# Halting Hackers: Safety Secured.

The world is evolving into a hyper-connected world, where what only a few years ago seemed like science fiction is becoming a reality thanks to IOT devices. These IOT devices range from refrigeration systems, automated manufacturing systems, medical systems and even coffee pots are connected.

## Introduction

Medical systems are becoming the largest front-runner in this world, with recent reports pointing to over 3.7 million medical devices are being used to monitor the health of patients all over the world, [1] and the number is growing. However, with the growing numbers of the IOT device market, inevitably the security risks that will affect these devices are also increasing.

> “*...the security risks that will affect these devices is also increasing.*”

While securing regular systems is a daunting task in a world where even the cyber-attacks are becoming automated, securing IOT systems compounds the difficulty exponentially due to the devices rarely having built-in or even third-party defenses such as anti-malware. With medical equipment being used to monitor vitals, 3d print heart valves and having robots to assist in surgery, the risk of not securing these devices has risen far above just the loss of PII or HIPPA violations.

An attacker gaining access to a patient's vitals with intent to manipulate the output is a scary thought. However, an attacker accessing the network, connected to a 3d printer, being used to print out a heart valve, and disabling the temperature safety features could potentially cause a fire within a lab which would be utterly terrifying.

## Past vulnerabilities within IoT devices

IoT devices have already seen their fair share of "newsworthy" attacks. However, these are merely the ones detected or at the very least reported.

### *The Mirai Botnet*

In 2016, the most massive DDOS attack ever was launched against the service provider, Dyn, using an IOT botnet. This attack crippled a large portion of the internet, including Twitter, the Guardian, Netflix, Reddit and CNN, proving that no one is truly immune to DDoS attacks. Attackers were able to control these IoT devices using a malware dubbed Mirai. The malware once present on a system continuously scanned the internet for vulnerable IoT devices, attempting the default usernames and passwords to log in to the devices. Such a wide variety of IoT devices were being used in the attack that it made it impossible for companies merely to patch or update the system.

### *Cardiac Devices at St. Jude*

In 2016, the FDA confirmed that St. Jude Medical's cardiac devices contained vulnerabilities that could allow an attacker to gain access to the device. [2] An attacker controlling these devices could either purposefully administer incorrect pacing or shocks. The implications of cardiac devices malfunctioning due to attacker intervention are staggering.

## Importance of IoT security within the medical field

While important for every IoT owner, the need for securing these devices within the medical field holds higher consequences for not doing so.

Healthcare breaches are on the rise and those breaches have resulted in the theft or exposure of at least 176,709,305 healthcare records. [3] The average settlement for these HIPAA violation cases: $500,000.00 USD.

Most IoT medical devices contain PII about the patient they are attached to at that moment. From "doomsday" scenarios of further injury to patients to attackers gaining control are both terrifying HIPAA violations that are a more realistic and more prevalent issue that faces the medical field concerning IoT devices.

## Securing the IoT

As with all systems, there are a few key ways to best guard your systems from attackers and IoT devices are no exception.

- Don't connect the IoT devices to your network unless necessary
- Create a separate network from your main network
- Change the default passwords of your IoT devices
- Ensure firmware upgrades are installed
- Keep personal devices separate from work IoT devices
- Track and assess all company-owned IoT devices

However, these steps are only the beginning, and with the need for a constant network connection for most IoT healthcare devices, these steps may not be appropriate for the needs of the business.

All is not lost though, as there is monitoring software out there that will secure and protect IoT devices from outside influences. While IoT security is a hot commodity at the moment, there are three major players in the IoT security game: Zingbox, CloudPost and Medigate. These are three of the early stage providers for IOT cyber security product providers which specialize in Healthcare.

With Secure Nation's team of skilled IT security experts and their background in IT management, information security, risk assessment, security policy audit and development, penetration testing, overall network design and project management, you're in good hands. We help you to build a stronger information security and technology program. We work to not only strengthen your compliance status; but, also heighten your overall security posture without increasing cost.

> *"All is not lost though, as there is monitoring software out there that will secure as well as protect IoT devices from outside influence."*

***References***

*[1] Internet of Things (IoT) Healthcare Market is Expected to Reach $136.8 Billion Worldwide, by 2021. https://www.marketwatch.com/press-release/internet-of-things-iot-healthcare-market-is-expected-to-reach-1368-billion-worldwide-by-2021-2016-04-12-8203318*

*[2] FDA Warns St. Jude Pacemakers Vulnerable to Hackers | Inc.com. https://www.inc.com/will-yakowicz/fda-warns-st-jude-pacemaker-vulnerable-to-hackers.html*

*[3] Sivilli, F. (2018, July 31). HIPAA Violation & Breach Fines | List of HIPAA Violations. Retrieved from https://compliancy-group.com/hipaa-fines-directory-year/*