Diagnosing a Healthcare Cybersecurity Crisis: The Impact of IoMT Advancements and 5G

Published on Alvarez & Marsal | Management Consulting | Professional Services (https://www.alvarezandmarsal.com)

December 17, 2021

INTERNET OF MEDICAL THINGS (IOMT) TECHNOLOGY REMAINS IN EARLY STAGES OF ADOPTION, BUT ADVANCEMENTS AND BREAKTHROUGHS ARE QUICKLY MOVING THIS PROCESS FORWARD.

INTRODUCTION - A CRISIS BREWING

As an industry, healthcare has an advantage when it comes to technology, as it is beneficial for both consumers *and* providers who seek to leverage new solutions to receive and provide efficient and effective care, improve services, and optimize value. This symbiotic relationship establishes a requirement for the development and rapid evolution of new platforms. This requirement, in turn, provides the energy fueling a continued technology evolution. The results of this evolution can eliminate barriers to service and move healthcare further into the home, enabling richer, and more effective collection of personal health data.

Healthcare has traditionally lagged when it comes to technology relative to other industries. Many organizations trail behind other leading industries like financial services by at least 10-15 years. A key driver for Healthcare trailing other industries is due to the sensitivity of patient and health information. The Government imposes very stringent regulations (e.g. Health Information Portability and Accountability Act (HIPPA) with significant fines for non-compliance). For example, according to HIPAA journal, the Department of Health and Human Services' Office for Civil Rights (OCR), which is an enforcement are for HIPAA, has imposed more than $100M in fines since 2008 [1] . These controls have led to an increased focus on security of customer data and seemingly at the expense of innovation and experimentation. COVID-19 eliminated the question of whether or not this industry can digitally transform. The next question is, will it last?

The concept of the Internet of Things (IoT) was one of the first developments that embedded technology directly into our homes and personal lives with the open intention of swapping personal data for the provision of a good or service. What was previously referred to as IoT has matured into unique industry verticals, including healthcare, which is seeking to change the status quo. This industry offshoot of IoT has become known as the Internet of Medical Things (IoMT), which presents substantial benefits as well as security risks.

The intent of IoMT, even if only loosely envisioned at the outset, has been to use embedded consumer end-point technology as a means for providing real-time diagnostic measures, enhancing care, and connecting providers to their patients closer to a time-critical medical event and operating in a preventative nature for non-emergent care. While concerns and skepticism remain around the cybersecurity and privacy of Electronic Health Records (EHR) and the use of IoMT, the opportunities for the healthcare industry to benefit from these innovations are seemingly limitless. With the proper focus, cybersecurity and privacy concerns can be

managed and eventually mitigated.

The most impactful influence in this direction has been the COVID-19 pandemic, shifting cultures overnight and propelling a digital revolution in a matter of months. At no time in human history has such a monumental shift taken place in the way the public consumes and contributes to the global information library. Cultural norms have rapidly adjusted to leverage technology and remote access in a manner never before experienced.

For example, consumers have traditionally preferred to see their doctors in-person where their vitals and critical health information were captured at the point of care. This traditional model had gaps in access to care that were mainly due to accessibility issues relating to qualified providers and patient locations. As a result of the pandemic, the traditional model has been disrupted, and technology has responded by removing physical barriers and by connecting providers and patients in new ways.

The pandemic introduced physical impediments that required the healthcare system to look beyond cultural barriers and embrace technology in a revolutionary manner. Patients have recognized that the healthcare treatment and advice they receive during Telehealth visits, particularly for preventive care or managing chronic conditions, can mirror the effectiveness of care provided in the traditional brick-and-mortar model. Additionally, patients can now access a larger network of providers and specialists outside of their immediate physical geography. In turn, providers can instantly access patients' vitals via emerging technologies, when distance or other barriers previously presented challenges to access. This leveraging of technology has contributed considerably to the digital revolution globally.

The other most impactful factor driving this trend was not purpose-built for the healthcare industry but may be its biggest enabler. The most recent advancement in wireless technology, known as 5G, enables a level of communication that will facilitate a near real-time exchange of information. 5G technology relies on a high volume of closely meshed wireless towers that provide unprecedented high-speed wireless internet access. Cellular networks offering 5G will bring new capacity that will have a massive impact on the IoMT ecosystem, allowing far more devices to share more data simultaneously. The increased bandwidth and denser network switching will enable a manner of medical treatment and diagnostic innovation that was not possible on slower previous networks.

Healthcare will directly benefit from this technology as a means for digitally sharing patient information. Now empowered by 5G, providers can explore new mobile medical devices that are pre-configured and enable the exchange of information between patient and provider faster than ever before.

For instance, this capability takes virtual models of care like Telehealth and starts to enable an even more meaningful primary and post-acute care model. Providers no longer need to wait until the patient comes in and can intervene as information becomes available and during times previously inconvenient to the patient, not just when the patient was in a fixed location. Additionally, the technology, which was recently only science fiction, will soon be realized as the use of augmented and virtual realities and artificial intelligence all have a direct impact on medical care. This includes diagnostic modalities once found only in a facility, such as continuous patient monitoring and real-time pharmaceutical delivery. Each will only be effective if they can consume higher bandwidth and operate at faster speeds.

Healthcare IoMT devices, enhanced by 5G, will generate personal health data on a level previously unseen, in terms of the nature of the information captured, speed, and scale. Given the opportunity for the industry, a proliferation of at-home devices is anticipated, and the ubiquity of the technology will be here seemingly overnight. Additionally, cultural barriers to using technology for healthcare have been further reduced, creating a significant market opportunity that should be embraced and protected, so that it continues to grow and modernize healthcare for the better. However, a significant factor driving security concerns is the sheer variety of devices that are quickly becoming available. Whenever a new piece of hardware is created or adopted on a significant scale by the market, there is a catch-up period to be expected, wherein the security industry grapples with the new challenges this technology will generate. Given the highly anticipated ubiquity of 5G-enabled IoMT, unless security concerns are addressed proactively, we may never catch up.

Thus, a crisis is revealed in the confluence of these two independent and highly impactful new influences on our world. The industrial complex is racing to address market opportunities created by the culture shift. New technologies must acknowledge real and measurable cyber risks associated with new, medically focused consumer devices and applications that are exchanging information over the internet. Global consumers demonstrate that their interest is primarily on the benefits, while they appear to largely remain unaware of the risks associated with these fast-developing technologies. Consumer confidence could change instantly with one devastating breach of a once-trusted provider, eliminating the recent and future progress along with consumer

enthusiasm.

However, there is good news. There is still time and mechanisms to address these risks proactively, serving as a springboard for the continued acceptance and evolution these technology growth platforms enable.

IoMT is still in its early stages of adoption and its growth cycle. Advancements and breakthroughs are quickly moving forward, and there is a critical need for security to be a focus in the development of these new tools alongside design and utility. Given the rapid pace and potential magnitude of the coming advancements in IoMT, if these privacy and security risks are neglected, we could see a significant crisis grow in the form of more frequent cybersecurity breaches. This paper examines the market opportunities and risks associated with IoMT. It outlines a plan for proactively mitigating concerns and providing a platform to foster growth, modify attitudes and behaviors as well as continue to build consumer confidence in the overall health system without sacrificing security.

IoMT AND 5G MARKET DISRUPTION IS HERE AND UNAVOIDABLE

Before we examine IoMT, it is prudent to understand 5G as a key enabler for IoMT. 5G enables the next generation of mobility by establishing zero distancing between people and machines, expanding data transmission, and decreasing latency. In layman terms, data can move ultrafast via cellular transmission. In essence, Wi-Fi becomes obsolete because 5G is that fast. 5G has been shown to be 6x to 8x faster than Wi-Fi in all countries outside of the U.S [2] .

Relative to other developed countries, the U.S. is a laggard when it comes to widescale implementation of this new technology. Currently, 81% of consumers have a smartphone, which continues to increase 5-10 percent per year. The numbers are considerably higher for people under 65, equaling 95% [3] whereas equivalent Wi-Fi broadband access has hovered around 64% of the total population in the U.S. [4] So, what does this all mean? 5G is faster than Wi-Fi and will become much more accessible. As a result, technology that benefits from faster speeds and wider access will flourish, including IoMT.

IoMT is a network of medically related devices sharing data that can be translated into information that informs action. Many consumer's everyday life is already embedded with IoMT, whether it be through a smart watch, smart scale, Wi-Fi connected bicycle, etc. Most of these devices communicate via simple sensors (Radio Frequency Identification, infrared communication technology, Bluetooth, etc.) connected to smartphones. From a consumer perspective, most applications of IoMT are isolated to individual devices or configurations as described above or to very specific and unique applications when facilitated directly by a medical provider. This section analyzes the intersection of IoMT and 5G within the U.S. healthcare landscape.

IoMT IS MORE THAN BRILLIANT MARKETING AND TECHNICAL JARGON

"Alexa, what is the weather tomorrow?" AI technology, such as Amazon's virtual assistant Alexa, is an example of IoT that is already embedded in many consumers daily lives, and who experience it through in-home devices used for mundane tasks. These IoT capabilities have expanded via integration between applications that enable the applications to work even better together to provide information. Statista estimates that the market size for IoT will increase by 14x from 2017-2025, reaching $1.6 trillion [5] . While the focus for IoT implementation thus far has been primarily on the home, the move into city infrastructure marks a shift in the way internet-enabled devices are viewed — not simply as extra functionality for gadgets, but as integral components in how human society is run.

IoMT is revolutionizing medical device services and providing an opportunity that is being accelerated by the modern-day digital transformation. As a use case, Open Artificial Pancreas System (OpenAPS) is driving an initiative that highlights the value of IoMT. The OpenAPS project is an open and transparent effort to make safe and effective basic Artificial Pancreas System (APS) technology widely available to quickly improve and save as many lives as possible by reducing the burden of Type 1 diabetes.

OpenAPS originated from the need for the diabetes patient to have a more elegant method of monitoring and controlling their insulin. Type 1 diabetes sufferer Dana Lewis, together with her husband Scott Lebrand, modified her continuous glucose monitor (CGM) using their own home developed software. This software enabled the data feed from the CGM to communicate with the insulin pump, and automatically adjust the supply as required. The OpenAPS initiative demonstrates an IoMT solution in response to a need from patients for new ways to manage chronic conditions.

Telehealth is another example of a significant opportunity for IoMT. The COVID-19 pandemic created an environment that accelerated the need for exploration and adoption of Telehealth solutions. One use case example for IoMT and Telehealth is remote patient monitoring (RPM) capabilities to treat patients at home. An RPM system involves deploying biometric monitoring devices in

the patient's home and transmitting the biometric data collected back to the clinical team, often via a third-party Telehealth platform provider. RPM is a rapidly growing technology in the healthcare industry as it is cost-effective and convenient to use. RPM solutions engage multiple actors as participants in a patient's clinical care. These actors can include Telehealth platform providers, accountable care organizations, and the patients themselves. Each actor uses, manages, and maintains different technology components within an interconnected ecosystem.

The rise of IoMT is driven by an increase in the number of connected medical devices that are able to generate, collect, analyze, or transmit health data or images and connect to healthcare provider networks, transmitting data to either a cloud repository or internal servers. Ultimately, this connectivity between medical devices and sensors is streamlining clinical workflow management and leading to an overall improvement in patient care, both inside care facility walls and in remote locations.

WHAT IS THE IMPACT TO HEALTHCARE?

The impact of IoMT for the healthcare industry is endless and limited only by the imagination of the inventor, engineer, designer, etc. The U.S. HealthIT Market is estimated to generate $149.7 billion by 2025, growing at a CAGR of 11.7% from 2018 to 2020 [6] .

The opportunity for IoMT is propelled further by advancements in communication technologies like 5G. Furthermore, COVID-19 propelled an unprecedented digital revolution in healthcare. Cultural and psychology barriers to the resistance of healthcare digital transformation were rapidly overcome due to the immediate need for access to care coupled with the inability to access that care in-person. As a result, there was a perfect storm of opportunity to utilize advancements in technology to provide care to an individual's home.

OVERVIEW OF SECURITY LANDSCAPE

Proponents of 5G technology often point to the security enhancements that could characterize the transition to the next generation of connectivity. These enhancements generally are a result of, or at least related to, the faster connection speed available with 5G, that could include certain anti-spoofing and anti-tracking features that hamper malicious actors as well as better encryption capabilities when compared to other network technology. [7] 5G technology also enables larger volumes of data to be communicated and potentially protected.

Arguably, 5G also enhances the development and implementation of network architecture that allows sending multiple data streams as single, multi-layered signals, thereby using the same physical networking for different virtualized networks. This is known as network slicing, and it is at the core of 5G mobile networks. This slicing or form of segmentation likely improves a given network's security since each logical network is designed to serve only a specific purpose.

Notwithstanding potential strengths from a security standpoint, numerous cybersecurity risks remain associated with the use of this new technology, particularly when the focus is 5G-connected medical devices. While the threat landscape for such devices may not be unique to the medical space, the elements that characterize the assets themselves weigh heavily in an overall risk calculation to create a complex and somewhat fragmented risk profile.

The United States Cybersecurity and Infrastructure Agency (CISA) officially denotes five chief risks that surround the deployment of 5G technology [8] . These are:

1. *"Attempts by threat actors to influence the design and architecture of 5G networks."*
2. *"Susceptibility of the 5G supply chain due to the malicious or inadvertent introduction of vulnerabilities."*
3. *"Current 5G deployments leveraging legacy infrastructure and untrusted components with known vulnerabilities."*
4. *"Limited competition in the 5G marketplace resulting in more proprietary solutions from untrusted vendors."*
5. *"5G technology potentially increasing the attack surface for malicious actors by introducing new vulnerabilities."*

These risks represent significant challenges for the public sector, private enterprises, and consumers that will make use of this technology. While these cybersecurity risks are specific to the 5G deployment process, they also carry over into the emerging world of IoMT devices, where the potential stakes are considerably higher than for other technologies that will use 5G given the potential for direct impact on an individual's physical health and wellbeing.

As such, each of these risks takes on a new character as they are applied specifically to 5G-enabled IoMT and for our purposes can be layered into three broad categories: Supply Chain Risks, Networking Risks and Data Privacy Risks.

SUPPLY CHAIN RISKS

Before software, there must be hardware. This basic principle of computing technology is the starting point for understanding risk for IoMT devices. The IoMT supply chain may suffer degradation in the form of malicious and/or accidental use of compromised hardware, counterfeit parts, faulty manufacturing, and poor maintenance.

At this point in time, and in the general implementation of IoMT devices into the mainstream, the number of potential devices that will require novel types of components is boundless. The diversity of IoMT devices with unique sensors, cameras, electrical signals, and much more, meticulously calibrated for a hyper-specific purpose, showcases the long and winding supply chain that is behind each and every one of these devices. Along this supply chain any potential incorrect measurements, misconfiguration, or faulty parts can have fatal consequences.

In the traditional world of computing as we know it, there have always been supply chain concerns, so this is a familiar topic for IT and cybersecurity professionals. For example, ever since the widescale implementation of Automated Teller Machines (ATMs) by financial institutions, the risk presented by criminals who install a card skimming device onto the credit card port have been an area of concern for the supply chain behind this technology, both on the initial manufacturing end as well as for maintenance.

Likewise, the medical world has frequently grappled with supply chain risks. Most recently, this came to light with the global effort to combat the COVID-19 pandemic and the race to supply suitable pharmaceutical treatments to those in need. As part of this effort, supply chain risks became clear based on the fact that according to the U.S. Food and Drug Administration Center for Drug Evaluation and Research, the number of facilities in China supplying active pharmaceutical ingredients (APIs) had more than doubled since 2010 to 13% of all those serving the U.S. market [9] . This raised questions across the country about the sagacity of outsourcing the production of potentially essential medical products abroad. Not only does such an international supply chain pose a challenge for getting medical supplies quickly, but it is further complicated given the geopolitical boundaries it traverses.

5G-enabled IoMT devices represent the marriage between supply chain risks from the medical world and from the technology industry in such a way that the overall risk is actually magnified. This is most clearly evident with the IoMT devices known as “wearables” and implants. Such devices, which include cochlear implants, gastric stimulators, insulin pumps, and cardiac defibrillators/pacemakers, are either worn by a medical patient or directly inserted into the patient’s body. Needless to say, a faulty component in a piece of technology of this kind, regardless of whether it was maliciously tampered with or mistakenly inserted, could put someone’s life in jeopardy. A pacemaker could lose its pace, an insulin pump could deliver too much of the chemical, or an implant could break off causing internal bleeding and organ damage.

Beyond the concerns around the integrity and security of a device’s physical components, the supply chain for IoMT also faces risks from software application developers and providers that act as third parties in a doctor-patient relationship. Just as suppliers of hardware are a potential source of risk, so are the parties responsible for delivering the digital solutions that make the hardware function. This is particularly important when it comes to maintaining a device in operation.

While hardware will eventually have to be repaired or replaced, in general the pace of change for any computing device is faster on the software and application side. For the 5G-enabled future, this likely means that IoMT devices will be subject to at least semi-frequent software and application updates or patches. The parties that develop and apply these updates are a critical link in the overall supply chain and carry the responsibility to proactively update and patch against not only operational problems but security risks as well.

Lastly, supply chain risks also include threats against the availability of IoMT. As these devices continue to advance and become more popular, they will likely reach a point of medical necessity for countless people. At that stage, for a community, if not a nation, the potential risk of a supply chain outage would be critical. Just as supply risks against lifesaving drugs and hospital equipment cannot be tolerated, as IoMT becomes a greater part of the United States’ medical approach, these risks must be viewed in the same way.

NETWORK SECURITY RISKS

There are numerous network security risks that stem from the simple act of connecting a device to an internet network, or in the case of IoMT, to a lightning-fast 5G network. In this manner, this category of cyber risk will include many of the classes of attacks that are iconic and have come to define cyber-attacks in the public’s eye.

Cyber risks from a network security perspective include threat vectors such as viruses, worms, trojans, and malware of all kinds, which can lead to attacks like ransomware (extortion), data loss, corruption, etc. Network security risks also cover attacks that can result from simple unauthorized access to a system or denial of access to a system.

To set the stage, the key element behind networking risks for IoMT is the fact that 5G technology increases the "attack surface" for malicious actors by introducing a whole new class of targets to the internet-connected ecosystem. CISA builds on this reality, stating that:

5G technology increases the attack surface for malicious actors by introducing new vulnerabilities: The implementation of untrusted components into a 5G network could expose communications infrastructure to malicious or poorly developed hardware and software and could significantly increase the risk of compromise to the confidentiality, integrity, and availability of 5G [10] .

While it is impossible to postulate the infinite variations of attacks that could take place impacting new IoMT devices, in order to better understand the potential impact of the network security risks, two hypothetical scenarios illustrate how such attacks would take place: Denial-of-Service and Man-in-the-Middle attacks.

Denial-of-Service (DoS) attacks occur when a legitimate user or users are unable to access information systems, devices, or other network resources as a result of actions perpetrated by a malicious cyber threat actor. Such attacks are typically measured in terms of time and money lost by a victim when a site or system is not available. In the realm of IoMT, an attack like this could have life-threatening consequences. For example, a group of patients that rely on IoMT insulin pumps for essential management of diabetes may not be able to wait for a DoS attack to be resolved if their devices are down.

Man-in-the-Middle attacks take place when a malicious party is able to illicitly intercept communications between two given systems. In the medical technology world, this could involve a malicious actor intercepting communication between an IoMT device and a medical provider. Leveraging this position, a hacker could carry out an attack in a number of ways. The hacker could attempt to spoof the owner/user of the IoMT device by pretending to be a medical professional and tell the user to make inappropriate and dangerous changes to the device's configurations. Alternatively, the hacker could simply capture sensitive communication and either extort a patient or, if relevant, sell it on the dark web.

These are but two illustrations of the significant network security risks for IoMT that result from their high-speed 5G connectivity. The threats that drive these risks and their vectors have continued to plague the traditional Information Technology space for years, and so it remains likely that as the number of new medical devices come online, these threats will only continue to evolve.

PRIVACY RISKS

The final risk for 5G-enabled IoMT is data privacy risk. Data privacy as a concept continues to grow and change as the role that technology plays in society and daily life expands. Different countries around the world, and different states across the U.S., have already begun implementing various regulatory frameworks to define data privacy based on their own interpretation of cybersecurity, sensitive data, and individuals' rights that govern the use of their data and to whom the data belongs. While these frameworks differ from each other and are sure to change over the years, the introduction of IoMT, spurred by 5G, is likely to lead to significant risk for users and purveyors of these devices.

To illustrate the data privacy risks around the use of these new technologies, it is worth exploring the use of IoMT in the corporate workplace. A key element of an organization's cybersecurity program is asset management. In fact, any risk calculation should begin with the identification of "crown jewels." This will answer the central question of "what are you trying to protect?" For businesses, this consideration often focuses on employee-issued desktop and laptop computers and has also expanded to include smartphones; ultimately, it boils down to the data that resides on these devices. In this context, the question of whether an organization allows a bring-your-own-device model is paramount. An enterprise security program can only protect assets that it has inventoried and receive a standard set of security controls, defined by policies, including anti-virus solutions, and patching and disk encryption.

With IoMT, a new frontier for asset management has been opened; employees across companies around the world may bring a variety of new medical devices into their office and potentially connect them to enterprise networks. This simultaneously exposes the company network in question to any potential malicious activity on the device as well as the individual wearing or otherwise using the device to whatever may already be on the corporate network. The privacy risks described in this section lead to the question of whether companies will develop new acceptable-use policies that include stipulations for employee IoMT devices.

This also raises serious issues around employee privacy, especially if a company were to require employees to declare any medical devices they use or somehow collect or handle medical information from an employee's device that passes through an enterprise network. The Health Insurance Portability and Accountability Act (HIPAA) was established to govern the handling of such sensitive Personal Health Information (PHI) and could potentially apply to such a scenario. This regulation defines clear roles and responsibilities for parties involved in any way with this class of data, and organizations could be susceptible to serious regulatory risks stemming from a data privacy violation in this space.

This conundrum illustrates the wide reach of data privacy risks that surround and characterize the implementation of IoMT in the U.S. As such, these risks deserve attention alongside the supply chain and network security risks that also characterize this technological shift. Data privacy and cybersecurity, while separate and distinct domains, are inextricably related, and this relationship is more relevant than ever in the forthcoming shift towards 5G-enabled devices of all kinds.

RISK MITIGATIONS

Mitigating cyber risks in the current evolving threat landscape is already a challenge. With the development of 5G and devices that are always online with access to high-speed data, it will be exponentially harder if cyber security is not embedded in each and every step along the way from design to vendor selection, manufacturing, supply chain, software loading, deployment, maintenance, and disposal of these devices.

With this in mind, CISA's public response has been to promote a three-pronged approach:

1. *"Risk Management: Promote secure and resilient deployment by leading efforts to identify, analyze, prioritize, and manage risks.*
2. *Stakeholder Engagement: Actively engage with the key stakeholders whether it is internally within the organization, third party vendors, government or industry associations, academia, non-profit, and international partners to address the evolving challenges.*
3. *Technical Assistance: Enhance and develop tools, techniques and services to support stakeholders with the technical aspects of secure deployment."* ***[11]***

In the three-pronged approach outlined above, there are several strategic initiatives that should be taken that will help mitigate the risks.

First and foremost, the development of policies, standards and frameworks serve as the foundation for securing IoMT's widespread adoption. High-risk vendors and untested components have the potential to increase the susceptibility of the supply chain to unique and complex risks. Management of these risks will require timely and actionable IoMT risk management information sharing. A baseline framework should be developed for vendors, manufacturers, and service providers to attest to the best practices. There should be a task force to define processes that prioritize the risks based on their severity and impact to critical processes and functions.

In addition to developing policies and standards, there is a need for proper regulatory frameworks for better governance of the organizations developing and servicing the IoMT devices. Although at this early stage in the development of IoMT, it is difficult to fully predict what the risks of IoMT devices will be. In many cases, a combination of HIPAA and traditional Fair Information Privacy Practices (FIPPs) will aptly address IoMTs' privacy and security issues. [12]

Traditional privacy practices and principles, such as the FIPPs, continue to provide the core guidelines for the IoT. However, FIPPs do not establish specific rules prescribing how organizations should provide privacy protections in all contexts, but rather provide high-level guidelines. HIPAA establishes national standards to protect the PHI of users only in the U.S. One of the strategic initiatives of the CISA's 5G strategy is to, "[s]upport international 5G security and resilience policy framework development efforts" [13] . As IoMT becomes popular and is adopted globally, there is a need for more stringent global regulations and compliance standards.

Another major area of concern is vendor risk management and the supply chain. Considering that vulnerabilities in the software and firware of the IoMT devices may have life-threatening consequences, the efficiency of such devices needs to be at its highest. Currently, due to connectivity limitations, most of the devices need to be supported by external connectivity mechanisms via phones and mobile apps. However, with the roll out of 5G, the limitation around connectivity is no longer an issue, and IoMT devices will potentially always be connected to the Internet, thereby increasing the attack surface for malicious actors. This calls

for more stringent hardware design, supply chain, and software load process for manufacturers of such IoMT devices.

These may include:

1. Preventing device tampering or malware insertions in the componentry of devices.
2. Preventing malware insertions during the manufacturing process or during software loading or testing of the IoMT embedded operating system or firmware.
3. Preventing tampering with products in the warehouses or fulfillment channels.
4. Mitigating risks of purchases from non-authorized vendors.

Organizations often develop their own threat models that reflect only their understanding of the risks. Organizations should focus on creating robust and holistic threat models to identify and prioritize upstream as well as downstream supply chain risks.

If the vendors understood the aspects of the environment in which their product will be used and the intent of the threat actors, they can develop more holistic threat models. By doing so, this helps the organizations to manage supply chain risks regardless of where a product is designed, created, assembled, and maintained. Organizations should also focus on having up to date inventory of all their third party and “fourth-party” service providers, that is the vendors that a service provider relies upon, by classifying them based on the level of impact on the organization. Organizations should impose stringent controls on their direct and indirect vendors with continuous monitoring/site audits including the manufacturing locations and warehouses.

Lastly, the primary objective of developing and implementing all of the above mitigation controls is to protect users’ personal and health data. To be effective, data protection has to be everywhere, from the server to the IoMT endpoints, throughout the cloud, and across the web. Organizations should have accurate inventory and classification of the data they are handling and have proper access controls to avoid unauthorized access. Furthermore, organizations should consider storing sensitive information within the secure enclave within the IoMT device itself to avoid data leakage due to unauthorized tampering. They could go further by implementing two-way authentication wherein the IoMT device authenticates with the server using unique signature tokens, and the server authenticates with the device using a similar unique token to avoid Man-In-The-Middle attacks.

One of the strongest mechanisms to protect personal information is to render it non-personal, or de-identified. By removing the individual’s identity from the data being gathered or anonymizing it through technical means, the data is rendered useless if exposed. Furthermore, increased use of secure data sharing can save lives, improving the full context of a patient's clinical information. As stated in CIO Magazine, “We've killed more people because we didn't share data than because we did” [14] . De-identification of the data allows the users, organizations, healthcare firms, and service providers to achieve interoperability and have multiple IoMT devices from different vendors talk to each other.

CONCLUSION

This analysis focused on the impact of IoMT advancements and 5G for the healthcare industry, and then highlighted implications from a cyber security perspective. As expressed, IoMT enabled by 5G is a significant market disrupter that has been accelerated by the recent digitization propelled by the ongoing global pandemic. Healthcare, which has traditionally been a laggard as it relates to technology due to the high bar set by regulators, is embracing IoMT and exploring use cases to improve care to patients and breakdown physical barriers through the adoption of technology. In order for the healthcare industry to build upon this digital transformation and leverage IoMT effectively, the industry needs to ensure cybersecurity stays a priority via the six-point risk mitigation plan we have described.

The benefits of IoMT are evident. Healthcare organizations should implement risk management plans to ensure continuity of care that embraces technologies while protecting patient data and information.

[1] Alder, S. (2018, October 16). $16 Million Anthem HIPAA Breach Settlement Takes OCR HIPAA Penalties Past $100 Million Mark. Retrieved from HIPAA Journal: https://www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark/

[2] Fogg, I. (2020, May 05). 5G download speed is now faster than Wifi in seven leading 5G countries. Retrieved from OpenSignal: https://www.opensignal.com/2020/05/06/5g-download-speed-is-now-faster-than-wifi-in-seven-leading-5g-countries

[3] Mobile Fact Sheet. (2019, 06 12). Retrieved from Pew Research Center: https://www.pewresearch.org/internet/fact-sheet/mobile/

[4] Industry Data. (NA, NA NA). Retrieved from NCTA: https://www.ncta.com/industry-data/80-of-us-homes-have-access-cables-gigabit-internet-speeds?field_industry_data_categories_target_id[84]=84

[5] Takkovska, H. (2020, September 1). Forecast end-user spending on IoT solutions worldwide from 2017 to 2025. Retrieved from Statista: https://www.statista.com/statistics/976313/global-iot-market-size/#:~:text=The%20global%20market%20for%20Internet,around%201.6%20trillion%20by%202025.

[6] U.S. Healthcare IT Market to Reach $149.17 Billion, by 2025- Allied Market Research. (2020, April 21). Retrieved from GlobalNewswire: https://www.globenewswire.com/news-release/2020/04/21/2019390/0/en/U-S-Healthcare-IT-Market-to-Reach-149-17-Billion-by-2025-Allied-Market-Research.html#:~:text=Portland%2C%20OR%2C%20April%2021%2C,11.7%25%20from%202018%20to%202025.

[7] Siddiqui et al., M. S. (2016). "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks". Palo Alto, CA: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 44-49.

[8] CISA, C. a. (2020). “5G Security and Resilience.” . www.cisa.gov/5g.

[9] Woodcock, J. (2019, October 30). Safeguarding Pharmaceutical Supply Chains in a Global Economy. Retrieved from fda.gov: www.fda.gov/news-events/congressional-testimony/safeguarding-pharmaceutical-supply-chains-global-economy-10302019

[10] CISA, C. a. (2020). “5G Security and Resilience.” . www.cisa.gov/5g.

[11] CISA, C. a. (2020). “5G Security and Resilience.” . www.cisa.gov/5g.

[12] (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. - The White House.

[13] CISA, C. a. (2020). “5G Security and Resilience.” . www.cisa.gov/5g.

[14] Padmanabhan, P. (2017). Unlocking the value in patient-generated health data. CIO Magazine.

The final version of this article was published in Indiana University’s Kelley School of Business’s Business Horizons November-December 2021 edition here.

Source URL:https://www.alvarezandmarsal.com/insights/diagnosing-healthcare-cybersecurity-crisis-impact-iomt-advancements-and-5g