humanity's lives. That is why it is important for organization that uses IT, to be aware of the risks that they may face. With the invention of wireless technology, risks of using IT will be elevated due to the openness or availability of the network. Anyone with the knowledge to hack a network wirelessly would have amazing advantage to gain private information.

Wireless communication is one of the current disruptive technologies. According to [2], wireless network refers to the use of radio frequency signals to share information and resources between devices. Wireless networking offers numerous advantages and potential benefits in organization or workplace. Productivity of the employees can significantly improve due to greater accessibility to information resources.

Nevertheless, wireless technology also escalates new threats and changes the present information security risk profile [3]. Every organization faces a wide variety of risks but the challenging one is the risk associated with information and information systems; the cyber risk. In the late decades, cyber risks have evolved rapidly and bring devastating consequences to an organization [4].

In this paper, we present the advantages and disadvantages of implementing wireless network together with the cyber risk and threats to wireless networks in the second. The third section of the paper discusses the new trend in organization or workplace that leverage BYOD or Bring Your Own Devices initiative along with its potential benefits and risks of establishing it. In the fourth section, we identify some current threats in wireless networks to date. The fifth part discusses the attribute of secure wireless network should have. In sixth section, we provide a recommendation for cyber risk management in organization's wireless network and conclusion in the last section.

II. WIRELESS SECURITY RISKS

Most of the wireless attacks would be targeted through the layers in the Open Systems Interconnection (OSI) model. In [5], there are various kind of cyber security risk associated with wireless network system such eavesdropping, hijacking, Man-in-the-middle (MitM), Denial of Service (DoS), management interface exploits, authentication cracking, MAC spoofing and peer-to-peer attacks.

Eavesdropping is achieved by placing an antenna at the right place and being connected to a Wireless Local Area Network (WLAN) Network Interface Controller (NIC). The attack is possible due to the easiness of decrypting the encrypted data that is been sent through the wireless network. The attack on the wireless network can be done using WLAN analyzer application. Hijacking is the situation where an unauthorized user takes control of an authorized user's wireless LAN connection. In a WLAN, hijacking is done at Layer 2 (MAC Layer) for DoS attack and at Layer 3 for attacking purposes. Hijacking can be depicted as shown in Figure 3 below:

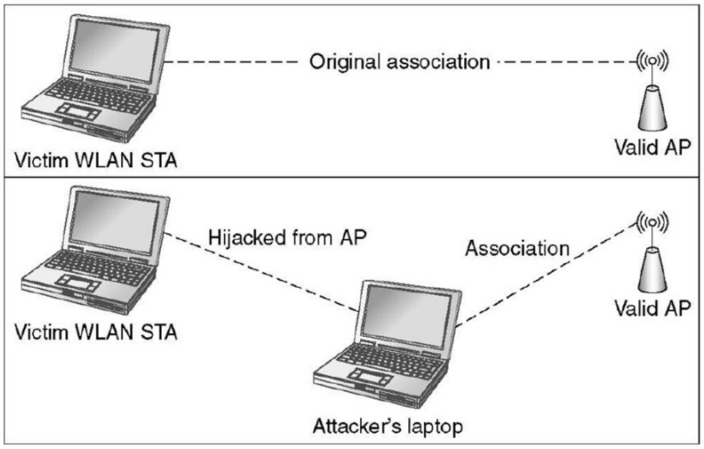

Figure 1: WLAN hijacking.

Man in the Middle (MitM) attack is a form of hijacking attack and when MitM is accomplished, it means that Layers 1,2 and 3 have been compromised. Denial of Service (DoS) attack is launched specifically against WLAN networks at Layer 1 (Physical) and Layer 2 (Data Link). DoS is a category of attacks that includes any actions resulting in the inability of users or systems to access needed resources.

Management interface exploits attack is done where an attacker firstly tries to connect to an open WLAN and the attacker will then exploit the IP address that has been assigned to the attacker. Say the IP address that the attacker has been assigned to is 10.10.10.18. The attacker then will try to connect to the IP address of 10.10.10.1 with the attacker's browser, this is because WLAN residential gateway and many wireless routers use this IP addressing scheme for their default configuration. Basically, all the attacker has to do is to attempt to connect to each IP address in the attacker's subnet, which is determined by inspecting the IP address and subnet mask in the attacker's configuration, or by using a scanning tool that will attempt to connect to port 80 on each IP address. Management interface exploits attack can also be done into a DoS attack by firstly gaining access to an access point (AP) or WLAN router then configure the MAC filters to only allow the attacker's client access. This would provide the attacker with a full access to the network's bandwidth for some period of time until the attacker's discovered.

Authentication cracking can be done by listening to the four-way handshake that is involved in the Wi-FI Protected Access (WPA) authentication process and for example using the CoWPAtty tool, to discover passphrase. If the attacker failed to get the four-way handshake, the attacker can transmit a disassociation frame to the station to force a new four-way handshake again.

Media Access Control (MAC) spoofing is when an attacker discovers a valid MAC address and changes his/her own network interface controller's (NIC) MAC address to match that discovered MAC address. Peer-to-peer attack occurs when one WLAN station attacks another WLAN station that is associated with the same access point. This kind of wireless attack is usually done to commit theft or damaging the victim's station. Another form of peer-to-peer attack is the attack on an ad-hoc or to an independent basic service set network. Since most computers are using Windows and that Windows always has its file sharing over a network option on, the probability of this attack is higher.

III. BYOD: NEW TREND IN ORGANIZATION

Recently, there is a new initiative implemented by certain organization called BYOD or Bring Your Own Devices as the mobile devices getting more portable and smarter. BYOD allows employees to bring and use their personal devices to access organization's network to complete their tasks in workplace. The key objective of BYOD is for the employee to have better control of their work in the office [6] [7] because most of employees nowadays choose to put in their personal and work associated matters in the same smartphones or tablets. BYOD requires the employer to come up with a comprehensive and effective policy to protect organization's credentials to be accessed by unauthorized employees [7].

The level of security awareness of the employee is the main issue of BYOD initiative. This is a significant threat to the local network as those devices were synchronized with the local network. The main concern in applying BYOD in these environments is the proper and solid segregation between authorized and unauthorized territory for the users. If they reach the core network there are many possibilities of malicious activities such as data modification, forgery, cheating and any other possible unethical doings [8]. The network must be very properly designed, so that all the users are allocated reasonable bandwidth, unless the users will get frustrated and bring their own access point to access the network.

According to [9], from organization's perspective, the most significant advantage that BYOD can convey alludes to improve mobility and better efficiency as representatives are presently ready to work wherever and at whatever point they like, while using their own devices [10] [9]. It is also believed that BYOD is bolstered inside the organization, employee will be more eager and connected with, and analytical abilities can be enhanced. Besides, the organization will actually appreciate the benefits of ingenious functionalities and technologies that utilized by the employees [11] [9].

Moreover, by allowing employees to make utilization of their own portable devices, organizations can diminish IT infrastructure costs. Meanwhile, from an employee point of view, the quality of their work is enhanced greatly, as they have the option to pick the services, applications and devices they wish for both personal and work purposes [12] [9].

Eventually, the pushing factor of BYOD is the IT self-sufficiency among employees who have owned mobile devices such laptops, tablets and smartphones. Their devices are more advanced compared to the computerize equipment provided by organization's IT departments. As part of consumerisation, BYOD encourages employees to work on devices they preferred with a sense of freedom to access corporate data and resources. However, it can jeopardize IT security and put organization's sensitive business systems at risk if not fully understood and regulated.

IV. WIRELESS CYBER THREATS IN ORGANIZATION

As organization deploying BYOD initiative in workplace, a multitude of cyber attack could penetrate into the wireless network subsequently. There is several popular cyber attack nowadays that threaten the security of organization's wireless network identified by [13] including:

- **Vulnerability scanning**
  Vulnerability scanning is a process when hackers use certain tools to scan the network with the in order to find the vulnerabilities and security level of the network. After scanning the network, the attacker may proceed to get into the network. Some of the tools used to establish this kind of attack are Netstumbler and Kismet. These sophisticated tools is used in war driving [14] [13] where the attackers will get into the network and do the password cracking activities to compromise user's credentials.

- **Man-in-the-Middle (MITM) attack**
  MITM attack is to position the attacker between two hosts in order to hijack connection and injecting traffic by installing a fake access point. It can occur as jamming by consistently transmitting signals to the existing wireless access points while providing clear signal from another fake access points. When MITM is accomplished, it means that Layer 1, 2 and 3 of OSI have been compromised.

- **Packet sniffing**
  Packet sniffing is an attack by using packet sniffer software such as Wireshark, Network Miner or Cain and Able. Wireshark for example, is a user friendly and free software for sniffing activity. In addition to that, its functions can be enhanced and integrated with other software as well. During this attack, attackers sniff the content of packets and access unencrypted usernames and passwords. By using tools such as Wireshark, sniffing activities can be done by anybody by little practice [15] [13].

- **Denial of Services (DOS) attack**
  One of the weaknesses of wireless network is the restricted usage of bandwidth. This situation is giving great advantage to hackers to launch Denial of Service attack by replaying packets in order to generate noise or by sending de-authenticate packets to the legitimate users in the subnet. DoS attack is launched specifically against the Layer 1 (Physical) and Layer 2 (Data Link) of the OSI model. It is categorized as an attack that includes any actions resulting in the inability of users or systems to access needed resources.

V. PRINCIPLES OF SECURED WIRELESS NETWORK

Upon the setting up of wireless network in organization, it is vital to consistently improve the network management to ensure better connectivity and accessibility without putting security on the line. As suggested by [16] [13] in their paper, here are some principles of what a secured wireless network should have.

- **Efficient Devices Management, Control and Monitoring**
  A secured network should have all the APs to be registered and an automated system must be deployed to enabling APs updating activities. Role Based Access Control (RBAC) is a system that will assign a role to any device based on how they were authenticated in order to avoid misuse and abuse of the network and other security breach. A secured wireless network management should be able to monitor users' activity in real time. This is important as there will be hundreds or of devices connected to the network, so it is important to monitor and manage the applications and programs that are using the network. All devices are also need to be registered and assigned unique IP from the network. To avoid hassle, network access control can allow the users to register themselves to the network.

- **Filtering and Firewall**
  As a network administrator we do not want any user to abuse the network to visit malicious websites or run prohibited programs, thus filtering process must take place. This is also to reduce the possibility the users spreading virus to the core network. A comprehensive security system which integrated firewall, intrusion prevention system and application identification and control is what every secured network is advised to have.

- **Proper Network Segmentation and Segregation**
  A clear and solid boundary of core network and wireless network should be defined so the network can be securely accessed by the users. This is to avoid unauthorized personnel to reach the core network intentionally or not. It is also important to eliminate device which tries to cross the limit out from the network.

- **Enforced policy**
  By having clear and understandable policy or agreement of prohibited actions in wireless network such as packet sniffing or placing any device which can act as a RAP might help to reduce malicious activities in wireless network. As to handle threats that might occur because of social engineering, a written agreement of policy between employees and employers must be taken place from the first day of work. Employees might be given certain unique password to login into company's wireless network and repeatedly reminding them not to share the password and other sensitive credentials to others. Precautions must also be taken when the users are using wireless network outside of their homes or offices, such as hot spots to safeguard confidential credentials from any attackers.

VI. RECOMMENDATION

In order to secure wireless network, organization has to have adequate cyber risk management plan in their IT planning. Based on [17], we come out with the following guidelines for organization to draw a comprehensive cyber risk management for their wireless network.

1. Assess risks, test and evaluate system security controls for wireless network.

Maintaining secure wireless network is continuing process which needs superior effort than that needed for other network systems.

The assessment to be done frequently because the wireless environment is fragile and the risk is much more damaging compare to others. Network administrator has to maintain a full understanding of the topology of the wireless network of the organization. They also needed to perform periodic security testing and assessment of the wireless network. To monitor and track wireless devices, a constant, randomly timed security audits has to be performed. There are also needs to observe the changes in wireless industry especially changes related to standards that enhance security features and for the release of new products. In addition, they have to monitor any emerging new threats and vulnerabilities in wireless technology.

2. Perform risk assessment and develop security policies for the wireless network.

The risks related with wireless network implementation is considerable and organizations should plan to protect their important operations before they implement it. Security assessments should be performed prior to implementation of wireless technologies in order to determine the threats and vulnerabilities that it would introduce in the organization environment. The assessment should consider existing security policies, recognized threats and vulnerabilities, system performance, reliability issues, technical requirements and etc. The organization can start to plan and implement the measures that it will put in place to protect its systems once the risk assessment is complete. The policies and measures that it puts in should periodically reassess because computer technologies and malicious threats are frequently changing.

3. Plan the wireless network installation.

The security of wireless systems, devices and its infrastructure should be taken into consideration from the initial planning stage because it is much more difficult to address the issue once the network has been set up. A detailed, well-designed plan can point the way to come out with a best security decisions for configuring wireless devices and network infrastructure. The plan will support the decisions associated with usability, performance, and risk of the network. Wireless technologies present unique security challenges due to immaturity of the technology, partial security standards, inadequate user awareness, faulty implementations, and negligent of administrative practices.

4. Apply security management practices and controls.

Network administrator should identify organization critical information system assets. Adequate policies, standards, procedures, and guidelines has to be well-developed, documented and implemented in order to ensure confidentiality, integrity, and availability of information protected. The developed wireless security policy should address the use of 802.11, Bluetooth, and other wireless technologies in the workplace. Standardized configurations for wireless devices should be implemented to reflect the security policy in ensuring the consistency of operations. Security training for employees is important to raise their awareness about the threats and vulnerabilities incur from the usage of wireless technologies. Data is transmitted over the radio channel; thus a robust cryptography is vital to protect the data.

5. Implement physical access controls to protect wireless system.

Adequate physical security measures comprise of access control systems, barriers and guards should be implemented act as the premier protection layer to wireless systems. It could lessen the risks such as theft of equipment and installation of rogue access points or wireless network monitoring devices. Portable and mobile devices which relatively small in size, low cost and constant mobility make them more likely to be stolen, misplaced, or lost. Thus, the physical security controls that protect desktop computers do not offer the same protection for them.

6. Deploy and consistently test security features for the system.

A renowned security features in wireless technologies such as authentication, encryption, firewalls and other appropriate protection mechanisms methods should be deployed and test consistently. Generally, wireless technologies come with some embedded security features, but those security features available in networks and devices may not be as comprehensive and robust as required. It may be weak; hence, a well-developed security mechanisms and robust cryptography should be adopted to achieve the highest levels of integrity, authentication, and confidentiality.

VII. CONCLUSION

As discussed in this paper, wireless network is vulnerable to attacks and exposed to many types cyber threats. Implementing wireless network in organization is essential in today’s working environment and challenging since the proliferation and usage of portable devices is on hype. Consequently, it leverages the BYOD to be implemented in workplace. Only when wireless networks and devices are protected and secured, organization and employees will gain the benefit from its resources. Organizations can mitigate the risks by applying countermeasures to address specific threats and vulnerabilities of their wireless infrastructure which involve information security management, procedure, policy, and technical controls. Although the measures will not preclude all penetrating cyber-attack from occurring, it could be an effective ways to minimize risks associated with wireless technology. The advancement in wireless and mobile technology has brought great benefit and leveraging the working environment today, but it comes with a significant risk as well. A cyber threats do not recognize organizational boundaries and any attack could lead to a devastating implications. Therefore, a comprehensive cyber risk management should be adopted to prevent, mitigate and remove the unforeseen impact to the organization.

References

[1] Rendulic, Dario Ilija, 2011, “Project of computer e-education with open access”, Retrieved from: http://www.itdesk.info/Basic-Concepts-of-Information-Technology-notes.pdf *[Accessed 26 November2015]*.

[2] Navpreet Kaur, Sangeeta Monga. 2014. “COMPARISONS OF WIRED AND WIRELESS NETWORKS: A REVIEW”. International Journal of Advanced Engineering Technology

[3] Steve Evans. http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise. *[Accessed 29 November2015]*.

[4] Bert Williams. http://www.remotemagazine.com/main/articles/securing-wireless-communication-networks/. *[Accessed 29 November2015]*.

[5] Student.ing. Chapter 9: Wireless Vulnerabilities and Attack Methods. Retrieved from: http://student.ing-steen.se/wlan/Chapter_9.pdf

[6] BYOD. http://www.securedgenetworks.com. *[Accessed 2 December2015]*.

[7] Dean Evans. “What is BYOD and why is it important?”. http://www.techradar.com/ . *[Accessed 29 November 2015]*.

[8] BYOD. https://en.wikipedia.org/wiki/Bring_your_own_device. *[Accessed 29 November 2015]*.

[9] Zoran Mitrovic, Ivan Veljkovic. (2014). “Introducing BYOD in an organisation: the risk and customer services viewpoints”. The 1st Namibia Customer Service Awards & Conference.

[10] Tim Baker. “What you think about BYOD”.http://www.scmagazineuk.com. *[Accessed 29 November 2015]*.

[11] Gordon Thomson . (2012) Feature: “BYOD: enabling the chaos”. Network Security, Vol. 2012, No. 2, pp. 5-8

[12] Suresh Santhana, Anoop Kumar. (2011). *“Mobilizing SAP Enterprise Applications”*. http://www.infosys.com/SAP/thought-leadership/Documents/mobilizing-enterprise-applications.pdf. *[Accessed 3 December2015]*.

[13] Mardiana Mohamad Noor, Wan Haslina Hassan (2013). “*Wireless Networks: Developments, Threats and Countermeasures”*. International Journal of Digital Information and Wireless Communications

[14] Huwida Said, Mario Guimaraes, Noora Al Mutawa, Ibtesam Al Awadhi. (2011). “*Forensics and War Driving on Unsecured Wireless Network”*. 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi.

[15] Adrian Hannah. “*Packet Sniffing Basics*”. http://delivery.acm.org. *[Accessed 5 December2015]*.

[16] SecuredEdge. “*11 Features Every Secure Wireless Network Should Have”*. http://www.securedgenetworks.com. *[Accessed 6 December2015]*.

[17] NIST. *“Security for wireless networks and devices”*. http://csrc.nist.gov/. *[Accessed 10 December2015]*.

Authors

First Author – Darul Mutakin, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and darul_mutakin@yahoo.com.

Second Author – Mohd Toriq Khan Niyaz Khan, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and mohdtoriqkhan@hotmail.com.

Third Author – Jamaludin Ibrahim, Adjunct Lecturer and Senior Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and jamal55@gmail.com