ManageEngine
PAM360

Healthcare IT and privileged access security:

An admin's guide

Table of contents

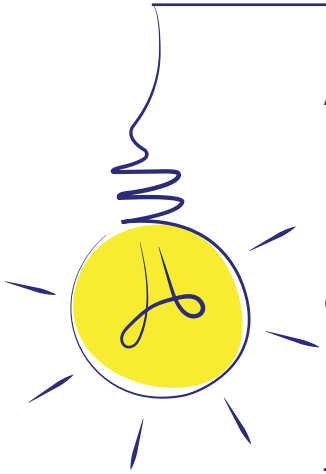
Overview

Overview

The digital revolution of Internet of Things (IoT) devices benefits multiple industries across the globe. When it comes to the healthcare industry, the scope of internet-connected medical devices earns it a unique categorization—the Internet of Medical Things (IoMT). IoMT is the integration of interconnected medical devices, software, and other services with healthcare IT systems over the internet. Healthcare IoT includes a wide range of products, including blood pressure monitors, MRI and CT scanners, pregnancy testing kits, X-ray machines, and pacemakers. IoMT enables healthcare organizations to streamline their operations and treatment processes, improve patient care and medical efficiency, reduce treatment costs, and even attend to patients from remote locations.

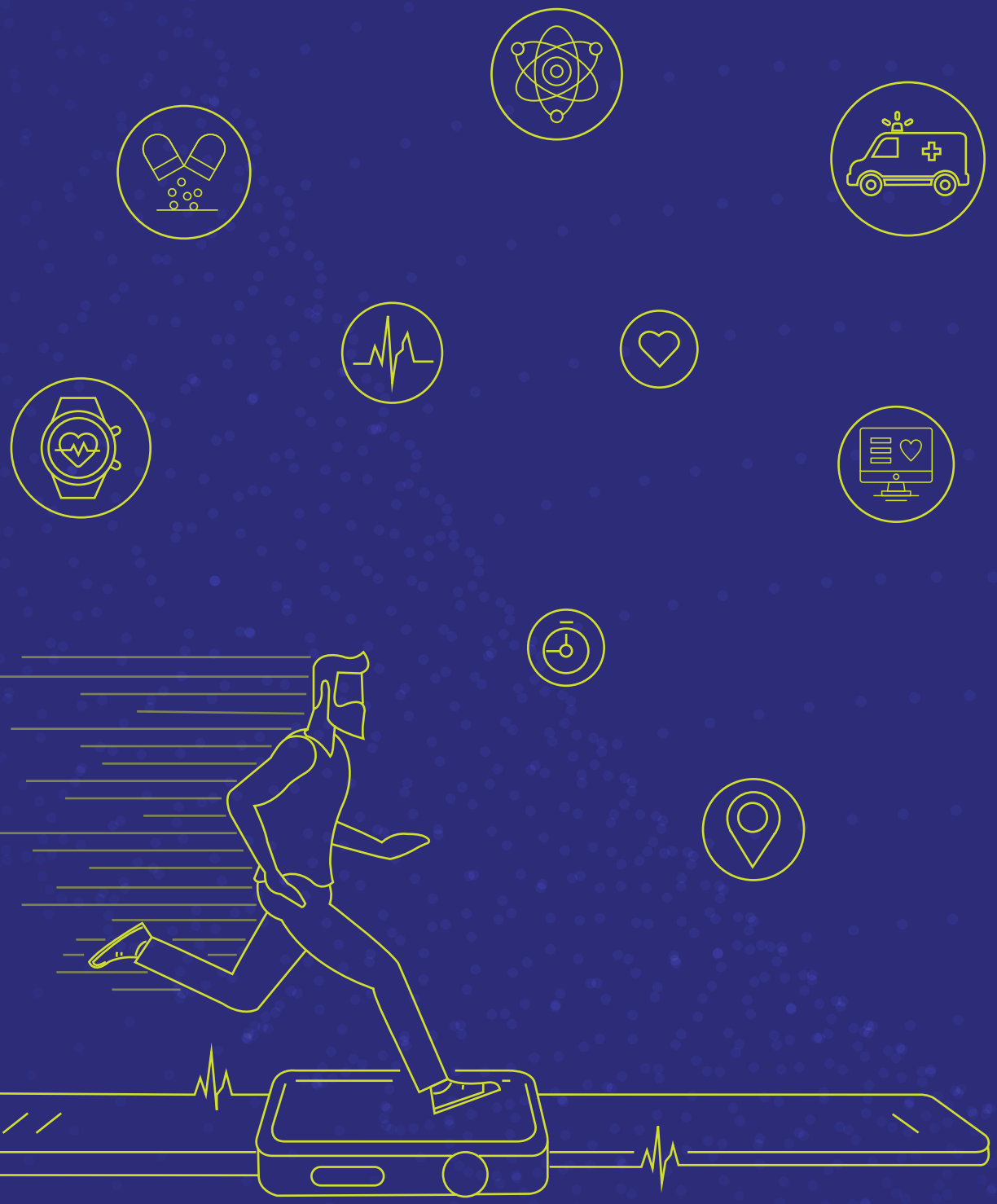
Although the healthcare sector offers critical medical services, it's plagued by a myriad of cybersecurity-related issues that are not always considered or addressed by healthcare organizations. Cybercriminals are always on the lookout to exploit the vulnerabilities that are coupled with glucose meters, blood pressure cuffs, and other devices that allow healthcare providers to automatically collect information and process the data to provide better services. Cyberattacks in healthcare have ramifications beyond financial loss and privacy breaches—a few organizations across the globe have even reported fatalities resulting from cybercrime!

With the proliferation of IoMT devices and advanced healthcare technologies, cybercriminals are also developing sophisticated tools and techniques to attack healthcare systems, steal critical data, or put healthcare operations on hold till a ransom is delivered. Privacy, safety, and security are major concerns that come with the rapid advancement of IoMT.



According to Grand View Research, the size of the global IoT healthcare market is expected to reach $534.3 billion by 2025.

This e-book talks about the various types of IoMT devices, the risks involved in their usage, cyberattack trends in the healthcare industry, the recommended security measures for every entity involved, and how ManageEngine's privileged access management (PAM) suite and other solutions help in mitigating such risks.



Categorization of IoMT devices

Categorization of IoMT devices

The notable growth of technology has paved the way for many innovations in the medical and healthcare industry. Today, medical devices are connected and wireless as opposed to the standalone, isolated devices of the past. Medical device manufacturers continue to develop new, sophisticated digital solutions that take IoMT to a whole new level. Some of such notable innovations are:

1. In-vitro diagnostic (IVD) medical devices

These devices assist in the in-vitro examination of key bodily metrics like blood pressure and blood chemistry without coming in direct contact with the patient. Closely tracking these indicators helps identify the early signs and risk factors associated with the onset of a disease, which in turn helps to treat the ailment in the initial stages. Some of the notable IVD devices are blood sugar monitoring systems and pregnancy test kits.

2. Devices to assist with recuperation

There are sensors that spare patients from spending postoperative recovery time in nursing homes and physiotherapy sessions, reducing their overall medical expenses. These wearable sensors guide patients on their exercises and provide therapists with remote monitoring capabilities to get timely understanding of the patient's behavior post treatment.

3. Prophylactic devices

Devices that actively engage and direct people with guided activities can help prevent injuries and diseases altogether. Some wearable devices can check a person's activity and detect anything unusual that might cause loss of balance and catastrophic falls. The Apple Watch is an example that uses the built-in inertial measurement unit to identify a fall or the likelihood of one and even

measure shivers pertaining to nervous system disorders.

4. Fitness tracking devices

Fitness tracking devices are equipped with sensors that can collect and analyze the physical activity data of an individual and transmit it to mobile applications. IoMT devices that fall under this category include wearables like bracelets, smartwatches, smart shirts, and smart rings, or non-wearables like sensors that can be installed under a person's bed. Users keep track of their fitness through the mobile applications connected to these sensors.

5. Clinical-grade wearables

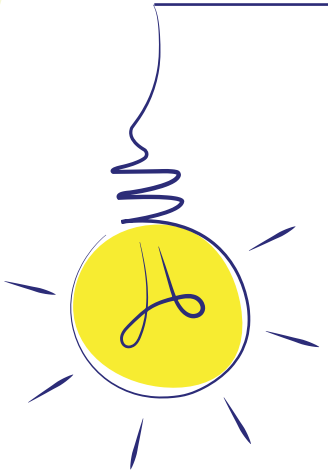
Clinical-grade IoMT devices are certified and approved by regulatory bodies and are generally used based on a physician's prescription to improve chronic health conditions and specific ailments. They're programmed to give doctors real-time health updates regarding their patients and notify physicians when a dangerous situation occurs, such as a change in white blood cell count. Examples include a wearable airbag or belt that protects people from hip injuries during a fall, and a chest strap embedded with sensors.

6. Mobile medical vehicles

Mobile medical vehicles and command units are specialized vehicles and mobile units that can be customized to deliver emergency medical treatments or any healthcare specialty like dentistry, testing labs, medical education, immunization, or blood banks. They're increasingly being used to improve health conditions in natural-disaster zones and underdeveloped or deprived communities and to provide care during multiple-injury scenarios such as road accidents or building fires.

7. Remote patient monitoring or in-home devices

In-home medical care devices include equipment like personal emergency response systems, which connect high-risk patients with local medical centers and emergency response teams. These devices facilitate virtual doctor visits and even virtual diagnoses. Information on the patient's vitals can be pulled in and medications can be prescribed virtually. Remote patient monitoring devices allow real-time monitoring of patients' vitals post discharge.



In July 2017, Brooklyn-based nursing facility Allure became the first skilled nursing facility to implement EarlySense, a remote monitoring system that tracks patients' vital signs.

8. Smart pills

Smart pills contain tiny ingestible sensor chips that get activated when they come in contact with stomach fluids, helping caregivers and doctors track patients' adherence to prescribed medication. For instance, a patient suffering from Alzheimer's would find it hard to take their medications on time. In such cases, the smart pill, upon activation, sends a message about medicine consumption to a wearable patch on the patient's arm that further transfers the information to a smartphone app. This data can also be accessed by doctors via a web portal. Abilify MyCite is a popular smart pill whose sensors get naturally discharged via the patient's GI tract after the drug is dissolved.

9. Clinical monitoring setup

Clinical monitors are one of the most important devices in a healthcare facility. These devices are used to record and store patients' health data

electronically, even in the cloud. Some examples of clinical monitoring setups include digital stethoscopes and pulse oximeters.

10. Other health devices and IoMT services

I) Ambulances that allow paramedics to access the patient's electronic medical records and provide initial consultation before admission, reducing the overall treatment time.

II) Asset tracking that helps hospital personnel quickly locate admission rooms, stretchers, and patients at any given time. Connected ventilators, monitors, and other devices enable doctors to monitor and respond to patient conditions in real time.

III) Surgical IoMT devices that enable surgeons to use a variety of digital tools and techniques during an operation.

IV) Smart contact lenses that use augmented reality to collect healthcare data. These also include microcameras that allow the wearer to take pictures with their eyes.

V) Ambient IoT sensors in nursing homes and care centers that monitor patient activities like bathroom trips and sleep timing and send out alerts when irregular patterns are detected.

VI) Mood-aware IoT devices that help address depression and other mental or emotional conditions by collecting and analyzing data such as heart rate and blood pressure.

VII) Optical IoMT devices that collect images of a person's retina, blood vessels, and optic nerve, helping optometrists detect early signs of eye diseases.

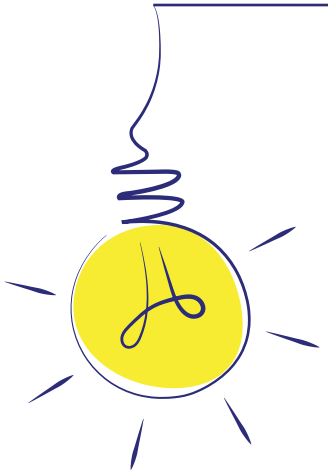
VIII) IoT-connected inhalers that help patients with conditions that usually involve sudden attacks, such as asthma, by monitoring the frequency of

attacks and identifying the environmental factors that triggered an attack. These inhalers can also alert patients when they leave inhalers at home.

IX) CAD/CAM software tools that help dentists take a 3D digital impression of their patient's mouth and create dental implants.

X) Internet-connected robots that assist surgeons in performing complex procedures with ease. Robotic surgeries can reduce the size of incisions, allowing faster healing.

XI) Laboratories and research units that use IoMT for medical trials and drug storage as well as distribution. Pharmaceutical companies can study a drug's effects through smartphones, wearables, and other sensors used by test subjects.



Forbes estimates 646 million IoT devices were used in hospitals, clinics, and medical offices in 2020.

Security and privacy challenges in healthcare and IoMT

Security and privacy challenges in healthcare and IoMT

The invention of smart medical devices and digital automation has transformed the existing healthcare infrastructure altogether. However, most IoMT devices are not completely secure by design, making them vulnerable to privacy and security compromise. Some detrimental practices and routines also put the entire healthcare network at risk. Healthcare practitioners must make it a top priority to protect personally identifiable information (PII), like phone numbers and social security numbers, and protected health information (PHI), like biometric identifiers and medical insurance beneficiary details. Explained below are some of the risks and challenges involved in healthcare IT that security experts must heed and understand to protect their network.

1. Large amount of personal data involved in healthcare

The adoption of IoMT and digital technologies has led to an upsurge in the amount of personal data generated in healthcare systems. According to security experts, by 2025, healthcare will generate more data than any other sector. With no proper data management policies in place, this gush of data generated by IoMT devices could cause potential risks pertaining to privacy and data security. Unauthorized disclosure of a patient's medical data may lead to violation of their basic rights.

Personal data is precious for identity thieves on the black market. They can hold personal records for ransom, file false insurance claims, or carry out fraudulent activities inside hospitals. According to an Infosec study, a single PHI record can fetch as much as $363 on the dark web, a far greater value than that of credit card information and social security numbers.

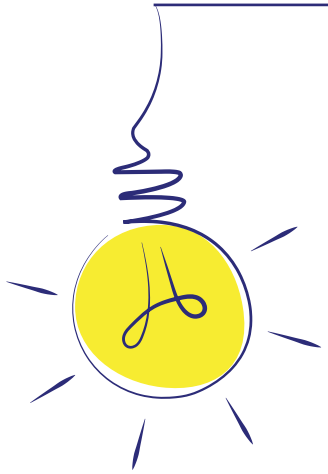
2. Poor network segmentation

Segmentation refers to the practice of splitting a network into subnetworks that are isolated from each other. Network segmentation offers many benefits, like safeguarding critical assets and information, limiting malicious lateral movement, lowering the chances of a breach, and improving performance. However, most healthcare organizations overlook network segmentation practices. As a result, any locally introduced vulnerability or malware can end up impacting the entire organization globally due to the lateral movement of data across devices and departments.

3. Security risks from insecure and outdated medical devices

Today there are millions of connected medical devices in use, most of which are insecure by design, leaving sensitive patient data exposed to attackers. A study by Palo Alto Networks revealed that over 70% of medical imaging systems run on outdated operating systems, like Windows 7, that get limited support and patching from their manufacturer, and another 27% of devices run on the long-dead Windows XP or old versions of Linux, Unix, Windows, and other embedded software.

Many healthcare organizations allow BYOD for outsourced physicians, independent medical groups, and medical students, and many of these devices are considered non-compliant. Even with good security policies in place to regulate and manage the use of personal devices, an unintentional security lapse is inevitable.



According to Paloalto Networks, 83% of medical imaging devices use unsupported operating systems

With remote work being the norm today, home devices located well outside the security perimeters of the healthcare network are also top targets for cybercriminals. Weak passwords and default IP addresses make home routers insecure and easy to hack. Attackers could exploit an unprotected home Wi-Fi network to deliver malware to the devices connected to that network, or to get access to hospital networks and activate malicious commands on other valuable assets.

4. Password hardcoding and other insecure practices

The use of hard-coded credentials that enable unrestricted access to a privileged account is one of the top vulnerabilities facing IoMT today. According to recent research by the security firm CyberMDX, dozens of medical imaging devices built by General Electric are secured with hard-coded default passwords that could be exploited to access sensitive patient scans, X-ray machines, CT and MRI scanners, and ultrasound and mammography devices. The researchers said that an attacker could trick an employee into opening an email containing malware and then use these unchanged hard-coded passwords to obtain sensitive patient data or disrupt the device from operating properly.

Some passwords are repeatedly used across different healthcare systems, clinical devices, and departments. The repeated use of similar passwords provides a backdoor into sensitive networks, threatening the integrity of healthcare infrastructures.

5. Irregular software updates and patches

Healthcare systems cannot afford to have service downtime or software updates while a medical device is being used to perform life-saving functions. However, failure to update critical software and install patches on medical devices can cause service disruptions and introduce vulnerabilities that go undetected. Consequently, most IoMT devices often continue to operate with

known vulnerabilities, making them easy targets of cyberattacks.

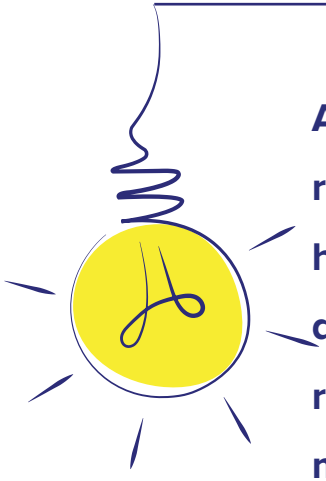
6. Unauthorized data access

Several healthcare IT teams require remote access that does not always follow cybersecurity best practices. When a healthcare staff member accesses a patient's medical record or any healthcare data without a legitimate reason and permission, there's the risk of exposure of sensitive patient information.

Healthcare organizations today are increasingly storing patient medical records in computer databases. This affects patient privacy, creating avenues for unauthorized access and identity theft.

7. Security loopholes in healthcare mobile apps

A majority of modern healthcare apps don't meet regulatory standards for legitimate information; proper, regular security updates; and compliance. In addition, most of these apps share user data with other firms, like Facebook, Google, and Amazon, which could then be passed on to other organizations such as advertising firms.



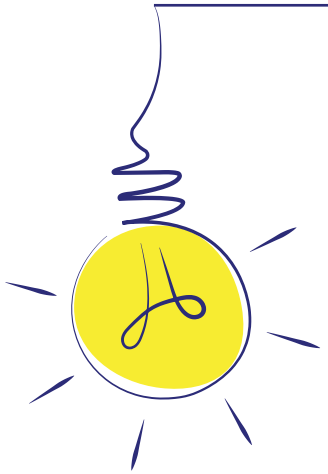
About one in four US citizens regularly or occasionally use health apps for self-diagnosis and about 64% of US adults regularly use an app to measure health metrics.

Healthcare apps promise tailored, cost-effective health assistance but often pose unprecedented risk to users' privacy by collecting sensitive information. Most of these healthcare apps do not disclose how and with whom they share user data.

8. Risks from malicious insiders

One of the biggest challenges for the healthcare sector is figuring out how to defend against insider threats. According to a Verizon report, internal misconduct accounts for 58% of all incidents in healthcare, making it the only industry where cyberharm is more often inflicted by insiders than hackers. Any individual with access to critical networks or privileged accounts could intentionally or accidentally put sensitive information at risk.

Insider threats can bring about heavy fines for compliance breaches and patient privacy violations, damage an organization's reputation, and leave the organization open to lawsuits. With an increase in the adoption of remote work, the need for improved transparency in the healthcare sector is paramount to prevent insider threats.



According to a Ponemon Study, 54% of healthcare associates say their biggest problem is employee negligence in the handling of patient information.

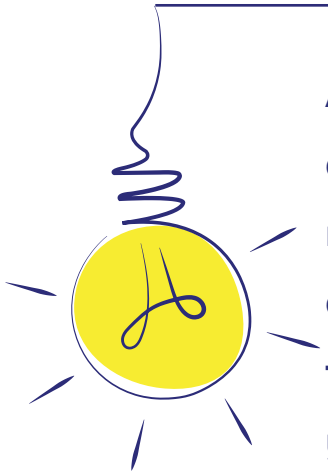
9. Risks from third parties and outsourced employees

Third parties and vendors with unrestricted access to PHI and PII represent a significant risk for the healthcare sector. Many organizations grant unlimited VPN access with open elevated privileges to various vendors and third parties. To make matters worse, some organizations don't have a complete list of vendors that have access to their network. According to a recent Ponemon

report, the average hospital has around 1,300 different external vendors under contract, like payroll, catering, and web development, each requiring some form of privileged access to perform their job duties. Managing and provisioning privileged access for each of these vendors is a major activity for healthcare administrators.

10. Increased attack surface

The proliferation of healthcare IoT devices has expanded healthcare organizations' attack surface. The COVID-19 pandemic has also prompted healthcare organizations to adopt cloud services to tackle remote access needs and scale operations, bringing in an unimaginably large attack surface. With the growth of the healthcare industry and the surge in medical device usage, hackers have discovered advanced tactics to infiltrate a system and mine for the most valuable data. Some of the most common cyberattack trends that target the healthcare industry are listed in the following section.



As many as 80% of CIOs and CISOs polled for a new report say they've experienced a breach originating with a third-party vendor in the past year, according to Healthcare IT News.

The healthcare threatscape and cyberattack trends

The healthcare threatscape and cyberattack trends

Healthcare has remained the sector most targeted by cybercriminals given the enormous amount of valuable data it holds. With the increased frequency and sophistication of attack methods, the risk and impact of breaches have also drastically increased. According to a Food and Drug Administration (FDA) report, there are an average of 164 cyberthreats detected per 1,000 connected host devices. Some of the major cyberthreats that largely target the healthcare sector are listed below.

1. Distributed denial-of-service (DDoS)

A DDoS attack is where multiple compromised systems are used to target a single system, causing that system to crash and making data unavailable. This can pose a serious problem for healthcare providers who need access to the network to provide proper patient care or who need access to the internet to send and receive emails, prescriptions, records, and other information.

DDoS attacks are typically carried out by botnets, which are a system of computers used to flood the target. These botnets are huge and can be very hard to stop.

According to a report, 4.83 million DDoS attacks occurred in the first half of 2020. The DDoS attack frequency jumped 25% during peak pandemic lockdown months (March through June 2020), and more than 929,000 DDoS attacks occurred in May.

2. Medjacking

Many insecure medical devices can be compromised by hackers looking to access or steal sensitive data from healthcare systems. Attackers usually hack medical devices, or medjack, to access and steal PII or PHI, but they can even change a patient's drug dosage to a lethal amount.

Recently, many software vulnerabilities have been identified in FDA-approved medical devices that, if exploited, could have affected patients fatally.

A verified report of such vulnerabilities detailed 11 vulnerabilities that might have affected as many as 200 million medical devices, allowing an unauthorized user to remotely hack these devices and alter drug delivery, interrupt dialysis care, or activate implantable defibrillators.

3. Theft or loss of confidential files

A recent study discovered 2.3 billion exposed files across SMB-enabled file shares, misconfigured network-attached storage devices, FTP and rsync servers, and Amazon S3 buckets. The files included a wide variety of personal information, including medical diagnostic images, passport scans, bank statements, and credentials.

Due to misconfiguration and lack of proper authentication, many of these files were accessible on the internet. Most of the exposed files were medical imaging files that contained patient names and other identifiers.

4. Ransomware

Ransomware is a type of malware that infects systems, rendering them inaccessible and inoperable until a ransom is paid. Healthcare organizations are put under immense pressure by ransom demands since failure to pay could disrupt critical medical services and put patients' lives at risk. An Emsisoft ransomware report shows that more than 759 healthcare providers in the US were impacted by ransomware in 2019.

- First surfacing in 2018, Ryuk ransomware has been the most profitable ransomware operation till date, procuring around $150 million in bitcoin payouts from its victims. According to an estimate, Ryuk is currently responsible for roughly 75 % of all ransomware attacks on the healthcare sector.

- In August 2019, California-based Wood Ranch Medical suffered a ransomware attack that held the medical records of 5,835 patients for ransom. The company's backup system

was also hacked and encrypted, making data recovery impossible. The impact was so severe that Wood Ranch Medical had to permanently stop its services.

- In October 2020, the Trickbot and Emotet trojans were key contributors to the sharp increase in ransomware attacks against healthcare providers globally. According to DHS CISA, the Emotet Trojan is one of the most prevalent threats and it typically functions as a downloader that proliferates across the network through malicious attachments in phishing emails.

5. Phishing attacks and email fraud

In a phishing attack, a hacker masquerades as a trustworthy source to lure sensitive information or data through fake emails. These emails are designed to trick users into providing sensitive information, like their credit card number, or clicking a link that leads to a fake website that looks like Amazon or another popular website. These fraudulent websites can then install malware into the users' systems, allowing threat actors to steal personal information or take control of the entire device.

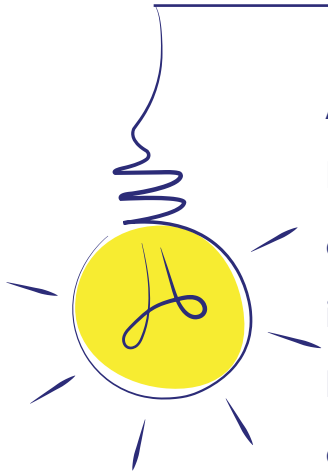
In a study, researchers sent around three million phishing emails to hospital employees with subject lines referencing mandatory training, gift cards, etc. to demand their urgent attention. Many recipients fell for the trap, leading to an astonishing 422,062 clicks. Such reckless activities could lead to the installation of malicious software on a sensitive medical system or the compromise of a privileged credential, wrecking the entire healthcare network.

6. Social engineering

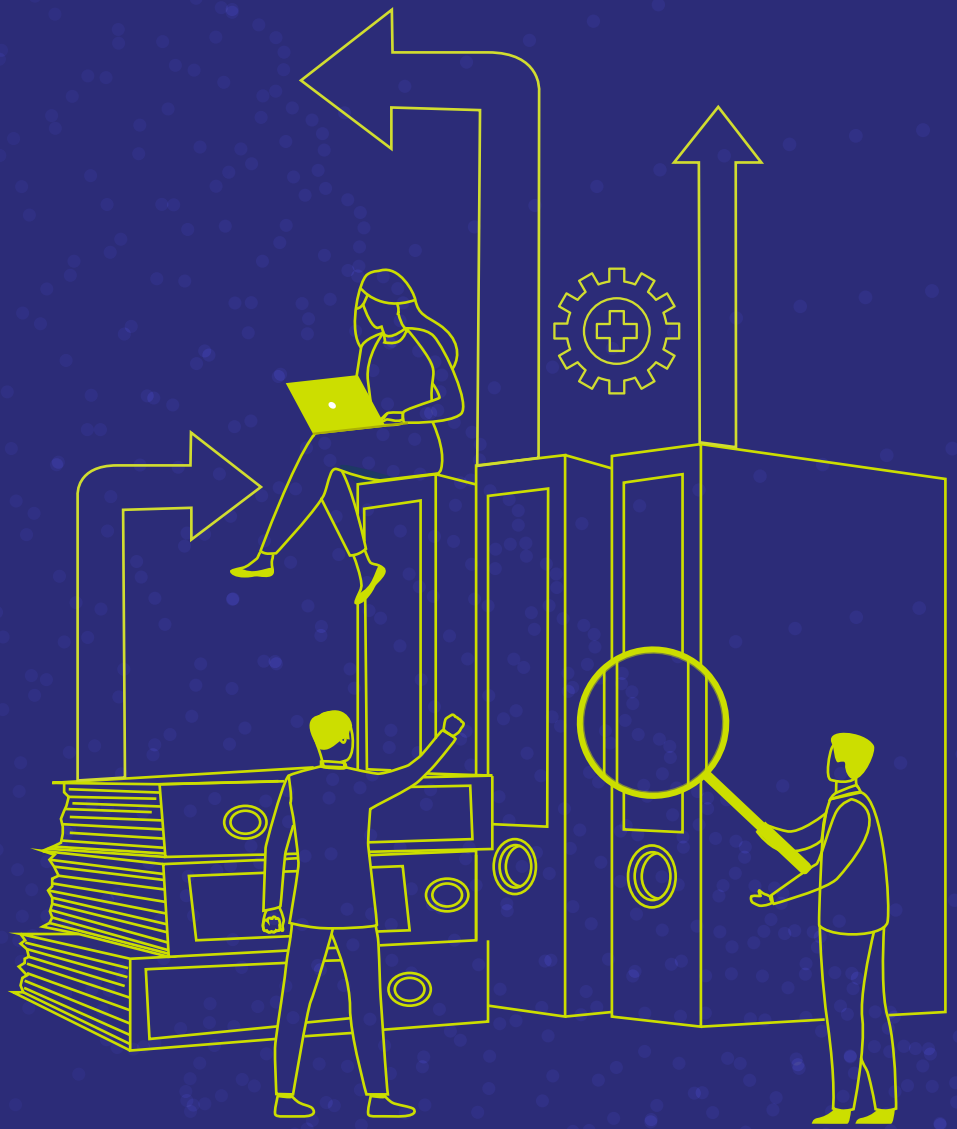
Social engineering is the process of manipulating human psychology for one's own gain. In an IT landscape, a social engineering attack often targets an enterprise's weakest link—its employees. According to HealthData Management, 99% of cyberattacks in 2019 involved some

form of human intervention, and only 1% exploited a hardware or software vulnerability.

Apart from emails and calls, social engineering could also involve a fake nurse skimming through patient files and other sensitive information, an attacker getting into the hospital through tailgating, a cybercriminal disguised as a new hire or an IT technician taking a tour through hospital rooms, etc.



According to HealthData Management, 99% of cyberattacks in 2019 involved some form of human intervention, and only 1% exploited a hardware or software vulnerability.



Adopting remediation and security measures

Adopting remediation and security measures

Considering the complexity of the healthcare threatscape and the number of entities involved, healthcare security risks should be tackled at all levels. The onus of ensuring a secure IoMT environment is not on healthcare organizations alone. Hospital staff, governments, device manufacturers, and healthcare admins must all equally take initiative to guard the healthcare industry from cybercrime. Here are some of the ways in which the entities mentioned above can help achieve secure, efficient functioning of IoMT environments.

1. Regulatory bodies

The primary focus of regulatory bodies must be on the security, storage, and transmission of PHI through connected medical devices. Since PHI is among the most valuable personal data, the policies set forth by regulatory bodies for healthcare entities must include strict data protection mandates that come with hefty penalties in case of violations.

If you regulate compliance standards or work with healthcare regulatory firms, you must monitor medical facilities, check and approve medical devices, ensure legal compliance, and improve the effectiveness of healthcare services. You must also establish rules for healthcare staff through on-site inspections to evaluate workplace practices, provide educational materials, and spread awareness regarding healthcare security best practices.

Regulatory bodies such as the FDA in the US, the Medical Device Directive that mandates CE marking in the EU, and the Central Drugs Standard Control Organisation in India have mandated various standards for medical device manufacturers based on the classification of a device and its software configurations. In addition, medical devices need to be HIPAA-compliant, and healthcare organizations must ensure that patient

information is secure and accessed only by authorized people for authorized purposes. To fully achieve these goals, it's imperative for every entity involved to adopt appropriate security measures and policies.

2. Medical device users and healthcare employees

Healthcare staff and medical device users must be educated on the secure ways of using IoMT devices and the acceptable practices in a healthcare environment. Today, a lot of healthcare data theft arises from careless employees unaware of sound security practices and not mindful of their actions; they must intuitively know that a medical device cannot be used to play online games, surf websites, or stream online entertainment. Here are some of the ways in which employees and end users can ensure safe healthcare practices and avoid violating the recommended security protocols:

- **Stay aware of HIPAA and other regulations:** Educate yourself on all areas of the concerned regulations by attending regular training or other online courses.

- **Don't share confidential patient information with anyone:** Never share private information about patients with colleagues and third-party vendors. Keep conversations regarding patients limited to the workplace and refrain from sharing confidential data or posting pictures of patient information via social media because this can lead to substantial penalties.

- **Be careful not to expose medical data:** Ensure your medical devices are password-protected to reduce theft or access by unauthorized people. Adopt multi-factor authentication (MFA) to prevent the misuse of medical records.

- **Never store medical data on insecure or unauthorized devices:** Don't share medical data via smartphones or unauthorized mobile devices since cybercriminals can easily interpret the conversation if the communications line is unencrypted.

3. Medical device manufacturers

IoMT device manufacturers must ensure their products are protected from cyberthreats, with a security design that makes the devices effective and safe for use throughout the product life cycle. Here are a few basic security measures that manufacturers can apply at the design and production stages of medical devices.

- **Invest in DevSecOps:** DevSecOps involves the integration of security at every phase of the software or product development life cycle—from initial design through testing, deployment, and delivery. Review and test the code throughout the development cycle for security issues and address them instantly.

- **Check for design vulnerabilities:** Thoroughly examine medical devices for vulnerabilities before launching them in the market. Ensure that every device can detect any disruption to its security posture and defend itself against malicious activities.

- **Introduce regular security updates and fixes:** Invest in an automatic, orchestrated process that ensures only authorized users can make changes to the device during software updates. Configure instant alerts for failed updates so the device can be replaced.

- **Provide clear instructions on device installation and configuration:** Educate patients or device users with clear instructions on how to install and configure the device. In the case of in-home devices, enlighten users on the hazards of insecure Wi-Fi networks and the need to use a secure connection to transmit data to their doctor.

- **Issue proper certificates for authorized users:** Issue certificates for healthcare devices to authenticate end users and ensure only authorized entities can access the device. Use digital certificates to encrypt healthcare data and sign the messages sent to a medical device, keeping the data private and intact.

4. Healthcare organizations

With an alarming surge in the number of connected medical devices, healthcare organizations should increasingly focus on IoMT security and the recommended best practices. Once a medical device is exposed to the internet, healthcare organizations need to be cautious of the potential threats and proliferation of malware. Below are some of the ways healthcare administrators and security heads can contribute to a secure working environment and achieve a strong defense strategy against cyberthreats.

- **Know your IoMT environment and devices:** Gain visibility into all the devices on your network and ensure you know about the types of threats they're susceptible to. Place better threat detection controls around vulnerable devices and establish a centralized security strategy to bridge any gaps across operations. Ensure no device auto-connects to your network without undergoing a cybersecurity risk assessment.

- **Implement password management policies:** Change all default passwords to strong ones for all devices and their users. Adopt advanced technologies to identify hard-coded credentials and instantly remove them. Enforce stricter policies on password sharing among employees and third parties to prevent password abuse.

- **Enforce MFA:** Implement an MFA strategy to prevent many of the most serious vulnerabilities on all endpoints across the

healthcare network. Microsoft data shows MFA blocks 99.9% of all automated cyberattacks.

- **Introduce network segmentation:** Gain insights into data flow across different departments inside the perimeter by internally segmenting the network. You can also rely on Internal Segmentation Firewalls that can detect and prevent the movement of malware or malicious code from one segment to another, thereby isolating the threat. This way, you can prevent devices from talking across your network and stop hackers from gaining unrestricted access to data inside the network.

- **Grant access to sensitive systems only when necessary:** Grant trusted, authorized entities secure remote access to medical systems on a role-based, least privilege basis. This will prevent unauthorized users from gaining access to sensitive data for an unlimited amount of time.

- **Embrace a Zero Trust, least privilege policy with integrated controls:** Don't implicitly trust the people, devices, services, applications, and networks that require access to the corporate network. Each of these entities represents a threat vector that needs to be verified explicitly, checked for anomalies, and monitored for risky behavior. A robust Zero Trust security model involves three key principles:

  - **Verify explicitly:**
    Scrutinize and validate every access request made by users, endpoints, applications, and networks before granting access. Know why they need access and for how long.

  - **Enable least privileged access:**
    Strengthen security by enabling granular access controls with risk-based policies,

while enabling users to elevate their privileges for just the required time frame when the situation calls for it.

- **Assume a breach will occur:**
  Assume that every entity requesting access is likely to cause harm and perform a malicious action. Use AI- and ML-based strategies to detect and mitigate threats across your hybrid environment.

- **Continuously monitor your entire network:** Monitor, scan, and detect vulnerable or comprised IoT devices on your network to safeguard against security issues. It's recommended to deploy a tool that can monitor all the traffic to and from IoMT devices and restrict unsafe communication between the devices and external entities.

- **Invest in antivirus software and firewalls:** Install antivirus software on medical devices and update them with security patches regularly. Also install a firewall and configure it to limit traffic between the network and IoMT systems to only necessary ports and IP addresses.

- **Conduct regular risk assessments:** Conduct regular risk assessments to proactively mitigate potential risks by identifying security vulnerabilities and shortcomings across the healthcare network. Evaluate security risks periodically to avoid costly data breaches, reputation damage, and penalties from regulatory agencies.

- **Ensure compatibility in data across all medical devices:** Maintain a unified console to consolidate data gathered from different types of medical devices using different types of protocols. To leverage IoMT to its full potential, ensure consistency and compatibility of data rendered by different devices.

- **Regularly back up data to a secure location:** Regularly back up data with strong encryption and controlled access to ensure that life-saving data is secured.

Achieving a holistic IoMT security posture with ManageEngine

Achieving a holistic IoMT security posture with ManageEngine

Modern healthcare systems need a comprehensive program to proactively protect against the various security risks discussed in this e-book and detect and respond to attacks in progress before attackers wreak havoc on the entire network.

ManageEngine provides an all-inclusive suite of powerful enterprise IT security products aimed at making businesses more effective and efficient. This includes solutions for PAM, network utilization, performance monitoring, device security, help desk management, email archive management, and real-time QoS management. As novel healthcare practices replace traditional methods, ManageEngine helps the healthcare sector achieve a holistic approach to ensuring IoMT security and offers a myriad of benefits, including:

- Elevating patient and employee experiences.
- Ensuring continuous availability of critical applications and resources.
- Providing secure access to all users and governing the privileges and access controls of the expanding workforce.
- Securing ePHI against loss or any form of breach of privacy, integrity, or confidentiality.
- Implementing modern network infrastructure and optimizing IT operations to perform efficiently across distributed or hybrid environments.
- Supporting legacy systems with automatic updates, vulnerability patches, and other maintenance routines.
- Leveraging AI- and ML-driven capabilities to proactively monitor critical systems in real time, detect intrusions, and prevent cyberattacks.
- Fortifying cybersecurity by protecting the organization's network, IT assets, and data against underestimated external threats.
- Ensuring compliance with complex healthcare regulations, such as HIPAA and HITECH.

Major ManageEngine solution suites that help secure various avenues of the healthcare landscape

ManageEngine offers a myriad of IT solutions that readily integrate with each other, enabling over 180,000 organizations across the globe and in various industries to secure their IT environment with a holistic approach. Delving into the details of how every single ManageEngine product helps healthcare organizations fortify their IT security is beyond the scope of this e-book, but here's a glimpse of the major solution suites and their key capabilities.

1. Service management:

A suite of help desk and service tools that offer the best support to employees and customers and help minimize disruptions. They help healthcare organizations:

- Streamline service delivery with proven ITSM best practices.
- Resolve tickets quickly and improve service availability.
- Standardize service delivery with visual process workflows.

2. Security information and event management:

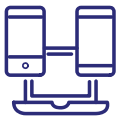
SIEM solutions that defend healthcare networks against threats, data breaches, and attacks by constantly monitoring and analyzing security data. These tools can:

- Detect and inspect threats with rule-based correlation.
- Spot anomalous user and entity behaviors.
- Uncover attackers' behavior with rapid forensic analysis.
- Automate incident response workflows.

3. Identity and privileged access management:

A powerful suite of products to manage user directories and digital identities across your IT environment and regulate access to critical resources. These tools enable admins to:

- Authenticate and authorize users across multiple platforms and provide single sign-on capabilities.
- Control, track, and audit privileged access to critical IT systems.
- Prevent privilege escalation with role-based access control.
- Meet compliance demands with audits and access policies.



4. Unified endpoint security management:

Device management tools that secure the ever-increasing number of endpoints, including desktops, laptops, mobile devices, and browsers. These solutions help:

- Manage heterogeneous endpoints and automate routine tasks.
- Troubleshoot systems remotely and securely.
- Secure endpoints to protect networks from zero-day attacks.

5. IT operations management:

Tools that help healthcare firms manage and monitor all the layers of their IT networks, servers, and applications. They can also:

- Monitor network hardware, virtual machines, and storage devices for health, performance, and storage space.
- Periodically back up startup and running configurations.
- Avoid downtime by tracking faulty configuration changes.
- Analyze and enhance firewall and internet security.

6. IT analytics:

AI- and ML-based tools that collect, analyze, and report on IT operations data to gain the necessary insights needed to optimize healthcare IoMT. These advanced tools help healthcare organizations:

- Blend data from multiple sources and make faster decisions.
- Securely share data and collaborate in real time.
- Forecast behavioral trends based on real-time patterns.
- Manage their budget and provide cost analytics for the public cloud.

ManageEngine PAM360: A unified privileged access management solution

ManageEngine PAM360: A unified privileged access management solution

PAM360 is a web-based solution from ManageEngine that defends enterprises against privilege misuse through powerful privileged access governance, smoother workflow automation, and advanced analytics. PAM360 readily integrates with various IT security solutions, enabling admins to correlate privileged access data with different avenues of their healthcare network for meaningful inferences and quicker remedies. Here are some of the ways that PAM360 helps healthcare organizations combat cyberthreats and maintain a healthy IoMT environment.

1. Automatically discover all privileged accounts in your network:

Most organizations don't have a complete list of the privileged accounts in their network. PAM360 helps prevent risks from stale, abandoned, or orphaned accounts by automatically discovering all privileged accounts that are used to gain access to sensitive systems and storing them all in a secure, encrypted vault.

2. Encrypt all your sensitive data—at rest and in transit:

Encryption is one of the most effective data protection methods for healthcare systems, making it almost impossible for attackers to decode patient data even if they gain access to it. PAM360 provides healthcare organizations with various options to implement strong data encryption measures best suited for their workflow, like the default AES-256 algorithm, SafeNet Luna PCIe HSM, FIPS 140-2 validated cryptography, or custom cryptography algorithms.

3. Improve authentication, authorization, and access policies:

To prevent unauthorized access by intruders, healthcare organizations must fortify the process of authenticating users into privileged accounts and restrict their actions during a particular session. This will give healthcare security heads the right to dictate who has privileged access and what exactly they can do with it. Healthcare organizations in particular must limit the number of privileged accounts they authorize for access. It's also essential that employees who leave the organization are instantly removed from the hospital network to prevent any detrimental activity—deliberate or unintentional—from their end. PAM360's granular access controls help bolster data security by limiting access to protected patient information to only those users who require access to perform their job.

4. Adopt automation capabilities:

Automation helps prevent human error, achieve greater visibility into every privileged action, and improve collaboration between various avenues of the IoMT network. It can be used to dynamically segment traffic, preventing malware in a compromised device from spreading laterally across the rest of the healthcare network. PAM360 helps track, detect, and patch vulnerable devices, apply or update security protocols, and modify policies in real time to acknowledge detected threats.

5. Provide secure remote access to the corporate network:

Healthcare organizations must invest in a secure remote access tool to grant privileged users with authorized, timely access to systems and applications in the network. It's also important to secure third-party access to privileged accounts that can expose the corporate network to external threats. PAM360 enables tunneled RDP, SSH, VNC,

SQL, and web access to critical systems with a single click, without the need for passwords.

6. Monitor user activities in real time:

One of the integral aspects of a PAM strategy is to monitor and shadow privileged sessions in real time. PAM360 screens all traffic to and from IoMT devices, enabling organizations to detect anomalous or malicious activities and instantly terminate the sessions to prevent potential attacks.

7. Maintain session recordings:

Having session recordings stored in a secure location ensures there's unalterable video proof for every privileged activity carried out in a particular session. PAM360's session recordings can be searched and traced back to a particular date or time, enabling security heads to identify malicious sessions and catch the intruder in time.

8. Easily demonstrate compliance with audit logs:

A detailed, tamper-proof audit trail of every privileged session helps organizations show compliance with various regulations, like HIPAA. PAM360's audit trails log every privileged activity, enabling security teams to scrutinize who is accessing what system, when, and from where. A comprehensive audit trail also helps security teams spot the entry points, determine the cause, and assess the damages should an incident occur.

9. Invest in privileged behavior analytics and threat detection tools:

PAM360 integrates with privileged user and behavior analytics tools that enable organizations to respond to anomalous activities instantly. These tools can capture all relevant threat-based intelligence data from across individual networks and correlate this intelligence with privileged access data rendered from the entire network, improving transparency and visibility into all

privileged activities. Security heads can then make well-informed business decisions or alter the existing security policies to better suit the circumstances.

10. Integrate SIEM capabilities into your PAM strategy:

PAM360 helps healthcare organizations seamlessly integrate SIEM solutions into their privileged access security strategy. SIEM tools can detect and evaluate threats in real time by correlating audit logs from PAM360 with network data from every solution deployed across the network. This cross-correlation provides healthcare IT teams with deeper insights into security incidents occurring across the distributed, hybrid environment.

Real-world scenarios

Below are two real-world use cases where PAM360 enables one of the leading medical equipment manufacturers in the US to tackle major challenges in securing IoMT systems:

i) Managing and securing critical endpoints:

The firm mentioned above manufactures, sells, and ships radiation oncology treatment devices to many hospitals and clinics across the globe. Since these devices are expensive and critical, they must be managed and monitored continuously to ensure good health and performance. The company overcomes this challenge through PAM360. Along with the hardware equipment, they also ship a server, usually a Windows machine, that has a PAM360 agent embedded inside it. This agent registers the equipment as an endpoint in PAM360, enabling admins to rotate its passwords remotely, monitor its functioning in real time, and manage privileged access to it by authorized users.

ii) Enabling secure remote access for technicians and maintenance staff:

In the above example, once the equipment is shipped to a remote location, the company hires consultants to monitor and configure the medical devices. The equipment manufacturer also sends their technicians to carry out periodic maintenance operations on the equipment. Using PAM360's mobile application, the technician can request access to the endpoint with a valid reason, and the admin can provide them with a one-time password that enables time-limited, least privileged access to the endpoint. PAM360 then automatically resets the equipment password once the task is completed.

Conclusion

Conclusion

The healthcare industry is and will remain one of the prime targets of cybercriminals owing to the huge volume of valuable patient information. With an ever-expanding healthcare ecosystem, it's imperative for healthcare systems to have robust security measures in place. Healthcare organizations should also have continual awareness of IoMT challenges and the best security practices to follow. Since most of the security incidents within the healthcare industry are attributed to unrestricted access to critical medical information, managing and securing privileged access is important. Adopting a Zero Trust strategy with clearly defined access control policies will go a long way towards protecting the integrity of valuable patient data and preventing access misuse.

Most of the PAM offerings in the market today are built to function as a standalone program. In this digital age where unification is the new norm, it can be a struggle for organizations to run PAM as a point solution. ManageEngine PAM360 is a robust PAM solution that provides complete privileged access security across your entire enterprise network. It fortifies your overall security strategy by contextually integrating with other IT security tools, helping you run a modern, effective PAM program with better service delivery. With healthcare IoMT becoming widely distributed and extensive, PAM360 enables you to keep your PAM agenda flexible, risk-based, and open to innovation.

Learn more about ManageEngine PAM360 and its IoMT security offerings.

Take me to the website

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360