SAMPLE ASSIGNMENT

 Network Security, Risks and Precautions

 Student Name

 Institution

NETWORK SECURITY, RISKS AND PRECAUTIONS

**Introduction**

Business organizations across the world constantly generate huge amounts of data in the form of transactions, records, medical prescriptions and reports, important information concerning their clients, consumers, patients etc. Maintaining confidentiality of such critical information plays a key role in ensuring a strong bond between the consumers and the enterprise involved in contract. One of the primary roles of IT departments is to develop and implement effective strategies, tools and methods that are capable enough to detect cyber risks and threats in advance, identify potential threats and its likely implications on the business, design effective techniques to prevent cyber attacks using advanced technological tools and applications to protect and safeguard critical information concerning the various aspects of a business. This paper will examine various possibilities of vulnerabilities and threats that are likely to affect a health care facility based in Riyadh and it will also provide suitable recommendations on how to overcome such risks relating to IT with an emphasis on wireless networks.

**Existing Vulnerabilities and Threats**

 Internet has definitely provided many advantages to people and businesses across all sections of our society. Health sector being an indispensable component of our society relies on internet for fast, efficient, effective and convenient mode of communication. Internet services are network based posing various vulnerabilities and threats to people and organizations and failure to protect critical information can prove fatal for any business and health facilities can never be an exception to this fact. Serious network related problems may arise due to poor network and its design, user carelessness, failure to implement latest technological tools and techniques, inappropriate configuration of software and hardware of the system and intentional irresponsible acts performed by the concerned employees within the health care facility that can eventually compromise the network security resulting in data leakage and loss (Dillion, 2013). Ineffective network firewalls and antivirus are the primary causes of data loss, data theft and security related issues normally encountered by business organizations. Therefore identification of vulnerabilities and threats plays a key role in determining appropriate strategies to defend against cyber attacks. This will include examination of network devices such as hosts and servers and evaluating its configuration, technical weaknesses and security policies. Failure to implement effective technological measures to prevent unauthorized intrusion will result in data leakage and information misuse causing irreparable loss to the organization (see Figure A). It is always recommended to implement the latest security software available as updated and upgraded versions of cyber security tools are capable to effectively address the latest threats and vulnerabilities.



Figure A. showing how network security is compromised using latest technologies. The figure shows how data transmissions between laptops and computers are exposed to cyber vulnerabilities.

**Effective Tools and Methods to Overcome Cyber Threats**

Health care facilities are vulnerable to cyber threats as conventional IT security tools fail to identify and prevent the latest breed of attacks leaving the facility vulnerable to data theft and loss. Effective protection against such latest emerging threats can be possible only through proactive endpoint security tools. An integrated security system that includes antispyware, effective firewall, antivirus, application controls and device controls, intrusion prevention, and signature based security are some of the key features that are imperative for the facility to ensure complete security against latest cyber threats (Security and Privacy for Health Care Providers, 2009). Advanced and latest antivirus and firewall applications effectively prevent various threats and attacks making it a difficult task for the attackers to intrude and access critical data and devices (see Figure B).



Figure B. shows how a firewall filters unwanted data transmission coming from external computers. In this figure, a firewall effectively protecting a computer from external sources is shown.

**Encrypting the Wireless Network**

 There are different wireless network encryption techniques available today depending on user suitability and business requirements. Encryption plays a crucial role in protecting the data transfer between wireless devices by making the information undecipherable and ensuring a safe and convenient data transmission across the wireless network. Important encryption techniques normally adopted by individuals and businesses across the world include WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 (Wi-Fi Protected Access 2). WEP is commonly used encryption technique however because of technical limitations and control weaknesses, this type of encryption is deemed to be the most vulnerable to emerging cyber threats. Therefore, it is suggested that businesses employ stronger encryption technologies to ensure complete protection of data transmission across the network (Fitzpatrick, 2013).

 Wi-Fi Protection Access (WPA) is an advanced replacement to WEP encryption technology that effectively addressed the weaknesses and vulnerabilities that are beyond the reach of WEP. Its unique features allows to track down any intrusion by checking if any unauthorized access has altered any packets of data during transmission between the client and the access point. However, despite of its unique features WPA encryption technique too has several drawbacks and is exposed to latest vulnerabilities hence it cannot be deemed as appropriate to our health facility. WPA2 is the most advanced version of WPA and has superseded WPA by introducing some significant changes such as CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) Fitzpatrick, 2013). The following diagram shows how to select a preferred encryption to ensure a secured network.



Figure C. This figure shows how to setup an appropriate encryption type for a network. The figure provides different options of encryption available to select for a network depending on the level of security required.

The WPA2 is enabled with a wireless security shield that restricts attackers from directly intruding the network and access the network devices as attackers require to gain access of the Wi-Fi network first in order to access certain security keys before reaching the network devices. It is also known as WPA2-802.1X because of the security standards and complex technology it implements. This system being a advanced and complex tool is specially designed to meet the latest cyber threats encountered by today’s enterprises requiring complex hardware components for installation and maintenance. The unique features provided by this technology include secured access to information using a login name and password for each client, encrypted transmission to each client using a new encryption key for each network device, RADIUS (Remote Authentication Dial in User Service) enabled server making it a highly complicated system for intruders to access information (Hoffman, 2013). The WPA2 is an ideal option for our health care facility considering the latest emerging cyber threats as is equipped with a complicated system of security layers that hardly provide an opportunity for unauthorized access.

**Measures to Prevent Cyber Attacks**

Considering the emerging cyber threats, attacks and vulnerabilities, it is suggested that health care organizations adhere to stringent rules and regulations enforced by authorized organizations and government bodies and regularly update and upgrade their IT capabilities to ensure adequate cyber security measures are implemented by the facility. This will ensure that the facility operations can be carried out without any scope for illegal access to the information systems and loss by data misuse.

 Today’s health care facilities are exposed to various cyber attacks and threats that can potentially ruin the reputation of a business and cause immense monitory loss by data theft and its misuse. Such situations can be prevented provided adequate security measures are taken in advance. Modern medical devices contain configurable embedded software systems that are easily vulnerable to latest cyber threats. This is mainly because these electronic devices are interlinked via facility networks, internet, other medical and digital devices, tablets, smart phones and laptops, etc that pose serious threats from unknown hackers and attackers. Some of the most important steps to be taken by the health care facility to safeguard its critical information include- preventing unauthorized access to all the network enabled devices whether medical or non-medical, ensuring that indispensable tools such as network firewalls, antivirus, and other security tools are up to date, regular monitoring of network traffic and ensuring no unauthorized intrusion takes place, conducting a routine examination of network components for updating any security patches and blocking unrequited services and ports, immediately contacting the device manufacturer or any cyber security expert in case of any security related issue and lastly building an effective strategy to ensure critical functionalities are maintained as expected especially during adverse situations (Cyber security for Medical Devices and Hospital Networks: FDA safety communication, 2013).

**Conclusion**

On the basis of discussions and analysis presented in this report, it is understood that implementation of advanced cyber security tools is imperative for the health care facility regardless of its size. The discussion presented in this report recommends implementation of latest software tools to protect data generated on a regular basis from unprecedented cyber attacks and threats and also suggests appropriate methods and practices to be followed to prevent future vulnerabilities and threats effectively. Health care facilities must always adhere to the rules and regulations as directed by government authorized institutions to ensure they follow standard security measures and mitigate any chances of cyber threats in the future.

 References

Cyber security for Medical Devices and Hospital Networks: FDA safety communication. (2013). *U.S. Food and Drug Administration* Accessed from <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm>

Dillion J. R. (Ed) (2013). Vulnerabilities, Threats, and Attacks *Network of Lies* (pp. 2-6). Blackpool, UK: Revidion Web Accessed from

<http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf>

 Fitzpatrick Jason. (2013). HTG Explains: The Difference between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters). *How To Geek* Accessed from <http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/>

Hoffman, Chris. (2013). WPA2, WEP, And Friends: What’s The Best Way To Encrypt Your Wi-Fi? *Make Use Of* Accessed from <http://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi-fi/>

Security and Privacy for Healthcare Providers (2009). *Symantec Corporation* Accessed from <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-security_and_privacy_for_healthcare_WP_20934020.en-us.pdf>