



MedTech's security and regulatory landscape

SYNOPSYS[®] |  **MEDTECHDIVE**

Custom content for Synopsys by studioID

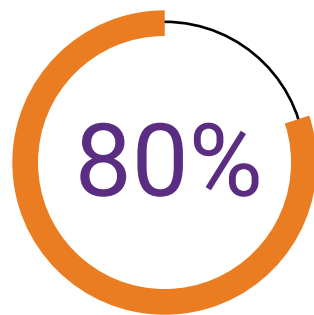
Medical devices have come a long way from being standalone technologies, and they continue to advance rapidly to deliver better quality care to patients. A significant number of medical devices and systems— from radiology equipment to wearables and implantables— have software components and interconnectivity capabilities. Their adoption in clinical practice is also considerably high. On average, U.S. hospitals have between 10 to 15 connected devices per bed.

This has improved patient monitoring, patient experience, care delivery efficiency, workflow management, and overall clinical outcomes. But it has also inadvertently made these network-connected devices more vulnerable and susceptible to malicious attacks and privacy violations.

The abundance of available data stored and transmitted by connected medical devices has, in part, made the healthcare industry a popular target for malicious actors or opportunistic attackers. In fact,

healthcare is currently the most targeted sector for data breaches, with attack rates increasing over time. According to the U.S. Department of Health and Human Services' Office for Civil Rights' breach portal, healthcare data breaches increased by 25% from 2019 to 2020.

Medical device manufacturers and healthcare stakeholders are hyper-aware of these risks, and have experienced their materialization. A 2021 survey of senior executives at Fortune 1000 medical device manufacturers, digital and mobile health companies, and telemedicine providers found that 80% of its participants had suffered at least one cyberattack in the past five years. But despite this, only 13% of these leaders in the Internet of Medical Things (IoMT) believe their business is very prepared to mitigate future risks. More, only 18% believe that the security built into their medical device products is strong. The majority of the rest rate their defenses against cyber attacks as just adequate or not robust.



of its participants had suffered at least **one cyberattack in the past five years.**



FDA guidelines

The U.S., the Food and Drug Administration (FDA) regulates medical devices and their safety in the U.S., and has been proactive in the medical device cybersecurity area. It has issued several regulatory and guidance documents on pre and post-market medical device cybersecurity. The *Content of premarket submissions for management of cybersecurity in medical devices—Final guidance for industry and FDA and the Postmarket Management of Cybersecurity in Medical Devices*, released in 2014 and 2016, respectively. The FDA also released a premarket draft guidance *Content of premarket submissions for management of cybersecurity in medical devices—Draft guidance for industry and FDA* in 2018. These guidance documents are intended to help medical device and system vendors address cybersecurity issues in connected medical devices.

Finally, in mid-2018, the FDA adopted UL 2900-2-1 as the consensus standard for software cybersecurity for network-connectable products. The UL 2900-2-1 sets specific criteria for cybersecurity testing of network-connected medical devices and supports existing risk-based methodologies. That said, the FDA does recommend several other reference standards as many of the security concepts that may be included in a particular design could require additional best practices guidance.

The requirements contained in the *Content of premarket submissions are mandatory, while the use of the Postmarket Management of Cybersecurity in Medical Device* guidance document and the standard is not compulsory.

The importance of **building security** into the development process of medical devices

Until the past ten years or so, medical device developers did not usually consider cybersecurity risks as part of a product's design. Security has become a significant topic in the medical device landscape, as the potential consequences of insecurely built medical devices are serious and numerous. Compromised patient safety, reputational damage, exposure to litigation, and non-compliance with privacy regulations are some of them.

Forty percent of healthcare delivery organizations and 31% of device makers surveyed in a Ponemon Institute study are aware that patients experienced an adverse event or harm due to an insecure medical device.

Making security a part of the device development process is a proactive step that device makers should always take. When a product receives approval, goes to market, and starts being widely used, security issues and vulnerabilities become considerably more challenging and more expensive to fix. A medical device with security built into it throughout its development process is less likely to face security issues post-market. More, when security features are tacked on after design, they tend to be implemented poorly and hinder ease of use.



Forty percent of healthcare delivery organizations and 31% of device makers surveyed in a Ponemon Institute study are aware that **patients experienced an adverse event or harm due to an insecure.**

Security Challenges for MedTech Developers

Technical know-how

Eighty percent of medical device manufacturers in the Ponemon Institute study say that medical devices are very difficult to secure. Synopsys principal consultant, Michael Fabian, primarily attributes this to the inadequacy of technical know-how and lack of clear and robust security processes.

“Most of the challenges that MedTech developers have with securing the devices they create center around the ‘how’. The security standards and compliance requirements for device makers to meet are outlined in guidance documents and regulations, the ‘what’” he explains.

“However, in practice, implementing these standards proves to be significantly more complicated than simply reading these documents may suggest. They are written to apply to a multitude of potential

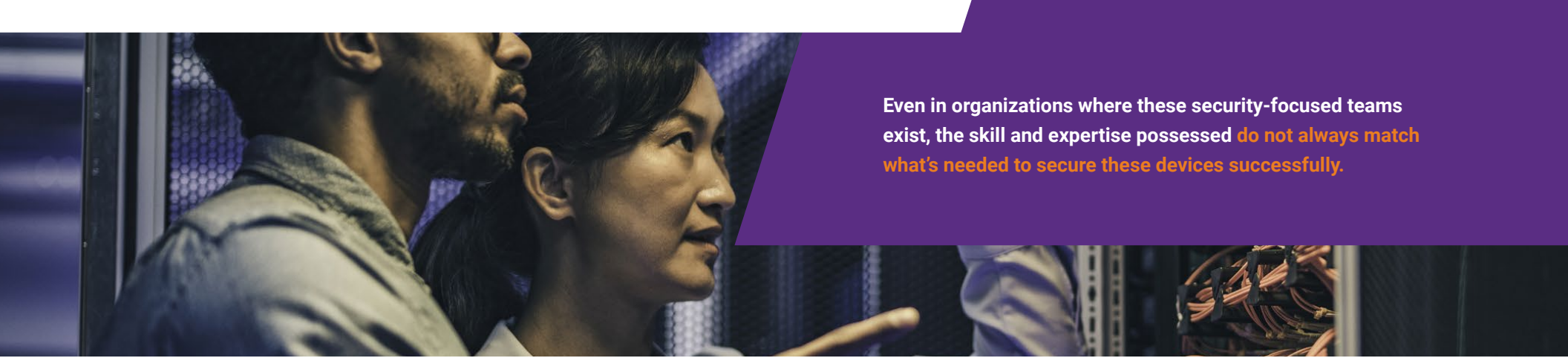
devices and require thoughtful analysis to apply to a specific design and development process.

Medtech developers often have gaps in the knowledge, skill, and know-how required to implement these security standards and processes. The standards themselves are not technical, but the derivative work required to implement them is.

For instance, the FDA’s adopted UL 2900-2-1 primarily specifies the requirements for network-connected medical devices to meet, but does not set out which specific testing methods should be used. The device developer must themselves decide what testing methods and criteria to use after considering both the standard and the product’s risk factors.



of medical device manufacturers in the Ponemon Institute study say that **medical devices are very difficult to secure.**



Even in organizations where these security-focused teams exist, the skill and expertise possessed **do not always match what's needed to secure these devices successfully.**

Other challenges—some of which partially stem from this lack of expertise—include:

Funding

While difficulty in acquiring funding is not limited to just cybersecurity, the problem seems to be more pronounced here than in many other areas of product development. With cybersecurity, proving returns on what can sometimes be a considerable investment is hard—and oft-times nearly impossible. If there are no successful incidents, it suggests that the current security measures are working. However, it is difficult to prove that any attempts were made to attack the systems in the first place.

Security professionals have models and calculations they employ to prove positive financials/returns on investments. Still, those don't often translate well when it comes to medical devices—especially newly developed ones where there is an unsurprising dearth of data on the number, types, and forms cyberattacks will take.

Most times, substantial increases to budgets only happen after serious attacks or data breaches have happened.

Absence of shortage of cybersecurity expertise

Large medical device companies often have teams dedicated to implementing security standards and meeting compliance with various levels of experience. Smaller companies, with more limited resources, typically do not. As a result, they are sometimes limited in their capacity to build security into their devices from the early stages of development.

Still, even in organizations where these security-focused teams exist, the skill and expertise possessed do not always match what's needed to secure these devices successfully.

Mergers and acquisitions

In many cases, software is part of the deal when medical device companies undergo mergers and acquisitions. Determining code quality and properly analyzing risks that come with these acquired software is not often prioritized during the restructuring process. Unfortunately, undetected issues can pose serious risks to data security and patient safety, not to mention lengthen deal timelines and increase remediation costs.

Best Practices and Solutions

Complying with and meeting the FDA's guidelines and standards is a step in the right direction. However, it should be highlighted that compliance with regulation does not always equate to quality security. Compliance is a demonstration against a set of static principles. Good security, on the other hand, needs to address individual and dynamic devices and intended environments. Here are some of the best practices for building safe, secure medical devices.



Integrate security early in the development process:

Security should be part of the process and not a post-development add-on. Medical device developers need to get engineering and security teams to work together as early in the development life cycle of devices as possible. Incorporating exercises and activities such as threat modeling, architecture risk analysis, static application security testing (SAST), and penetration testing throughout the development process is also essential to building security into the development process.



Undergo security training: Development teams should complete security training, where they learn how to properly interpret security standards guidelines and documents, as well as gain knowledge of the types of processes they need to have in place to apply them. Security training should also focus on ingraining the importance of designing security into medical devices, as it is only with this mindset that security can truly be prioritized.





Perform audits during M&A process: When undergoing mergers and acquisitions, software audits should be performed to identify, understand, and mitigate risks. These audits include open-source and third-party code audits, open-source risk assessments, web services and API risk audits, penetration test audits, static application security test audits, security controls design analysis, code quality audits, software development audits, and design quality audits. Collectively, these audits are known as Black Duck audits.



Assess your AppSec threats, risks, and dependencies: Security risk assessments should be carried out to enable identification of missing or weak security controls, understanding of secure design best practices, and mitigation security flaws that will increase risk of breaches. Risk assessments allow you to evaluate risk from different vantage points, create risk profiles, and leverage risk rankings to assess business impacts and prioritize remediation planning.



Repeated testing: Testing your solutions throughout the software development life cycle helps you find and fix quality and compliance issues early. Executing tests such as static application security testing, dynamic application security testing, and mobile and network testing regularly is recommended.



Use compliance tools and services: Insecure code is often the cause of medical device software failures and breaches. There is a myriad of tools available to help streamline typically infinite potential security issues and system failure causes to a manageable number. Some of them include such as static code analysis, software composition analysis, and fuzz testing. They effectively produce repeatable results and quantifiable metrics for auditing purposes. Using these tools can help lower risk and cost without extending time to market.



Partner with trusted advisors: Navigating the medical device development landscape can be complex. More specifically, prioritizing device ease of use while fulfilling regulatory cybersecurity requirements simultaneously can seem quite challenging. Consequently, it's essential to partner with leading experts in medical device security like Synopsys. Your security partner should ideally have experience tailoring medical security needs to peculiar cybersecurity needs. For instance, at Synopsys, our security program strategy and planning, risk assessments and architecture reviews, and device- and protocol-specific security testing all combine tools and services employed in ways that suit our clients' individual needs.

Using a multi-point solution vs. one-point solutions

Medical device security is already complex; why complicate it further by using many different vendors and partners?

Increase visibility, improve efficiency, and cut down vendor administration by partnering with a vendor like Synopsys.

Synopsys provides the right combination of tools, services, and personal support for your development process.



The Bottomline

Integrating security into the end-to-end development process is key to shipping fully secure medical devices. To do this, device developers must successfully navigate the security and regulatory landscape—a process that requires continuous support. Partnering with experienced software security specialists can make the journey faster and smoother.

SYNOPSYS®

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

[LEARN MORE](#)



studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

[LEARN MORE](#)