Wireless Airspace Security for Healthcare: A CIO Guide

Executive Summary

Hospitals now account for 30% of all large data breaches, at a cost of $21 billion in 2020 alone.

82% of healthcare organizations have experienced an IOT-focused cyberattack[4]

Security budgets in healthcare are tight. On average, hospitals allocate 6% of their IT budgets to security[1], whereas other industries such financial services spend about 10%.
A significant challenge facing CISOs/CIOs is the widespread use of mobile and smart device technologies which has gotten ahead of the security infrastructure used in most hospitals.

Hospitals and healthcare delivery organizations (HDOs) have fully embraced wireless and smart device technologies to improve efficiency and quality of patient care. The medical device industry is constantly producing innovative solutions using IoMT technologies. The result is an average mid-sized hospital network now hosts tens of thousands of IoT, IoMT and mobile devices. They are difficult to secure because security agents (e.g., anti-virus) cannot be installed on them, they often do not have identities within the IT infrastructure, many are unmanaged, and many have unmonitored wireless interfaces. In short, hospitals are home to a diversity of devices that operate outside the scope of traditional security technologies. The challenge this creates for CIOs/CISOs is how to address the security gap within the constraints of budget, people, and time.

This white paper provides information to help hospital CIOs/CISOs evaluate and respond to the risks to operational continuity, patient data and patient safety that result from the prevalence of Wi-Fi, Bluetooth and other RF devices used in hospitals. The paper addresses how to evaluate and prioritize those risks, and it offers practical approaches to mitigating the risks given the opex, capex and staffing constraints facing hospital CIOs.

Out-of-band, passive wireless monitoring has proven to be an effective approach to meeting these security challenges in hospital environments. This approach delivers all the required elements of a robust security framework, and it can be implemented and operated at low cost. The Harmony IoT solution from Orchestra Group uses this approach. It combines a non-invasive architecture leveraged by advanced AI/ big data technologies to protect hospitals from current and evolving wireless airspace threats.

The Airspace Attack Surface

Hospitals are realizing great gains in efficiency and quality of care by enabling mobility for their staff and medical equipment, and by using smart medical device technologies. This transformation is well underway but has come about without a comprehensive security strategy. The result is widespread use of wireless devices and wireless networking while securing this infrastructure is playing catch-up. Today, hospitals can have twice as many IoT, IoMT and mobile devices[2] on their networks than traditional wired devices, but the security architecture they have in place was designed for a wired networking model. Two elements comprise the hospital airspace attack surface:

Devices

The devices deployed in the hospital that have wireless connectivity.

Protocols

The wireless protocols that can be used to compromise those devices.

A device-centric view of the attack surface reveals a staggering diversity of potential targets. The average hospital bed has 10 - 15 connected devices (monitors, sensors, medication pumps). These devices are connected both to the patient and to the wireless network. A recent survey showed the average hospital has over 10,000 Internet of Medical Things (IoMT)[3] devices comprising a wide range of functions, manufacturers, ages, and maintainability. These are especially sensitive attack targets because they provide access to the hospital network and because of the direct threat to patient lives if they are tampered with.

The other component of the mobile/wireless attack surface comprises standard IoT devices – building system components (HVAC), smart lightbulbs, cameras, conference room gear and more. These devices have been successfully used by cybercriminals to steal patient data and as pathways to ransomware attacks.

A large hospital may have 85,000 medical devices connected to its network[5]

Finally, there are mobile devices used by staff – tablets, laptops, smartpens, wireless printers, etc. This last category can host end point security agents, but they are still exposed to hacking via their wireless interfaces.

Unmanaged and IoT devices outnumber managed devices in 69% of the organizations surveyed · 84% of respondents believe that unmanaged and IoT devices are more vulnerable to cyber-attacks than corporate-managed device[10]

The other element of the attack surface comprises the wireless protocols the devices use to communicate. The primary wireless protocols used by IoT, IoMT and IT devices are Wi-Fi, Bluetooth, BLE, Zigbee, Z-wave and Lutron. There is much less diversity of attack pathways (only a few protocols) in contrast with the list of potential target devices. Just as hospitals have long used firewalls and network monitoring to secure assets connected to the wired network, a strategy that uses wireless policy control and airspace activity monitoring can bring security up to the standards of the wired infrastructure. This is especially important as maintaining end point security on the devices themselves is often not possible and where possible, not sufficient.

Current State of Defenses

Unlike wired infrastructure (network access points and devices), it is not possible to prevent physical access to the wireless airspace. Hospitals are open to the public, giving attackers unchecked access to the airspace both from within hospital buildings as well as from their surrounding areas. It is relatively easy for attackers to compromise wirelessly connected devices and gain access to the network. Current security tools such as traditional NAC (network access control) systems and mobile device management systems (MDM) lack visibility into many devices in the hospital environment and do not monitor activity in the airspace. In short, NAC and MDM solutions do not prevent the hospital airspace from being used as an attack vector.

Wi-Fi is the most widely deployed protocol in hospitals. Because it is so prevalent and because of its longer range than other wireless protocols such as Bluetooth and Zigbee, it is the easiest and most frequently used vector for wireless borne attacks. An attacker can work unnoticed from a waiting room, lobby or from the parking lot, using inexpensive tools and easy to implement techniques. In a recent report, the office of the inspector general demonstrated how easy it is to attack Wi-Fi networks.[9]

Common Wireless Attacks

Evil Twin, Karma

The evil twin is perpetrated by setting up a rogue access point (a hotspot) that broadcasts the same SSID as a legitimate AP in the hospital network. This hotspot is not attached to the hospital network and therefore is not detected as a rogue AP by standard NAC defenses. The attacker can use passive or active techniques to induce devices (IoMT, laptops, tablets, etc) to attach to the AP and from there can deposit malware on the victim systems or act as a man in the middle (MiTM) between the device and the legitimate hospital AP. At this point the hospital is breached.

Denial of Service

Attackers can disrupt legitimate wireless traffic using layer 1 techniques which interfere with wireless transmissions using an RF signal generator. Some DOS events are not actually malicious, but occur because of RF noise from microwave ovens, cordless phones, etc.

More commonly, attackers use layer 2 techniques to disrupt service. There are many different layer 2 DOS attacks but in general they involve spoofing deauthentication frames, causing devices to disconnect from the legitimate AP. This can have serious consequences where the devices are delivering care.

MAC Spoofing

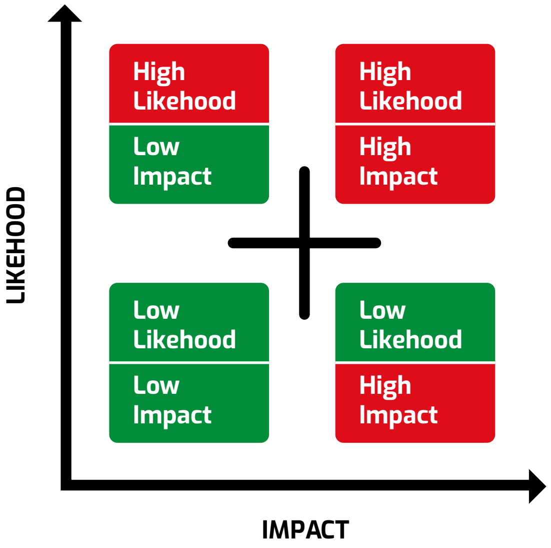
The attacker can discover the MAC address of a legitimate access point (AP) and configure his device to pose as the legitimate AP. This can be a means to create a denial of service (DOS) attack, steal confidential information, or infect end points with malware.

Eavesdropping

Eavesdropping can range from relatively benign monitoring for SSIDs to capturing all traffic – in short, the same as wiretapping but in the wireless context. Organizations need to ensure encryption standards for authentication and data are in place on every access point to prevent attackers from obtaining confidential information and user credentials.

Evaluating Risk

Risk is a combination of the likelihood of a successful attack and the impact/ consequences of the attack. Lowering risk requires reducing likelihood, impact, or both. Risks can be classified in a quadrant, providing a straightforward framework for prioritizing risks and allocating resources to address them, as shown below.



Hospitals and HDOs are frequent targets of attack. The most frequent target is patient data. In a recent survey 89% of hospitals in the US reported a data breach within the last 2 years. The next most common attack is ransomware. These are both high impact events. Reducing the impact of these attacks is often very difficult if not impossible. Therefore, HDOs need to take steps to reduce their likelihood. Attackers have favored email phishing techniques to breach hospital networks. As HDOs improve their defenses against social engineering attacks attackers are moving on to less well defended entry points, such as wireless IoT and IoMT.

Perhaps the highest impact risks are those that threaten patient lives. If compromised, the monitors, medication delivery systems and devices used in operating rooms can have catastrophic consequences for the patient. Hospitals should assess how exposed they are to attacks on medical devices and take appropriate steps to reduce their likelihood. The risk level with medical devices is high: 18% of provider organizations reported their medical devices were compromised by malware or ransomware in the past 18 months[6].

Finally, CIOs should take a broad view of the state of wireless security within their operations in terms of meeting basic security hygiene standards. There are security frameworks that can assist with that effort, such as SS-019[7] and NIST 800-53[8].

72% of provider organizations report that their resources are insufficient or too strained to adequately secure their medical devices. Poor asset visibility and ambiguous security ownership are top challenges.[11]

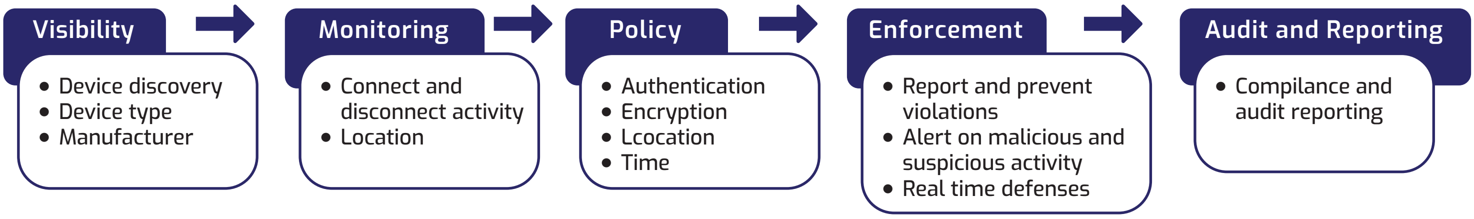
Mitigating Risks

It is no secret to hospital CIOs and CISOs that they have serious airspace exposures that need to be addressed, but they face budget, time and staffing constraints. What are the practical steps to address threat exposures created by the increasing use of wireless technologies? First is to assess the current state of security:

1. What is the state of visibility to wireless devices in the network?
2. What monitoring capabilities are in place?
3. What security policies are in place respect to wireless devices (encryption, authentication, acceptable use)?
4. What enforcement mechanisms are in place?
5. What security standards and frameworks are being followed?
6. What is being reported to audit committees?

Following this assessment CIOs can take steps to address the security gaps. In many cases the gaps will be significant (e.g., lack of visibility, activity monitoring, policy, and enforcement). However, these can be addressed without large capital outlays or large increases in opex, and without impacting network operations.

A simple framework for bringing the wireless, IoT and IoMT infrastructure up to a reasonable standard of security hygiene is summarized in the graphic below:



Visibility
- Device discovery
- Device type
- Manufacturer

Monitoring
- Connect and disconnect activity
- Location

Policy
- Authentication
- Encryption
- Lcocation
- Time

Enforcement
- Report and prevent violations
- Alert on malicious and suspicious activity
- Real time defenses

Audit and Reporting
- Compilance and audit reporting

The recommended approach for putting such a framework into action is to use an out-of-band solution monitoring and policy management solution. A key advantage of an out of band approach is it does not require modifications to the network it is protecting. It can be put into operation without the network operations team needing to provide the monitoring devices with IP addresses, DNS names, identities and so on. The time and cost to implement are therefore far less than solutions that must be installed on the network. Ongoing costs are less as well. It does not add additional infrastructure that IT operations needs to maintain and account for when making changes. Finally, an out-of-band solution does not become part of the attack surface of the network it is protecting.

The system must provide the capabilities needed to implement the security framework: visibility, continuous monitoring, policy control, enforcement, real time mitigation and reporting. It should have an easy-to-use management system so security operations can easily create rules, policies and enforcement that clearly map to the standards of the security framework. Reporting should also be clear and easy to understand, thus saving time for security and audit committees.

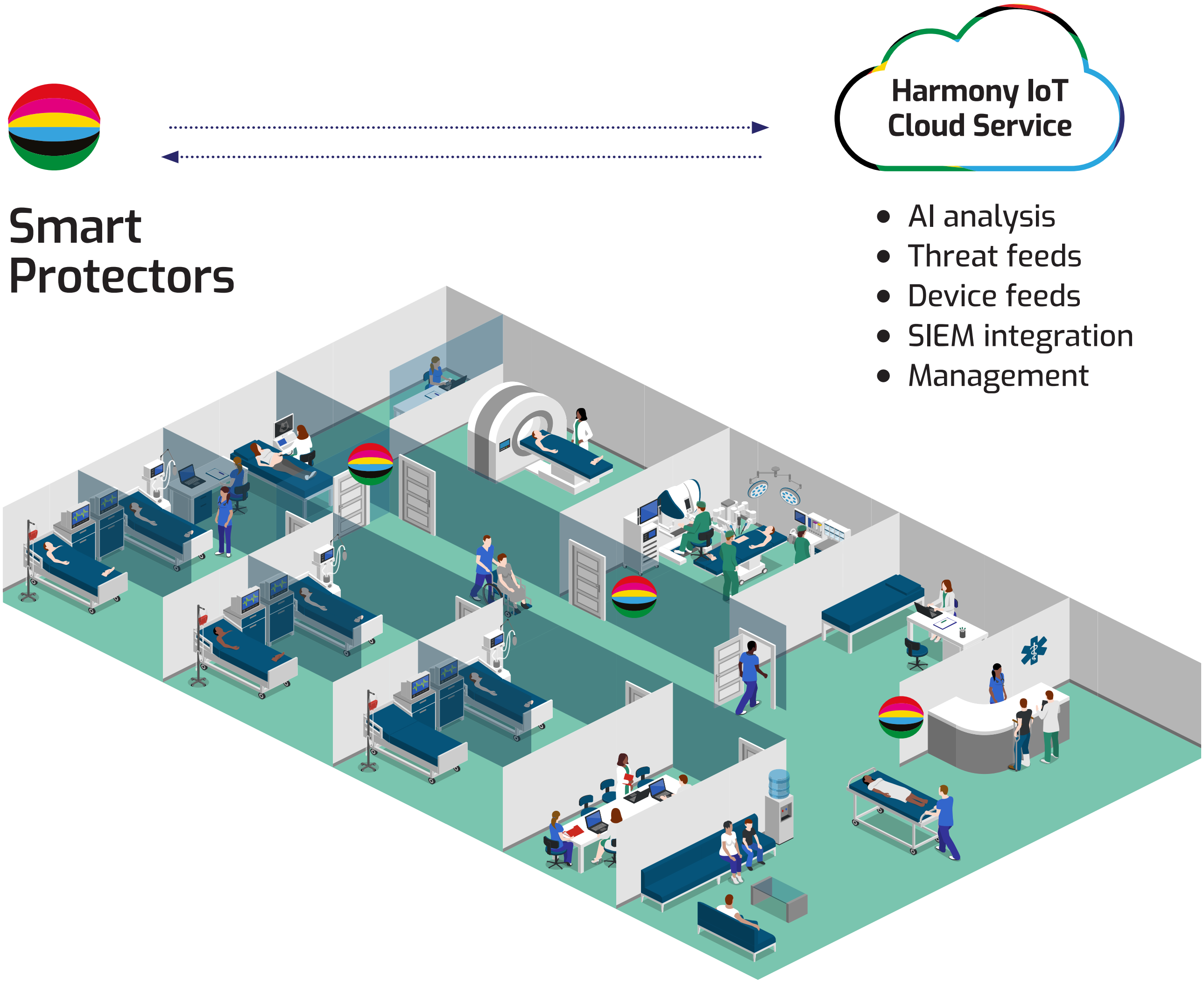
Implementation can be approached incrementally. Identify areas or functions of high sensitivity, such as operating rooms, emergency rooms and waiting areas, and install wireless monitoring in those locations. This provides a good start to securing the highest value, highest risk targets and is achievable at very low cost. It also allows the team to get familiar with the system capabilities, making for an easy transition to securing the broader wireless environment.

The Harmony IoT Solution

Harmony IoT from Orchestra Group is an out-of-band wireless security solution that addresses the wireless security challenges and risks facing hospitals and HDOs. It provides the full scope of capabilities outlined in the framework shown above.
The system has two components: The on-premises component comprises small, low-cost sensors (“Smart Protectors”) that each monitor and protect 100-200m^2 of wireless airspace.

The sensors passively monitor and collect wireless traffic at the data link layer. This poses no potential violation of HIPAA and GDPR regulations. The link layer traffic collected enables the Smart Protectors to perform all the required security functions – providing device visibility, activity reporting and, when needed, enforcement actions.

Smart Protectors process large volumes of data locally and send much smaller volumes of meta-data to a central, cloud hosted system, which is the second component of the solution. The cloud component is an AI/big data system that continuously learns from all Smart Protector deployments. It identifies what is normal/suspicious in terms of device type as well as what is normal/abnormal behavior specific to each customer environment. For example, it understands a patient monitor should show a regular pattern of transmission. It also learns normal patterns of behavior within a hospital – such as when and where specific devices connect. Unlike signature-based systems which are easy to defeat, Harmony IoT uses behavioral methods to identify and mitigate attacks even as attackers evolve their methods to escape detection by traditional WIPS (wireless intrusion prevention systems). This learning architecture means the security value of Harmony IoT is constantly growing, as more and more Smart Protectors contribute knowledge to the system.



Harmony IoT Cloud Service

Smart Protectors

- AI analysis
- Threat feeds
- Device feeds
- SIEM integration
- Management

Summary

Hospitals and HDO's have fully embraced wireless and smart device technologies to improve efficiency and quality of patient care. The medical device industry is constantly producing innovative solutions using IoMT technologies. The result is an average mid-sized hospital network now hosts tens of thousands of IoT, IoMT and mobile devices.

This change has come about quickly and often without sufficient security safeguards. The deployment of wireless IoT and IoMT in hospitals has outstripped the means to secure them. CIOs and CISOs must play catch up to establish the fundamentals of security in the wireless airspace; visibility, continuous monitoring, policy enforcement, attack mitigation and reporting.

Out-of-band, passive wireless monitoring has proven to be an effective approach to meeting these security challenges in hospital environments. This approach delivers all the required elements of a robust security framework, and it can be implemented and operated at relatively low cost. The Harmony IoT solution from Orchestra Group uses this approach. It combines a non-invasive architecture leveraged by advanced AI/big data technologies to protect hospitals from current and evolving wireless airspace threats.

References

1. 2020 HIMMS Cybersecurity Survey in Healthcare HIMSS Healthcare Cybersecurity Survey | HIMSS
2. https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-of-medical-things/
3. Medical Device Security CHIME Edition Medical Device Security CHIME Edition 2018 | KLAS Report (klasresearch.com)
4. https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds
5. Office of Inspector General Issue Brief, June 2021 OEI-01-20-0220 https://oig.hhs.gov/oei/reports/OEI-01-20-00220.pdf
6. Medical Device Vulnerabilities Continue to Plague the Industry https://healthtechmagazine.net/article/2018/12/medical-device-vulnerabilities-continue-plague-industry
7. Security Standard Wireless Networks SS-019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882775/dwp-ss019-security-standard-wireless-network-v1.1.pdf
8. NIST 800-53 Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
9. How the OIG successfully attacked the Department of Interior Wireless Network https://www.oversight.gov/report/doi/evil-twins-eavesdropping-password-cracking-how-oig-successfully-attacked-doi%E2%80%99s-wireless
10. State Of Enterprise IoT Security in North America: Unmanaged and Unsecured, Forrester Research, 2019
11. Medical Device Security 2018, a KLAS-CHIME benchmarking report

About Orchestra Group
Orchestra Group is a privately held company led by top cybersecurity and data-science experts. Our Harmony IoT solution protects financial institutions, banks, data centers, governments, healthcare organizations, manufacturing facilities, defense contractors, and SCADA companies. Visit us at www.orchestragroup.com