Health IT Security Journal

Volume 1, No. 3

A publication of the HITSF

Risk homeostasis:
An instinctive response to risk

How secure is the medical device?

Health IT Security Journal

Volume 1, No. 3

HITSF

IN THIS ISSUE

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to helping healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Editor in chief: Hadi Syahrial

Review Board

- Eric Vanderburg
- Dr. Nurhizam Safie
- Dr. Moedjiono
- Dr. Lukas

Editorial Board

- Bambang Suhartono
- Gregorius Bimantoro
- Seyed Mohammad Motahar

Letter from the editor

Dear readers,

This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

www.healthitsecurity.org

Risk homeostasis: An instinctive response to risk

by Eric Vanderburg

How often do you speed? What is your investment strategy? Questions like these could provide insight on your level of acceptable risk. We embrace or avoid risk, consciously and unconsciously, based on the degree of risk we are willing to accept. Risk choices apply to our use of computers as well. With the constant influx of new threats and the implementation of security controls, the level of risk felt by employees can fluctuate causing an increase or decrease in risk-taking behavior.

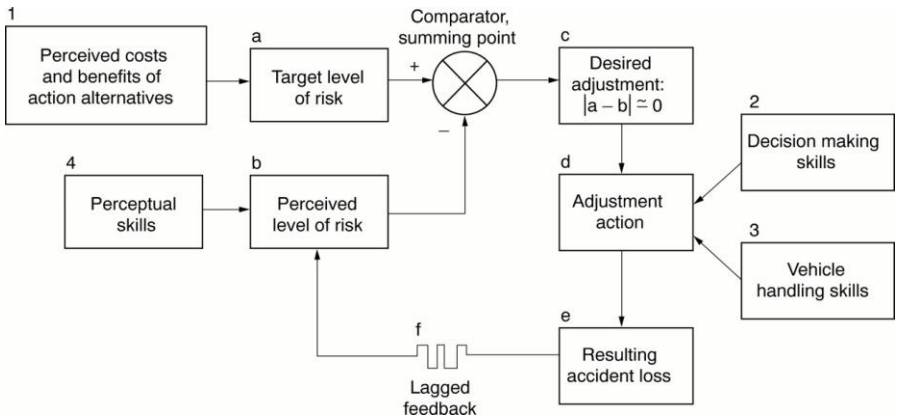
For example, a new policy takes effect, and all laptops are encrypted. It does not seem like such a big security risk to leave a laptop lying around anymore since the drive is encrypted. After all, if someone were to take it, they would not be able to read the data, right. However, leaving a computer unattended could result in other risks to the data especially if the computer is left unlocked. Everyday situations like this undermine the overall goal of security initiatives and inhibit the reduction of expected risk.

Gerald Wilde postulated an interesting theory to explain this called risk homeostasis (http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1730348/pdf/v004p00089.pdf). His theory states that people have a level of acceptable risk. When risk in one area decreases to a level below their acceptable level, the individual will take riskier actions in the act of risk compensation to bring the overall risk back to their acceptable level. This theory is by no means without its flaws and opponents, but some evidence for risk homeostasis can be seen in human behavior such as in the scenario above. Awareness of risk homeostasis can improve decision makers' selection of security controls and evaluation of risk reduction.

Consider the scenario in the light of risk homeostasis. Employees were careful not to leave their laptops unattended for fear that the data on them could be lost. This fear was diminished once encryption was added to the laptop, so their vigilance decreased. Wilde would call this risk compensation, and because of it, the addition of the encryption security control will not achieve the desired reduction in risk. Few laptops were stolen before the encryption was enabled but those that were stolen often resulted in data loss. After the encryption was enabled, a greater number of laptops were stolen, but fewer resulted in data loss.

It is human nature to do only what we think necessary to keep risk at an acceptable level, but acceptable levels are not the same for everyone. Organizations that implement security controls do so in order to reduce the risk that they see as unacceptable. This is an essential part of the risk management role, but risk managers must also understand risk homeostasis and the impact of risk compensation in the decisions people make.

The effect of risk homeostasis may not be immediately noticeable. Risk homeostasis is a process and thus compensating actions are gradually introduced as the value of the security control is intrinsically accepted. For this reason, it is important to measure the effectiveness of controls over time. Awareness of the risk can also aid in adjusting personal risk acceptance levels to bring them more in line with organizational risk levels. However, this can be difficult in areas where risk apathy has set in due, often as a result of continued high levels of risk. Risk apathy can be compared to the airport security alert status where



individuals become desensitized to the risk since airport risk status is routinely at a high level.

Think back on all the security controls implemented last year and consider these questions. Do you feel safer or more comfortable with those controls in place? Have you relaxed your vigilance in another area due to this feeling? Do others in your organization feel the same way?

You've planned and implemented security controls and spent valuable time and effort, now make sure that they meet your expectations. Address risk homeostasis by educating employees of the risks both before and after the implementation of a security control. Reinforce this by explaining the value of existing controls and how they are needed in conjunction with newer controls. Lastly, measure effectiveness of overall security over time with the knowledge that security in one area may drop when another rises.

About the Author:
Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

How Secure is the Medical Device?

by Hadi Syahrial

The use of medical devices (MD) is constantly increasing. What is a medical device? a medical device is any instrument, appliance, equipment, material, product, with the exception of products of human origin, or other article alone or in combination, including the accessories and software involved in its functioning, intended by the manufacturer to be used in humans for medical purposes and whose principal intended action is not obtained by pharmacological or immuno-logical means or by metabolism, but whose function can be assisted by such means.

MDs that are designed to be implanted in whole or in part in the human body or placed in a natural orifice, and that depend for their proper functioning on a source of electrical energy or any other source of energy other than that generated directly by the human body or gravity, are called active implantable medical devices (AIMD). Implantable Medical Device (IMD) use short range telemetry to communicate wirelessly from inside the human body to external equipment. Other types of medical devices are therapeutic, surgical/clinical tools, diagnostic, instrument disposable, etc.

How secure is the medical device? It is basically unanswerable, not many hospital staff understood about the security vulnerabilities facing medical devices and their software. Types of the vulnerability related to medical devices for example weak or non-existing authentication, limited battery capacity, wired communication, unencrypted communication, weak encryption, software / firmware vulnerabilities, electromagnetic interference, social engineering, traffic analysis, and unsecured physical access. SCADA systems bear similarities with IMDs on abstract level and characteristic level.

Roger Baker, assistant secretary for information and technology at the U.S. Department of Veterans Affairs, said during the past 14 months more than 122 medical devices have been compromised by malware. "The major challenge with securing medical devices is that, because their operation must be certified, the application of operating system patches and malware protection updates is tightly restricted," Baker said (http://www.informationweek.com/healthcare/security-privacy/va-security-compromised-by-medical-devic/225200097) (Date accessed: 27 June 2013).

The problem of vulnerable devices on sensitive networks has been latent for years. But today three trends are converging to make it an immediate risk:

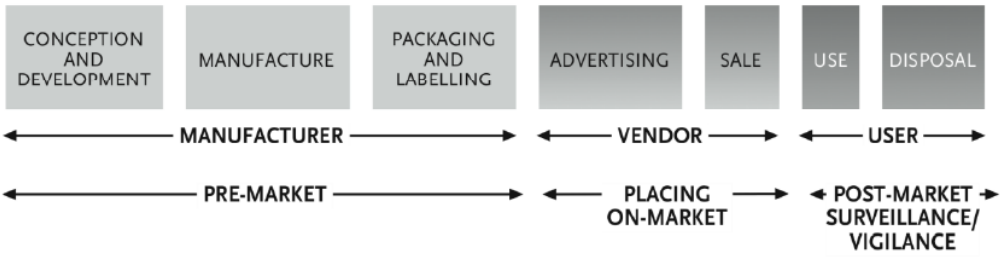
- Sharp rises in the volume, sophistication, and focus of malware, raising the likelihood of, and damage from, malware attacks and data breaches.
- Medical devices that incorporate more off-the-shelf hardware and software, increasing their vulnerability to malware, hacking, and data theft.
- New government incentives and mandates to share patient information electronically, simultaneous with severe penalties for any loss, diversion, or exposure.

What makes network-attached medical devices so different? The answer is that even though newly released medical devices operate more like computers, they are still treated as though they are different—in ways that carry serious ramifications for security and data protection.

Who is responsible for ensuring the security of medical devices? The medical device manufacturers and healthcare delivery organizations or healthcare providers are responsible for ensuring the security of medical devices. It is critically important that medical device manufacturers and healthcare delivery organizations (HDOs, or hospitals) do not only implement a full risk assessment process of a medical device but also ensure that a solid risk management is also implemented. This way, the potential risk of a product can be readily addressed from the time it was being conceptualized to the moment when it is released and disposed. Manufacturers are also responsible for ensuring that products meet the requirements and design specifications.

The international standard for risk management of medical devices is ISO14971. The standard covers the risk determination and application activities for the whole life cycle of a medical device from design, development, and manufacturing. The ISO 14971 standard defines the process of managing risk throughout the lifecycle of a medical device, from initial identification of hazards associated with the device to assessment and control of risks to monitoring of the effectiveness of the control measures.

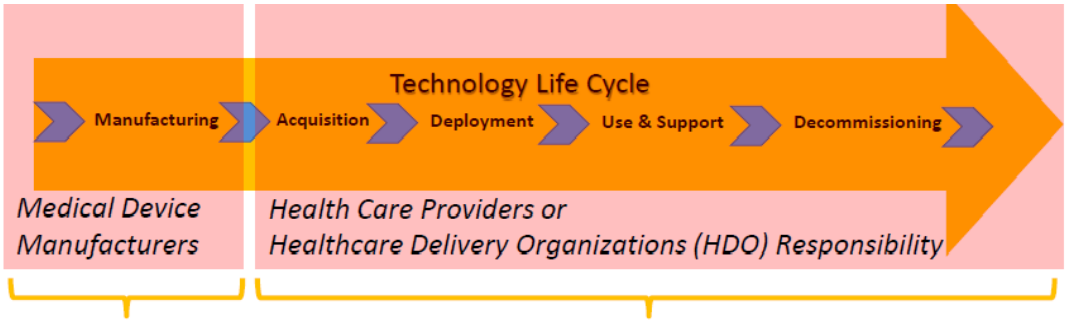
When placing a medical device on the market the manufacturer must have demonstrated through the use of appropriate conformity assessment procedures that the device complies with the relevant essential requirements covering safety and performance.



Stages of a medical device life span (WHO, 2003):

There is a standard to assist healthcare delivery organizations (HDOs or hospitals) in managing risks associated with medical IT networks. The standard is ANSI/AAMI/IEC 80001-1:2010.

ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities aims to ensure both the delivery of safe, high-quality healthcare, and the security and privacy of patient data as medical devices and information management systems converge.



IEC 14971 : 2007

80001-1 specifies general requirements for the application of risk management of IT-networks incorporating medical devices that achieve essential properties such as safety, effectiveness, data & system security and interoperability. It defines responsibilities for parties such as medical device manufacturers, non-medical device manufacturers, the responsible organization, IT-network integrator, and potentially others, engaged in installing, using, reconfiguring, maintaining and decommissioning IT-networks incorporating medical devices. This Standard addresses risks related to patients, operators and/or third parties.

With the information about the architecture, characteristics, and security properties, the healthcare delivery organizations also could conduct a security assessment on the medical devices to monitor the level of security risk of the devices.

IEC 80001-1 : 2010

OWASP ASVS and SANS 20 Critical Security Controls (CSC) v4.0 can be used for security assessment standards. They are widely used, open and free available under the Creative Commons Unported License.

About the Author:

Dr. Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.