RISKSENSE

Internet of Medical Things (IoMT)

IoMT Is Here and the Risks Are Real

It's always about the money

While hackers could leverage exploits to modify systems and cause physical harm to other humans, it's more likely they'll be motivated to use stolen PHI for financial gain, to gain access to other systems, or encrypt it for use in ransomware attacks. Healthcare records fetch higher prices, as much as 60 times that of stolen credit card data, because they contain much more information a cybercriminal can leverage and sell. "Criminals want what they refer to as "fulls", or full information about their victim. Name, birth date, Social Security number, address, anything they can learn about their victim. All that information is in your healthcare records," said Etay Maor, an executive security advisor at IBM Security in a 2016 interview with CNBC. "While ***a Social Security number can be purchased on the dark Web for around $15, medical records fetch at least $60 per record*** *because of all that additional information, such as addresses, phone numbers and employment history. That in turn allows criminals to file fake tax returns. According to the IRS in the 2016 tax filing year 1.4 million returns were filed with confirmed identity theft, totaling $8.7 billion".*

In a June 30th 2016 article by Quinten Plummer in TechNewsWorld entitled, "The Internet of Medical Things, a New Concept in Healthcare", Stu Bradley, Vice President of cybersecurity at SAS noted that, "The proliferation of IoMT technology, and the healthcare industry's enthusiasm to adopt it, has put the veritable cart before the horse in terms of security. Manufacturers will need to embed more robust security solutions into IoMT devices, meaning they must proactively address security concerns instead of retroactively responding".

In a timely highlight to this issue, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published an advisory in late May 2017, centered on a hard-coded password vulnerability that impacts medical devices. The vulnerabilities were discovered by researchers at Cylance, who found hard-coded password vulnerabilities within roughly 300 medical devices, manufactured by some 40 different vendors, which could be exploited to potentially change critical settings and/or modify device firmware.

According to the ICS-CERT advisory, "The affected devices have hard-coded passwords that can be used to permit 'privileged' access to devices such as passwords that would normally be used only by a service technician. In some devices, this access could allow critical settings or the device firmware to be modified." In addition to pacemakers or defibrillators, the devices impacted by the security failure also include surgical and anesthesia devices, ventilators, drug infusion pumps, patient monitors, as well as laboratory and analysis equipment.

In addition, ICS-CERT went to the Food and Drug Administration (FDA), which in-turn issued a warning to medical device manufacturers, hospitals, medical device user facilities, health care IT and biomedical engineers, urging them to address the known flaws and to work harder to prevent similar issues in the future. ICS-CERT provided a list of vendors that have released security advisories to warn customers of the risks and provide them with recommendations on how to prevent attacks. The list includes Rockwell Automation, BD (Becton, Dickinson and Company), Schneider Electric, ABB, Siemens, General Electric, Philips, Smiths Medical, Johnson & Johnson, and Medtronic. Some of these vendors have also issued warnings about the threat posed to their industrial products. BD published a list of tens of potentially vulnerable devices and provided recommendations for how to secure the underlying Windows-based systems; Siemens has released separate advisories for their Healthineers product line, including magnetic resonance, laboratory diagnostics, tomography, radiography, X-ray, mammography, molecular diagnostics, and molecular imaging devices and also says it's working on updates that will patch Server Message Block (SMB) vulnerabilities in the affected products. Until patches are available they are providing suggested countermeasures.

Operating Technology versus Information Technology

In a recent study by Virta Laboratories, Inc. into post-market medical device security monitoring, it was found that medical devices would often be shipped with older, unsupported operating systems. As medical devices can stay in clinical use for decades, these outdated operating systems contribute to the healthcare industry's overall vulnerability. Operating technologies like these devices are harder to patch exposing organizations to the effects of event common malware.

Tracking and Location

A number of medical devices enable the tracking and geolocation of the user to increase improvement in patient outcomes. An example is asthma inhalers and elder care, where several inhalers use mobile apps via Wi-Fi to collect data about location and medical information, such as the time and date of an asthma attack. In the case of elder care, general location awareness is collected from a wearable device. The use of Wi-Fi as a means to collect and share location data can increase privacy and security concerns if not correctly implemented. This can lead to man-in-the-middle attacks (MitM), resulting in stolen protected healthcare information (PHI), and even physical security concerns.

Implantable Devices

Medical devices that are physically implanted into the body (IMD's) are the most intrusive devices known. As detailed in Homeland and the hacked pacemaker, due to the devices intimate use, IMD's pose the greatest security concerns for patients and may have potentially fatal consequences. A study on IMDs by the University of Madrid in Spain found that IMDs were subject to MitM attacks across unsecured Wi-Fi connections. The study stated that IMDs contain significant Personally Identifying Information (PII) such as name, address, social security number, and PHI which is at risk of theft from eavesdropping.

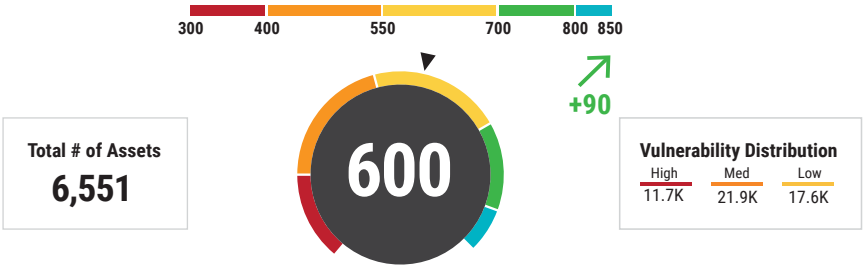
Cyber 'Health' Profiles For Medical Devices

In an environment where ePHI is a highly attractive commodity for a criminal, cyber weaknesses will be exploited. As medical devices became ever more likely to be Internet-enabled and to share data across cloud platforms, we also need to take precautions against the unauthorized interception of patient data. Ensuring safe Wi-Fi implementation and setup, and using encryption for data both in transfer and at rest, will help to ensure a healthy outlook for medical devices and the patients that use them.

A Clinical Analysis

How to uncover and diagnose cyber risk:

- Duration: How long has this condition lasted? Looking at the scanning data how long has the vulnerability existed?
- Experience: Have you had a similar issue in the past, new variant of an older CVE? Is this nothing you've experienced before, new threat or zero day?
- Severity: What's the CVSS score and am I exposed to this vulnerability? Do I have effective counter measures in place?
- Most Important to Address: While there are many things to be concerned about for healthcare IT and OT, taking action against the highest risk items for the business will reduce negative cyber health impacts quickly.
- Pace of Change: Is threat and vulnerability management getting better over time?
- Susceptibility: Why am I seeing this today? Can I perform temporal analysis to see if this is a one-time issue or has been an ongoing issue that was not previously identified.



The RiskSense platform manages the massive volume of vulnerability scan data across the spectrum of IT and OT technologies; network, endpoint, DB, and even medical devices or IoT for healthcare. It provides the intelligence to unify and contextualize the feeds with external threat intelligence and evaluate business impact. RiskSense delivers the priority issues and actions needed for effective remediation. Customers will know the most important threats and vulnerabilities are getting addressed as RiskSense continually reports on cyber health risk. Like a credit score, the higher the value of the Risk Sense score indicates a committed focus on cyber security health and well-being. Enterprises are seeking solutions to unify and contextualize the feeds from these disconnected, siloed tools and then prioritize and remediate those cyber risks that pose the biggest business impact.

About RiskSense

RiskSense®, Inc. is the pioneer in threat and vulnerability management. The company provides enterprises and governments with clear visibility into their entire attack surface, including attack susceptibility and validation, as well as quantification of risks based on operational data.

The RiskSense Software-as-a-Service (SaaS) platform unifies and contextualizes internal security intelligence, external threat data and business criticality to transform cyber risk management into a more proactive, collaborative, and real-time discipline. It embodies hands-on expertise gained from defending critical government and commercial networks from the world's most dangerous cyber adversaries.

By leveraging RiskSense threat and vulnerability management solutions, organizations can significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, reduce costs, and ultimately reduce the attack surface and minimize cyber risks.

RiskSense Platform – the industry's most comprehensive, intelligent platform for managing cyber risk.

Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG

SB_Healthcare_02112018