The Internet of Things and Medical Devices: Challenges and the Road Ahead

www.securanceconsulting.com

INTRODUCTION

The COVID-19 pandemic shifted healthcare delivery to an unchartered, interconnected, and virtual model. As the Internet of Things (IoT) continues to develop, over 55 billion global devices are expected to be connected to the Internet by 2025, with adoption accelerating at a rapid pace.[2] Healthcare IoT technologies collect health-related data from computing devices, wearables and smart bands, mobile phones, implantable surgical devices, digital medications, and other portable devices.

This new healthcare delivery model comes with its own rewards and risks. The major concern over this kind of interconnectivity, or interoperability, is how a medical device's security vulnerabilities could be exploited by cyber criminals, impacting patient health and healthcare facilities' operations, and exposing protected health information (PHI). While the U.S. Food and Drug Administration (FDA) evaluates medical devices before commercial release for safety and cybersecurity guidance for manufacturers and healthcare entities, many challenges still exist for healthcare networks and their security postures.

This paper details risks associated with IoT medical devices, as well as what the healthcare industry stands to gain from properly, and securely, implementing these technologies.

> "Healthcare organizations are an inviting target for financially motivated threat actors because their broad attack surfaces make it relatively easy for cybercriminals to find vulnerabilities and monetize their exploits."[14]

Medical Device Threat Scenario

<table>
<tr><th>Exploit:</th><th colspan="3">Risk and Impact:</th></tr>
<tr><td rowspan="4">» Hacker Attacks
» Denial of Service Attacks
» Malware Infections
» Botnet Hijacks
» Errors in System Code</td><td>Patient Safety</td><td colspan="2">Data Breach</td></tr>
<tr><td>» Delay in treatment and care
» Threats to patients' health and safety</td><td colspan="2">» Loss or destruction of data, PHI, PII, settings, credentials, or configurations</td></tr>
<tr><td>Business Continuity</td><td>Revenue | Cost</td><td>Brand and Reputation</td></tr>
<tr><td>» Impact to service and care delivery
» Device availability
» Network performance</td><td>» Remediation cost
» Downtime impact on revenue
» Lawsuits
» Fines/penalties</td><td>» Loss of trust (patients, referring physician)
» Impact on staff and morale</td></tr>
</table>

The Internet of Things: Impacts on Healthcare Security and Privacy, Berkeley Research Group, 2016

SECURITY CONCERNS

In a 2022 post by the HIPAA Journal, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center revealed that 14 of 16 critical infrastructure sectors reported at least one ransomware attack between June and December 2021.[1] The healthcare and public health sector was the worst affected, accounting for 148 out of 649 attacks.[1]

IoT Medical Devices

As hospitals manage unexpected and widespread change due to the pandemic, malicious attacks directed at medical devices, in particular, continue to rise at a steady pace. Typically, the assault is two-fold. First, bad actors attack easily discoverable and outdated devices and use the compromised devices to get on a provider's network, where they can plant ransomware and steal data. Electronic medical records are a valuable target; worth at least 20 times more than credit card information, they fetch from $10 to $1,000 per record in online marketplaces. [17]

It's tempting to assume that medical technologies, such as insulin pumps, X-ray machines, and nurse call stations, are among the most secure IoT devices, because they are so critical to healthcare delivery and patient outcomes. But, experts warn that they are among the most vulnerable and far more insecure than PCs, servers, and other business hardware.

The security company ZingBox found that U.S. hospitals beds average between 10 and 15 connected devices each. A large hospital can have more than 5,000 beds, which means anywhere from 50,000 to 75,000 IoT devices. Every one of these devices, and the systems supporting it, is a target for hackers and malware— and the devices are rarely well-protected. For example, a survey by researchers in Britain and Belgium exposed security flaws in the communication protocols of third-generation implantable cardiac defibrillators.[8] More disturbing, a Trend Micro survey revealed more than 36,000 internet-enabled and potentially vulnerable devices could be scanned and found by an IoT search engine tool called Shodan. Sometimes referred to as "the world's deadliest search engine," Shodan is popular with hackers for its user-friendly interface, resembling a Google search, and its ability to access upwards of a billion records on a single server. [8]

> "Even if a network is running the latest operating system, hackers can repackage new malware as an archaic virus the system will ignore as non-threatening because it already has safeguards against it." [16]

These vulnerabilities occur often, as many connected medical devices were manufactured 5 to 15 years ago, with only basic levels of security built in. As a result, hackers can disguise new malware as an archaic virus the system will find non-threatening. Effectively, the virus will slip by any endpoint security software and embed itself in medical devices.[16] Even worse than outdated software are insecure user practices, such as installing rogue applications and visiting risk websites— which cause 71 percent of ransomware infections in medical devices.

By far, the biggest risks are to patient livelihood. There is overwhelming evidence that medical devices can not only be hacked, but also controlled by attackers remotely. Researchers from ZingBox hacked into insulin and IV pumps and changed drug dosages[8], and, in March 2020, Vedere Labs and CyberMDX discovered seven new vulnerabilities that could allow hackers to remotely alter system configurations, execute code, and access files.[10] Collectively named Access:7, these vulnerabilities affect medical imaging and laboratory devices and are a challenge to patch. The impacted component, which allows the manufacturer to perform remote maintenance, updates, and configuration changes, is shared across the supply chain. Bad actors can break into the device through this component, then use it to change appointments, tamper with lab results, exfiltrate data, or deny patient services. Unfortunately, the cybersecurity teams within healthcare organizations cannot install their own security tools on many medical devices, due to technical and manufacturing limitations.

Main Security Issues Associated with Networked Medical Devices

- Untested, unpatched, or defective software and firmware
- Theft or loss of networked medical devices (external or portable)
- User practice issues
- Lack of security standards
- Cybersecurity and privacy vulnerabilities
- Unauthorized device setting changes, reprogramming, or infection via malware
- Denial-of-service attacks
- Targeting mobile devices via wireless technology to access patient data, monitoring systems, and implanted medical devices

Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication, 2022

> The federal government recognizes the need to protect against cyber attacks targeting medical devices.

SECURITY STANDARDS FOR MEDICAL DEVICES

FDA Guidance

In 2016, the Food and Drug Administration (FDA) published its first draft of Cybersecurity in Medical Devices: Quality System Considerations and Content and Premarket Submissions. The most recent update, issued in April 2022, emphasizes the importance of ensuring medical device design safety, urges manufacturers to mitigate emerging cyber risks throughout the total product life cycle, and outlines more definitive recommendations for addressing cybersecurity concerns in premarket submissions.[6]

However, unlike other healthcare security regulations, such as HIPAA and HITECH, the guidelines remain lenient, with no fines or other penalties to enforce them. That said, they still represent a step in the right direction. For one

thing, buying hospitals may choose to purchase devices that meet the draft guidelines, with the goal of saving time and money when the administration publishes official standards in the future. Another benefit of these guidelines is their potential to influence legal action. If a manufacturer has access to best practices from the FDA and chooses not to implement them in their hardware, attorneys could paint this as negligence in a civil case, thus motivating manufacturers to raise their security standards.[11]

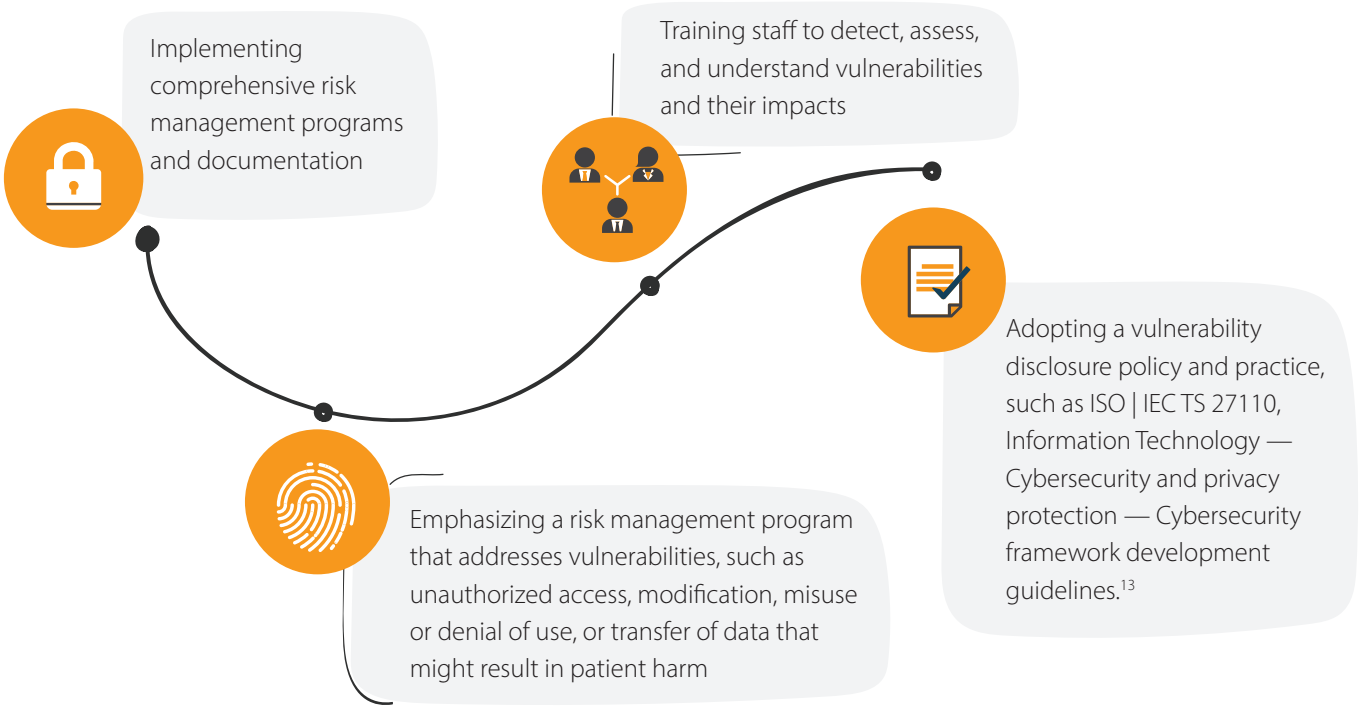
Guidelines for Manufacturers

Healthcare facilities, patients, providers, and medical device manufacturers have a shared responsibility when it comes to the cybersecurity of medical devices, as far as the FDA is concerned. However, the initial development and implementation of acceptable security protocols lies squarely with the manufacturer, whom the FDA suggests should apply the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover).[5] Providing a specific framework is important to garnering uniformity across the industry and is a reminder to manufacturers that when the framework is updated, their medical devices should be, as well.

The FDA also recommends a pre-market cybersecurity vulnerability and management approach, including the identification and assessment of:

- Assets, threats, and vulnerabilities
- Impact of threats and vulnerabilities on device functionality and end users | patients
- Likelihood of threat | vulnerability exploitation
- Risk levels and appropriate remediation strategies
- Residual risk and risk acceptance criteria

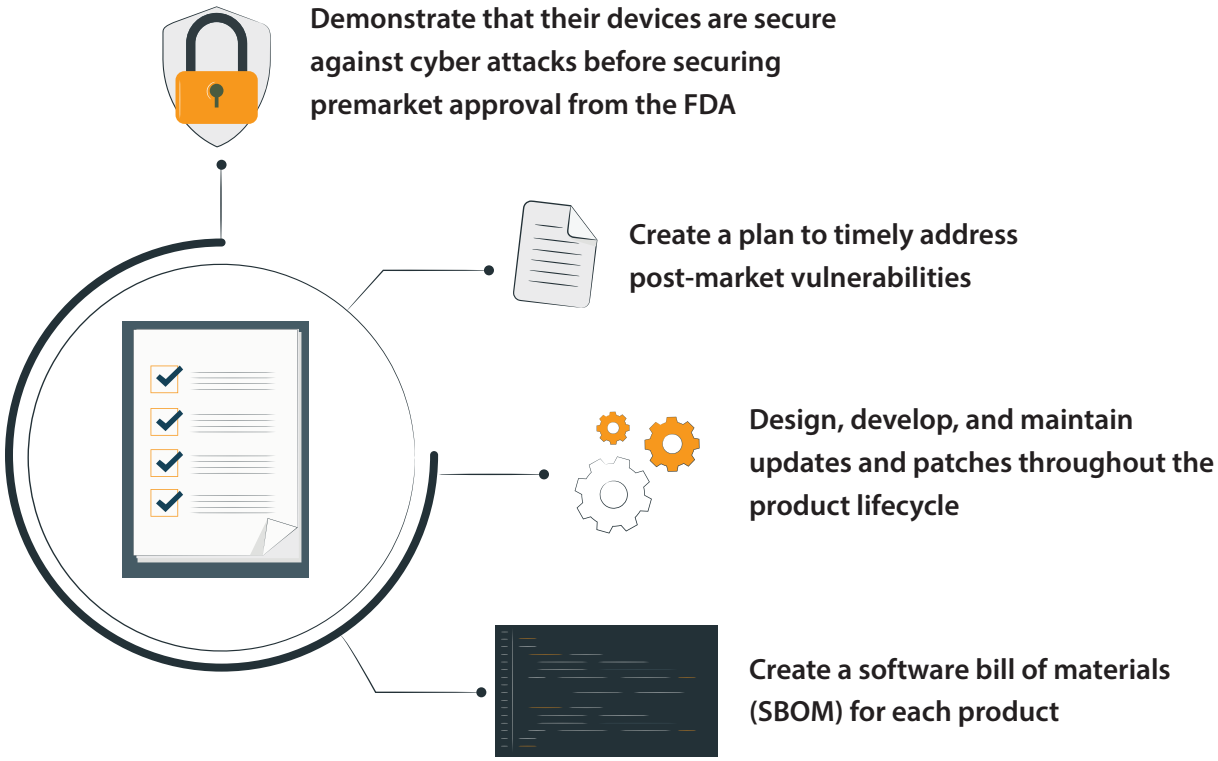
Important to note is that the FDA recognizes that cybersecurity risks are always evolving, and has therefore stated that manufacturers cannot rely on premarket controls to ensure the security of their medical devices indefinitely. Post-market considerations include:



With the FDA finally taking a stand on the issue of medical device security, more concrete guidelines are taking form in the U.S. House and Senate.

Introduction of the 2022 PATCH Act and Healthcare Cybersecurity Act

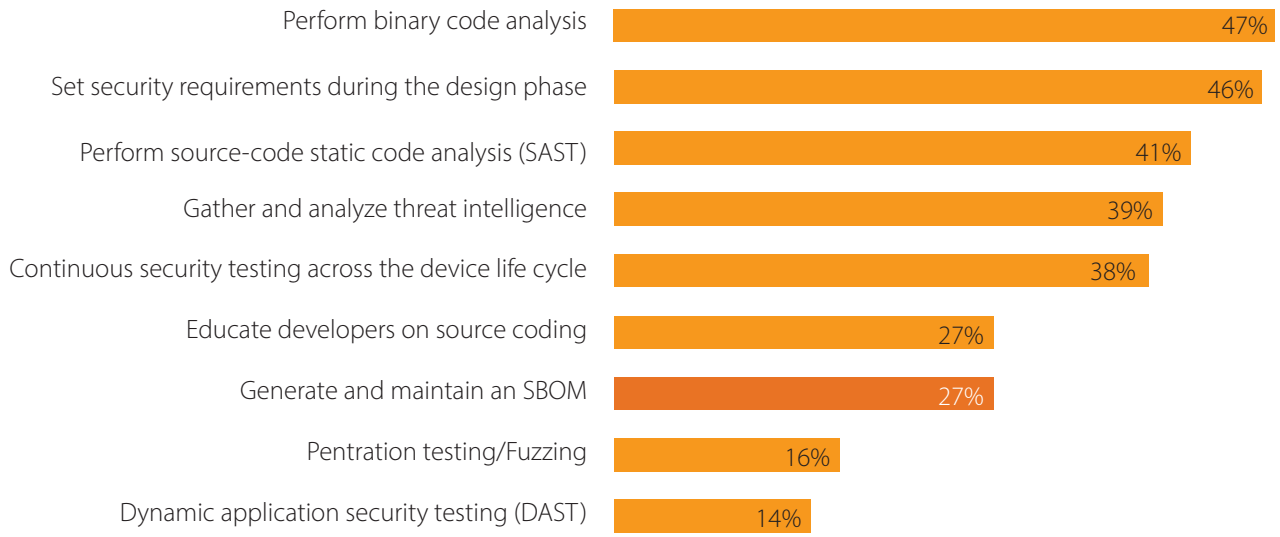
This year, the Protecting and Transforming Cyber Health Care (PATCH) Act was introduced, with the intention of ensuring medical device security at the premarket stage.[9] If passed, the PATCH Act would require manufacturers to:



SBOMs are especially critical to building security into a medical device. By tracking all of the software components within the device, they reveal hidden vulnerabilities and dependencies that could contribute to security risks. In fact, President Biden's 2021 Executive Order on Improving Cybersecurity called out SBOMs as an essential tool to securing the software supply chain and directed the National Telecommunications and Information Administration (NTIA) to publish minimum requirements for SBOMs.

But, until formal legislation is passed, manufacturers will likely be slow to adopt best practices. The cybersecurity platform developer, Cybellum, surveyed responses from 150 compliance and security decision makers in the medical device industry and found that just over one-fourth of medical device companies generate and maintain SBOMs.[4] Implementation of other security measures similarly lags behind federal and industry guidance. The most common methods of securing devices are binary code analysis and integration of security requirements into the design phase— but both are used by less than half of medical device companies.

Device Security Challenges of 2022



Medical Device Cybersecurity: Trends and Predictions, Survey Report, April 2022

Best Practices for Healthcare Facilities

Though many of the current guidelines apply to manufacturers, healthcare providers share the responsibility for securing their devices. The FDA recommends healthcare facilities regularly evaluate network security and implement mitigating controls to counteract vulnerabilities and threats. But, despite the FDA releasing guidelines and medical device security becoming a prevalent discussion in the medical community, the issue remains of comparably low concern to healthcare organizations' executives, who are focusing more on web and cloud security.

In a recent study, nearly two-thirds (64.8 percent) of the 50 C-level and other healthcare executives polled revealed that ransomware will be a major concern to their organizations over the next 12 months, but only a third of the corporate leaders have simulated an attack to prepare for such an incident.[12] The truth is, medical devices themselves are not advanced enough in their security measures to detect malicious attacks, so the data surrounding their level of risk to patient health is largely unknown. This makes it difficult for healthcare decision makers to prioritize medical device security in their cybersecurity action plans.

> In a recent study, nearly two-thirds (64.8 percent) of the 50 C-level and other healthcare executives polled revealed that ransomware will be a major concern to their organizations over the next 12 months, but only a third of the corporate leaders have simulated an attack to prepare for such an incident.[12]

FDA GUIDELINES FOR MANUFACTURERS' CYBERSECURITY PLANS

IDENTIFY

1. Maintaining Safety and Essential Performance

Manufacturers should define the safety and essential performance of their device(s), the severity of patient harm it could cause if compromised, and the risk acceptance criteria.

2. Identification of Cybersecurity Signals

Manufacturers are required to identify existing and potential causes of products that do not conform to normal standards or have other lapses in quality by analyzing complaints, returned products, service records, and all other data available to them.

PROTECT | DETECT

1. Vulnerability Characterization and Assessment

Manufacturers should characterize and assess identified vulnerabilities in order to triage remediation efforts.

2. Risk Analysis and Threat Modeling

The FDA recommends manufacturers perform routine cybersecurity risk analyses and threat modeling of their devices, with the goal of prioritizing vulnerabilities for efficient remediation.

3. Analysis of Threat Sources

Manufacturers should analyze possible threat sources, intents, and methods associated with the exploitation of vulnerabilities.

4. Incorporation of Threat Detection Capabilities

Manufacturers should consider implementing features to establish or improve the device's ability to detect attacks independently and sufficiently report suspicious or malicious events.

5. Impact Assessment on All Devices

Manufacturers should have a process for assessing the impact of a cybersecurity signal horizontally (across all medical devices) and vertically (if there is an impact on specific components of a device).

PROTECT | RESPOND | RECOVER

1. Compensating Controls Assessment

Manufacturers should implement device-based features, such as a primary mechanism to mitigate the risk of harm to patients, and compensating controls to further decrease the risk of patient harm.

RISK MITIGATION OF SAFETY AND ESSENTIAL PERFORMANCE

1. Risk to Patient Health

After implementing the preceding steps, manufacturers should determine if they have implemented effective controls in their medical devices to mitigate the risk of patient harm, and should evaluate residual risk, benefit | risk, and any risk introduced by remediation activities.

CONCLUSION

What the Future Holds

Despite the hurdles medical devices and IoT present, the healthcare industry should not abandon its goal of working to make the benefits of networked devices outweigh the risks. Networked medical devices promise new innovations and efficiencies for patients and doctors that are impossible to ignore. For example, a wearable device or implant that can aggregate longitudinal patient data and send alerts and updates to a physician or other provider could expedite care in an unprecedented manner.[7]

Before providers can reap the benefits, however, devices need to be secure. Current guidance from the FDA and potential future legislation lay the onus on manufacturers to build security into the development process, and continually update and patch their devices post-market. This, combined with providers' security measures, will go a long way in keeping threats to IoT devices from becoming actual exploits.

To ensure that your organization's security posture is ready to support new medical technologies, contact Securance today.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. Alder, S. (2022, March 24). FBI: At Least 148 Healthcare Organizations Suffered Ransomware Attacks in 2021. HIPAA. Retrieved from https://www.hipaajournal.com/fbi-at-least-148-healthcare-organizations-suffered-ransomware-attacks-in-2021/
2. Arm Limited. (2022). The Internet of Things has reached a turning point. Retrieved from https://report.psacertified.org/: https://report.psacertified.org/introduction/?submissionGuid=d7dc318b-8626-4b32-9ee8-4d016ff85d01
3. Cybellum. (2022, April). Medical Device Cybersecurity: Trends and Predictions, Survey Report, April 2022. Retrieved from https://7512951.fs1.hubspotusercontent-na1.net/: https://7512951.fs1.hubspotusercontent-na1.net/hubfs/7512951/Assets/Medical%20Device%20Cybersecurity%20-%20Trends%20&%20Predictions%20-%20by%20Cybellum.pdf?utm_campaign=State%20of%20Medical%20Device%20Cybersecurity%202022&utm_medium=email&_hsenc=p2ANqtz-8
4. Dark Reading Staff. (2022, April 22). Many Medical Device Makers Skimp on Security Practices. Retrieved from www.darkreading.com: https://www.darkreading.com/tech-trends/many-medical-device-makers-skimp-on-security-practices
5. FDA. (2016, December). Postmarket Management of Cybersecurity in Medical Devices. Retrieved from www.fda.gov: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
6. FDA. (2022, April 8). Cybersecurity. Retrieved from www.fda.gov: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
7. Gillis, A. S. (2022, March). What is the internet of things (IoT)? Retrieved from www.techtarget.com: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
8. Gralla, P. (2017, September 25). Medical IoT devices: the security nightmare that keeps CIOs up late at night. Retrieved from www.hpe.com: https://www.hpe.com/us/en/insights/articles/medical-iot-devices-the-security-nightmare-that-keeps-cios-up-late-at-night-1709.html
9. McKeon, J. (2022, March 8). 7 New Vulnerabilities Threaten Supply Chain Medical Device Security. Retrieved from www.healthitsecurity.com: https://healthitsecurity.com/news/7-new-vulnerabilities-threaten-supply-chain-medical-device-security
10. McKeon, J. (2022, April 4). Senators Introduce PATCH Act to Ensure Medical Device Security. Retrieved from www.healthitsecurity.com: https://healthitsecurity.com/news/senators-introduce-patch-act-to-ensure-medical-device-security
11. Mello, J. P. (2016, January 28). FDA Guidelines Target IoT Medical Device Security. Retrieved from www.technewsworld.com: https://www.technewsworld.com/story/fda-guidelines-target-iot-medical-device-security-83042.html
12. Mello, J. P. (2021, September 14). Execs Fear Ransomware While Most Unprepared To Fight It. Retrieved from www.technewsworld.com: https://www.technewsworld.com/story/execs-fear-ransomware-while-most-unprepared-to-fight-it-87271.html
13. Naden, C. (2021, February 16). Keeping Cybersafe New guidance on cybersecurity frameworks just published. Retrieved from www.iso.org: https://www.iso.org/news/ref2629.html
14. Skahill, E., & West, D. M. (2021, August 9). Why hospitals and healthcare organizations need to take cybersecurity more seriously. Retrieved from www.brookings.edu/: https://www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/
15. The White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. Retrieved from www.whitehouse.gov: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/?utm_source=link
16. TrapX Labs. (2015, May 7). ANATOMY OF AN ATTACK. Retrieved from https://cdn.securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf
17. William J. Gordon, M. M., Wright, PhD, A., & Aiyagari, MD, R. (2019, March 8). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. Retrieved from jamanetwork.com: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270

The Internet Of Things And Medical Devices: Challenges And The Road Ahead

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com