Lindsay jarvis

Education, Special Education

In modern day world, technology plays a major role in our day to day lives mainly through the use of the internet, to enable easy access to information, banking services, entertainment purposes and communication, this undoubted comes with certain drawbacks. The so ever increasing presence of technology has led to the increase of cybercrime and the imperative need for cyber security.

A number of countries globally experienced Ransomware attack, called WannaCry. The national healthcare system across Europe was affected though it was not the specifically the intended target. Hospitals were not infected with the virus but certain services were stopped, or taken offline such as emails as to reduce exposure to risks. In return this highlighted the reliance of computer systems and technology, in the healthcare sector, required security improvements and much needed security awareness campaigns.

What is cyber security?

Cyber security is the safeguarding of internet-connected systems that consist of data, hardware and software from cyber-attacks. Information Security subsequently becomes a subset of cyber security with intentions to maintain the confidentiality, integrity and availability of data.

Security risks where cyber security is concerned are problematic as the threats evolve as technology evolves, and in practice the approach by most organizations was to put more resources on known risks for crucial system components and leaving unknown threats undefended.

However advisory organizations are encouraging a more proactive and adaptive approach, which has resulted in the increase of investments in cyber security technologies and services. A projection of 7% increase in information security products and services to reach $83. 4 billion from 2016 to 2017 and would continue to grow to reach $93 billion in 2018 by Gartner was made.

Types of cyber-security threats

It is imperative to keep abreast with new technologies, security trends and threat intelligence to be able to protect information and other assets from cyber threats. These threats may take many forms, which may include the following:

Malware is a malicious program or any file used to harm a computer user, which is worms, computer viruses, Trojan horses and spyware. It gains access to the system through email attachments, software downloads or operating systems vulnerabilities.

Social engineering is an attack that relies on human interaction whereby access is gained to sensitive information by tricking the victim into breaking security procedures in place.

Phishing is a form of fraud, whereby the attacker poses as trustworthy and respectable sources such as banks requesting information, with the intention to steal sensitive data, such as credit card information. It works by redirecting the user to a dummy site, where they will enter personal or sensitive data.

Ransomware is a type of malware whereby the attacker locks the user's (victims) system files by encryption usually and requests a payment in exchange for decryption key.

What cyber security can prevent?

Using cyber security can assist preventing cyber-attacks, identity theft, data breaches, and aid in risk management. As alluded earlier having a strong sense of network security for an organization allows better prevention and mitigation tactics when these attacks occurs, as well as an effective incident response plan.

Cyber-attack

Cyber-attack is any attack against a computer system, network, or internet-enabled application or device, a variety of tools to launch attacks is used by hackers, such as malware and Ransomware and other methods. Intentions of cyber criminals often dictate who the victims of cyber-attacks. The speediness and reach of WannaCry cyber-attack has made it one of the most notable cyber-attacks. In 2017 Britain's National Health Service was one of the initial targets, whereby files became encrypted and hospitals were shut down across the United Kingdom as the news of the Ransomware outbreak occurred, having more than 150 countries hit globally.

Two major contributing factors that made " WannaCry cyber-attack", possible firstly, some of Windows 7 operating systems had failed to patch. Secondly Windows vulnerabilities exploited through hacking tools that were stolen from National Security Agency (NSA).

User awareness in cyber security

User awareness implies understanding of what cyber-attacks are by user, pooled together with right attitude, and action to safeguard the information assets from these threats. Cyber Security Intelligence Index in 2014 stated that, human error amounted to 95% of all security incidents, whereby double clicking on infected attachment or unsafe URL, being the most prevalent mistake.

With such alarming numbers it undoubtedly that the largest risk in organizations has become end users. Hackers may gain access through employees, through no fault of their own but due to lack of user awareness and education. To reduce risk of exposure organizations need to develop end user education and awareness campaigns on cyber security.

These campaigns, which if properly implemented will continue with assisting in educating, monitoring, and ongoing maintenance of security and security awareness within the organization.

The elements of awareness campaign will primarily include the following:

A. Organizational Security Awareness:

An effective campaign would include establishing a security awareness team, role-based security awareness, appropriate training content, and communication of security awareness within the organization.

B. Security Awareness Content:

It’s critical that the right content is selected and disseminated to the appropriate audience based on their roles within the organization. This will

ensure the right audience receives the correct training. All end users will receive general security awareness training, whereas management will receive intermediate security training.

C. Security Awareness Training Checklist:

Developing checklist may assist in developing, monitoring, and/or maintaining a security awareness training program.