EPIDEMIOLOGY | RESEARCH ARTICLE

Protecting the Internet of medical things: A situational crime-prevention approach

Murugan Anandarajan1* and Sarah Malik1

Abstract: The Internet of Things (IoT) is defined as a collection of identifiable things or nodes with the ability to communicate over wired or wireless communication media. Projections indicate that by 2020, 40% of IoT-related technology will be health related, more than any other category, making up a $117 billion market. Numerous applications such as heart rate monitors and blood pressure monitors are already in use in the IoT for medical devices and are poised to revolutionize the functioning of the healthcare industry. However, this interconnectivity leaves medical devices vulnerable to security breaches, increasing concerns that the connectivity of these medical devices will directly affect clinical care and patient safety. Therefore, the focus of this study is to identify potential security threats to the Internet of Medical Things (IoMT) devices and propose control mechanisms using the situational crime-prevention theory to reduce the likelihood and impact of such threats.

Subjects: Technology

Keywords: Internet of Things; medical devices; Internet of medical things; IoMT; situational crime prevention; security

ABOUT THE AUTHORS

Murugan Anandarajan is a Professor of MIS at Drexel University. His current research interests lie in the intersections of the areas of crime, IoT, and analytics. His work has been published in journals such as Decision Sciences, Journal of MIS, and Journal of International Business Studies. He has authored eight books, including The Internet and Workplace Transformation (2006) and its follow up volume, The Internet of People, Things and Services (2018). He has been awarded over $2.5 million in research grants from various government agencies such as the National Science Foundation, U.S. Department of Justice, National Institute of Justice, and the State of Pennsylvania.

Sarah Malik is currently pursuing a Bachelor of Science in Business and Engineering at Drexel University in Philadelphia. She is actively involved in undergraduate research both in Drexel’s LeBow College of Business and College of Engineering. Her main research interests include the Internet of things, Data analytics, and Data security.

PUBLIC INTEREST STATEMENT

This research is important for healthcare institutions, medical device regulators, and healthcare data security personnel in the United States. Given the exponential growth of the Internet of Things (IoT) devices, we must understand the security vulnerabilities of these connected devices. Threats to connected medical devices will directly affect clinical care and patient safety. This study identifies potential threats to medical IoT devices and proposes control mechanisms using the situational crime-prevention theory to reduce the likelihood and impact of such threats. The study will help healthcare security professionals make informed decisions about reducing vulnerabilities in medical devices. Ultimately, the proposed control mechanisms will help build stronger trust between the healthcare system and patients.
1. Introduction

The Internet of Things (IoT) is defined as a collection of identifiable things or nodes with the ability to communicate over wired or wireless communication media (Thangavel, 2015). IoT is the third wave in the world information industry after the introduction of the computer, the Internet, and mobile telecommunication networks (Shen & Liu, 2010). According to Gartner, over 26 billion devices will be connected through IoT and result in $1.9 trillion in global economic value added through sales by 2020 (Gartner, 2013). Furthermore, 40% of IoT-related technology will be health-related, more than any other category, making up a $117 billion market (Bauer et al., 2014). A report by Allied Market Research predicts that the IoT healthcare market will reach $136.8 billion worldwide by 2021 (Marr, 2018).

IoT devices in the healthcare industry such as sensors can have numerous applications including heart rate monitors, blood pressure monitors, and endoscopic capsules (Al Ameen, Liu, & Kwak, 2012). This network of sensors, actuators, and other mobile communication devices are poised to revolutionize the functioning of the healthcare industry (Khanna & Misra, 2014). Such networks, called the Internet of Medical Things (IoMT), is the connected system of medical devices and applications that collect data that are then provided to healthcare IT systems through online computer networks (Marr, 2018). Today, 3.7 million medical devices are in use and connected to and monitor various parts of the body to inform healthcare decisions (Marriott, 2017). Some of the literature refers to the Internet of Things in healthcare as IoT-MD, IoMT, Medical IoT, mIoT, and IoHT. We use IoMT to refer to the Internet of Medical Things based on Marr’s (2018) definition.

IoMT interconnectivity leaves medical devices vulnerable to cyber security breaches in the same way other networked computing systems are vulnerable. However, unlike these other networked computing systems, there is an increasing concern that the connectivity of these medical devices will directly affect clinical care and patient safety (Williams & Woodward, 2015). For example, the Identity Theft Resource Center reported that the U.S. medical and healthcare sector experienced roughly 28% of the total data breaches in 2017, and even with regulations, 94% of healthcare organizations have been the victim of cyber attacks (Filkins, 2014; Tatham, 2018). Therefore, it is imperative for patients, clinicians, hospitals, and other healthcare facilities to understand potential IoMT threats to reduce future attacks. The focus of this study is to outline the potential vulnerabilities of IoMT devices and propose a framework to reduce threats to them.

In the following section, we provide a classification of medical devices based on wireless architectures. We then describe the general framework for IoMT devices. Next, we report incidents of wireless and medical device cyber-attacks, and provide recommendations to reduce future IoMT attacks. Finally, we discuss the limitations of the current study and recommend future directions for research in this area.

2. Literature review

A number of technologies can reduce the overall costs for the prevention or management of chronic illnesses (Dimitrov, 2016). One of the leading technologies is the increase in the interconnectivity between medical devices and other clinical systems. Based on a review of the literature, we have classified medical devices into three categories based on the wireless architecture and interaction with the patients: (1) wireless implantable and wearable devices, (2) wireless emergency response devices, and (3) wireless medical adherence devices.

2.1. Wireless Implantable and Wearable Devices

Implantable and wearable medical devices include any device that collects the body’s internal signals and outputs the signals to an external device. Wearable devices include any device that touches the patient’s skin. Implants refer to any device that is inserted into the body. These devices capture vital signs such as heart information, insulin and glucose levels, and other bodily measurements. From the medical device, data travel to a smart phone, laptop, or computer and are viewed and analyzed by the user. The user may be the patient, healthcare clinic, or doctor.
Table 1 outlines some brands that offer wireless implants and wearable devices. Some examples include Fitbit Activity Trackers and Medtronic’s pacemakers. The device collects medical and other forms of health data from individuals in one location and electronically transmits that information securely to healthcare providers in a different location for assessment and recommendations (CCHPCA, 2018). Figure 1 depicts the wireless structure for patient monitoring using wireless wearable or implantable medical devices.

### 2.2. Wireless Emergency Response Devices

Emergency response devices connect patient monitors specifically to emergency services. Multiple nodes in the patient’s home provide the patient’s geographical location and health condition. Data from the patient’s sensors combine at a modem and are forwarded to the ambulance base station. The local EMTs and paramedics use PDAs or tablets to enter patient information as the patient is being evaluated, and treatment is provided in the field. The information is linked to a real-time sensor data timeline by the web service application. Each patient’s medical history is available in the field (even when disconnected from the Internet), and on the central server (Hashmi, Myung, Gaynor, & Moulton, 2005). The overall goal is to send secure, end-to-end, real-time information including medical, environmental, and geo-location details to first responders, who can then provide situational awareness to support local decisions and the global management of resources (Hashmi et al., 2005). Table 2 describes some wireless emergency response devices. Some examples include Life Alert and Qmedic Medical Alert Bracelets. Figure 2 illustrates the wireless structure for emergency response devices.

### 2.3. Wireless Medical Adherence Devices

A wireless medication dispenser’s goal is to solve the problem of a patient’s lack of adherence to medication regimens. This device is especially helpful for the elderly and people with cognitive limitations. Medical adherence devices log when and if medication is taken, medication bottle

---

Table 1. Brief overview of brands that offer wireless implants and wearable devices

| Brands       | Wireless Implants and Wearable Devices                                                                 |
|--------------|--------------------------------------------------------------------------------------------------------|
| Medtronic    | MyCareLink Smart Monitor is a device that uses a reader to receive pacemaker data. The data are sent to the MyCareLink Smart Mobile App and further to the patient’s clinic. (Medtronic, 2018a) |
| Medtronic    | The Reveal LINQ is Medtronic’s insertable cardiac monitoring system. It continuously monitors heart rhythms and records them to an app-based mobile manager. The mobile manager connects with the CareLink network with certified technicians who can review cardiac data and create actionable reports. (Medtronic, 2018b) |
| Miracle-Ear  | The company offers a variety of hearing aids with Bluetooth capabilities that can connect to smart phones, music apps, TV, or other devices. (Miracle-Ear, 2018) |
| Dexcom      | The Dexcom G5 is a smart glucose monitor including a smart sensor inserted underneath the skin, and data sets are sent to a smart device via Bluetooth. The smart device can send alerts about spikes in sugar level sent to phone, healthcare provider, or family members. (Dexcom, 2018) |
| Insulet      | The OmniPod Insulin Management System is a tubeless Pod and a handheld Personal Diabetes Manager that allows the patient to wireless program insulin delivery. (Omnipod, 2018) |
| CardioNet wEvent | The wireless cardiac event monitor collects asymptomatic and symptomatic events to detect heart arrhythmias. These data are automatically transmitted wirelessly through a cellular network to the physician. (BioTel, 2018) |
| Fitbit       | Fitbit provides a wearable watch to measure heart activity, sleep patterns, and more. The data sets are transmitted to a smart device with the Fitbit app. (Fitbit, 2018) |
| Dario        | The Dario All-in-One Smart Glucose Meter automatically tracks blood sugar with a tiny meter that plugs into a smart phone’s audio jack. Blood glucose readings are directly tracked, charted, and analyzed within the app. (Dario, 2018) |
| Welch Allyn  | The Welch Allyn Home Hypertension Program allows connectivity between the Welch Allyn Home Blood Pressure Monitor with the Blood Pressure App to send readings directly to doctors and stores to track results. (WelchAllyn, 2018) |
closures, and medication dosage values. Once the alarm is activated, the device can also dispense the medication. To remind patients, the device can send SMS messages or notifications through smart phone applications. The uploaded data can be used by the caregivers, Physicians, and other legitimate stakeholders for different purposes including monitoring medication adherence (Mondol, Emi, & Stankovic, 2016). For our classification, any voice activation tool such as Amazon Alexa or Google Home can be categorized as a medical adherence device because these tools can also provide medication reminders. Voice-activated devices have speech recognition and text-to-speech technologies for improved user experiences. Table 3 presents some wireless medical adherence tools. Some examples include intelligent personal assistants such as Amazon Alexa or E-pill medication dispensers. Figure 3 depicts a wireless structure for medical adherence tools.

2.4. IoMT device architecture
According to Gartner’s 2017 Hype Cycle for Real-Time Health System Technologies, medical device connectivity is at the plateau of productivity phase (Runyon & Pessin, 2017). Therefore,
approximately 20% of the technology's target audience has adopted or is adopting the technology. Medical devices are increasingly connected through wireless networks. Wireless radio frequency (RF) medical devices perform at least one function that utilizes wireless RF communications such as Wi-Fi, Bluetooth, and cellular/mobile phones to support healthcare delivery. Examples of functions that can utilize wireless technology include controlling and programming a medical device, monitoring patients remotely, and transferring patient data from the medical device to another platform such as a cell phone (FDA, 2018f). Figure 4 illustrates a potential IoMT device architecture with a wireless sensor network framework.
In the perception layer, the system aims to acquire, collect, and process the data from the physical environment. The system consists of two parts: the sensor device and the wireless sensor networks (Zhu, Wang, Chen, Liu, & Qin, 2010). In Phase 1 of Figure 4, each sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit, and a power unit (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). The transceiver unit is responsible for connecting the sensor node to the network. The goal is to connect the RFID reader to an RF transceiver that can forward information to and from the reader over distances of approximately 100 or 200 meters, depending on which RF transceiver that is used (Englund & Wallin, 2004). Various naming conventions such as Wireless Body Area Network (WBAN), Body Area Network (BAN), or Body Sensor Network (BSN) are used for the connectivity of body sensors. The nodes in a wireless sensor network need to communicate among themselves to transmit data in single or multi-hop sensor networks to a base station (Gubbi, Buyya, Marusic, & Palaniswami, 2013). A wireless sensor
network (WSN) generally consists of a base station (or “gateway”) that can communicate with a number of wireless sensors. Data are collected at the wireless sensor node, compressed, and transmitted to the gateway directly or if required, use other wireless sensor nodes to forward the information to the gateway. The transmitted data are then presented to the system via the gateway connection (Wilson, 2004).

In the transmission layer, the system transfers data over a large area or long distance, which is constructed based on the traditional mobile broadband communication network, Wi-Fi, and other communication technologies (Zhu et al., 2010). In Figure 4, all the arrows between the Phases represent the transmission layer because the data flow from each phase. Between Phases 1 and 2 is a Wireless Personal Area Network (WPAN) that allows electronic devices on and near the human body to exchange digital information through near-field electrostatic coupling (Zimmerman, 1996). Between Phases 2 and 3, data flow from the patient’s personal server to the medical server through a Wireless Wide Area Network (WWAN). WWAN is a cell phone’s high-power cellular radio network, used to access the Internet over the entire cell phone coverage area (Houser & Thornton, 2005). WWAN also transmits data from Phases 3 and 4, and Phases 4 and 1.

The application layer houses data processing and services (Zhu et al., 2010). In Figure 4, Phases 2, 3, and 4 are part of the application layer. The data from the transmission layer are handled by corresponding management systems, and then various services are provided to different kinds of users (Zhu et al., 2010). The core set of services in this layer might include event processing services, integration services, analytics services, user interface (UI) services, and security and management services (Choi, Li, Wang, & Ha, 2012). The devices on the personal and medical server such as phones, tablets, and laptops share information through a Wireless Local Area Network (WLAN) or the Internet. WLAN provides high bandwidth to users in a limited geographical area (Clarke, 1997). The cloud or server processes data about the connected devices, allowing end users to interact with the cloud through a mobile application. Users send requests to the cloud. The cloud then identifies the device and sends a corresponding request to the appropriate sensor network using gateways (Kimura & Latifi, 2005). The end user may include the physician, personal device assistant (PDA), caregiver, healthcare provider, or emergency services. In an IoMT structure, information can be sent from Phase 4 to Phase 1 and allow for feedback to the sensor system.

3. General wireless network attacks
The explosive growth in wireless networks over the last few years resembles the rapid growth of the Internet within the last decade (Arbaugh, Shankar, Wan, & Zhang, 2002). Wireless networks serve as the transport mechanism between and among devices and the traditional wired networks. Wireless networks are many and diverse but are frequently categorized into three groups based on their range of coverage: wireless wide area networks (WWAN), WLANs, and wireless personal area networks (WPAN) (Karygiannis & Owens, 2002).

The very idea of a wireless network introduces multiple venues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. Wireless networks only know the boundaries of their own signal: streets, parks, nearby buildings, and cars all offer a virtual “port” into any wireless network (Hassell, 2004). The Privacy Rights Clearinghouse recorded 913 hacking or malware attacks in 2015, 2016, and 2017 within the business, education, government, military, nonprofit, and healthcare industries (PRC, 2018). Table 4 provides a brief overview of wireless attacks in 2015, 2016, and 2017. The table does not include all the attacks but does show the various types of general wireless attack incidents.

3.1. Wireless medical device network attacks
Privacy Rights Clearinghouse reported 913 incidents of hacking or malware attacks in 2015, 2016, and 2017 within the business, education, government, military, nonprofit, and healthcare...
industries in the United States. The medical industry was the leading target, with about 418 reported hacking or malware attacks and nearly 285 records indicating a network attack (PRC, 2018). The use of wireless sensor networks (WSN) in healthcare applications is growing at a fast pace. Given that most of these devices and their applications are wireless in nature, there are major areas of concern in violation of data privacy for patients and medical personnel. The direct involvement of humans also increases the sensitivity (Al Ameen et al., 2012). Thankfully, there have been no recorded cases of injuries or deaths resulting from a cyber attack on devices interacting with the body. All demonstrations so far have been conducted for research purposes only. However, if somebody decides to use these methods for nefarious purposes, it might go undetected (Wadhwa, 2012). Table 5 is a review of the highlighted instances that demonstrate the vulnerability of medical devices to attacks.

Based on a review of vulnerabilities in current medical devices, it can be predicted that IoMT devices may incur similar types of security attacks. Due to the increased connectivity of IoMT devices, classification of attacks for wireless sensor devices can be adapted. A Survey of Attacks, Security mechanisms and Challenges in Wireless Sensor Networks provides general attacks within wireless sensor devices. We have adapted the general attacks with an IoMT lens to portray the substantial security problem facing IoMT devices (Padmavathi & Shanmugapriya, 2009).

1. Node outage

The IoMT device stops working and prevents the patient from using their smart insulin pump or pacemaker. This may result in death or physical injury to the patient.
Table 5. Six wireless medical device attacks from to portray the vulnerability of wireless medical devices

| Year | Device                          | Vulnerability                                                                 | Source                        |
|------|---------------------------------|-------------------------------------------------------------------------------|-------------------------------|
| 2008 | Wireless Pacemakers, Cardiac    | -Access to patients' medical information                                      | (Halperin et al., 2008; Thurston, 2008) |
|      | Defibrillators                  | -Turning off device                                                           |                               |
|      |                                 | -Delivering electric shock to patients                                        |                               |
| 2011 | Insulin Pump                    | -Releasing lethal dose of insulin without alerting patient                    | (Goodin, 2011; Wadhwa, 2012)  |
| 2013 | Wireless Pacemaker              | -Remote control of device                                                     | (Eastwood, 2014)             |
|      |                                 | -Disabling wireless functionality                                             |                               |
| 2014 | Bluetooth Enabled Defibrillators, Wireless Infusion Pumps, X-Rays, CT scans | -Remote control of devices                                                    | (Williams & Woodward, 2015; Zetter, 2014) |
|      |                                 | -Unencrypted and unauthenticated communication between devices                |                               |
|      |                                 | -Easy to access hand-coded passwords                                          |                               |
| 2015 | Infusion Pump                   | -Remote control of pump                                                       | (Finkle, 2015, 2016)         |
|      |                                 | -Releasing lethal dose of insulin without alerting patient                    |                               |
| 2017 | Cardiac Implants                | -Remote control of cardiac device                                             | (FDA, 2017a)                 |
|      |                                 | -Rapid battery depletion if accessed                                          |                               |
|      |                                 | -Releasing inappropriate pacing or shocks if accessed                         |                               |

2. Physical attacks

A hacker may physically install a pseudo sensor in the IoMT architecture and cause the hacker to receive health information. The hacker may physically alter the device to state false readings, resulting in the patient receiving heavier medication.

3. Message corruption

The criminal may alter sensor readings on the IoMT device data and send a virus with the data when sent to the physician.

4. False node

A hacker may cause patient one’s data to show in patient two’s readings and vice versa. False information would unknowingly cause inaccurate diagnosis to both patients.

5. Passive information gathering

As patient data is sent to the physician, the hacker would collect the data as an intermediary. He could store all patient data in a geographical area and sell that data to insurance companies.

6. Routing attacks

Routing attacks would affect the network layer of the IoMT device. The hacker could create an infinite loop between the various sensors in the IoMT network and the data would constantly overwrite itself.
7. Monitoring and eavesdropping

The hacker could use the wearable IoMT device to track the patient’s voice commands and listen on personal conversations. Those conversations could be recorded and used to blackmail the patient.

8. Traffic analysis

When a patient sends data from their IoMT device to their family or friends, the hacker could track the communication patterns and send additional messages to the recipients.

9. Denial of service

The patient’s insulin sensor may lock with a password encryption and prevent a patient from maintaining their blood sugar level. The hacker would provide the password only if the ransom is paid.

10. Node malfunction

The criminal may erase emergency phone numbers on an emergency response sensor and prevent patient’s from calling emergency services.

4. Examining IoMT device security through the situational crime-prevention lens

Situational crime prevention offers a theoretical perspective for organizing the dimensions, or indices, used in our analysis of security vulnerabilities and risks of victimization from cybercrime in public access Internet facilities. The theory differs from most other criminological theories in that it does not attempt to explain the motivation to commit a crime, but rather, tries to explain the conditions and circumstances that create the opportunity to commit a crime.

According to this theory, the likelihood that a crime will be committed depends on the manipulation of the conditions in the environment (Clarke, 1997). Preventing criminal activity becomes a function of changing the environment to increase the efforts and risks involved in committing a crime, reduce the rewards an offender hopes to reap from the crime, and make an attack difficult for criminals to justify their activities using common excuses. The situational crime-prevention approach has been used to guide preventative efforts in cyberspace surrounding e-commerce crime (Newman & Clarke, 2013), insider threats from employee computer crime (Siponen & Willison, 2009), identity theft (Copes & Vieraitis, 2009), and cyber stalking (Reyns, 2010). Furthermore, the situational crime-prevention approach has been used in context of protecting maritime attacks (Bruinsma & Johnson, 2018; Bryant, Townsley, & Leclerc, 2014; Shane, Piza, & Mandalà, 2015; Townsley, Leclerc, & Tatham, 2015). These studies focus on the prevention of maritime piracy by developing strategies for guardians and ship protection methods. Shane, Piza & Mandalà evaluate the effectiveness of situational crime-prevention techniques in piracy attacks across the globe.

Work done in the United States has enhanced the development of the situational crime-prevention theory. Hindelang, Gottfredson, and Garofalo (1978) used data on patterns of crime to develop a theory of personal victimization. Their lifestyle/exposure theory postulates that the lifestyle and routine activities of people place them in social settings with higher or lower risks of being victimized. For example, people who spend a great deal of time in public places at night have a greater risk of being robbed than do people who spend most of their evenings at home. A major implication of the lifestyle/exposure theory is that people’s risk of being victimized can be reduced by altering their patterns of activity.

Cohen and Felson (1979) broadened the lifestyle/exposure theory into the routine activities approach. This theory, which examines the circumstances around incidents of crime recorded by
the Privacy Rights Clearinghouse, rather than the characteristics of the offenders, posits that three elements are needed for a crime to occur: a motivated offender, a suitable target, and the absence of an effective guardian against some violation. Routine activities are events that we engage in on a daily basis, which could include work, school, leisure activities, or social interactions. Cohen and Felson (1979) point out that routine activities can occur within the home, at work, or in other places outside the home. Since the end of World War II, there has been a trend toward an increase in activities that occur outside the home. With this increase, people have become more vulnerable to victimization unless a capable guardian is present.

The routine activities theory has been a useful theoretical lens in our understanding of how technological shifts affect a wide variety of criminal offenses (Bossler & Holt, 2009). The three necessary elements posited by the theory are present in cyber crime. First, as already discussed, there are millions of incidents of cyber crime. Second, suitable targets are in no short supply, with 78% of adult Americans and 93% of teens using the Internet (Madden, Lenhart, Duggan, Cortesi, & Gasser, 2013). In this landscape, individuals may unknowingly provide their information to someone engaged in a scam. Third, we trust the public environments we are in and expect the authorities to be capable guardians, safeguarding our information. The situational crime framework provides tools that these guardians can use in cyberspace to protect us.

In the following section, we provide an application of the situational crime framework with the context of IoMT devices. To conceptualize the role of the situational crime-prevention theory, a brief case study on medical device protection follows. Currently, there is no literature regarding medical devices and the situational crime-prevention theory therefore, the case study provides a brief connection between a current protection method and situational crime prevention.

4.1. Crime-prevention strategies
Cornish and Clarke (2003) proposed five methods that guardians could use to protect potential victims from crime: increase the effort, increase the risks, reduce the rewards, reduce provocations, and remove excuses.

Each of the five approaches for reducing opportunities for crime can be operationalized through a series of security techniques that aim to inhibit criminal activity. Table 6 lists the five major approaches for reducing opportunities for crime and the corresponding techniques for doing so. Before describing the twenty-five techniques and presenting examples of each, it should be noted that there is some unavoidable overlap among the categories (Cornish & Clarke, 2003). All twenty-five techniques can be used to reduce opportunities for both in-home and hospital IoMT device attacks.

| Increasing Perceived Effort | Increasing Perceived Risks | Reducing the Reward | Reduce Provocations | Removing Excuses |
|-----------------------------|---------------------------|---------------------|---------------------|------------------|
| Target hardening            | Extend Guardianship       | Conceal Targets     | Reduce Frustrations and Stress | Set Rules       |
| Control Access to facilities| Assist Natural Surveillance| Remove Targets     | Avoid Disputes       | Post Instructions|
| Screen Exits                | Reduce Anonymity          | Identify Property   | Reduce Emotional Arousal | Alert Conscience|
| Deflect Offenders            | Utilize Place Managers     | Disrupt Markets     | Neutralize Peer Pressure | Assist Compliance|
| Control Tools/ Weapons       | Strengthen Formal Surveillance| Deny Benefits     | Discourage Imitation   | Control Drugs and Alcohol |
4.1.1. Increasing perceived effort

Increasing perceived effort includes strategies designed to make the cyber-attack more difficult to carry out. Five strategies that can increase perceived effort include target hardening, control access to facilities, screen exits, deflect offenders, and control tools/weapons.

For IoMT, target hardening refers to creating physical barriers between the attacker and the medical device. For example, the device may lock after a certain radius and therefore prevent the attacker from removing it from the patient’s home or hospital. Furthermore, if each device is made from a specific material that cannot be deconstructed, it can prevent attackers from extracting the memory chip from the device.

Access control refers to preventing potential offenders from entering the medical device. Frequent password changes and multifactor authentication to access the medical device at the patient’s home or hospital will reduce unauthorized personnel from accessing patient data. Since patient data is private information regarding the patient’s health, the data should have view-only permissions.

Screening exits allows regulators to detect objects that should not be removed from the protected area (Clarke, 1997). A regulatory body, either the device manufacturer or healthcare provider, could perform daily checks on irregularities in device usage or location. In hospitals, a designated security personnel should check whether all medical devices are in the correct location and are locked when not in use. When deregistering the device, all authorized personnel should be erased from the device’s memory, and the regulatory body could cross-reference the initial authorized personnel for the device.

By using the deflecting offender’s strategy, cyber criminals will be dissuaded from trying to hack medical devices. If the data sent from the medical device are encrypted and encoded through multiple data security layers, the hacker will be less likely to be able to translate the data at each of the transfers. Doing so will require more equipment and software for the hacker and deter them from pursuing the device further. In addition, routine checks by the authorities will reduce the likelihood of a device attack because it will increase the fear of being caught.

By controlling tools and weapons, the hacker will have limited opportunities for attacking the IoMT device. Restricting the sale of radio frequency devices to juveniles will limit the hacker’s ability to decode device signals. If IoMT devices are tracked by device manufacturers or healthcare providers, the hacker will not be able to use one IoMT device to hack into other IoMT device in the network. Table 7 outlines strategies for increasing the perceived effort of hacking a medical device through an IoMT lens.

4.1.2. Increasing perceived risk

Increasing perceived risk involves strategies that make the hacker assume the risk is greater than the benefit. The five strategies that increase perceived risk include extend guardianship, assist natural surveillance, reduce anonymity, utilize place managers, and strengthen formal surveillance.

The extend guardianship strategy involves taking routine protection measures to reduce the opportunity for crime (Clarke & Eck, 2005). For IoMT devices, home users should store their medical device in a secure safe after usage. In medical facilities, IoMT devices that are not in use should be stored in secure rooms and designated personnel should verify that all devices are in the correct location.

Assisting natural surveillance would include making it simpler to report suspicious activity by friends and family, the community, and medical personnel of IoMT device users. Creating a specific report number and report email would create a quick method to report unusual activity.
means, such as improving lighting in hospitals, would make it clearer to spot medical device activity. To incentivize medical personnel or anyone to report any irregular usage or data loads, rewards and incentives could be offered. Although tangible rewards such as monetary awards, recognition awards, or physical goods are possible, they are not compulsory. Encouragement of surveillance by patient visitors and community would instill a guardianship aspect to report suspicious activity. Intangible incentives such as recognition and praise may also be considered.

The patient should have permission to grant viewable access to the IoMT device data to reduce anonymity of others. To reduce the possibility of an attack, the patient should be permitted to allow only three users to access the data: the patient, the patient’s physician, and one additional family member or friend. If there are a certain number of users per device, it will be simpler to detect irregular activity and reduce the ability of the patient to provide access to unknown individuals.

In the context of IoMT devices, place managers would include medical personnel, and everyone employed in the hospital. Having two physicians analyze IoMT device data will allow physicians to verify the privacy of data. Once again, rewards or incentives may be offered, however they are optional. Giving medical personnel the power to report suspicious activity would instill a sense of guardianship and trust. IoMT device security training for all medical personnel and device users would provide power and establish a procedure of reporting suspicious activity.

Formal surveillance is provided by police, security guards, and store detectives, whose main function is to serve as a deterrent threat to potential offenders (Clarke, 1997). To protect medical devices from being hacked physically, home security and cameras should be installed in all in-home device locations. Furthermore, authorized security personnel should physically check in-home medical device usage monthly to ensure the device is being used for its intended purpose. Formal surveillance in hospitals can be increased by having security guards at all entrance points, requiring all hospital visitors to show federal or state ID before entering, and scanning each visitor’s bag Table 8 outlines strategies for increasing the perceived risk of hacking a medical device through an IoMT lens.

| Table 7. Strategies to increase perceived effort in carrying out a cyber attack for IoMT devices |
|-----------------------------------------------|
| **Target hardening**                          |
| - Require usage of medical device within certain radius of main house/hospital unless approved by physician |
| - Medical device locked beyond radius of main house/hospital |
| - Require all medical devices to be made with a certain material to prevent deconstruction of the medical device |
| **Control Access to Facilities**              |
| - Require changed passwords on medical devices every 15 days |
| - Require only medical personnel with IDs to access any hospital medical records and equipment |
| - Only authorized people with background checks, ID numbers, fingerprint authentication can access patient data |
| - No access to edit/update patient information (view-only permission at all times) |
| - Require fingerprint authentication and patient password before unlocking the medical device to collect or send patient data |
| **Screen Exits**                              |
| - Regulatory body and trained software performing daily checks on irregularities in device usage or location |
| - Designated security personnel checking if all medical devices are in the correct location and locked on premise |
| - Dereister all personnel with access to device at the end of the device usage |
| **Deflect Offenders**                         |
| - Regulatory body performing monthly checks on transfer of data from patient to medical personnel |
| - No access to edit/update patient information |
| - Ensure patient data are sent from in-home devices in raw numbers and later translated in hospital servers |
| **Control Tools/ Weapons**                    |
| - Restrict wireless/radio frequency decoding device sales to juveniles |
| - Use RFID tracking to track IoMT devices     |

Anandarajan & Malik, Cogent Medicine (2018), 5: 1513349
https://doi.org/10.1080/2331205X.2018.1513349
4.1.3. Reducing the reward

Reducing anticipated reward includes strategies to decrease the perceived reward for hacking into a medical device. These strategies include conceal targets, target removal, identifying property, disrupt markets, and denying benefits.

Conceal targets involves hiding IoMT devices to reduce temptation by hackers. Simple measures, such as storing IoMT devices in secure safes after usage and using devices in rooms with no windows would support this strategy.

Target removal may include the removal of the physical medical device or the storing of data away from the medical device. Sending data to the cloud and not storing patient data on the medical device itself would prevent hackers from trying to access the physical device and create more barriers to entry. Furthermore, the data would need to be encrypted from the initial sensing stage through transport to ensure a stronger barrier to entry. Removing data from the physical device may also include creating data security layers, each of which would be illegible without the key. Since data would be parsed into parts, the hacker would need to combine different data sources and dissect the encoded values to understand the metrics. As a result, more effort would be needed to understand and gather the patient’s data.

For IoMT, identifying property may include authenticating the device as belonging to the patient. Once the device is registered to the patient, the patient should be the only one to access and load data onto the device. For example, implanting a microchip in the device that can be opened only with the patient’s ID will help stop the hacker from opening or reselling the device.

Disrupting markets for IoMT devices may include limiting resale opportunities for hackers. This would include resale of data or the physical IoMT device. Currently, the FDA is the main regulating body over medical devices and radiation-emitting products (FDA, 2018a). As the number of IoMT devices increases, more federal regulatory bodies focused on illegal medical device resellers would be beneficial. Furthermore, online retailers or in-store retailers could deny any resale of medical devices because patient data may still be stored on the device.

| Table 8. Strategies to increase risk in carrying out a cyber attack for IoMT devices |
|-------------------------|---------------------------------------------------------------|
| Extend Guardianship     | - Keep IoMT devices in secure safes after home usage         |
|                        | - Lock IoMT devices in a secure room in the hospital         |
|                        | - Designate one security personnel to check if IoMT devices are stored safely everyday |
| Assist Natural Surveillance | - Designate a report phone number and report email for medical device misuse |
|                        | - Improve lighting in hospitals                              |
|                        | - Encourage patient’s family/friends to check device usage and data loads |
|                        | - Reward reports by the patient’s family/friends to through monetary or other means |
| Reduce Anonymity        | - Register all medical devices to one user; each user can only allow three additional users to access the data |
|                        | - Include microchip in IoMT device with patient identification that can only be opened by patient’s ID |
|                        | - Add medical authentication seal with ID on all medical devices |
| Utilize Place Managers  | - Encourage medical personnel to check device usage and data loads |
|                        | - Have two physicians analyze IoMT device data                |
|                        | - Reward reports by medical personnel through monetary or other means |
|                        | - Require IoMT device security training for all medical personnel and device users |
| Strengthen Formal Surveillance | - Increase home security cameras and alarms for in-home medical devices |
|                        | - Increase hospital security cameras and alarms for hospital medical devices |
|                        | - Require authorized security personnel to check in-home medical devices monthly |
|                        | - Require all hospital visitors to show federal/state ID before entering |
|                        | - Scanning of all bags entering hospital                      |

Anandarajan & Malik, Cogent Medicine (2018), 5: 1513349
https://doi.org/10.1080/2331205X.2018.1513349
Denying benefits includes impeding the resale of the medical device. Increasing the difficulty of reselling the physical device would lessen the benefit of stealing it because it would worthless in the market. Table 9 outlines strategies for reducing anticipated rewards through an IoMT lens.

4.1.4. Reduce provocations
Reducing provocations was added to the original 16-technique model for the situational crime-prevention theory. According to Wortley, the situational prevention theory focused too heavily on opportunities crime and did not consider situations that encourage crime (Clarke & Eck, 2005). Reducing provocations involves making the IoMT device simpler to use for patients. Although this seems counter intuitive towards preventing cyber attacks, creating a simpler device will encourage patients to safely store their device and promote safely discharging the device. Reducing provocations can be accomplished through reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralizing peer pressure, and discouraging imitation (Cornish & Clarke, 2003).

Reducing frustration and stress for patients using IoMT devices will promote well upkeep of the device. If a patient were to become frustrated with the device's performance, they may be tempted to dispose of it through resale or discarding it. Therefore, ensuring polite service for IoMT device technical support will help patients learn about how the device works. For similar reasons, it may be useful for training for physicians to ensure they can answer basic questions by patients.

Reducing disputes between patients and physicians regards to the device would reduce the temptation of hackers to attack the IoMT device. If the device is controlled by hospitals or vendors, the patient can stay at peace knowing they are responsible for technical support and deregistering the device. To prevent resale of the device, all IoMT devices should be returned to the medical facility if the device is defected. The medical facility should be responsible for contacting vendors and ensuring quality of the device.

According to Wortley’s critique of the situational crime-prevention theory, crime is provoked during an adverse emotional arousal. These emotional arousals can result from frustration, crowding, invasion of privacy, or environmental irritants (Cornish & Clarke, 2003). For IoMT devices, creating a simpler IoMT device would reduce frustration with the equipment and decrease the likelihood of the patient to lessen their protection measures. For example, if the password change for an IoMT device required extensive password constraints, the patient may get frustrated with the frequent changes and password character limitations. Thus, they may place temporary physical barriers around the IoMT device and leave the medical device unlocked. Leaving the device unlocked would increase temptation for cybercriminals to hack the device. Reducing emotional arousal would require IoMT device manufacturers to learn more about their device’s usability through customer surveys.

| Table 9. Strategies to reduce rewards in carrying out a cyber attack for IoMT devices |
|-----------------------------------|-------------------------------------------------|
| Conceal Targets                   | Store IoMT devices in secure safes at home      |
|                                  | Use IoMT devices in rooms with no windows       |
| Remove Targets                   | Reduce number of in-home medical devices        |
|                                  | Data storage all sent to cloud                  |
| Identifying Property             | Register all medical devices to one user        |
|                                  | Include microchip with patient identification that can only be opened by patient’s ID |
|                                  | Add medical authentication seal with ID on all medical devices |
| Disrupt Markets                  | Increase Federal regulating bodies on medical devices |
|                                  | Deny resale of medical devices on any online or in-store retailer |
| Denying Benefits                 | Deny any resale of medical devices              |
|                                  | Deny reuse of medical devices                   |

Anandarajan & Malik, *Cogent Medicine* (2018), 5: 1513349
https://doi.org/10.1080/2331205X.2018.1513349
Patients’ may be subject to peer pressure if others request to use their IoMT device. Regular campaigns about “saying no” to medical device misuse would encourage safe IoMT device usage. The campaigns could be distributed through newsletters or mail.

If a hacker attacks an IoMT device, it should be quickly dealt with to ensure there are no “copycat” crimes (Clarke & Eck, 2005). Rapid discharge of IoMT devices would prevent other hackers to target the device. Table 10 outlines strategies for reducing provocations through an IoMT lens.

4.1.5. Remove excuses
Removing excuses involves utilizing techniques to prevent the hacker from misunderstanding the regulations governing the use of medical devices. Removing excuses can be accomplished through setting rules, posting instructions, alerting conscience, assisting compliance, controlling drugs and alcohol.

Rule setting involves establishing fixed procedures and frameworks for hackers. For IoMT, new federal legal procedures could be devised specifically for device hackers. Furthermore, new legally binding agreements could be made between the patient, physician, and anyone with access to the patient’s data to ensure that the three parties agree to keep all information private. (Wellington, 2013) concludes that the current legal structure is insufficient in preventing cyber-attacks in medical devices.

Post instruction involves creating physical signs or contracts to promote behavior. On page 98 of the U.S. Department of Justice’s report by Clarke and Eck, it states despite post instructions wide use, there have been few evaluations of the preventive effectiveness of posted instructions, but they are an essential tool of law enforcement and are often used in problem-solving efforts (Clarke & Eck, 2005). A series of campaign slogans are listed in Table 11 that may assist patient’s using IoMT devices for its intended purpose.

Stimulating conscience regarding medical devices can occur at hospitals and in the community. Display boards within the hospital about the privacy of patient data and the repercussions of hacking can highlight the importance of the issue. In Crowe & Fennelly’s book Crime Prevention Through Environmental Design, it states that the visual sense is the most comprehensive means of collecting information about the environment. It has been estimated that about 90 percent of our information about the external world comes as a result of visual perceptions (Crowe & Fennelly, 2013). A visitor in the hospital may recognize a new visual display when they walk in to see a patient. It is necessary to use light and color components to ensure the image rises to a high level of consciousness because unless there is something significant about the image, the image will remain in the subconscious (Crowe & Fennelly, 2013). Penetration testing with short quizzes for visitors would access the effectiveness of the visual campaigns. Increased awareness of the FDA

Table 10. Strategies to reduce provocations by the hacker after carrying out a cyber attack for IoMT devices

| Reduce Frustrations and Stress | -Ensure polite service for IoMT device technical support  
-Ensure medical personnel are trained about basic functions of the IoMT device |
|--------------------------------|------------------------------------------------------------------------|
| Avoid Disputes                 | -Controlling of devices by hospitals or vendors  
-All IoMT Devices should be returned to the medical facility |
| Reduce Emotional Arousal       | -Guide IoMT device manufacturers to creating simple-to-use devices |
| Neutralize Peer Pressure       | -“Say no to medical device reuse” campaign  
-“It’s YOUR medical device, it’s okay not to share” campaign |
| Discourage Imitation           | -Rapid discharge of IoMT devices  
-Safe discarding of medical devices in hospitals |
regulation of medical devices will provide the community with information about who is responsible for the safety of all medical devices and make it simpler to report an issue. For IoMT devices, cyber criminals may be lightly influenced by alerting conscience techniques due to the severity of the crime (Clarke, 2004). Hacking IoMT device data may cause physical injury or death to the patient and posting instructions may not be seen by cyber criminals. However, we suggest some campaign slogans that would support the safety of IoMT devices.

Assisting compliance for IoMT devices would include making it simpler to report suspicious activity with a report number and report email. To prevent resale of the device, the IoMT device should be returned to the medical facility. Also, by involving hospital personnel in the process of ensuring medical device safety, it may make them more inclined to report irregular activity and share with colleagues.

Drugs and alcohol impair judgment and offenders may become unaware of their actions. For IoMT device usage at home, it may be useful to regulate the amount of alcohol consumption in the home to prevent device misuse. Table 11 outlines strategies for removing excuses through an IoMT lens.

| Table 11. Strategies to remove excuses by the hacker after carrying out a cyber attack for IoMT devices |
|-------------------------------------------------|--------------------------------------------------|-------------------------------------------------|
| Set Rules                                      | Post Instructions                                | Alert Conscience                                |
| -Specific correction procedure for device hackers | -“Keep medical devices locked”                    | -Increase awareness on Medical Device security |
| -Medical device agreements between patient, hospital, and physician | -“Don’t compromise your health”                     | -Increase awareness on FDA regulations and policy on medical devices |
| -Medical device registration/deregistration before/after use | -“See something, say something”                    | -Display boards in hospitals with patient data regulations and repercussions |
| -Medical device codes and policy shared with anyone with access to patient data | | -Monthly mail to anyone with access to patient data about regulatory policies |

Class I devices are subject only to general controls. They typically present the lowest potential for harm and are simpler in design than Class II or Class III devices. Examples of Class I devices include elastic bandages, examination gloves, and hand-held surgical instruments. Class II devices are those for which general controls alone are insufficient to provide a reasonable assurance of safety and effectiveness. In addition to complying with general controls, Class II devices are also subject to special controls identified by the agency, which may include special labeling requirements, performance standards and post market surveillance. Examples of Class II devices include powered wheelchairs, infusion pumps, and surgical drapes. Class III devices

4.2. Case study with medical device attack and situational crime-prevention theory

The Center for Devices and Radiological Health (CDRH) is part of the Federal Food and Drug Administration responsible for regulating medical devices. According to the Section 201 (h) of the Food, Drug and Cosmetic Act, a medical device is any healthcare product that does not achieve its principal intended purposes by chemical action or by being metabolized (FDA, 2018c). The FDA classifies all medical devices into three distinct classes based on potential risk to the patient. Based on the classification, the FDA has established a series of protocols before the device is secure for use.

Class I devices are subject only to general controls. They typically present the lowest potential for harm and are simpler in design than Class II or Class III devices. Examples of Class I devices include elastic bandages, examination gloves, and hand-held surgical instruments. Class II devices are those for which general controls alone are insufficient to provide a reasonable assurance of safety and effectiveness. In addition to complying with general controls, Class II devices are also subject to special controls identified by the agency, which may include special labeling requirements, performance standards and post market surveillance. Examples of Class II devices include powered wheelchairs, infusion pumps, and surgical drapes. Class III devices
generally are those for which insufficient information exists to determine that general or special controls are enough to provide a reasonable assurance of safety and effectiveness. Examples of Class III devices include replacement heart valves, silicone gel-filled breast implants, and implanted cerebellar stimulators (FDA, 2006). After the classification, Class I devices require FDA Product registration. Class II requires Pre-Market Notification, 510(k) or De Novo, and Class III requires Pre-Market Approval (PMA) or Humanitarian Device Exemption (HDE). As the risk increases, the class increases and there are more steps within the approval process.

The 510(k) process demonstrates how the proposed device is similar to one or more similar legally marketed devices. Support claims are made to the predicate until the device is determined SE (substantially equivalent) by the FDA. If the device is not determined SE, the device is classified NSE (not substantially equivalent) (FDA, 2018e). When the device is classified NSE, it is placed in Class III and can undergo the De Novo process. The De Novo process requires additional demonstrations and meetings with the FDA to propose Class 1 or Class II classification (FDA, 2018b). De Novo requires additional time commitment than the 501(k). Pre-Market Approval is the most stringent type of device marketing application required by the FDA. The PMA requires clinical data and trials with additional scientific evidence. The PMA also requires additional safety and effectiveness review (FDA, 2018d). Humanitarian Use Device (HUD) cannot be sold for profit without a HDE marketing application. And HDE includes a full description of the HUD, supporting technical information, quality systems, and other information (FDA, 2017b).

Class III devices are categorized with the highest level of safety. Implantable pacemakers and about 10% of medical devices fall into Class III devices (FDA, 2017c). One of the medical device attacks mentioned in Table 5 includes Halperin et al.’s study, which found security vulnerabilities in implantable pacemakers and implantable cardiac defibrillators (ICD). An ICD detects abnormal heart rhythms and delivers electric shocks to restore the patient’s heartbeat. The group reverse engineered an ICD’s wireless communications and eavesdropped on the incoming signals. Through two hardware tools, they were able to intercept the radio frequency signals emitted by the ICD and decode the signal (Halperin et al., 2008). Furthermore, the group was successful in implementing a series of replay attacks in which a cybercriminal eavesdrops on a secure network communication, intercept it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants (Lab, 2018). Halperin et al. were able to trigger ICD identification, disclose patient data, disclose cardiac data, change patient name, set the time stamp on sensor readings, change responses to cardiac events, induce fibrillation, and deny service on the ICD. Overall, the study portrayed the susceptibility of ICDs and how the hacker could violate the privacy of patient data.

After evaluating the vulnerability with ICDs, we can consider how the situational crime-prevention theory would make an attack on ICDs more difficult. Specifically, the first category, increase the effort would make the attack less likely to carry out. The authors suggest a number of protection methods including building the ICD with custom equipment with commercial programmers, creating a security measure that does not draw power from the device, and allowing security-sensitive events to be effortlessly detectable by patients (Halperin et al., 2008). These solutions would fit with target hardening technique by increasing the effort (Cornish & Clarke, 2003). Target hardening makes the crime more difficult to carry out and increases the probability of catching the hacker (Clarke & Eck, 2005). Also, the deflecting offenders technique is shown when the authors suggest they were successful because private data transmitted between ICD and programmer was not encrypted (Halperin et al., 2008). If the data had been encrypted, hackers would be less likely to extract data from the device. Deflecting offenders away from the device is an environmental change that decreases the chance of the crime.

Sametinger, Rozenblit, Lysecky, and Ott (2015) provide additional security challenges for Class III pacemakers. Specifically, the sensitive data about the patient and their pacemaker may be disclosed, data on the device may be altered, and the device may become inoperable (Sametinger et al., 2015). The author suggests the need for more information about how concerned patients are about the
security of the medical device and using different methodologies to increase security awareness of all stakeholders (Sametinger et al., 2015). This suggestion most closely follows Clarke’s remove excuses category because these techniques recognize that offenders make moral judgments about their behavior and how they rationalize their behavior (Clarke & Eck, 2005). Thomson and Von Solms (1998) highlight the critical role for an effective information security awareness and training program in order to create a safe environment. Furthermore, Sametinger et al. suggests that the devices’ security states must be more visible, understandable, and accessible for all stakeholders. This suggestion falls in line with Clarke’s technique about set rules and alerting conscience (Clarke & Eck, 2005).

This case study is provided merely to showcase how the situational crime theory could be applied to a specific medical device, pacemaker, with existing regulations and vulnerabilities.

5. Discussion and limitations
As the number of IoT devices grows, it is imperative to consider the security vulnerabilities in connected devices. In addition, the value of the information on these devices is also growing significantly. Some vulnerabilities include access to a patient’s medical information, releasing lethal doses of insulin without patient consent, and remote control of the device. We are at the precise moment in time when we need to consider installing control mechanisms for IoMT devices. These mechanisms fall into three categories: technological, management, and physical controls.

Technological control mechanisms involve a central IT team responsible for protecting medical devices. Frequent password changes and fingerprint authentication require medical devices to install additional software. Daily checks on irregularities in the use of the device would involve installing anti-spyware and antivirus software. ID number creation and access control of the medical devices would also require supervision by a central IT team. Technological control mechanisms would increase the perceived effort and risk and reduce the anticipated reward for cybercriminals.

Management controls involve the coordination between physicians and medical device users. Standard procedures that help ensure compliance with the use of the device will remove cybercriminals’ excuses. Medical device agreements between patients, healthcare facilities, and physicians will ensure that each stakeholder understands the intended purpose of the device. Creating simple procedures to report suspicious activity will allow management teams to quickly determine when and how the medical device is being misused. Management teams will need to be trained to regulate suspicious activities. If current policies do not cover all aspects of medical device safety, regulators will need to develop standardized procedures for medical device usage.

Physical controls will alert medical personnel and patients in healthcare facilities. Increasing awareness in healthcare facilities is crucial and can be accomplished by adding posters in hospitals about device safety or FDA regulations. For in-home medical devices, physical controls such as locking the device beyond a certain distance will prevent the cybercriminal from removing the physical medical device from the patient’s home.

Although implementing and controlling all twenty-five techniques may be difficult, the proposed mechanisms can influence reducing potential threats. This study provides a theoretical perspective on securing IoMT devices. Future work should determine experimentally whether the proposed mechanisms result in reducing IoMT device threats.

The study has several limitations that offer opportunities for future research. First, it is limited to medical devices prevalent in the American healthcare system. Future studies could examine international standards and devices. Second, given that thankfully no deaths have occurred due to attacks on medical devices, we use theory to predict potential attacks to and with IoMT devices. Future research in this area should attempt to expand the scope of the studies of medical devices.
used outside the United States and examine incidents of medical device attacks. Third, it will be useful to consider security ratings with IoMT devices, which would disclose the tradeoff between price, ease of use, and security. Although rating scales have not been created for IoMT devices, it will be a compulsory component as more consumers purchase IoMT devices.

Nevertheless, despite these limitations, our overall security recommendations, although not perfect and limited to the items used in the study, are useful and practical methods for safeguarding the security of IoMT devices.

Funding
The author received no direct funding for this research.

Competing interests
The authors declare no competing interests.

Author details
Murugan Anandarajan
E-mail: ma33@drexel.edu
Sarah Malik
E-mail: sm3658@drexel.edu
1 LeBow College of Business Drexel University, Philadelphia, PS, USA.

Citation information
Cite this article as: Protecting the Internet of medical things: A situational crime-prevention approach, Murugan Anandarajan & Sarah Malik, Cogent Medicine (2018), 5: 1513349.

References
Akylidiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8), 102–114. doi:10.1109/MCOM.2002.1024422
Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of Medical Systems, 36(1), 93–101. doi:10.1007/s10916-010-9449-4
Alert1. (2018). Alert1 medical alert devices. Retrieved from https://www.alert-1.com/system/overview/596
Amazon. (2018). Echo & alexa devices. Retrieved from https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011
Arbaugh, W. A., Shankar, N., Wan, Y. J., & Zhang, K. (2002). Your 80211 wireless network has no clothes. IEEE Wireless Communications, 9(6), 44–51. doi:10.1109/MWC.2002.1160080
Bauer, H., Patel, M., & Veira, J. (2014). The internet of things: sizing up the opportunity. Retrieved from: Mckinsey at https://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity.
BayAlarmMedical. (2018). GPS medical alert system. Retrieved from https://www.bayalarmmedical.com/m sprinkler-system/bradley/medical-alarm-system/bradley
BioTel. (2018). eWevent: Event monitoring. Retrieved from https://www.myheartmonitor.com/device/eevento
Bos, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400.
Bruinsma, G. J., & Johnson, S. D. (2018). The Oxford handbook of environmental Criminology. 198 Madison Avenue, New York, NY 10016, United States of America: Oxford University Press.
Bryant, W., Townsley, M., & Leclerc, B. (2014). Preventing maritime pirate attacks: A conjunctive analysis of the effectiveness of ship protection measures recommended by the international maritime organisation.

Journal of Transportation Security, 7(1), 69–82. doi:10.1080/15229198-013-0130-2
CCHPCA. (2018). Remote patient monitoring. Retrieved from http://www.cchpca.org/remote-patient-monitoring
Chappell, B., & Neuman, S. (2017). U.S. says North Korea ‘directly responsible’ for WannaCry ransomware attack. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacy-ransomware-attack
Choi, J., Li, S., Wang, X., & Ho, J. (2012). A general distributed consensus algorithm for wireless sensor networks. Paper presented at the Wireless Advanced (WiAd), 2012.
Clarke, R. V. (ed.). (1997). Situational crime prevention: Successful case studies (2nd ed.). Guilderland, NY: Harrow and Heston.
Clarke, R. V. (2004). [25 techniques of situational crime prevention].
Clarke, R. V., & Eck, J. E. (2005). Crime analysis for problem solvers in 60 small steps. Retrieved from http://www.popcenter.org/library/reading/PDFs/60steps.pdf
CMT. (2018). Medication management platform. Retrieved from https://cmtcares.com/solutions/
Cohen, L. E., & Felton, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608. doi:10.2307/2094589
Constantin, L. (2016). Hacker shows how easy it is to take over a city’s public Wi-Fi network. Retrieved from https://www.pcworld.com/article/609996/hacker-shows-how-easy-it-take-over-city-public-wi-fi-network/
Copes, H., & Vieraitis, L. M. (2009). Bound rationality of identity thieves: Using offender-based research to inform policy. Criminology & Public Policy, 8(2), 237–262. doi:10.1111/j.1745-9133.2009.00553.x
Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley’s critique of situational crime prevention. Crime Prevention Studies, 16, 41–96.
Crowe, T. D., & Fennelly, L. J. (2013). Crime prevention through environmental design (3rd ed.). Waltham, MA: Elsevier.
Dario. (2018). Dario blood glucose monitoring system. Retrieved from https://mydario.com/
Dexcom. (2018). Introducing the Dexcom G5® mobile CGM system. Retrieved from https://www.dexcom.com/com/g5-mobile-cgm
Dimitrov, D. V. (2018). Medical internet of things and big data in healthcare. Healthcare Informatics Research, 22(3), 156–163. doi:10.4258/hir.2016.22.3.156
DoesSmart. (2018). DoseSmart smart cap. Retrieved from https://www.mydosesmart.com/
Englund, C., & Wallin, H. (2004). RFID in wireless sensor network. In Citeseer. Göteborg, Sweden.
e-pill. (2018). e-pill medication reminders. Retrieved from https://www.epill.com/
FDA. (2006). Frequently asked questions about medical devices Retrieved from https://www.fda.gov/down
Cybersecurity vulnerabilities identified in St. Jude Medical’s implantable cardiac devices and Merlin@home transmitter: FDA safety communication. Retrieved from https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm55843.htm

FDA. (2017b). Getting a humanitarian use device to market. Retrieved from https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/HumanitarianDeviceExemption/ucm563286.htm

FDA. (2017c). Learn if a medical device has been cleared by FDA for marketing. Retrieved from https://www.fda.gov/MedicalDevices/ResourcesforYou/Consumers/ucm142523.htm

FDA. (2018a). Code of federal regulations (CFR). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=84.20

FDA. (2018b). Evaluation of automatic class III designation (De Novo). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.101

FDA. (2018c). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDA. (2018d). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDA. (2018e). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDA. (2018f). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDEH. (2018). FDA. (2017a). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDEH. (2017b). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

FDEH. (2018c). Premarket notification (510(k)). Retrieved from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfr/cfrsearch.cfm?fr=88.10

Filkins, B. (2014). Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon. Retrieved from https://sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

Finkle, J. (2015). UPDATE 1-FDA warns of security flaw in Hospira infusion pumps. Retrieved from https://www.reuters.com/article/hospira-fda-cybersecurity/update-1-fda-warns-of-security-flaw-in-hospira-infusion-pumps-idUSL1N1082MA20150531

Finkle, J. (2016). New rules for avoiding cyber bugs in medical devices. Retrieved from https://www.scientificamerican.com/article/new-rules-for-avoiding-cyberbugs-in-medical-devices/

Fitbit. (2018). Retrieved from https://www.fitbit.com/home

Gartner. (2013). Gartner says the internet of things installed base will grow to 26 billion units by 2020. Retrieved from https://www.gartner.com/newsroom/id/2936073

Goodin, D. (2011). Insulin pump hack delivers fatal dosage over air. Retrieved from https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

GoogleHome. (2018). Retrieved from https://store.google.com/product/google_home

Greenberg, A. (2018). Hackers remotely kill a jeep on the highway—With me in it. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Gubbi, J., Buyya, R., Marusic, S., & Polanisiwami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Halperin, D., Heyat-Benjamin, T. S., Ransford, B., Clark, S. S., Davidson, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.

Hashmi, M., Myung, D., Gaynor, M., & Moulton, S. (2005). A sensor-based, web service-enabled, emergency medical response system. Paper presented at the Proceedings of the 2005 workshop on End-to-end, sense-and-respond systems, applications and services.

Hassell, J. (2004). Wireless attacks and penetration testing (part 1 of 3). Retrieved from https://www.symantec.com/connect/articles/wireless-attacks-and-penetration-testing-part-1-3

Hindelang, M. J., Gottfriedson, M. R., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger.

Houser, C., & Thornton, P. (2003). Mobile educational technology. In M. Boyer, J. Conley, R. Davies, J. LeBlanc, & S. Ramelb (Eds.), Encyclopedia of Distance Learning (pp. 1289–1296). United States of America, United Kingdom: IGI Global.

Karygiannis, T., & Owens, L. (2002). Wireless network security. NIST Special Publication, 800, 48.

Khanna, A., & Misra, P. (2014). The internet of things for medical devices-prospects, challenges and the way forward. TCS White Papers.

Kimura, N., & Latifi, S. (2005). A survey on data compression in wireless sensor networks. Paper presented at the Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on.

Lab, K. (2018). What is a replay attack? Retrieved from https://www.kaspersky.co.in/resource-center/definitions/replay-attack

LifeAlert. (2016). Helping seniors live at home longer. Retrieved from http://www.lifealert.org/

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). Teens and technology. Retrieved from http://www.pewinternet.org/2013/03/13/teens-and-technology-2013/

Marr, B. (2018). Why the internet of medical things (iotm) will start to transform healthcare in 2018. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iotm-will-start-to-transform-healthcare-in-2018/#3ed660424a3c

Marriott, N. (2017). Why the internet of medical is the future of healthcare. Retrieved from https://www.nextive.com/press/why-the-internet-of-medical-things-is-the-future-of-healthcare

MedicalGuardian. (2018). Classic guardian. Retrieved from https://www.medicalguardian.com/products/classic-guardian

Medtronic. (2018a). MYCARELINK SMART™ U.S. Retrieved from http://www.medtronic.com/us-en/mobile/apps/patient-caregiver/mycarelink-smart-us.html

Medtronic. (2018b). Reveal LINQ ICM system. Retrieved from http://www.medtronic.com/us-en/healthcare-professionals/products/cardiac-rhythm/cardiac-monitors/reveal-linq-icm.html

Miracle-Ear. (2019). What can i do with bluetooth hearing aids? Retrieved from https://www.miracle-ear.com/hearing-aid/bluetooth-hearing-aids

Mondol, M. A. S., Emi, I. A., & Stankovic, J. A. (2016). MedRem: An interactive medication reminder and...
tracking system on wrist devices. Paper presented at the Wireless Health.

Newman, G. R., & Clarke, R. V. (2013). Superhighway robbery. London: Routledge.

Omnipod. (2018). Simple, nonstop insulin delivery for people with diabetes who insist life still comes first (pp. 1–42). Retrieved from https://www.myomnipod.com/sites/default/files/pdf/PatientResourceGuide.pdf#page=4

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

Pillsy. (2018). PillsyCap. Retrieved from https://pillsy.com/PRC. (2018). Data breaches. Retrieved from: https://www.privacyrights.org/data-breaches

QMedic. (2018). A smarter medical alert service. Retrieved from https://www.qmedichealth.com/

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety, 12(2), 99–118. doi:10.1057/cpcs.2009.22

Runyon, B., & Pessin, G. (2017, July 17). Hype cycle for real-time health system technologies, 2017. Retrieved from https://www.gartner.com/doc/3762663/hype-cycle-realtime-health-technologies

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74–82. doi:10.1145/2743559

Shane, J. M., Piza, E. L., & Mandala, M. (2015). Situational crime prevention and worldwide piracy: A cross-continent analysis. Crime Science, 4(1), 21. doi:10.1186/s40163-015-0032-7

Shen, G., & Liu, B. (2010). Research on application of internet of things in electronic commerce. Paper presented at the Electronic Commerce and Security (ISECS), 2010 Third International Symposium on. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267–270. doi:10.1016/j.im.2008.12.007

Storm, D. (2015). 2 more wireless baby monitors hacked: Hackers remotely spied on babies and parents. Retrieved from https://www.computerworld.com/article/2913356/cybercrime-hacking/2-more-wireless-baby-monitors-hacked-hackers-remotely-spedied-on-babies-and-parents.html

Symantec. (2017). Petya Ransomware outbreak: Here’s what you need to know. Retrieved from https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

Szary, W., & Auchard, E. (2015). Polish airline, hit by cyber attack, says all carriers are at risk. Retrieved from https://www.reuters.com/article/us-poland-lot-cybercrime/polish-airline-hit-by-cyber-attack-says-all-carriers-are-at-risk-idUKKBN0P21DC20150622

Tatham, M. (2018). Identity theft statistics. Retrieved from https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

Thangavel, P. (2015). Jot: security & privacy perspective. Hopkinton, Massachusetts: EMC Corporation.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. Information Management & Computer Security, 6(4), 167–173. doi:10.1108/0968529810227649

Thurston, R. (2008). Hacking attacks can turn off heart monitors. Retrieved from http://www.theregister.co.uk/2008/03/12/heart_monitor_hacking/

Townley, M., Leclerc, B., & Tatham, P. H. (2015). How super controllers prevent crimes: Learning from modern maritime piracy. British Journal of Criminology, 56(3), 537–557. doi:10.1093/bjc/azv071

Wadhwa, T. (2012). Yes, you can hack a pacemaker (and other medical devices too). Retrieved from https://www.forbes.com/sites/singularity2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/#641b1f5e6853

WelchAllyn. (2018). Home BP monitor. Retrieved from https://www.welchallyn.com/content/welchallyn/americas/en/products/categories/welch-allyn-home/connected-blood-pressure-monitors/home-bp-monitor.html

Wellington, K. (2013). Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions. Santa Clara High Technical LJ, 30, 139.

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices (Auckland, NZ), 8, 305.

Wilson, J. S. (2004). Sensor technology handbook. The United States of America: Elsevier.

Zetter, K. (2014). It’s insanely easy to hack hospital equipment. Retrieved from https://www.wired.com/2014/04/hospital-equipment-vulnerable/

Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010). Jot gateway: Bridging wireless sensor networks into internet of things. Paper presented at the Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on.

Zimmerman, T. G. (1996). Personal area networks: Nearfield intrabody communication. IBM Systems Journal, 35(3), 609–617. doi:10.1147/sj.353.0609
