2015

Security risks of medical devices in wireless environments

Krishnun Sansurooah
Edith Cowan University, k.sansurooah@ecu.edu.au

DOI: 10.14221/aeis.2015.1
4th Australian eHealth Informatics and Security Conference, held from the 30 November – 2 December, 2015 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/aeis/25

SECURITY RISKS OF MEDICAL DEVICES IN WIRELESS ENVIRONMENTS

Krishnun Sansurooah
School of Computer and Security Science, Security Research Institute
Edith Cowan University, Perth, Australia
k.sansurooah@ecu.edu.au

Abstract

The advancement of wireless medical devices technology, that has developed in hospitals and migrated into the home environment, has created unsustainability in in terms of the management of security for such devices. Through this paper, we shall attempt to explain how medical devices have completely changed the way security needs to be approached in the medical field. We shall also explore the history of medical devices and the organizational problems faced for the development of these devices, the different stakeholders strengths and weaknesses, especially if the device is implanted inside the body of a patient. Once the risk is understood we can then endeavour to mitigate it. We shall also explore how we can put in place a system of prioritization of medical devices that will enable us to reduce the risk threshold for our medical devices.

Keywords
Wireless medical devices, wireless environment, security risks, medical device security issues, medical device framework.

INTRODUCTION

Medical device have become omnipresent in today's technological society. Devices such as pacemakers, automated insulin pumps, which permit people to lead a near normal life, have been growing more and more complex in their design. The devices are extremely reliable, capable of operating for years if not decades inside the body of a patient, but on the other hand there is a distinct lack in security features such as encryption and authentication, which seem to be poorly planned for.

Careful designing choices need to be made when security features are implemented so that doctors can have the possibility of accessing their patients' devices easily whilst keeping at bay potential attackers. The provision of security guarantees is imperative as the complexity and the intrusiveness of the devices grows.

Security vulnerabilities are widespread and severe in wireless-connected medical devices. Not only the confidentiality of patients' data is at risk, but also involve the processing of unauthorized commands, which can turn out to be fatal. Several pacemakers have little to no security in wireless communication, although they allow for control commands to be transmitted wirelessly. This implies that a malicious attacker could spoof a command in order to send shocks to a patient Kirk, 2012). Insulin pumps can be commanded to manipulate dosage and other settings without the patients' knowledge (Mills, 2011).

Given the vast number of these critical vulnerabilities, the security of wireless communication in current medical devices is clearly inadequate. In this paper, we investigate economic, regulatory, and technological factors contributing to the prevalence of security flaws. Based on this analysis, we then propose policy changes to encourage the adoption and standardization of innovative security defense mechanisms, and to accelerate manufacturers' responses to security threats by requiring detailed security incident reporting.

One key reason for the continued existence of security issues stems in part from the inherent complexity of achieving security in medical devices. Implanted medical devices (IMDs) are particularly difficult to access physically. When security vulnerability is disclosed to the manufacturer, applying updates would require extracting the device from the patient's body if the device does not have wireless update capabilities (which is often difficult to implement in small devices).

Besides issues with updates, it is also difficult to pack enough computational resources inside implanted and other medical devices to be able to handle the full range of cryptographic operations needed to securely authenticate commands (Fu, 2009).

EVOLUTION OF MEDICAL DEVICES

Looking back at the history of a couple of medical devices is important for us to understand the complexity of the security issues we are facing today. There is a connection between the advancement of the medical market and the past advancements in wireless technology. Medical device industrials could learn a lot from the mobile device industrials in terms of the implementation of their security architectures.

In addition, mobile devices are at the very edge of evolving between two categories of technologies. Prior to the1920s, being diagnosed with diabetes meant that we could expect a shorter life expectancy and possibly even death. Many patients were experiencing complications from the disease and this inevitably became a major issue. Insulin pumps were considered an option, but presented many challenges in terms of their complicated use which inherently presented further problems for the patients. It is fair to say that between the periods of the 1920s and 1960s, diabetic patients were expected to lead a complicated life.

The 1960s saw the emergence of the first insulin pumps to be designed. However the sizes of these pumps was comparable to that of a backpack and were hence impracticable in terms of mobility for the patient. As the decade progressed, insulin pumps saw their size diminish as the technology advanced. The beginning of the 1980s saw the size of these insulin pumps reduced to the size of a deck of cards. On the 5th of July 1980 the first insulin pump was implanted into a human. Since their creation, insulin pumps have advanced in their technology, allowing patients to have greater freedom and maintain their blood sugar levels within acceptable ranges.

Today, the new systems possess software and wireless capabilities to track and manage the glucose levels of patients, allowing patients to better manage and monitor more efficiently their sugar levels. Patients now also have the possibility of managing their device hence allowing them the possibility to check if any malfunctions are occurring. This management is done by implementing Bluetooth 4.0 into a small system, which is attached to the belt of the patient.

In July 2012 the United States Food and Drug Administration (FDA) authorised the use of insulin pumps using Bluetooth 4.0, in order to communicate bidirectional information about the patient. The pump also allows the automatic administration of insulin. The system checks for glucose levels and communicates the need to administer insulin to the pump, which then injects the precise dose of insulin to the patient. The pacemaker followed a very similar path to that of the Insulin pump. In 1932 Albert Hyman created a device that he named the artificial cardiac pacemaker. During the next thirty years of the device the pacemaker became a lot smaller in size.

In June 1960 the first successful implantation of the pacemaker took place in Buffalo, New York. During the next thirty years pacemakers advanced when battery technology evolved. The 1990s saw a new type of pacemaker appearing on the market, which incorporated process called cardiac resynchronization therapy. The next big advancement of pacemakers was for it to connect wirelessly. Year 2009 saw the first pacemakers that incorporated Wi-Fi within their design being tested. Evidently the major advantage of this was that it allowed to remotely monitor the device, giving the ability to adjust the device and alert people and patients when the device was malfunctioning.

It is important to note that mobile devices share the same wireless connectivity possibilities and can be utilised to link to medical devices.

A second point that is important to take into consideration is the fact that medical devices developed their technology at a much later stage than mobile devices. This leaves the mobile devices with almost 10 years of experience in wireless security problem solving issues, thus leaving them with time to develop security protocols.

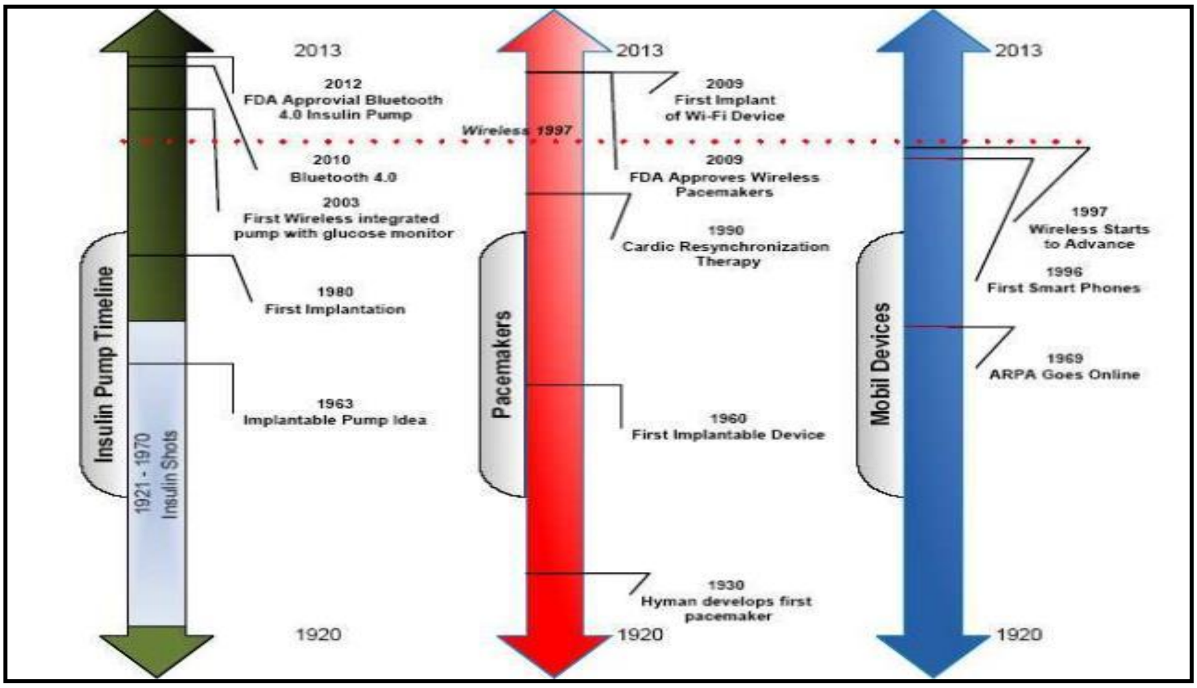


Figure 1. Depicts the evolution of the medical devices.

This can be considered as being a major factor as there are consequences that are much heavier for medical devices compared to mobile devices. It is also fair to state that comparatively speaking, the mobile device market is advancing so rapidly that major security risks could most probably come from this market. Mobile devices are equipped these days with all the necessary tools to perform sophisticated attacks on medical devices.

SECURITY ISSUES AND VULNERABILITIES OF MEDICAL DEVICES RELATED TO THIS DEPENDENCY

The security of medical devices and information is currently a major issue. Hospitals are evolving into a paperless environment, the industry is also aggressively pushing out wireless medical devices that collect the personal health data of people, such as heart and sleep pattern monitoring, with the latter being capable of waking you at the right time.

It is already possible to perform malicious acts such as stealing your identity, social security number, credit card information, as well as your medical information. This can then be used to leverage people or organisations. The principal reason as to why there is such a lack of understanding about this threat is mainly due to the fact that the information that is collected and stored in doctors' cabinets or hospitals has been relatively secure. This is mainly because the information was kept on paper and places in secure libraries that required physical access in order to extract the information. This in turn has developed a high level of trust with the medical systems placed in our society.

Medical devices were immune to hacking and security issues due to their inability to communicate via wireless means. This has also developed a trust in these devices from the people using these devices. With the advancement into areas where the MD industry is not completely aware of security vulnerabilities, the trust model will be seriously put to the test. In order to understand the complex issues of securing medical devices, it is paramount to comprehend the roles and challenges of each stakeholder in the elaboration of medical device security architecture.

Medical Device Manufactures

Like in any industry, the principal aim of the manufacturer is to increase profit, to the disadvantage of customer service. Recent medical devices have been demonstrated as being unsecure, having been compromised by universities and hackers. Due to a lack of spectacular attacks on medical devices, these companies have developed a position that security is not to be considered as an issue.

Software Developers

Design systems and understand how the technology functions inside the device. They run into issues when their objective is changed from creating a software solution to having to cater for security. The Developers also work on timelines and interpret code standards in a different manner, with a limited understanding of security threats, and developers are often put under pressure to privilege speed of development rather than properly securing devices.

Hospitals

Face difficult obstacles when dealing with the security of patients' medical devices. Often times they will possess very limited knowledge regarding current threats. This is due to the fact that up until a few years ago securities was not an integrated part of the hospitals function for implanted devices and have no working knowledge in order to provide security this way. They possess no knowledge of the technology that is inside of these devices.

Hospitals are also ill equipped in dealing with the possible failure of multiple devices simultaneously. A medical device such as a pacemaker requires specialist intervention in order to be replaced; most hospitals only possess one to two specialists at any given time. Should a wide scale attack on pacemakers occur, the hospitals would be in the incapacity of dealing with the situation in such a short period of time?

Government Health Authorities

Government health authorities around the world have not as yet developed appropriate procedures to obtain and store data. For example the Federal Drug Administration (FDA) in the United States of America performs a very good job at developing mitigation techniques for unintended attacks on medical devices. Where the FDA is lacking is when a deliberate attack on a specific medical device occurs.

The reason being that there has been no real structured attacks on individual devices. It would be strongly advisable that medical device manufacturers and companies begin to implement security strategies from the creation of a device up to its commercialisation. In the current state of affairs, should an attack occur on medical devices, there would be a void in currently established procedures?

In March 2012, the Information Security and Privacy Advisory Board (ISPAB), an American public private federal advisory committee, published a number of recommendations to the federal government regarding the security of medical devices offering wireless capabilities (NIST, 2012). In May 2012 the Department of Homeland Security (DHS) issued a national security bulletin on security risks to medical devices (eWeek, 2012). Information Security researchers demonstrated that insulin pumps and pacemakers presented vulnerabilities. It is evident that there is a need for a clearly defined forensic process in order to enhance the ability of the device manufacturers in developing devices that mitigate the security risks that these devices present.

Risk Management

To develop a functional system that meets the requirements in terms of security for hospitals and people, the manufacturers of these devices need to know how to manage the risk and assess what type of exposures they face. We shall be addressing a series of security threats that wireless medical technologies face. In order to assess the risk that the manufacturers are exposed to, we need to implement a list of possible threats that these medical devices are exposed to. Manufacturers need to understand this in order to properly mitigate the risks and minimize any incurring legal expenses that they could be faced with.

Devices such as pacemakers need to possess very high standards of integrity in order to maintain patient safety and running costs low. It is therefore important to look at the different types of attacks that affect the performance of medical devices. Not only should we consider immediate attacks, we should also consider designing a framework in order to predict future attacks. The forecasting of these attacks have been one of the Achilles heel of the government agencies. This is why it is paramount that manufacturers need to look beyond the guidance of the government when managing these challenges.

Exploits

As we know the intention of an exploit is to cause an unprotected or unattended system to fail. Research has recently demonstrated that insulin pumps have been compromised with the result being that complete control was taken and insulin could be injected on command. This type of exploit can be complicated to deal with as it exploits software-coding malfunctions.

A software weakness can result in information being modified within a device, creating new possibilities for criminals to take advantage of, such murder, and denying proper access to patient treatment. A likely event to occur will be the advent of a virus or worm that will cause the device to cease functioning by draining its battery or setting of an electric shock, thus killing the patient.

Eavesdropping

The information stored on medical devices often include personal information about the current patients' health status, the location and medical history. This information could possibly be used for identity theft and to gain an advantage whether political or financial.

Social Engineering

People design medical devices, and these same people can be potentially manipulated into creating potential security holes such as backdoors or malware within a system in order to exploit at a later stage. Social engineering makes it difficult to protect devices which have a predesigned vulnerability. Security protocols will need to be implemented by manufacturers for the handling of medical information.

It is currently relatively easy to obtain information about medical devices from a customers and manufacturers alike. Manufacturers will need to develop protocols that search for malicious code before a device is implanted into a patient at the hospital.

MEDICAL DEVICE SECURITY ISSUES

According to a recent FDA report (2013), it identified some the challenges that hospitals will be facing. As recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including: Network connected/configured medical devices infected or disabled by malware;

- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passw0rds, for software intended privileged access device (e.g. to administrative, technical and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection."(US, FDA, 2013)

Careful analysis of data loss demonstrates that hospital policy is a major concern regarding the security of medical devices, and that only a small percentage of exploits resulted from a vulnerability within a system.

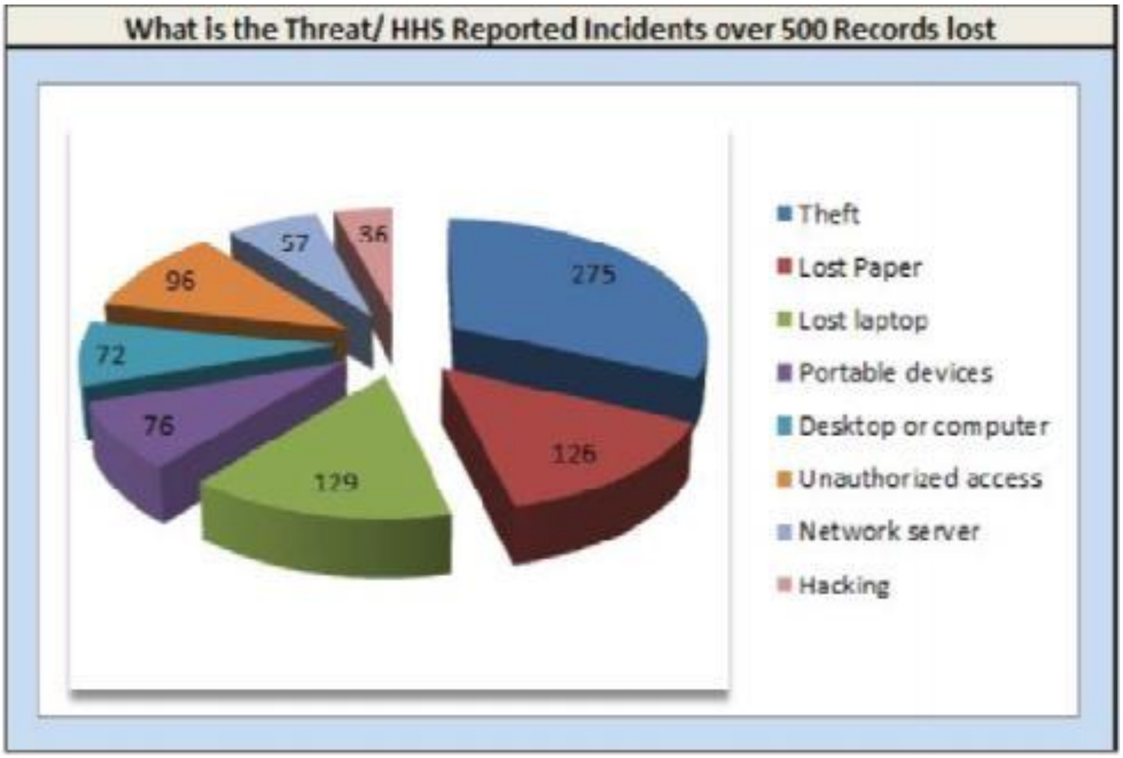


Figure 2. Report listing all breaches reported when hospitals or medical facilities loss individual records (2013).

Proper understanding of where the vulnerabilities are located within a hospital are important to identify in order to properly develop policies and design system wide mitigation strategies.

SOLUTION ENTERPRISE SECURITY ARCHITECTURE FOR MEDICAL DEVICES

Major advancements are starting to take place within the medical device industry. An analysis of solutions needs to be done when dealing with a challenge of this scope. Some hospitals are already dealing with over fifty thousand connected devices located within their hospitals. This excludes patient devices, laptops, mobile devices and other wireless technologies that are brought into the hospital by visitors.

This situation mandates the development of a proper solution that englobes all aspects of a hospitals functioning, the solution would need to unite the objectives and goals by the different risk handlers of the departments. Choosing another type of solutioning will only have a short term effect and will not maintain long term sustainability. Designing a technical fix to a problem will only resolve the issue in the short term, this strategy has proven ineffective with the manufacturers and hospitals. Primarily due to the amount of devices located within a medical facility. A more systemic and prioritization type of approach needs to be achieved.

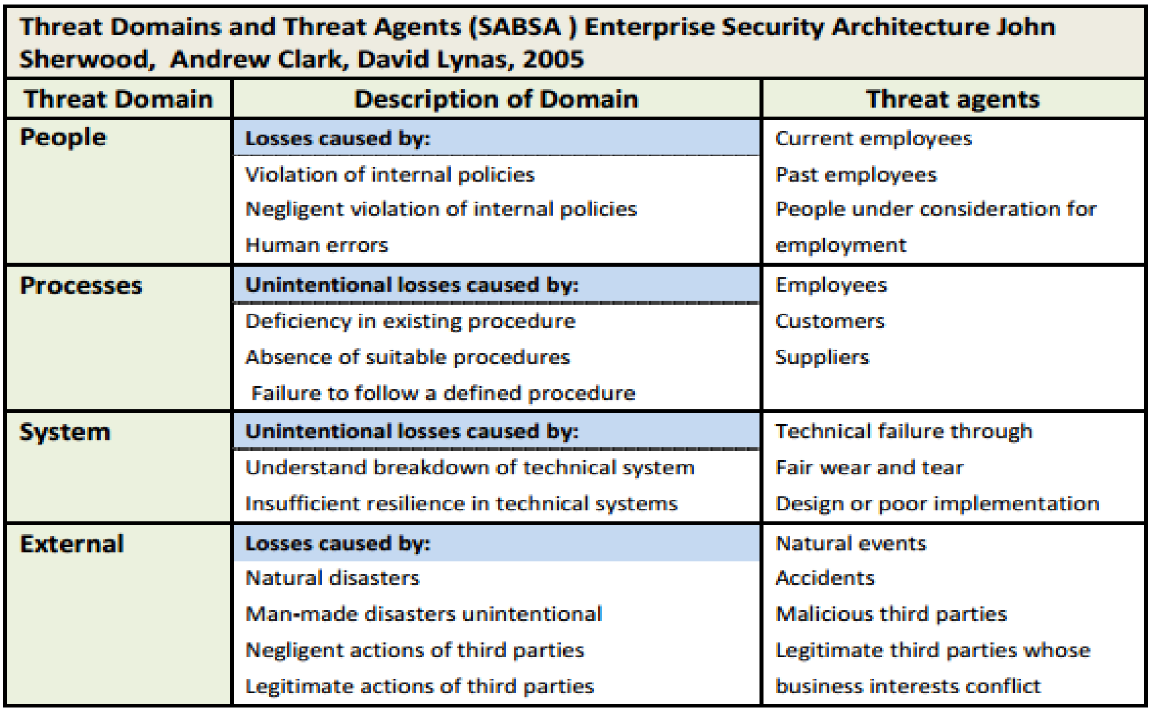
It is therefore paramount to pair the technological fixes in conjunction with an organisational architecture that supports security. This is the only way to achieve long dealing of security issues. Looking at security from a bottom up component level approach leads to misunderstandings and confusion as to why certain devices need to be secured. A short-term security is achieved via this approach, due to technology advancements. This then causes a negative feedback loop within the system, which causes a substantial amount of financial loss. A gap in communication develops between the security and business departments.

Business and security objectives tend to contradict each other due to communication issues between the security professionals and management. It is essential to find a common understanding and alignment between the organisation and the security department.

Threat Domains and Threat Agents

In order for hospitals to assess possible threats it would be recommended that they use a framework based on a threat modelling technique. The framework that we shall be concentrating on is the Sherwood Applied Business Security Architecture (SABSA) threat modelling framework. This framework presents the user with the possibility of defining possible threats via the use of Domains and Agents.

The domains being represented by people, processes, systems, and external events. The Agents are represented by examples of the domains. The example presented in the table below is from the Enterprise Security Architecture: A Business Driven Approach book.



Threat Domains and Threat Agents (SABSA) Enterprise Security Architecture John Sherwood, Andrew Clark, David Lynas, 2005

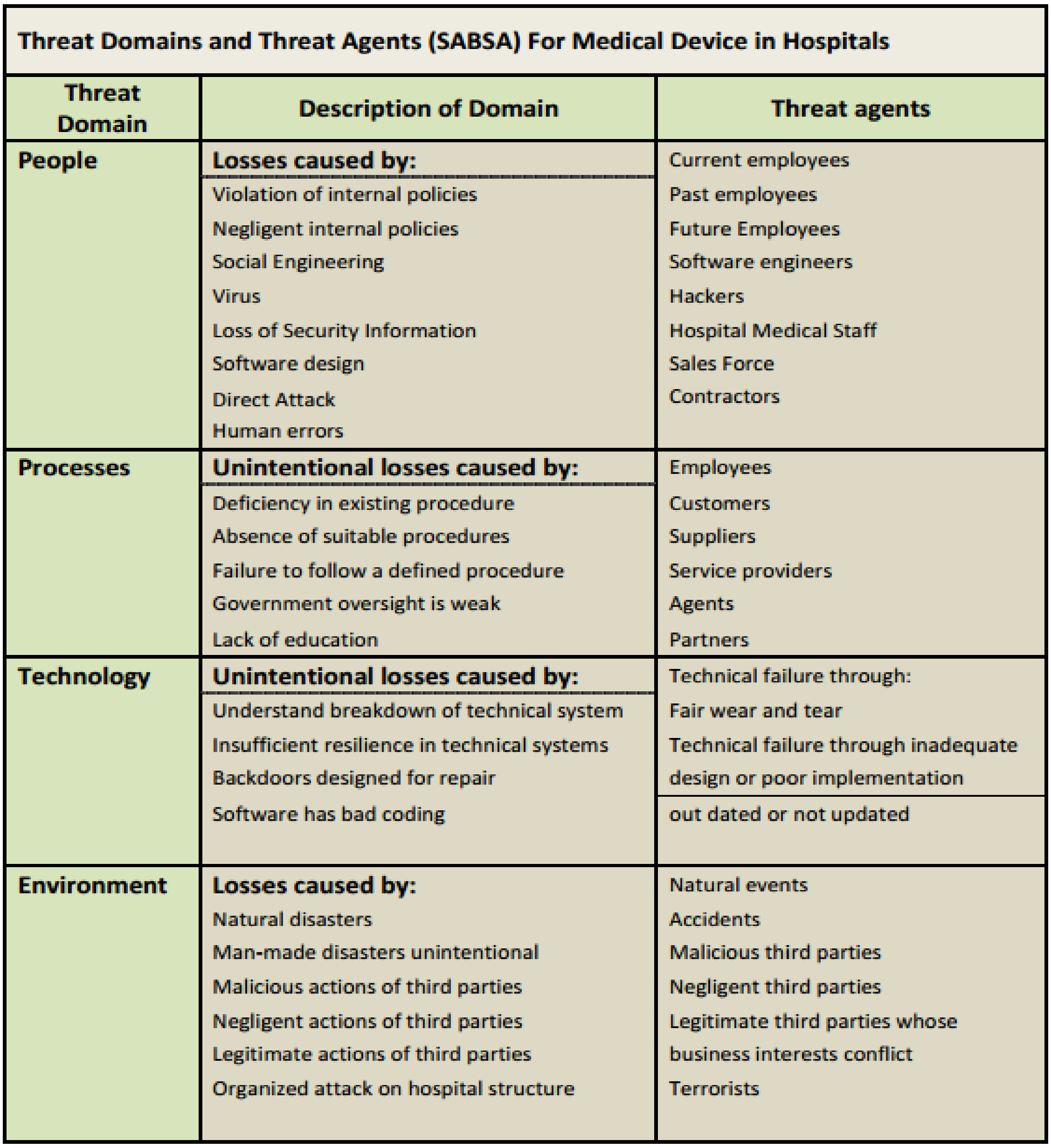
Threat Domain	Description of Domain	Threat agents
People	**Losses caused by:** Violation of internal policies Negligent violation of internal policies Human errors	Current employees Past employees People under consideration for employment
Processes	**Unintentional losses caused by:** Deficiency in existing procedure Absence of suitable procedures Failure to follow a defined procedure	Employees Customers Suppliers
System	**Unintentional losses caused by:** Understand breakdown of technical system Insufficient resilience in technical systems	Technical failure through Fair wear and tear Design or poor implementation
External	**Losses caused by:** Natural disasters Man-made disasters unintentional Negligent actions of third parties Legitimate actions of third parties	Natural events Accidents Malicious third parties Legitimate third parties whose business interests conflict

Table 1. A business driven approach of the threat agents and domains. (ESA, 2013).

Applying the SABSA Framework to Medical Devices in Hospitals

Hospitals need to commence using complex threat modelling frameworks in order to better predict possible security threats. Table 2 showcase another example of SABSA threat framework that has been applied to the Hospital environment (ESA, 2013). A framework such as this takes into account multidimensional aspects that will aid in mitigating threats that are associated with wireless medical and implantable devices. Hospitals are recommended in developing in depth security countermeasures and policies.

The designing of a clear analysis of where threats are emerging from provides the possibility of a more systemic deployment of security and the capacity to design mitigation strategies to the overall objectives of each department. This will allow for security professionals to create and implement strategies that has the objectives of the organization in mind, hence improving compliance with security rules.



Threat Domains and Threat Agents (SABSA) For Medical Device in Hospitals		
Threat Domain	**Description of Domain**	**Threat agents**
People	**Losses caused by:** Violation of internal policies Negligent internal policies Social Engineering Virus Loss of Security Information Software design Direct Attack Human errors	Current employees Past employees Future Employees Software engineers Hackers Hospital Medical Staff Sales Force Contractors
Processes	**Unintentional losses caused by:** Deficiency in existing procedure Absence of suitable procedures Failure to follow a defined procedure Government oversight is weak Lack of education	Employees Customers Suppliers Service providers Agents Partners
Technology	**Unintentional losses caused by:** Understand breakdown of technical system Insufficient resilience in technical systems Backdoors designed for repair Software has bad coding	Technical failure through: Fair wear and tear Technical failure through inadequate design or poor implementation out dated or not updated
Environment	**Losses caused by:** Natural disasters Man-made disasters unintentional Malicious actions of third parties Negligent actions of third parties Legitimate actions of third parties Organized attack on hospital structure	Natural events Accidents Malicious third parties Negligent third parties Legitimate third parties whose business interests conflict Terrorists

Table 2. Showcase an example of SABSA threat framework. (ESA, 2013).

VULNERABILITY ASSESSMENT

An important process in risk management is the vulnerability assessment of a device and the possible consequences that this could have in the worst possible cases. This process can be sometimes complicated as the different stakeholders have different values for the evaluation of this risk. Vulnerability assessments can be very difficult to correctly assess, and requires a properly defined procedure that is adopted within the medical device industry in order to achieve the best outcomes.

Reducing the possibility of a company that will attempt to misrepresent a risk that a device poses signifies that there needs to be a way to monitor these risks and how a company labels these risks. Once the risk is understood and the organisation can understand how it is related to it, the next step is to design a model to show the different oversight responsibilities of each attribute. This will allow the hospital to have the possibility of prioritizing which devices need the most comprehensive security in order to meet the overall objectives set within the attributes. The CFO would then be the person who accepts the risk for the attributes.

CONCLUSION

In this struggle between industrials and hospitals, there will have to be a drive from the hospitals to start providing guidelines for the manufacturers to follow. They're in a strategic position where they have direct access to all the different stakeholders. Hospitals generally have the capability of incorporating advanced security infrastructures in order to keep patient data safe.

This would be implemented through the designing of a clear architecture, which would not allow devices to be placed within a hospital environment without having to pass a certain number security standards. Personnel need to be made aware of the security risks within a hospital, so that they may better understand the consequences of patient data being compromised. Appropriate policies and communication throughout the organisation are to be implemented in order to fully comprehend what procedures need to followed when the acquisition of new technologies are desired.

For the future, hospitals will need to collaborate with each other in order to develop a common operating picture where they will have the same standards in terms of security. The example of the pacemaker is just one of the devices that could have a devastating effect if a major attack were to occur on its systems. Prioritizations of devices within the security architecture are to be created so as to better determine where these devices fit within the structure. Hospitals need to develop their proactivity regarding the implementation of security as a service to the patients.

It would be inconceivable to have state sponsored attacks or criminals affecting the outcome and performance of medical technology. The population needs to be able to trust the technology, and having systems built with security built inside creates this trust.

REFERENCES

Ayers, R., Jansen, W., Moenner, L. & Delaitre, L. (2007). A. Cell Phone Forensic Tools: An Overview and Analysis Update. Rep. no. NISTIR 7387. National Institute of Standards and Technology, Mar. 2007.

Breeuwsma, M., De Jongh, M., Klaver, C., Van Der Knjiff, R. & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory." Small Scale Digital Device Forensics 1.1.

Cusack, B & Kyaw, A., K (2012). Forensic Readiness for Wireless Medical Systems. Retrieved from http://ro.ecu.edu.au/adf/108/

eWeek. (2012). Department of Homeland Security Issues Warning on Medical Device Threats. Retrieved from http://www.eweek.com/c/a/Health-Care-IT/Department-of-Homeland-Security-Issues-Warning-on-Medical-Device-Threats-193136.

Ferguson, J., E & Redish, D. (2011). Wireless communication with implanted medical devices using the conductive properties of the body Expert Rev. Med. Devices 8(4), 427–433 (2011). LEN OTT, Chief Technical Officer, Socket Mobile, The Evolution of Bluetooth in Wireless Medical Devices 2010.

Filkins, B. (2014). Health Care Cyber threat Report - Widespread Compromises Detected, Compliance Nightmare on Horizon. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.

Fu, K. (2009). Inside Risks: Reducing Risks of Implantable Medical Devices. Communications of the ACM, 52 (6), June 2009. Retrieved from http://dl.acm.org/citation.cfm?id=1516055

Fu, K. (2011). Software Issues for the Medical Device Approval Process. Speech. The Special Committee on Aging

United States Senate Hearing. 13 Apr. 2011.

Fu, K. (2011). Medical Devices: Security & Privacy Concerns. Amherst: University of Massachusetts, 14 July 2011. Retrieved from https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf.

Kirk, J. (2012). Pacemaker hack can deliver deadly 830-volt jolt. Computer World. Retrieved from http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html.

Mahn, T., G. (2013). Wireless Medical Technologies: Navigating Government Regulation in The New Medical Age. Retrieved from http://www.fr.com/files/Uploads/attachments/FinalRegulatoryWhitePaperWirelessMedicalTechnologies.pdf.

Mills, E. (2011). Researcher battles insulin pump maker over security flaw," Retrieved from CNET, http://www.cnet.com/au/news/researcher-battles-insulin-pump-maker-over-security-flaw/

NIST, 2012). Information Security and Privacy Advisory Board (ISPAB). Retrieved from http://csrc.nist.gov/groups/SMA/ispab/index.html

Sherwood, J. & C & David, L. (2005). Enterprise Security Architecture: A Business-Driven Approach, November 12, 2005 | ISBN-10: 157820318X. Book

Stouffer, K., Falco, J. & Scarfone, K. (2013). NIST Special Publication 800-82 Revision 1 “Guide to Industrial Control Systems (ICS) Security”.

Storm, D. (2012). Pacemaker hacker says worm could possibly 'commit mass murder. Retrieved from http://www.computerworld.com/article/2473402/cybercrime-hacking/pacemaker-hacker-says-worm-could-possibly--commit-mass-murder-.html

Thompson, J.J.J. (2013). Securing Medical Devices While Maintaining FDA Compliance. Retrieved from http://www.infolawgroup.com/2013/10/articles/information-security/the-internet-of-things-fda-releases-guidance-on-securing-wireless-medical-devices-what-medical-device-manufacturers-should-know/

US FDA (2014). What we do. Retrieved from http://www.fda.gov/aboutfda/whatwedo/default.htm,

Wellington, B., K. (2014). Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. Retrieved from http://digitalcommons.law.scu.edu/chtlj/vol30/iss2/1/

Wirth, A. (2014). Cybercrimes Pose Growing Threat to Medical Devices. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/21322805

Wirth, A. (2014). One if by land, two if by sea” and three if by cyberspace. Retrieved from https://nesce.org/wp-content/uploads/2014/11/Wirth-Cyberterrorism.pdf.

Witters, D. (2014) US FDA – Radio Frequency Wireless Technology in Medical Devices. Retrieved from http://www.fda.gov/OHRMS/DOCKETS/98fr/06d-0504-gdl0001.pdf.

Youssef, A (2013). Wi-Fi Connectivity Puts Pressure on Health Care Security. Retrieved from http://connection.ebscohost.com/c/articles/93671487/wi-fi-connectivity-puts-pressure-health-care-security