

# HEALTHCARE CYBERSECURITY REPORT

Q1 2022



# A WORD FROM THE EDITOR

MIRKO ZORZ, EDITOR IN CHIEF, HELP NET SECURITY



Since the start of the COVID-19 pandemic, security incidents at healthcare organizations have become more common. This not only increased costs for an already struggling industry, but inflicted a burden on the individuals whose personal information was exposed.

To make matters worse, healthcare organizations have an abundance of legacy equipment, most of it vulnerable to attack. Cynerio researchers found that security threats related to IoT and related devices within healthcare environments have remained sorely under-addressed, despite increased investments in healthcare cybersecurity. Data shows that 53% of connected medical devices and other IoT devices in hospitals have a known critical vulnerability.

As exhausted healthcare professionals worldwide struggled with an extraordinary situation, their IT departments faced critical skills and staffing shortages. In fact, research from Critical Insight found that those

departments continue to be stretched so thin dealing with pandemic-related crises that routine security measures may fall by the wayside, breaches may go undetected for weeks, and efforts to validate the security measures undertaken by affiliates and third parties may fall short.

The idea behind this report is to provide you with an overview of the information security issues healthcare is dealing with, offer expert insight on what is needed to move defense capabilities in the right direction, and provide food for thought for those working to protect healthcare infrastructures worldwide.

A stylized, handwritten signature in white ink, likely belonging to Mirko Zorz, positioned in the bottom right corner of the page.



# TABLE OF CONTENTS

<b>2</b>	<b>Impressum</b>
<b>4</b>	<b>Healthcare cybersecurity: The current lay of the land</b>
<b>12</b>	<b>As medical devices become more advanced, security becomes critical</b>
<b>16</b>	<b>How to reduce critical healthcare IoT cyber risks and respond to live attacks</b>
<b>23</b>	<b>The importance of improving technology to keep healthcare organizations secure</b>
<b>26</b>	<b>Out of the pan and into the fire: From pandemic to threat of cyber war</b>
<b>30</b>	<b>Do we need another major breach to take the security of connected medical devices seriously?</b>
<b>34</b>	<b>Safeguarding medical devices from vulnerabilities and cyber attacks</b>
<b>47</b>	<b>Moving your healthcare organization to the cloud? Here's what you need to know</b>
<b>51</b>	<b>Despite private storage, healthcare organizations are a top target of ransomware</b>

---

Report by Help Net Security  
[www.helpnetsecurity.com](http://www.helpnetsecurity.com)

# HEALTHCARE CYBERSECURITY: THE CURRENT LAY OF THE LAND

**If there was ever any doubt that the healthcare sector is part of a nation's critical infrastructure, one just needs to recall the disruption that ensued when, in May 2021, Conti ransomware hit the Irish Department of Health and the Health Service Executive, an organization that provides public health and social care services in all of Ireland.**

**Zeljka Zorz**, Managing Editor, Help Net Security

**The disruptions of service that some cyber attacks lead to have immediate negative consequences, but the compromise of sensitive data also leads to long-lasting ones.**

According to a recently released post-incident review by PwC analysts, "many hospitals were forced to cancel outpatient appointments completely, while others were operating with significant delays." Also, the incident had a "significant impact" on diagnostic services and radiotherapy services, "with cessation of radiation treatment across the five HSE centres." For some of the affected patients, this incident likely had grave consequences.

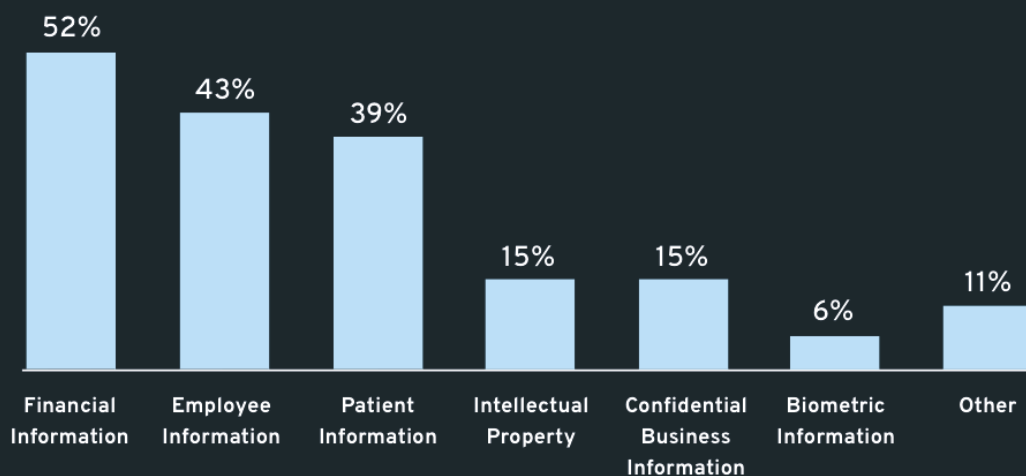
But it's not only the patients who are harmed by this (unfortunately predominant) type of attack: the employees' day-to-day work is

thrown in disarray and they can't discharge their duties.

Also, cyber attackers that go after organizations in the healthcare sector don't limit themselves to stealing only patient records. According to the results of the 2021 HIMSS Healthcare Cybersecurity Survey, threat actors usually go after financial and patient information (both types of data are contained in electronic medical records, the former to enable billing), but often grab employee information, as well.

The disruptions of service that some cyber

**TARGET(S) OF THREAT ACTORS FOR MOST SIGNIFICANT SECURITY INCIDENT**



*SOURCE: The 2021 HIMSS Healthcare Cybersecurity Survey*

attacks lead to have immediate negative consequences, but the compromise of sensitive data also leads to long-lasting ones – to name just a few: identity theft, extortion, loss of patients' trust, and considerable monetary loss by the healthcare organization.

On that last point: The Ponemon/IBM Security Cost of a Data Breach Report 2021 says the average cost of a healthcare data breach has reached \$9.23 million.

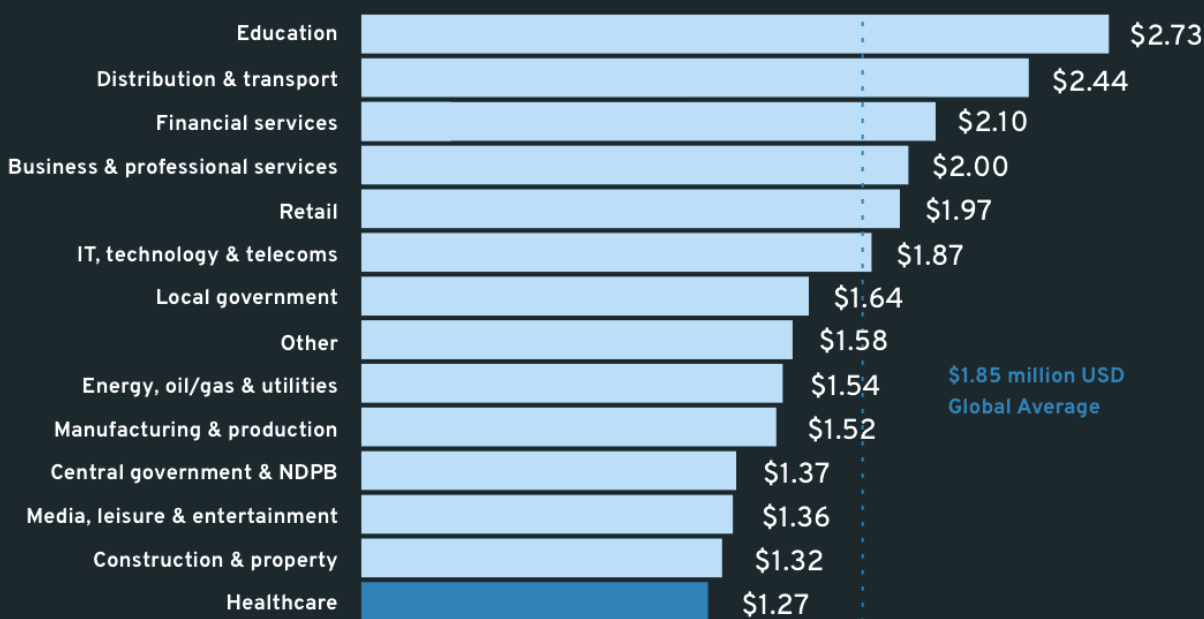
But, according to the Sophos State of Ransomware in Healthcare 2021 report, healthcare has the lowest ransomware recovery cost of all sectors (\$1.27 million) – though, with two caveats: healthcare

organizations' remediation efforts are often limited by low budgets, and given that in many parts of the world healthcare is a public service, people have little choice but to use certain healthcare facilities, meaning the reputational or opportunity costs are lower than in other sectors.

### Who are the targets?

According to Critical Insight's H2 2021 Healthcare Breach Report, which is based on the breaches reported to the U.S. Department of Health and Human Services (HHS) by healthcare organizations, there were 679 breaches of unsecured protected health information affecting 500 or more

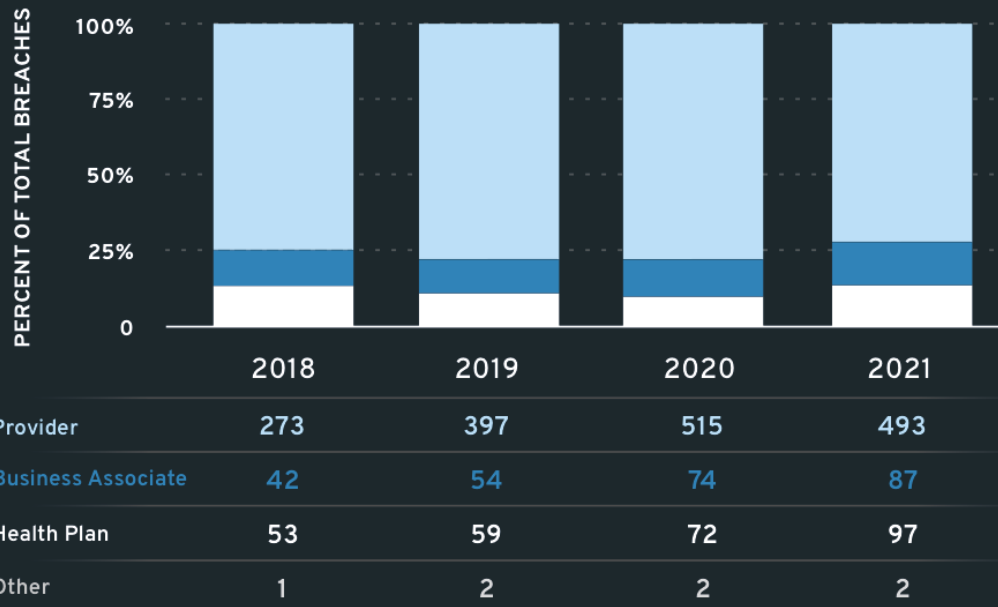
#### AVERAGE RANSOMWARE RECOVERY COST (DOWNTIME, RANSOM PAID, HOURS LOST, ETC.) BY SECTOR



SOURCE: The State of Ransomware in Healthcare 2021 report by Sophos and Vanson Bourne



## BREACHES BY ENTITY



SOURCE: Critical Insight H2 2021 Healthcare Breach Report

individuals in 2021. Of those, 500 were caused by hacking or IT incidents.

It must also be pointed out that while healthcare providers remain the most targeted entities in the sector, in 2021 attacks against health plans increased by nearly 35%, and against business associates/third party vendors by nearly 18% when compared to the previous year.

"Business associate-related breaches accounted for nearly 13% of total breaches, but almost one quarter of the total individual records [exposed]," Critical Insight's analysts also determined.

Of course, attackers are not limiting themselves to hitting U.S.-based organizations – victims are spread all around the world. In the past year, ransomware

**In 2021 attacks against health plans increased by nearly 35%, and against business associates/third party vendors by nearly 18%.**

gangs have hit the Macquarie Health Corporation, UnitingCare and Eastern Health in Australia, a hospital in Villefranche and the Dax hospital center in the Landes (France), the Handa Hospital in Japan's Tokushima Prefecture, the healthcare system in the Canadian province of Newfoundland and Labrador, a Singaporean eye clinic, a medical diagnostics provider in Brazil, the Hillel Yaffe Medical Center in Israel, and many others.

Healthcare organizations are, in many ways, perfect targets for attackers: they hold and share a lot of sensitive and valuable data, which flows throughout their networks but also third-party ones (business associates, insurers, third-party healthcare partners, and so on), and most of these networks are vulnerable to outside attack due to a variety of factors.

For example: CynergisTek's State Of Healthcare Security & Privacy 2021 Annual Report has found that many U.S. healthcare organizations fail to conform to the [HIPAA Security Rule](#) and way too many fall short when it comes to [NIST Cybersecurity Framework](#) conformance.

The PwC's post-incident review has revealed that even an organization as important to the nation as the HSE made many security mistakes that made the attack possible (and its fallout likely worse than it should have been): it had no CISO, no security monitoring capabilities, no cyber incident response playbooks, no thorough IT recovery plans...

It should not surprise us, then, that many healthcare organizations with considerably less resources – e.g., family medicine clinics, outpatient facilities, specialists' offices,

nursing homes, hospices, dental offices – fall victim to cyber attacks.

## Healthcare organizations' weak spots

Compared to organizations in other sectors, healthcare organizations have the added disadvantage of dealing with a constantly expanding attack surface fueled by:

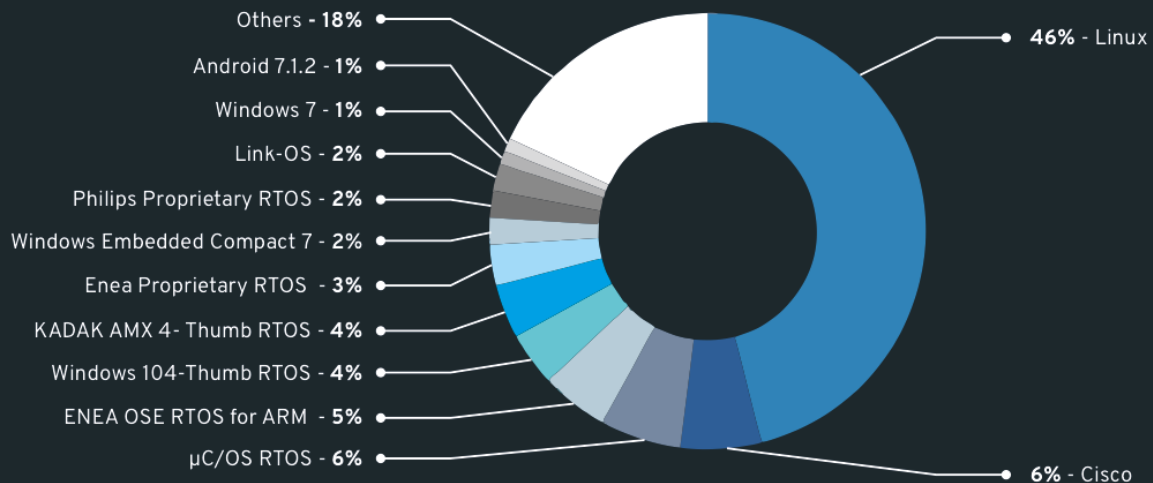
- The rapid adoption of telehealth technology
- IoMT (patient monitors, infusion pumps, ultrasound machines, etc.)
- IoT, OT and control systems (IP cameras, VOIP phones, HVAC, pneumatic tube systems, physical security systems, etc.)
- Legacy devices
- Many and diverse supply chains and partnering third parties

Many healthcare organizations use devices that run on legacy operating systems. Also, many older healthcare IoT devices have not been designed with cybersecurity in mind but replacing them is out of the question because of associated cost.

Cynerio's recently released IoT Device Security 2022 report lays bare the extent of the problem:

- IV pumps and patient monitors are the most common healthcare IoT devices in hospitals (38% and 19% of IoT/IoMT devices, respectively), and 73% of those IV pumps have an exploitable vulnerability

## TOP OPERATING SYSTEMS OF HEALTHCARE IOT DEVICES (BY PERCENTAGE OF TOTAL IOT DEVICES)



SOURCE: *The State of Healthcare IoT Device Security 2022 report by Cynerio*

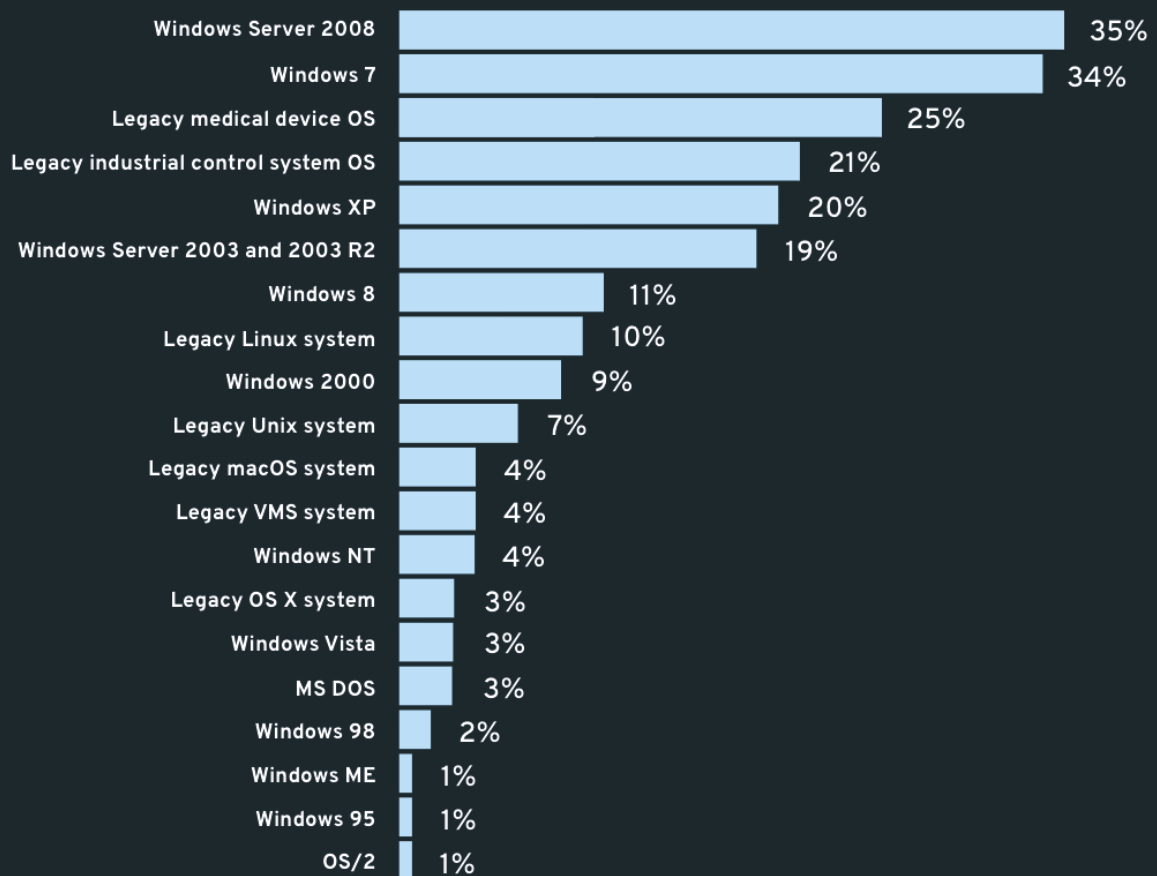
- The variety of operating systems running on healthcare IoT devices is considerable, and many of them can't have security solutions installed on them
- Healthcare IoT running outdated Windows versions are prevalent in critical care sectors like pharmacology, oncology, and laboratory services (65%, 53% and 50%, respectively)
- Manufacturers of healthcare IoT are much more diverse than computer or mobile phone manufacturers, and keeping all those devices secure – even just patched within a reasonable timeframe – is a complex endeavor

"Unsupported legacy operating systems are commonplace in healthcare organizations and the footprint is growing," the 2021 HIMSS Healthcare Cybersecurity Survey has also revealed. "Some healthcare organizations may not necessarily be planning for obsolescence of these operating systems."

### **Slim cybersecurity budgets and not enough cybersecurity staff**

Budget is the biggest security challenge for nearly half of the 167 healthcare cybersecurity professionals polled by HIMSS in the above mentioned survey, which means that many healthcare organizations must carefully pick and choose their next

### LEGACY (UNSUPPORTED) OPERATING SYSTEMS IN PLACE AT RESPONDENTS' ORGANIZATION(S)



SOURCE: 2021 HIMSS Healthcare Cybersecurity Survey

cybersecurity investments.

The good news is that most respondents (59%) said that their cybersecurity budgets have increased in 2021.

But in light of the fact that phishing, human error and social engineering are the predominant initial points of compromise for

security incidents, it's interesting is that these increases have been funneled much more towards buying and upgrading security solutions and increasing cybersecurity staff than towards security awareness training and cybersecurity training for IT and IT security staff.

That's not to say that cybersecurity staff is



## IMPACT OF CYBERSECURITY BUDGET INCREASES – 2020 TO 2021

Outcomes	Percentage
More upgrades of security solutions	63%
More acquisitions of new security solutions	56%
Increase in cybersecurity staffing	53%
More maintenance of existing infrastructure	48%
More security risk assessments or more comprehensive security risk assessments	48%
More robust security risk management	47%
Increased security awareness training	34%
More frequent penetration testing	31%
Increased cybersecurity training for IT & IT security staff	28%
Other	2%

*SOURCE: 2021 HIMSS Healthcare Cybersecurity Survey*

not important, or more of it sorely needed.

According to the Ipsos's Perspectives in Healthcare Security report (sponsored by CyberMDX and Philips), almost half of the 130 hospital IT and IT Sec executives and BioMed technicians and engineers they polled said that they find their medical device and IoT security staffing inadequate.

"Conversely, the industry has been experiencing a cybersecurity talent shortage and 100+ day lag to fill jobs," Ipsos analysts found.



PATRICK MAW, MEDICAL DEVICE CYBER SECURITY EXPERT,  
UNIVERSITY COLLEGE LONDON HOSPITALS NHS  
FOUNDATION TRUST

## AS MEDICAL DEVICES BECOME MORE ADVANCED, SECURITY BECOMES CRITICAL

---



As medical devices become smarter and more connected, cybercriminals become stealthier, which emphasizes the importance of enhancing the security of such devices to protect healthcare organizations as well as their patients.

**Mirko Zorz**, Editor in Chief, Help Net Security

## **What type of damage can attackers do if they take control of a connected medical device? Can there be a threat to patient safety?**

Most imaging devices – ultrasound machines, CT and MR scanners – have had the ability to be connected to networks for many years, and now many other devices are following this trend. On the other hand, most of the critical life support medical devices are limited in their connectivity.

Medical devices are connected to hospitals' network so that data can be extracted and included in centralized electronic patient records (EPRs). There are ways to enable this while reducing hackers' ability to compromise these devices. There are standard network protection mechanisms such as segmentation. So, the answer to the question is: Yes, there is danger in having medical devices connected to the organization's network, but this danger can be minimized or eliminated through good design of how these devices are connected.

## **What challenges do medical device manufacturers face when it comes to securing their devices? Why do so many devices have weak or no security?**

A significant challenge to manufacturers of medical devices is the regulatory framework for certifying that the devices as safe to use. This regulation means that whenever flaws in commonly used operating systems such as Microsoft Windows are identified, it will take

time for updates to be approved for release to solve the issue. This creates issues with how the devices are deployed in healthcare organizations, because devices could be compromised while waiting for the approved update. Regulations also limit or restrict the use of other protective measures such as antivirus or agent-based intrusion detection systems.

Historically, devices were not intended to be networkable but EPRs forced that need. The problem is that, from the outset, they were not designed with defensive measures appropriate for networkable devices and


adding on security is never as good an option as implementing it from the get-go.

Also, some companies are naïve to the threats of hacking and don't even consider protecting their devices. Some use inadequate

protection (e.g., antivirus, but with rarely updated signatures), so they can confirm to potential customers that they do have protective measures. They can sell the device, but they are presenting the customer with vulnerabilities. Another example is the inclusion of a firewall on the device but without any rules to restrict traffic, which is also pointless.

Finally, cyber threats are constantly evolving, and it is difficult to keep up with the changes due to lack of suitably trained staff.

## **If you could influence the development process of a connected medical device,**



**There are standards available to give guidance on how devices are managed when they are connected to an organizational network.**

**what security measures would you implement from the get-go?**

I would insist on a constant review of current security practices, with the aim to include the latest techniques in the protocols for interconnection. There needs to be a whole spectrum of choices – from simple to complex – to accommodate the different practices within healthcare organizations.

**Most medical devices tend to be in use for years and even decades. They can use a legacy operating system, lose updates and support along the way. How can a hospital make sure their equipment is secure in the long run?**

The obvious solution is to replace the devices on a regular basis, i.e., between 5 to 10 years. But they are generally used at least until manufacturer support is withdrawn, and sometimes even until they are unable to be repaired under best efforts contracts.

The standard solution is to segment the network and place medical devices on isolated virtual or actual LANs, with appropriate firewalling at the boundaries. There are also several AI-based intrusion detection systems that can detect when devices are compromised, and intelligent networks that can then isolate a device until the compromise has been resolved. It is,

therefore, possible for organizations to safely use legacy devices.

**What advice would you give to the CISO of a large hospital that deals with thousands of connected medical devices? Is there a way to increase their security in general, especially when dealing with a multitude of devices from different manufacturers?**

There are multiple ways to protect non-medical devices that are also applicable to medical devices. These include segmentation with firewalls, implementing AV and updating devices where and as soon as possible, and using the latest AI-based intrusion protection solutions. There are also systems that can provide up to date threat intelligence on medical devices so that resources can be funneled to the ones that present the most risk.

It's essential to be on good terms with the medical device experts within your organization. They can give you an accurate inventory of the devices that are capable of being networked and those that are, so you can be sure that all devices have been accounted for and secured.

**Are there regulations and/or laws in the works that are aimed at improving medical device security? If there are,**



## **how long do you think until we're starting to see their influence?**

There are standards available to give guidance on how devices are managed when they are connected to an organizational network. An important one is ISO 80001 and all its technical reports that give guidance based on a risk assessment and management strategy that allows devices to connect while ensuring patient safety, interoperability data security and enhancement of delivery of care. ISO 80001 has been around for around 10 years and is in the process of being updated, but the update leaves a lot to be desired.

There is also the Data Security and Protection Toolkit (DSPT), which covers mostly standard IT but has recently been updated to cover connected medical devices. It obligates organizations to have an inventory of medical devices that are networked.

Unfortunately, standards are not always widely publicized and are often unknown to those who should follow them. There are some initiatives from bodies such as NHS Digital to bring together the community of cyber professionals to share knowledge, and this is a good start.

## **What should legislators keep in mind if they want to create laws that can realistically work given the current situation on the ground?**

Lawmakers should always consider the practical application of laws and standards and keep in mind that the real world often has many variations and complexities. They need to engage with knowledgeable groups

or individuals to ensure that what they are proposing is realizable in healthcare organization of different shapes and sizes.

They should make sure that medical device regulations mandate cyber security to be included in the design phase and that standards such as ISO 80001 are clear enough. ISO 80001 has several technical reports that can aid organizations in the implementation of the standard. These technical reports need to include case studies where possible, so that those organizations with limited resources can still achieve the required levels of security.

NHS Digital (NHSD) has also deployed several solutions to aid in setting up secure networked systems. One such solution is the Secure Boundary, which employs the latest techniques for advanced next generation firewalls (NGFWs) and web application firewalls (WAFs). They are also encouraging the use of Microsoft Advanced Threat Protection with Windows 10.

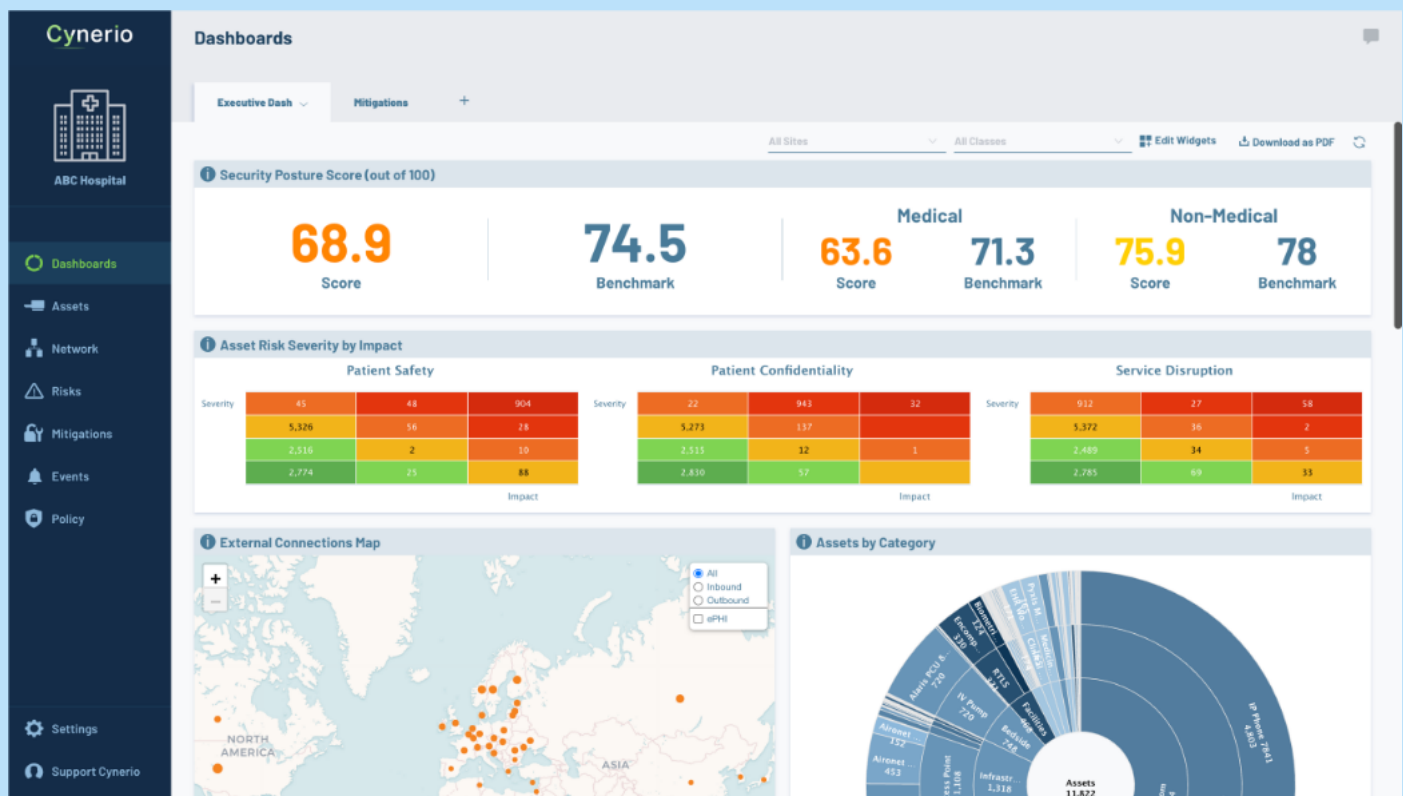
NHSD and NHSX are soon going to merge into NHS England (NHSE) and NHS Improvement (NHSI) to help improve care for patients. When the dust settles after this merger, organizations should get in touch with their experts for advice on how improve the security of their medical devices and networks.

# HOW TO REDUCE CRITICAL HEALTHCARE IOT CYBER RISKS AND RESPOND TO LIVE ATTACKS

---

**When it comes to healthcare cybersecurity, the current situation is - quite literally - the opposite of ideal: As COVID-19 rampages across the globe, cybercriminals continue targeting organizations in this critical sector by taking advantage of their lack of budget, personnel, and suitable security tools.**

**Zeljka Zorz**, Managing Editor, Help Net Security



**Figure 1** - Cynerio's platform prioritizes risk by how much a given vulnerability could potentially affect patient safety, data confidentiality and service disruption. In this way, hospitals quickly know what issues need to be fixed right away.

Hospitals' attack surface is also widening, as the number of connected medical devices they use continues to grow without adequate security oversight.

In fact, when cybersecurity company Cynerio is called in to help a new customer, the team will sometimes find the hospital using plain old Excel for keeping track of all the devices on the network, and limited security tools, especially for IoT.

"They might have a firewall that's protecting some of the IT assets, and a NAC solution for basic control of access. Asset management is usually done manually with Excel or with a slightly more advanced solution (e.g., ServiceNow). They don't have security solutions that can protect – or even accurately identify – the many and diverse IoMT, OT and enterprise IT devices on their network," says Daniel Brodie, the company's co-founder and CTO.

What Cynerio offers is a tool capable of identifying and reducing all critical healthcare IoT risks in under 30 days, but also detecting and responding to live IoT attacks as soon as the solution is implemented.

## The challenges of securing connected devices

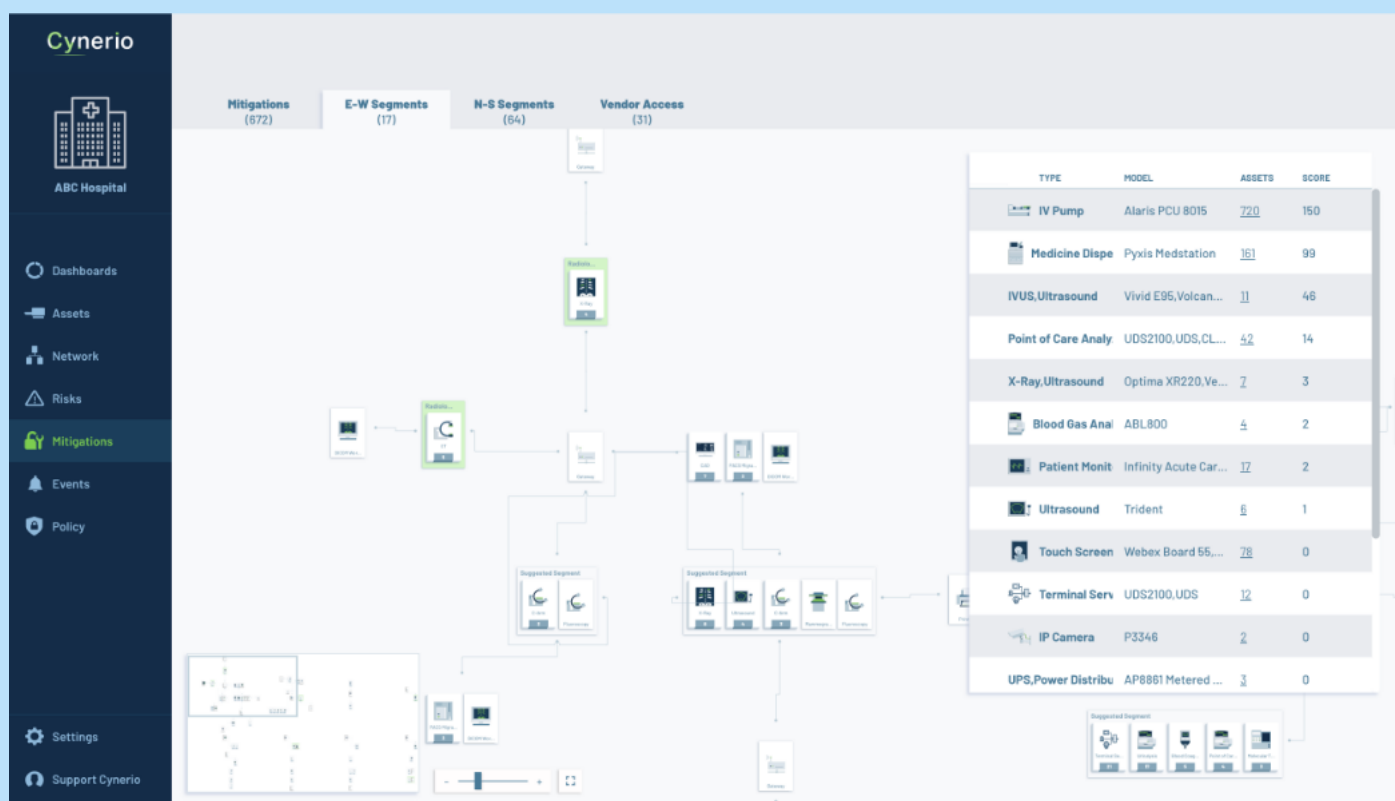
The lack of visibility into IoT has led attackers to view these devices as an unguarded attack vector, ultimately making the security of healthcare IoT both a technology and a healthcare problem, as these devices have an impact on the health of the organization, patient care, and healthcare service delivery.

As ransomware gangs leverage healthcare IoT vulnerabilities and many data breaches originate on IoT devices, the need for healthcare-specific cybersecurity solutions is obvious: healthcare delivery organizations simply don't know how many different devices they have, whether they are open to

attack, and they don't know how to protect them.

The challenge is very specific, as many of these devices are connected to the network, run old operating systems, may not be getting security support from the vendor, come with vulnerable services out of the box, and can't have a security agent/software installed in case it might affect their functioning and, consequently, patient care.

"There are two ways of reducing cyber risk introduced by medical IoT devices: device-level remediation and network-level remediation. The former includes doing things like updating firmware, implementing patches, changing default passwords and so



**Figure 2** - The Cynerio platform's virtual segmentation capability automatically delivers safe and effective policies in a matter of weeks by customizing segmentation policies for every device type, limiting the attack surface and ensuring that clinical services remain intact no matter how threats might evolve.



on, but in general, this type of risk reduction is limited because of those specificities," says Brodie.

"The rest of the risk reduction has to be done using the network infrastructure. This includes closing device ports, applying access-control lists (ACLs) on the internet east-west and north-south traffic, and microsegmenting devices from the core information in the organization. Microsegmenting is, in fact, sometimes the only solution for old, unsupported devices – both to reduce the risk of them being compromised or, if they have been infected but the hospital still needs them to function, to relegate them to a closed-off area so the infection doesn't spread to the rest of the network."

But there's another problem: the effects of incorrect micro-segmentation of medical devices can be very damaging for business continuity and even deadly for patients if it leads to the interruption of care.

Cynerio's Healthcare IoT Cybersecurity Platform solves that problem elegantly, by collecting all the information needed to identify and map all IoT, IoMT, and OT devices on the network; analyzing that data; and providing the security team with different virtual segmentation policies they can test, edit and validate before executing them. Effectively, Cynerio takes the guesswork out

of the whole process.

## Cynerio's Healthcare IoT Cybersecurity Platform


The platform is purpose-made to detect and protect healthcare organizations':

- IoMT (patient monitoring and therapy devices, smart beds, diagnostic machines, anesthesia devices, etc.)
- OT (pneumatic tube systems, IP cameras, digital access systems and locks, etc.)
- Enterprise IoT assets (VOIP phones, printers, etc.)

Cynerio offers each customer the possibility to contract one of their Technical Account Managers, who acts like an extension of their team and works with them to optimize the platform's implementation and calibration.

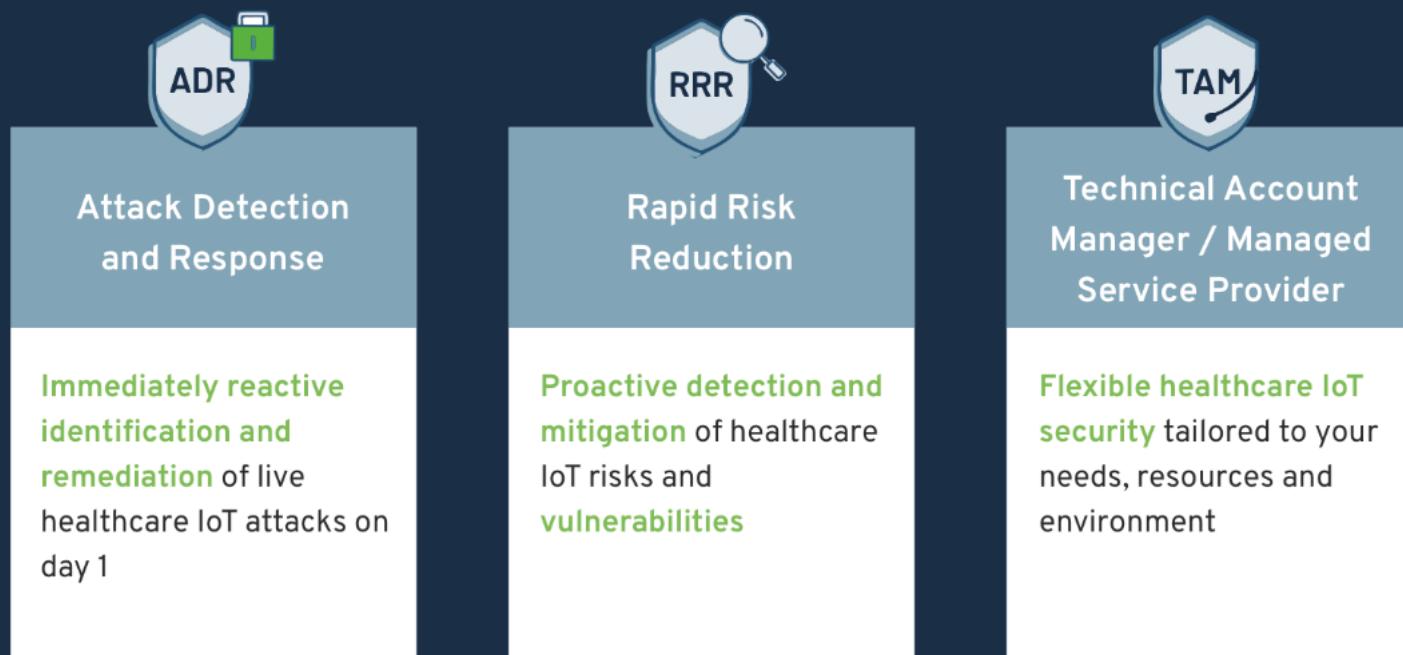
"The deployment of our security solution is pretty straightforward and very similar to that of other network monitoring solutions," Brodie explains.

"We have a Cynerio sensor/collector – an off-the-shelf server with our software installed on it – and we install it next to a core switch. We get a copy of the traffic from, for example, a Gigamon TAP, and the server



**The effects of incorrect microsegmentation of medical devices can be very damaging for business continuity and even deadly for patients if it leads to the interruption of care.**

## The Cynerio Platform



**Figure 3** – The Cynerio Platform consists of three pillars: Attack Detection and Response (ADR) identifies and stops live attacks on IoT and medical devices, Rapid Risk Reduction (RRR) preemptively detects and addresses device vulnerabilities so that they won't enable future attacks, and Technical Account Managers (TAMs) give hospitals a fully managed and optimized IoT security solution without needing to hire additional personnel.

uploads the metadata to the cloud, where we analyze it."

The platform uses deep packet inspection, device fingerprinting, and behavior analysis to profile and locate every device, and to deliver granular information about them: serial number, MAC address, vendor, model, OS/firmware version, open ports, and so on.

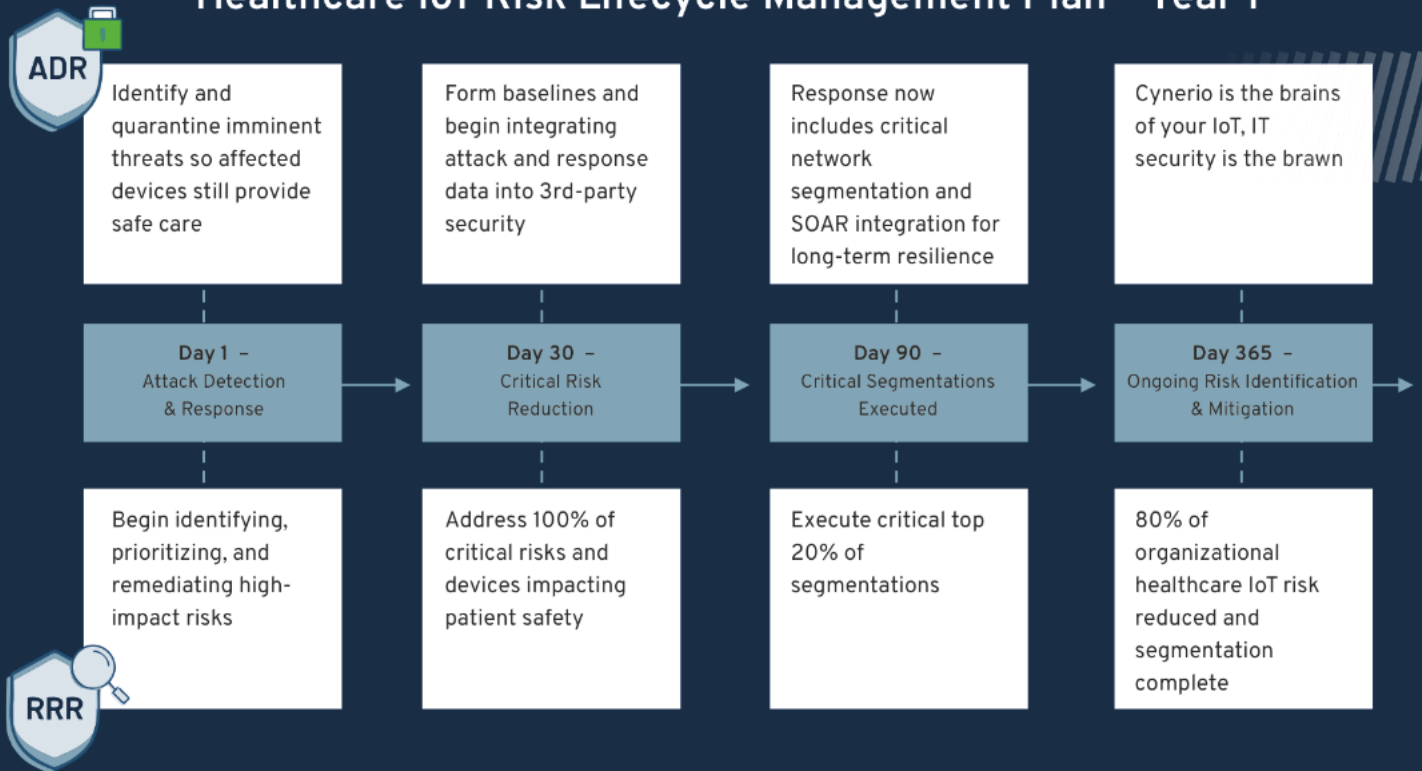
The next step is integration with the hospital's infrastructure and IT solutions.

"If, for example, a hospital wants to prevent radiologists from doing their web browsing and online shopping from a radiology device, they won't be able to do it if they just have a

firewall set up, as it won't be able to recognize the device and block that activity," Brodie illustrates.

"But our platform can connect with firewalls, NACs, and other risk management solutions that the organization has. We can enrich the information they already have with ours and make these IT solutions useful for working on healthcare IoT. So now the firewall recognizes the radiology devices on the network and organizations can implement a firewall policy that allows them to connect to only specific servers they need to function. Cynerio will tell you which servers those are and will push that policy. In practice, we are the brains, and the IT tools are the muscle."

## Healthcare IoT Risk Lifecycle Management Plan – Year 1



**Figure 4** – Hospitals don't just need IoT cybersecurity – they need practical guidance on its implementation. Based on successful implementations of the platform, Cynerio has developed a series of best practices that include step-by-step procedures for optimal internal governance and security outcomes.

Aside from risk reduction, Cynerio's platform is also capable of detecting and responding to live attacks on medical, IoT and OT devices within hospital environments.

"For the past nine months or so, we have been working with healthcare organizations that have been under ransomware attack, and we were able to see what they are doing that's good, what they fail to do, and what they need to do. The result is the Cynerio Attack Detection and Response module," Brodie notes.

"Through integration with the hospitals' SIEM, SOAR, and other IR tools they have, we can trigger alerts when we detect a device

engaging in suspicious and potentially malicious behavior. We can tell these tools how to immediately respond by containing and quarantining the device, and jumpstart an investigation, a suitable response, and advise on a post-attack solution."

### Conclusion

Healthcare delivery organizations have more and more patients whose care depends on an increasing number of connected devices working as intended. Unfortunately, this also means that cyberattacks that result in their compromise and the disruption of their normal functioning may lead to a variety of bad outcomes for the hospital and its patients.

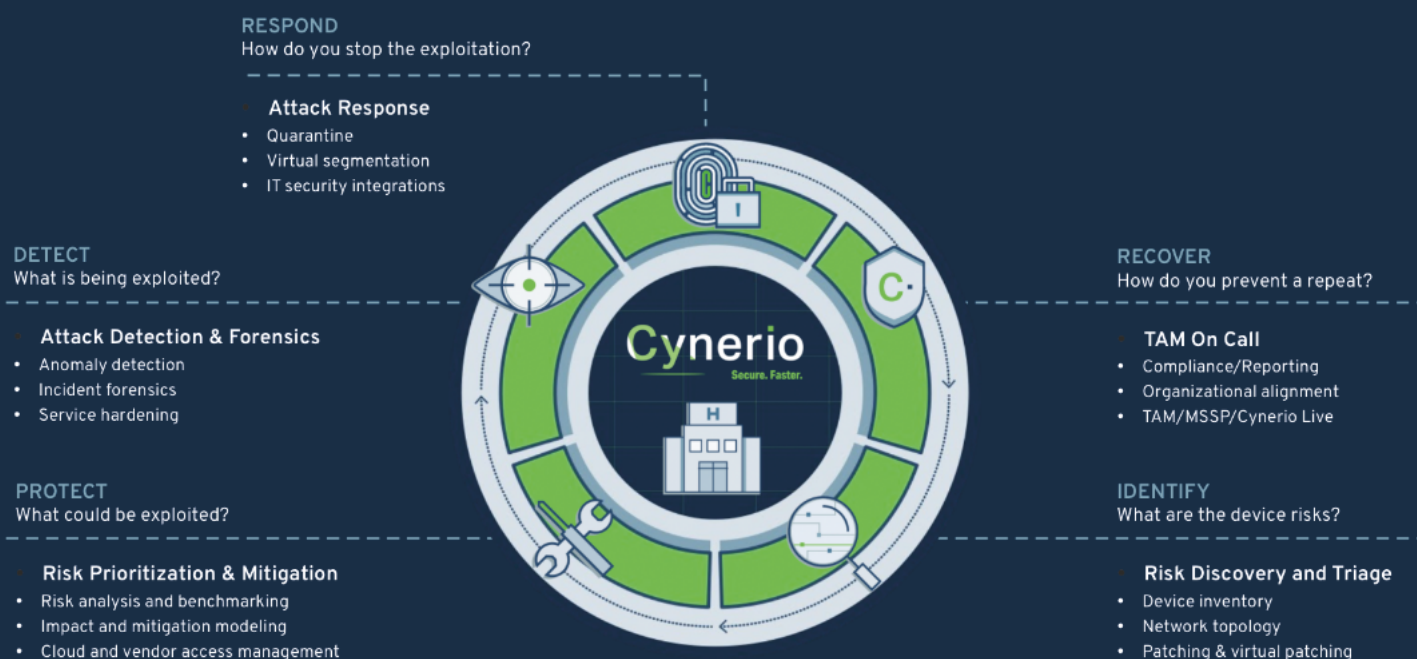
## Aside from risk reduction, Cynerio's platform is also capable of detecting and responding to live attacks on medical, IoT and OT devices within hospital environments.

We may still be far from solving the problem that is COVID-19, but there is a good strategy for handling ransomware and data security threats, and it includes implementing the right security policies to minimize the risk of these attacks and to cut them short when they do happen.

"A lot of attackers – and especially

ransomware gangs – are looking for the low-hanging fruit. Even just implementing basic security controls like using endpoint security tools and changing default passwords may make them turn away. The 'trick' is to make the bar for effective compromise high enough for cybercriminals to move on to easier prey," Brodie concludes.

### Extending the NIST Cybersecurity Framework to Healthcare IoT



**Figure 5** – Cynerio applies the NIST Cybersecurity Framework to Healthcare IoT. Because of technology differences, especially the wide variety of device manufacturers and operating systems, this has been difficult to apply to IoT until now.

RAJ SAMANI, CHIEF SCIENTIST & FELLOW, TRELLIX

# THE IMPORTANCE OF IMPROVING TECHNOLOGY TO KEEP HEALTHCARE ORGANIZATIONS SECURE



The past few years have shown that no sector is immune to cyberattacks, and this is true for healthcare too. With the surge in hospitalizations, the overall quantity of data circulating, and the poor cybersecurity practices of most healthcare organizations, it was an easy task for cybercriminals to plan and execute these cyberattacks.

**Mirko Zorz**, Editor in Chief, Help Net Security

## Based on what you're seeing in the wild, what are the most significant threats to hospital networks in 2022?

There are many, but the one recurring issue that remains highest priority is the impact a significant disruption can have. Of course, this will include ransomware and the detrimental impact this has on patient care is something we have witnessed with alarming regularity.

Such attacks have been widely discussed, but when combined with double extortion (where data is also released) the impact is particularly troubling for data subjects.

We have to accept that in order for healthcare organizations to provide the best patient care, they will depend on accurate/comprehensive data about the patient. This in itself becomes more attractive to those looking to cause the most damage and ultimately demand/force payments.

**The healthcare industry deals with unique challenges. Telehealth is on the rise, practitioners require secure remote access to patient records, all while attackers are targeting health data more than ever. How can a healthcare organization make sure it has the proper visibility and control?**

Information Governance is critical within the healthcare sector. It demands that organizations understand the data they hold, but also clearly define how the data is

**Information Governance is critical within the healthcare sector. It demands that organizations understand the data they hold, but also clearly define how the data is governed within the organization.**

governed within the organization. Although this may seem like a relatively simple process we have to appreciate the sheer volume of data; and the number of employees and contractors that will likely need access.


**When thinking about hospital cybersecurity, one immediately thinks about not just data, but patient safety. Since all sorts of connected devices have been already hacked, is there a reason for concern? What can we do to protect internet-connected healthcare devices?**

Of course, the headlines paint a frightening picture, and as we move toward a more connected society the healthcare environment is an area that demands massive technological improvements. These security issues are something that can be managed, and the risk can be mitigated to levels that we deem as acceptable.

We have to embrace these technologies, the ability to incorporate and leverage technology to not just manage but to detect anomalies with patients is critical.

More tactically for IoT devices; we have experienced differing approaches by vendors in how they deal with security vulnerabilities. There have been instances where some medical device vendors have actively





**The main thing I believe is that within cybercrime there is not one sector, or organization that will be immune to criminal attempts to compromise.**

commitment to establishing more secure devices. There have also been those which have been less open.

**Taking advantage of a deepening resource strain due to the pandemic, attackers have increased their targeting of healthcare organizations using ransomware. What trends are you seeing when it comes to ransomware attacks on healthcare? What should organizations do in order to minimize the damage?**

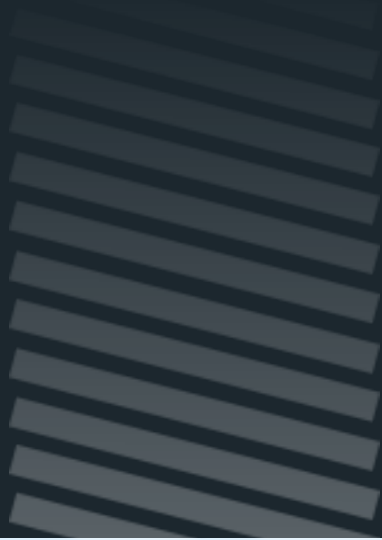
Healthcare was one of the most targeted sectors during the pandemic. Without wishing to over simplify however, many of these attackers use the same methods to gain access to networks.

Strong hygiene measures are critical. What this demands is that organizations should for example consider the typical initial entry vectors leveraged by ransomware groups. Take for example the use of RDP: Is there appropriate focus on securing systems that require RDP to be open and of course measures to identify where RDP is enabled without authorization. This is only the tip of the iceberg: ultimately remember – don't pay, and use [Nomoreransom.org](https://nomoreransom.org) as a source for more guidance.

**How do you see threats to the healthcare sector evolving? What trends should CISOs pay attention to?**

I was a little naïve when the pandemic hit, I listened to the promises by various ransomware groups that promised not to hit healthcare. Guess what? They lied and healthcare was one of the most targeted sectors.

The main thing I believe is that within cybercrime there is not one sector, or organization that will be immune to criminal attempts to compromise. Whether you are in healthcare or any other sector, it is an important point to understand – you have to not only protect your environment, but have a plan for the possibility of being compromised.





# OUT OF THE PAN AND INTO THE FIRE: FROM PANDEMIC TO THREAT OF CYBER WAR

---

For the first time in many years the external threat is bigger than the internal threat to healthcare systems and data. Organized criminals, environmental factors, even geopolitical events are parts of the industry's threat profile.

**Mac McMillan**, CEO, CynergisTek

Since the onset of the COVID-19 pandemic, the healthcare industry has been inundated with headlines regarding repeated vulnerabilities and cyberattacks that not only threaten health systems' and providers' digital infrastructure, but that also jeopardize the health and safety of patients themselves. From ransomware attacks with the potential to cripple back-office operations and expose patient data, to more sinister 'killware' that can compromise vital healthcare equipment – and in turn patients – the past two years have introduced a wave of new threats that healthcare providers must address on top of the existing stress of the pandemic. If that weren't enough, stress healthcare like every other critical infrastructure element in America now watches closely the happening in Eastern Europe and the threat of cyber warfare.

Unfortunately for those fatigued organizations, 2022 is unlikely to bring any easy answers. Not only will threat actors continue to relentlessly target the healthcare sector, but events on the international stage could lead to evolving attacks, keeping security teams scrambling to protect their organizations.

The best that healthcare security leaders can do is anticipate and prepare for trends that we know are likely to emerge in the coming months. Below are seven of the key developments that we expect to see shape the healthcare cybersecurity landscape in 2022.

- **Supply chain challenges and disruption**


**will continue to plague the industry.**

In 2021, we saw several high-profile attacks on supply chains in healthcare and other industries. In the healthcare industry, the sheer size and complexity of the supply chain, including nuances of data access and privileges, combined with how data is increasingly moving in and outside of the healthcare system via third-party vendors (e.g., leveraging wearables, data analytics, AI, etc.), has created several points of failure.

Although accelerating digital transformation, enabling greater interoperability, and increasing the use of data analytics across the supply chain may lead to increased efficiencies and improved care, it also increases the number of vulnerable points across the attack surface that the threat can exploit, leading to potential disruption of hospital operations. We'll see more and more of this in 2022.

- **Disruption will be the primary target.**

While still valuable, patient data on its own is no longer the holy grail for threat actors. Instead, we'll see these actors increasingly adopt wartime strategies, engaging in multi-pronged attacks that apply indirect pressure on critical infrastructure and cause compound disruption across the entire healthcare value chain. This will include major healthcare systems and other essential services such as water, energy, and utilities. As a result, this not only has the potential to cripple our healthcare system and put patients at risk, it will also put at risk the surrounding economy



**Unlike other industries, given the truly life-or-death nature of the healthcare industry, healthcare organizations will continue to pay a higher price when it comes to the rapid increase in ransomware demands.**

and infrastructure more broadly.

- **Healthcare will continue to represent a large percentage of ransomware attacks.**

Unlike other industries, given the truly life-or-death nature of the healthcare industry, healthcare organizations will continue to pay a higher price when it comes to the rapid increase in ransomware demands.

Ransomware attacks will become more difficult to control and mitigate as they go from a single tier to triple tier attacks. This will not only impact already-strained healthcare budgets, but will continue to jeopardize patient safety, extend hospital stays, increase botched procedures, and adversely impact our nation's mortality rate.

- **API security could undermine the success of interoperability.**

APIs enable systems to quickly transfer patient information, things like prescriptions, medical history, treatment records, etc. But when those APIs are insecure, they create additional attack vectors for the threat to disrupt care procedures and operations. 9 in 10 healthcare executives say APIs are important or mission critical, but less than 24% of organizations are using APIs due mainly to security, compliance and cost.

When addressed properly, APIs actually enhance security and compliance while delivering all the benefits usually attributed to them. For interoperability to succeed, healthcare will have to address the security of APIs.

- **Cybersecurity insurance will cover less, cost more and be harder to get.**

Given the current cybersecurity landscape and the increased threat of attack – specifically in the healthcare industry – organizations are going to see cybersecurity premiums move sharply up and to the right. Not only will those premiums increase, but organizations will need to meet ever more stringent underwriting requirements in order to take out cost-effective policies. As a result, in 2022 we'll see organizations recalibrate the cost-benefit analysis they conduct when determining the most appropriate insurance coverage for their organization. The focus will shift to prevention and resilience.

- **War between Russia and the EU/NATO threatens to spill over.**

Any time there is war, there is stress on the US economy and the markets. The specter of Russia invading neighboring Ukraine is affecting nations and economies around the


world. The threat of cyberwar and attacks on those aiding Ukraine or siding opposite Russia in this conflict may experience cyberattacks either directly or indirectly as a result of US interests in Europe. These attacks threaten to be destructive as extortion is not the goal.

• **Lack of cyber talent will stymie efforts to improve security.**

Experienced cyber talent is becoming an even scarcer and more expensive commodity and healthcare will continue to lag in attracting and retaining the talent it needs to improve its efforts to security data and systems. The paradigm needs to shift to all information technology professionals receiving related cyber training to their skill and efforts to motivate greater migration into cyber professions. Partners will become even more important to address all of the cyber skills

and efforts organizations need to be successful.

Healthcare has seen its threat profile steadily grow as the threat continues to evolve. A threat that did not abate as we entered and weathered the pandemic. And now it faces the specter of attacks related to a potential war in Europe. More than ever healthcare entities need to embrace becoming more resilient through active monitoring and testing of its entire attack surface. For the first time in many years the external threat is bigger than the internal threat to healthcare systems and data. Organized criminals, environmental factors, even geopolitical events are parts of the industry's threat profile. It's not enough to invest in security technology, you need to validate that your controls are performing as expected. To use the words of a former President, you must Trust, but Verify.



**Experienced cyber talent is becoming an even scarcer and more expensive commodity and healthcare will continue to lag in attracting and retaining the talent it needs to improve its efforts to security data and systems.**

MARIE MOE, SENIOR CONSULTANT - INCIDENT RESPONSE AND THREAT  
INTELLIGENCE AT MNEMONIC | ASSOCIATE PROFESSOR AT NTNU

## DO WE NEED ANOTHER MAJOR BREACH TO TAKE THE SECURITY OF CONNECTED MEDICAL DEVICES SERIOUSLY?

---

Connected medical devices are a great achievement of modern society, enhancing healthcare organizations' quality of service and the lives of numerous patients. But the lack of seriousness when it comes to securing those devices is worrying, as failures in that arena could have grave consequences.

Helga Labus, News Editor, Help Net Security



**Technology has been going hand in hand with healthcare for quite a while now, with many positive changes. Of course, there's the other side of the medal: vulnerabilities that could greatly affect patients and their wellbeing. What worries you the most about connected medical devices?**

I am particularly worried about all the legacy medical devices that are vulnerable and unpatchable. Medical devices that were not originally designed to be connected have been getting internet connectivity “bolted on” without taking cybersecurity into account, since there were no requirements and awareness at the time.

These legacy devices are still used by patients and in many cases remain vulnerable to cybersecurity threats despite increased awareness and willingness of mitigating cyber risks, because the cost of fixing legacy devices is too high or they simply can't be patched due to design limitations.

**What are the many ways that medical devices can be compromised?**

Medical devices can be compromised by targeted attacks, but more likely due to malware that was not designed to target medical devices but that happens to exploit vulnerabilities commonly found in medical device software.

One example of this is the infamous WannaCry ransomware incident in May 2017,

which hit a large number of hospitals in the UK and also infected connected medical devices that were running on outdated Windows operating systems.

**Are manufacturers not taking into consideration the consequences of vulnerable medical devices?**

Manufacturers of medical devices were for a long time living in a world without any cybersecurity requirements from the regulatory bodies, and the awareness of cybersecurity threats was low. When

researchers like me started to investigate this area more than a decade ago to try and raise awareness, they were commonly met with ignorance, disbelief and hostility.

Today the maturity has increased considerably both on the manufacturers and the regulatory side, and I am pleased to have

seen this progress over the years since I started working on my [pacemaker hacking project](#).

**What should manufacturers do to improve the security of medical devices?**

The manufacturers should use threat modeling early in the design process and build-in cybersecurity protections instead of bolting them on as an afterthought. The US FDA has recently published a [playbook for threat modeling](#) that can be of use in this process.

**Medical devices can be compromised by targeted attacks, but more likely due to malware that was not designed to target medical devices but that happens to exploit vulnerabilities commonly found in medical device software.**



Another initiative that can improve security is the concept of a Software Bill of Materials (SBOM), which is somewhat like a label with an ingredient list for all the software components of a device, including third-party software libraries. If manufacturers are required to make this available, it can be incredibly useful for medical device cyber risk management, in particular for keeping track of what systems need upgrades, patching or other mitigating measures.

### **What drove you to start The Pacemaker Hacking Project?**

I had a pacemaker implanted in 2011, and since I already had a PhD in information security and was at the time working with incident response at the Norwegian National CERT team, I was naturally curious about the security of my own device. I started doing some research and found the technical manual of my device, and that was when I learned that my pacemaker had two wireless communication interfaces.

No-one had informed me that my pacemaker could connect to the manufacturers' backend servers via a home-monitoring device and transmit my patient data. When I looked for published research on the security of this communication channel, I found none, and that was why I decided to seek out this information myself.


So, I got hold of some second-hand home monitoring units, a pacemaker programmer and eventually even some used pacemakers, and started The Pacemaker Hacking Project.

### **What vulnerabilities did you uncover in the Home Monitoring Unit (HMU)?**

The project started in 2015, and it has been a long process. Early on it was a self-funded hobby project with the help of my friends in the security community. Then I started getting publicity, and I received a small amount of funding. I have a side-job as an Associate Professor with the Norwegian University of Science and Technology (NTNU), and I proposed several MSc projects on pacemaker hacking.

Luckily, some brilliant students signed up for this and, so far, six of them have published their master's theses with various results related to vulnerabilities.

Among the uncovered vulnerabilities were the use of improper authentication with backend servers, cleartext transmission of sensitive information, missing encryption and storing passwords in a recoverable format. Some of these vulnerabilities did get embargoed while being reported to the manufacturer, the FDA and the CISA as part of a coordinated vulnerability disclosure process. They were finally published as CVEs



**Among the uncovered vulnerabilities were the use of improper authentication with backend servers, cleartext transmission of sensitive information, missing encryption and storing passwords in a recoverable format.**



in 2020, and an academic paper describing the results has been presented by Guillaume Bour at the conference BIODVICES 2022 on February 11.

### **What changes should be introduced in the HMU authentication process?**

It is challenging to retrofit security into these devices. In the case of the Biotronik HMU, the legacy devices themselves did not get patched – the mitigating measures were all implemented in the backend (server) side. Hardcoded credentials are a big problem, especially when devices are improperly decommissioned, and the credentials can be easily accessed via hardware hacking or by simply opening the device and finding a still valid SIM card. There are many improvements that could prevent these types of attacks when newer devices are designed with threat scenarios in mind.

The practice of using proprietary communication protocols should also be avoided. I think that securing communication using standard protocols that have been scrutinized by the wider security research community is a much better approach and will make various devices interoperable.

### **When it comes to medical devices' security, do you expect any progress in the immediate future?**

I probably shouldn't say this as not to jinx it, but if another devastating cyber incident such as WannaCry impacts a large number of hospitals and medical devices in the near future, we would probably see an increased adoption rate of new guidelines and various measures to increase the security and the

**I have seen an increase in security maturity in both regulators and manufacturers, as well as in the clinical community when it comes to awareness, interest in discussing the topic and doing something about it.**

preparedness to responding to further incidents.

As I mentioned before, I have seen an increase in security maturity in both regulators and manufacturers, as well as in the clinical community when it comes to awareness, interest in discussing the topic and doing something about it.

I have been active with the grassroots organization I Am the Cavalry since 2015, and this has introduced me to some amazing individuals that are truly passionate about making the world a safer place, especially when it comes to securing systems that can impact human lives. I think that this group (among others) has been successful in raising the general awareness level.

# SAFEGUARDING MEDICAL DEVICES FROM VULNERABILITIES AND CYBER ATTACKS

**Guy Gilam**, Head of Product Marketing, Cybellum

**Medical device manufacturers and their suppliers are under constant pressure to accelerate digital innovation and product releases, while keeping medical devices safe, secure and compliant.**

In the development process, they leverage commercial software and components, and open-source code to become more agile. While speeding up the development process, vulnerabilities and cyber-threats are often introduced into the device, through the lack of secure coding know-how, accidental errors and


inadequate testing procedures.

Research shows that as much as 65% of medical software is based on open-source code, with the rest being third party commercial code or in-house developed software. With common vulnerabilities and exposure (CVE) numbers on the rise, there is no shortage of



Exposing and managing software vulnerabilities is a major challenge, rendered even more so for the medical device industry and its complex supply-chain. In many cases, developers don't have access to the source-code of the software they are integrating, which can blind development and security teams from vulnerabilities and threats.

35



## Exposing and managing software vulnerabilities is a major challenge, rendered even more so for the medical device industry and its complex supply-chain.

unauthorized usage. FK needed to create new versions of their device to address these vulnerabilities. They identified ~1,200 pumps that would need hardware changes.

The above case clearly illustrates that late discovery of vulnerabilities can lead to costly recalls, device re-architecture, and a direct hit on the organization's brand and reputation of reliability.

Regulators and policymakers across the world are very concerned about these risks. Notable examples include the FDA's premarket and postmarket cybersecurity management guidelines and the more recent International Medical Device Regulators Forum "Principles and Practices for Medical Device Cybersecurity." In addition, on May 12, 2021, US President Biden issued the Executive

Order on Improving the Nation's Cybersecurity, which discussed the requirements for cybersecurity across the supply-chain, including the need for Software Bill Of Materials (SBOM) and Zero Trust Architecture.

To safeguard their customers, comply with regulation and remain competitive, stakeholders in the medical device supply-chain must monitor for vulnerabilities and potential cyber-attacks during all stages of development, even after the device is in the market. They need to be able to rapidly comply with the ever-changing US FDA and internationally recognized standards and guidance for security, in order to sell in the global markets and ensure that the components and software they receive from their supply-chain are also without vulnerabilities,

especially during times when manufacturing resources are scarce.

### What is vulnerability management?

The intended purpose of vulnerability management is a continuous practice of exposing, prioritizing, assessing, remediating, or mitigating, and tracing software vulnerabilities, throughout the medical device lifespan.

Continuous vulnerability management enables consistent development and effective maintenance of secure products. When done right, it allows you to:

- Produce secure products that safeguard device operations and patient's lives
- Comply with regulations,

standards and internal policies

- Cut incident response times
- Improve your risk posture
- Control your spending

In order to operate continuously, it must involve dedicated resources, defined processes, agreed-upon policies and enabling

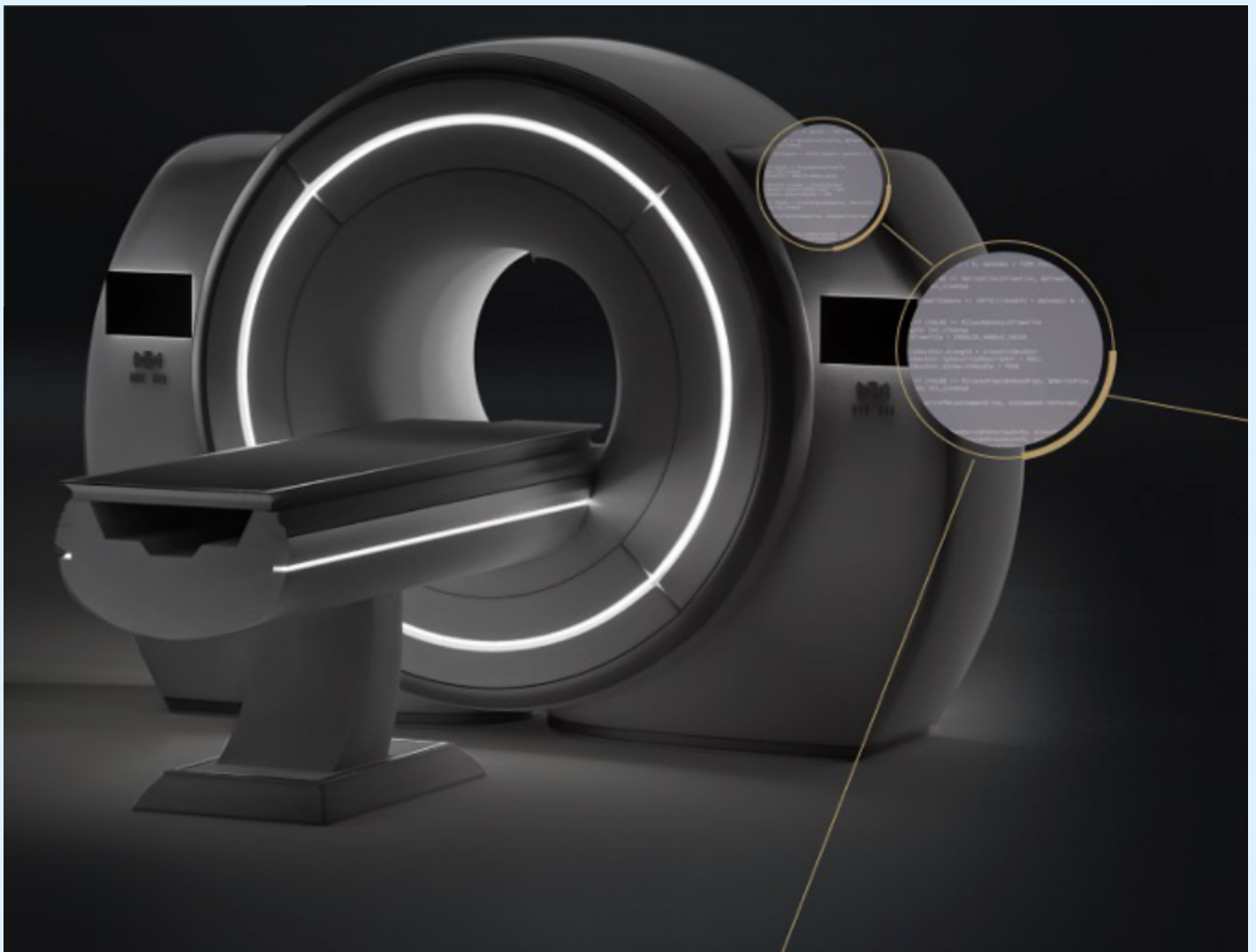
technologies to fend-off cyber-threats. It is a critical cybersecurity practice and will become even more so for the healthcare industry with the adoption of more comprehensive medical device cybersecurity regulations, standards and best practices.

There are two major job functions that handle most of the vulnerability

management operations:

**Product security** – Acts as the subject matter expert on product security within the development organization, with a broad scope of enhancing the security of medical devices.

**Program security champion** – Responsible for the security of the specific component or medical device development program.





In addition to these core functions, there are two more entities which are involved with vulnerability management operations.

The Product Security Incident Response Team (PSIRT) that springs to action to mitigate security incidents post-production and in some organizations, there is also a Red Team that emulates hacking scenarios to proactively discover cyber weaknesses.

Let's highlight the key responsibilities of these functions and how they interact, without going into specific job titles or team structures, as these vary considerably depending on available resources and corporate culture.

## Product security

Responsible for overall product security lifecycle management within the organization, product security includes product security education, culture and governance and orchestration between the parties that contribute to product security. Some of the key responsibilities include:

- Define and monitor

adherence to internal product security policies (e.g. software hardening mechanisms, secure development frameworks, cryptography related guidelines, privacy/PII related policies and more) in support of "security by design"

- Set requirements for compliance with relevant regulations and standards such as FDA-2018-D-3443 and IMDRF/CYBER WG/N60

- Assess product vulnerabilities and escalate issues to development teams and external suppliers

- Manage and prioritize actions with regards to mitigating potential threats that have been identified

- Continuous overall product risk posture tracking across the product lifecycle, including impact analysis across products



- Raise awareness and educate the organization (with special focus on R&D teams) on product security issues (e.g. secure development lifecycle)

This is a dedicated function working in parallel with IT and OT security experts.

### Program security champion

Responsible for product security requirements within a specific development program:

- Define cybersecurity risk goals for the program, taking into account internal guidelines and customer requirements
- Work alongside

development organization and external suppliers on secure product design and architecture

- Own “CVE hunting” triggered by customer questions (usually executed together with the product security team)

This function reports to the specific program leadership team within the R&D organization.

### Red Team

Focuses on proactive ethical hacking and vulnerability analysis of proprietary software (in-house developed or 3rd party):

- Analyze device components to identify coding

weaknesses, using various pen-testing techniques

- Escalate detected issues to development teams, external suppliers, program and product security teams
- Support PSIRT operations when needed

This function is often outsourced to external vendors and typically (though not always) managed by the product security team.

### PSIRT

Responsible for Product Security Incident Response, post production:

- Analyze incident data to assess potential risk impact





- Perform root-cause analysis to zero-in on the incident source
- Work alongside development teams and external suppliers on a mitigation plan
- Manage the incident response process and communicate with internal (e.g. corporate communications, legal) and external (e.g. security researchers, hackers) stakeholders as needed
- Generate an incident report with lessons learned and future remediation tasks
- Handle threat hunting in coordination with the product and program security teams, so that preventative measures can be taken across all affected programs

This function may be part of the Security Operations Center (SOC) if one exists.

## Create vulnerability management processes and policies

Setting the ground for compliance with the most advanced and comprehensive medical cybersecurity guidelines and standards from the IMDRF, European Commission MDCG, FDA and others, vulnerability management requires processes and policies to govern how vulnerabilities are assessed, mitigated and continuously monitored.

## Vulnerability assessment

Risks and vulnerabilities are analyzed to determine their impact on medical equipment and underlying components pre and post production, typically involving the following steps:

### Step 1 - Software composition

A Software Bill of Materials

(SBOM) or Cybersecurity Bill of Materials (CBOM) is created for each medical device or component. This inventory of software components can be generated through source code analysis, but this is often not available to the manufacturer. The alternative is using binary code analysis and/or reporting of the software inventory provided by suppliers and internal R&D teams.

This is ideally carried out by an automated exposure solution such as Cybellum, which generates a Cyber Digital Twin including a detailed CBOM and mapping of underlying HW architectures, OSs, configurations, controls flows, API calls and more.

Manufacturers in the US may need to provide their customers extended information on device security, in line with the



**A Software Bill of Materials (SBOM) or Cybersecurity Bill of Materials (CBOM) is created for each medical device or component.**



NEMA and HIMSS  
“Manufacturer Disclosure  
Statement for Medical Device  
Security” (MDS2).

## Step 2 - Threat intelligence gathering

Most organizations track publicly known vulnerabilities (CVEs) as published on the NIST National Vulnerability Database (NVD). Threat intelligence gathering and analysis is a challenging task on its own and benefits greatly from automation. Data must be continuously

aggregated, normalized and analyzed in support of continuous vulnerability assessment during development and post-production monitoring.

## Step 3 - Vulnerability assessment

A list of suspected CVEs is compiled for each software component. This is performed by correlating the SBOM with threat intelligence related to vulnerabilities and exploits. The manufacturer typically uses the standard CVE


database and common exploit databases for vulnerability matching and prioritizes threats for immediate action.

## Step 4 - Proprietary code analysis

Follow-up the vulnerability assessment coverage, with vulnerability analysis on proprietary software (licensed from 3rd parties or developed in-house). Such an analysis may expose coding weaknesses that could be exploited enabling attackers to remotely execute code or perform a DoS attack, so they can ultimately overtake or crash the device.

## Step 5 - Compliance validation

This is where the analyzed software component is validated against medical cybersecurity regulations and standards. Those require manufacturers to have a vulnerability management process in place, to be able to validate adherence to security requirements and document the related actions and decisions (more on this in the next section). Additionally, this is when the analyzed software is validated for compliance with internal



**Vulnerability management operations should be performed as an on-going process, that continues also after the medical device has been released to the market (postmarket).**

security policies, set by the product security function.

### **Step 6 - Reporting and monitoring**

Risk exposure dashboards and reports should be generated to enable tracking of the vulnerability management status within and across development programs, and ensure better collaboration between internal and external parties around any required remediation activities.

Once identified and assessed, be it during development or once medical devices are in use, cyber-threats and vulnerabilities must be addressed within a reasonable timeframe. For each vulnerability impacting the product, a mitigation and remediation plan should be devised, executed and documented.

This involves documenting who owns the specific vulnerability, the status of the vulnerability, and any technical and business justification in support of the mitigation plan. This will serve as future reference, in support of auditing and enabling ongoing monitoring activities if the threat level changes.

### **Vulnerability monitoring**

Vulnerability management operations should be performed as an on-going process, that continues also after the medical device has been released to the market (postmarket).

This is a critical aspect of vulnerability management, mandated by the FDA's postmarket management of cybersecurity in medical devices (section V point B), the IMDRF principles and practices for medical device cybersecurity (section 6.3.1),

the European Commission's MDCG guidance on cybersecurity for medical devices (section 3.8) and other regulations, standards and best practices.

The goal is to continuously identify and assess new vulnerabilities, as well as changes to previously known ones like a new exploit of a vulnerability, which may impact devices in use. This is done through ongoing manual or automated processes including threat intelligence gathering and analysis, vulnerability assessment, and when relevant, mitigation of threats.

### **Incident response**

Once medical devices are in operation, cybersecurity incidents are typically handled by the Product Security Incident Response Team (PSIRT) and the following activities typically

occur:

- **Root Cause Analysis** – Intended to find the reasons for the vulnerability to exist and reach the production stage, and to gauge the damage a vulnerability may have on components/devices.
- **Close-Loop** – A process to identify all possible mitigations in design, development and testing procedures that could prevent this, and other similar vulnerabilities from threatening the software in the future.

While not mandated by regulations and standards, when a cybersecurity incident happens, the Product Security team will want to execute an impact analysis playbook to

proactively discover similar issues across other products and development programs.

As the risks and costs related to medical device cyber-threats are significantly higher, post-production, manufacturers and their suppliers should ideally create a real-time (or near real-time) monitoring process that is automated, scalable and can be integrated into their asset-management and software update systems, so they can minimize the time it takes to identify impacted products and roll-out fixes when required.

### **Prioritization and escalation methodologies**

The below policies are typically used in support of

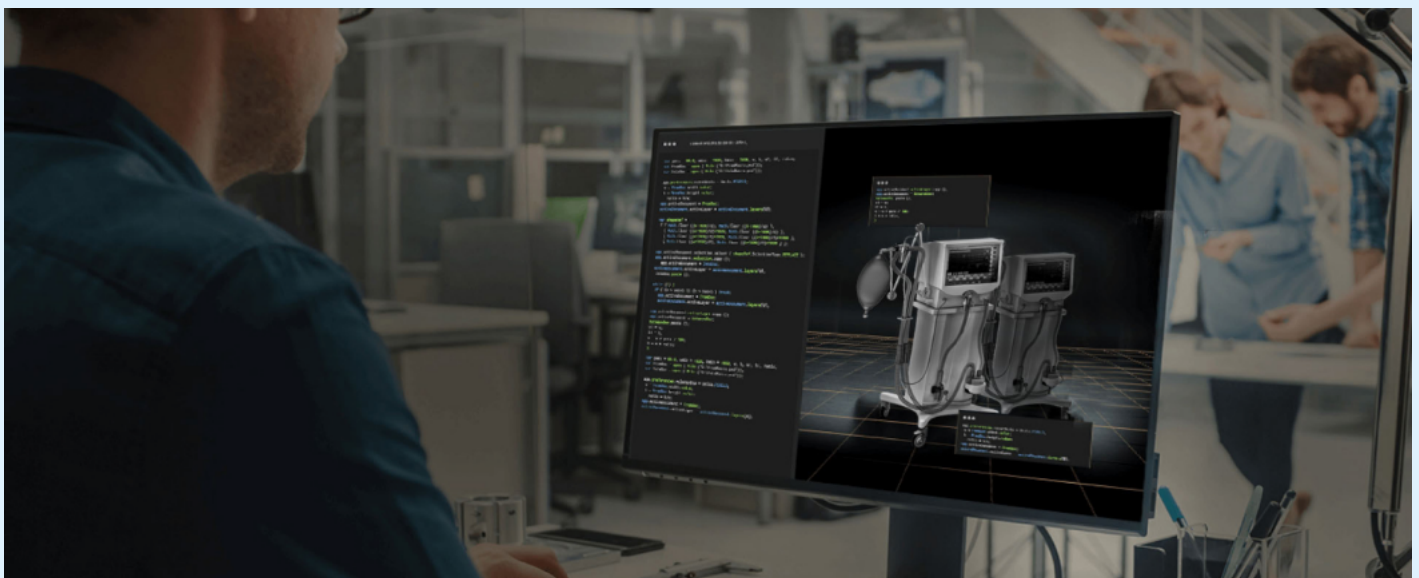
the vulnerability management process.

### **Prioritization methodology**

Once threat intelligence about various vulnerabilities and weaknesses that may risk a medical device is available, it must be assessed for exploitability. In order to focus on the most pressing issues, a threshold based on certain vulnerability attributes is set to determine which of those will be further analyzed.

### **Public vulnerabilities (CVEs)**

The following is an example of the minimum base attributes required for public vulnerabilities to be further analyzed, based on the CVSS



v3.0 attributes, although each organization may adjust it as seen fit:

- Attack Vector (AV) – Adjacent
- Attack Complexity (AC) – is Low (L)
- Privileges Required (PR) – is None
- User Interaction (UI) – is None (N)
- Scope (S) – is Unchanged (U)
- Confidentiality (C) / Integrity (I) / Availability (A) Impact – low or high

### Proprietary software weaknesses

These are categorized according to their potential impact. As a rule-of-thumb, all CWEs that may cause a loss of application service because of a user or external input, should be further

reviewed, but OEMs and their suppliers should devise a policy that caters to their understanding of the threat landscape.

### Escalation methodology

The vulnerability escalation process defines the escalation of issues to internal development groups and external suppliers.

### Implement the right technology stack


Technology is your best ally when it comes to setting up your vulnerability management program. Gone are the days where security assessments could be handled manually by a handful of skilled experts. The old ways don't scale well with the growing complexity of product software, the increase in cyber-threats, and the need to proactively manage your cyber-risk.

To support your vulnerability

management program, the following key systems and technologies should be top of your mind:

- **Software asset management** – a centralized repository of all software components used for product development, with contextual data on their composition and characteristics, will facilitate in-context validation of their security posture throughout the development process and will assist impact-analysis assessment when a security incident occurs post production.

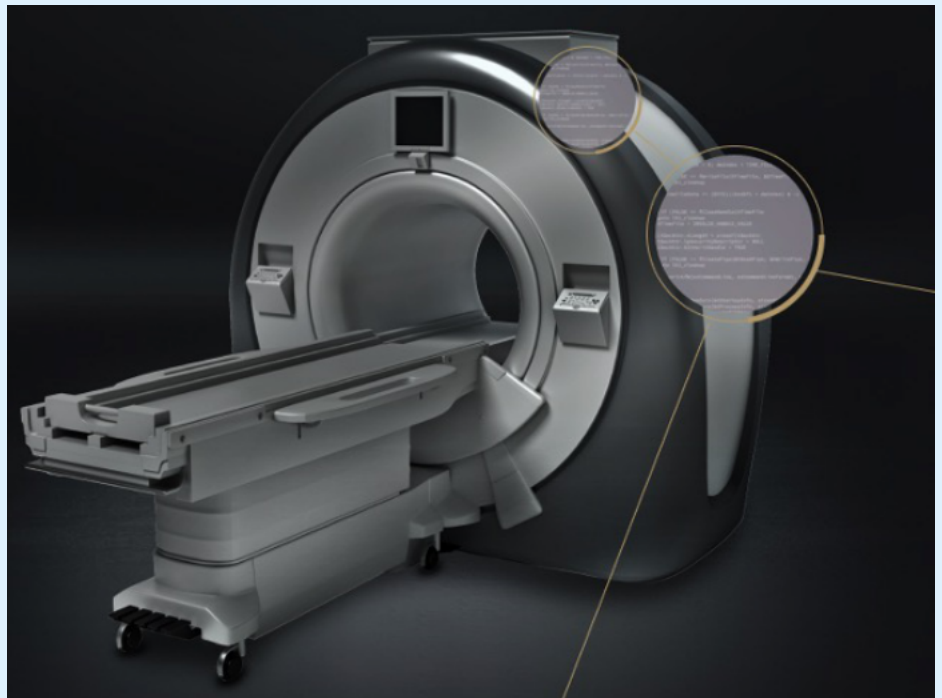
- **SBOM/CBOM generator** – will validate the compositions of your firmware (software packages, versions, associated licenses) and expose vulnerabilities lurking within your code and throughout your supply-chain. Leading solutions will go above and beyond simple SBOM/CBOM generation, providing extended contextual data needed for vulnerability



**Technology is your best ally when it comes to setting up your vulnerability management program.**



management tasks (e.g. info on the underlying OSs, hardware architectures, cryptographic properties, network interfaces, APIs and more). Make sure this is an automated tool that can cope with the growing volume of software – manual procedures don't scale well. Additionally, as in many cases you don't have access to the software source code, a binary analysis solution will cope with your close-source code/firmware.



- **Consolidated threat intelligence feed** – you need the most relevant threat intelligence to keep track of vulnerabilities, security threats and exploits. Make sure you can aggregate information from multiple sources – public vulnerability databases (e.g. NIST NVD, VulnDB, ExploitDB), regional vulnerability databases (e.g. JVN, CN-NVD) GitHub issue trackers, bounty programs, the Dark Web and other 3rd party and private threat sources.

- **Compliance validation engine** – this will include a policy engine that lets you define rules and requirements, that can be automatically validated as

part of your vulnerability management workflow. Leading solutions will have predefined policies covering relevant medical cybersecurity regulations and standards, OSS licensing policies and can also be customized to support your own unique policies.

- **Automated zero-day detection engine** – dealing with CVEs is one thing, but when it comes to proprietary code, you want to have the ability to discover coding weaknesses such as buffer overflows, double free and other weaknesses that may lead to risky DoS or remote-code-execution scenarios.

- **Automated triaging and prioritization** – scale and focus are essential when it comes to vulnerability management, so you want to automate as much as possible your triaging activities, filtering out any vulnerabilities that do not affect your code and prioritize the reminder based on impact and severity.

- **Integrated workflows** – to be most effective and close the security loop as quickly as possible, it will have to integrate with the other IT and operational systems and workflows you have in place such as ALM/PLM (to plan your product lifecycle also in the context of security), CI/CD,

## Vulnerability management is not a one-off SBOM or CBOM snapshot, but requires continuous monitoring of vulnerabilities throughout the product lifecycle.

ticketing and tracking systems and even remote software update systems and SOC systems. Make sure you have well documented APIs to enable such crucial integrations.

- **Continuous security monitoring system** – most, if not all, medical cybersecurity regulations and standards require that you keep track of threats, assess their impact on in-service equipment and fix any security issues. Make sure the processes you put in place are backed by an automated product security operations system, that automatically assesses new threat intelligence and its impact on our products.

- **BI dashboards & reporting engine** – make sure you can track your security status within and across development programs, supporting decision making and collaboration amongst management, internal teams and external suppliers. A

dashboard visualizing your security posture or an assessment report shared with your suppliers will go a long way in that regard.

### Summary

Vulnerability management is not a one-off SBOM or CBOM snapshot, but requires continuous monitoring of vulnerabilities throughout the product lifecycle. It is a strategic imperative for all medical device manufacturers for safeguarding their products and to enable rapid compliance of ever changing regulations and guidelines. Late discovery or improper handling of vulnerabilities can lead to costly recalls, device re-architecture, and a direct hit on the organization's brand and reputation of reliability.

Product security teams need to establish ongoing processes and supportive policies to proactively and collaboratively manage

cyber-risk in medical devices, together with their management, R&D organization and suppliers.

This involves gaining clear visibility and understanding of the make and characteristics of their software asset inventory, reliable and timely vulnerability data, automated workflows, that will drive cybersecurity within the organization and continuous vulnerability management well after medical equipment has been sold and deployed.

Learn more about Cybellum at [www.cybellum.com](https://www.cybellum.com)



# MOVING YOUR HEALTHCARE ORGANIZATION TO THE CLOUD? HERE'S WHAT YOU NEED TO KNOW

---

While the last two years accelerated digital transformation across a wide range of industries, this has been a long time coming for healthcare. Healthcare has been undergoing a massive shift to improve security, streamline operations, and enhance the patient experience - and much of that shift centers around the movement to the cloud.

**Tim Hinrichs**, CTO, Styra

## In the cloud, not only do apps need to be secure, but all platforms those apps run on top of need to be secure as well.

Cloud-native ostensibly offers a better, more accessible user experience marked by enhanced uptime, reliability, and efficiency. Here are just a few of the elements impacted by the movement to the cloud:

**Telemedicine.** Once a niche offering, telemedicine exploded in popularity during the pandemic and has all the signs of becoming a mainstay. The security concern: every app and every connection needs to be secure and HIPAA-compliant.

**Fast Healthcare Interoperability Resources (FHIR).** The healthcare industry has been gradually shifting to electronic healthcare records, along with the digital storage and sharing of those records. The upside of electronic health care records is that healthcare professionals can access critical information about patients almost instantly. The security concern: how do you guarantee that only the right people get access to sensitive records when needed? The industry is trying to standardize APIs to mitigate risks while facilitating necessary access.

**Regulations.** Compliance and regulations vary widely by state. For example, in California, parents no longer have access to their child's healthcare records once that child turns 12. How do you standardize processes across non-standard regulatory environments?

The common theme in all of these: ensuring

security without compromising standards of care or the patient experience. That's a tall order, to say the least. And it's one that the movement to the cloud is designed to accommodate.

And yet, moving to the cloud comes with inherent security risks. In the cloud, not only do apps need to be secure, but all platforms those apps run on top of need to be secure as well. Securing a cloud application means moving beyond firewalls and the assumption that the application is running on a local network; it means embedding security controls into every piece of software.

If your healthcare organization is accustomed to having everything stored and processed locally, the cloud can feel overwhelming. Modern cloud-native applications may now be composed of dozens or hundreds of microservices, housed in containers and hosted on immutable, dynamically scaling platforms like Kubernetes. If all of that sounded like another language to you, that's because it is another language—and the language of cloud-native has a steep learning curve. The key takeaway: modern applications and the platforms they run on are built out of possibly hundreds of individual components, each of which must be secured.

Does that mean you should avoid the cloud? Not at all. When navigated appropriately, the benefits of moving to the cloud (flexibility,

scaling, iterative capability, user interface, functionality with the decentralized workforce, operations that don't break down if you have a local issue, etc.) far outweigh the risks. But it does mean you should plan. Here's how.

## Embed security

The best way to optimize security and functionality when moving to the cloud is to build security into your people processes and software. Specifically, that entails addressing the authorization side of security: the rules that decide who can update information when using your software, e.g., which healthcare records a doctor can read.

When it comes to policy, a key to success is to fully embrace a policy-as-code approach.

Adopting policy-as-code means decoupling policy from your application code and using a dedicated, declarative language to define the conditions and rules that make up that policy.

Can application X access information Y at Z time from location Q? The policy code decides. No human intervention required. No need to implement it repeatedly throughout your application.

Can Bob in patient services access Maria's file and send it to Acme Insurance Company via an encrypted email? The policy code decides. No human intervention required.

Adopting policy-as-code means developer teams can focus on creating features that help customers; security and compliance teams can audit policies without digging through reams of application code written in different languages; operations teams can enforce the rules that make the cloud platforms themselves safe. In short, policy as code helps each team focus on their strengths, working together to deliver secure software to customers as quickly as possible.

If healthcare organizations adopt a policy-as-code approach from the beginning of their move to the cloud, productivity increases and risks are reduced. This sounds great in theory, but how do you do it?


**The best way to optimize security and functionality when moving to the cloud is to build security into your people processes and software.**

## Best practices for adopting policy-as-code in healthcare

**1. Get on board with zero trust.** A zero-trust framework means baking security right into your software, so a move to the

cloud means that no matter where your applications are deployed, security goes with them. Zero trust ensures that every action a person (or machine) takes is vetted, without relying on other safeguards that were supposed to be checked earlier.

**2. Put a security framework in place, not a security band aid.** When you establish a security framework, bringing in new people, software, or iteration doesn't involve starting from scratch. Instead, those new elements can snap right into the existing framework. Nothing gets deployed that isn't already secure, because it's all part of the framework.



**If healthcare organizations adopt a policy-as-code approach from the beginning of their move to the cloud, productivity increases and risks are reduced.**

Not only does this streamline security and make it more reliable, it also bridges the gap between DevOps and security/compliance teams: everyone's on board with the framework, everyone knows what to expect, and changes don't automatically require new conversations and new approvals.


**3. Shift Left.** It's essential to ensure that the framework makes things easier for developers, not harder. You can't have a framework that inhibits developer productivity. The framework should be set up in a way that makes security controls fully accessible and understandable to developers early in the dev process. They need to know right away if something they've developed doesn't fit in the framework, and they shouldn't have to wait for delayed feedback. Shifting left means failing quickly and iterating just as fast.

**4. Get a policy-as-code engine on board.** Adopting a policy-as-code approach is only as easy as the engine you have doing the heavy lifting for you. A policy-as-code engine like Open Policy Agent (OPA) can smooth out the shift to cloud-native. Why? Because it's decoupled from your tools, so your team can take the wheel without steering you into the ditch. OPA is also designed with enough

architecture flexibility to deliver zero trust authorization wherever you want policies enforced.

### **A policy as code approach enhances security and productivity**

A healthy move to the cloud is one that is done securely and without inhibiting productivity. In fact, doing it right means drastically enhancing security and productivity. Again, the best results come from starting early and adopting a policy-as-code solution from the get-go, but if you're already wandering around the cloud, it's not too late.



# DESPITE PRIVATE STORAGE, HEALTHCARE ORGANIZATIONS ARE A TOP TARGET OF RANSOMWARE

Ray Overby, CTO, Key Resources

**As client demand for seamless access to patient data from wireless-capable devices grows, so does the likelihood that hackers will reach the goldmine of data stored on the mainframe.**

Within the last decade, healthcare organizations have spent tens of millions of dollars to digitize our health records. The move promised ease of access and greater collaboration between doctors, insurers, and pharmacies, but the fact remains that these records contain some of the most personal, sensitive data in our digital world, and should be adequately secured.

Most of these records exist natively on the mainframe and, oddly, healthcare organizations aren't taking the right steps to protect them. As a result, healthcare has become a prime target for hackers; one recent report highlighted that 67% of healthcare delivery organizations (HDOs) have been victims of a ransomware attack. With shutdowns, legal fees, and total loss of business

on the line, why aren't healthcare organizations taking the steps to protect their mainframe?

Healthcare organizations are obviously aware of how sensitive healthcare records are and the legal implications associated with improper disclosure; unlike organizations in other industries, they have been hesitant about moving data to the cloud, and many have opted to maintain their own data centers. But even though the mainframe upholds its reputation for strong security, it's not impenetrable. Mainframe attacks happen, and it's up to organizations to invest in solutions to prevent them and/or mitigate them.

### Healthcare data on the move

As client demand for seamless access to patient data from wireless-capable devices grows, so does the likelihood that hackers will reach the goldmine of data stored on the mainframe.

Mainframes are increasingly connected to distributed systems to provide access to personal data that could open doors.


Take, for example, a prescription filled at your pharmacy: the prescription and its refill information live on the mainframe, but the actual refilling process runs across a distributed system – your doctor electronically posts the prescription, sends it to the pharmacy, your pharmacy settles with your insurance provider. The apps you use to review your prescription, regardless of which provider they belong to, likely exist on distributed systems as well. With so much interconnectivity occurring between healthcare organizations, the number of potential holes for hackers to slither through is endless.

### Ransomware in healthcare could cost dollars and lives

Because there's no wall between the mainframe and

the distributed system where an app lives, hackers are part of the network as soon as they get into the app. Once hackers gain access to distributed records or accounts, all it takes is one exploit to piggy-back into the mainframe. Once on the mainframe, they can use software vulnerabilities to escalate their privilege and be able to do whatever they want.

Ransomware is the worst-case and unfortunately the most likely scenario. Since the data healthcare organizations hold is extremely sensitive, the likelihood organizations will opt to pay the ransom is high but paying doesn't guarantee that they'll get all their data back. Shutdowns related to attacks also cost organizations; in a [recent survey](#) of IT leaders and biomedical engineers and technicians sponsored by CyberMDX and Philips, 48% of hospital executives reported either a forced or proactive shutdown in the last 6 months as a result of



**Mainframe attacks happen, and it's up to organizations to invest in solutions to prevent them and/or mitigate them.**



external attacks or queries. For midsize hospitals, shutdowns averaged nearly 10 hours, costing \$45,700 per hour.

What's worse, ransomware-induced shutdowns can impact patients. In the most extreme case, this year saw the first alleged ransomware death, as a baby delivered mid-hack later died, due to a lack of heart monitor visibility during delivery. As the number of ransomware attacks increase in number and severity, tragedies like this one could become more common.

## HIPAA compliance raises costs

Healthcare organizations could face additional costs due to aspects of HIPAA that apply to digital information. If organizations aren't proactively protecting their IT, they're in direct violation of the following HIPAA requirements, and could face fines in the event of a breach. Under HIPAA organizations must:

- Implement policies and procedures to prevent, detect, contain, and correct security violations

**If organizations aren't proactively protecting their IT, they're in direct violation of the HIPAA requirements, and could face fines in the event of a breach.**

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Implement procedures to regularly review records of information system activity
- Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes
- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner

## How to protect your organization

Organizations need appropriate staff to maintain a secure environment, mitigate excessive access, and fend off attackers.

The previously mentioned survey reported that almost half of all respondent types find their medical device and IoT security staffing inadequate. This doesn't just put those systems at risk, but the mainframe as well. Health data that these devices maintain most likely comes directly from the mainframe. If hackers can gain access to mainframe-connected devices and applications, all it takes is one vulnerability to provide eventual mainframe access.

Beyond staffing the IT team, organizations also need to

designate one lead protector/guardian of the mainframe: the mainframe security architect. If an organization has struggled with accountability for the mainframe in the past, designating this role is the answer. They need to be both business and tech savvy, understanding the direction the business is going (i.e., the integration of platforms) and what needs to be done to maintain integrity at all levels.

Lastly, to support their strapped IT teams, organizations can deploy automatic processes to check for excessive access issues on a regular basis. Currently, 65% of IT teams in hospitals rely on manual methods to review their devices. While excessive access checking can uncover hundreds of thousands of findings, it's an arduous process when done

manually, and manual checks only uncover which groups have access to data sets or resources, not specific users. Automation speeds up the process and helps organizations drill down to the user level, to get a detailed report of who has access to what.

Across the industry, many healthcare industries live with a false sense of security, instilled in them by the decision to maintain their own data centers. But as hackers' tactics, techniques and procedures become more sophisticated, even the strongest of fortresses are at risk of attack. If IT teams don't have the people or tools required to protect their mainframe, it's only a matter of time before organizations fall victim to ransomware and face devastating costs.



# HEALTHCARE CYBERSECURITY REPORT