Protecting the IoMT and your business

A guide to medical device cyber-attacks and effective threat modeling

IriusRisk

IriusRisk

Threat Modeling to support digital transformation

Modern healthcare is increasingly reliant on digital services and connected medical devices. But with the unstoppable wave of digital transformation comes a devastating tsunami of cybercrime activity.

Criminals see cloud-connected medical equipment as a prime target; patient data and records hold great value on the black market since bad actors can use them to make false insurance claims, access drugs illegally, or sell the data. And if hackers can get into a medical facility's network through a back door left ajar by a vulnerable medical device, then they can effectively hold it to ransom.

The results are costly. A medical device manufacturer found to be at fault faces severe financial penalties and chronic reputational harm and could lose licensing to sell products in some regulatory territories. But businesses can and must fight back.

Introducing automated threat modeling to device development processes identifies risks that can be eliminated on the fly. Avoiding vulnerabilities in this design and build phase is cheaper than patching the finished device. IriusRisk is a global leader in cybercrime threat modeling across vulnerable sectors like healthcare and financial services.

This report expands on the cyber issues faced by the Internet of Medical Things and explains how IriusRisk is the ideal and easy-to-use partner for medical device manufacturers.

Contact us to request a demo

The growing threat from cybercriminals

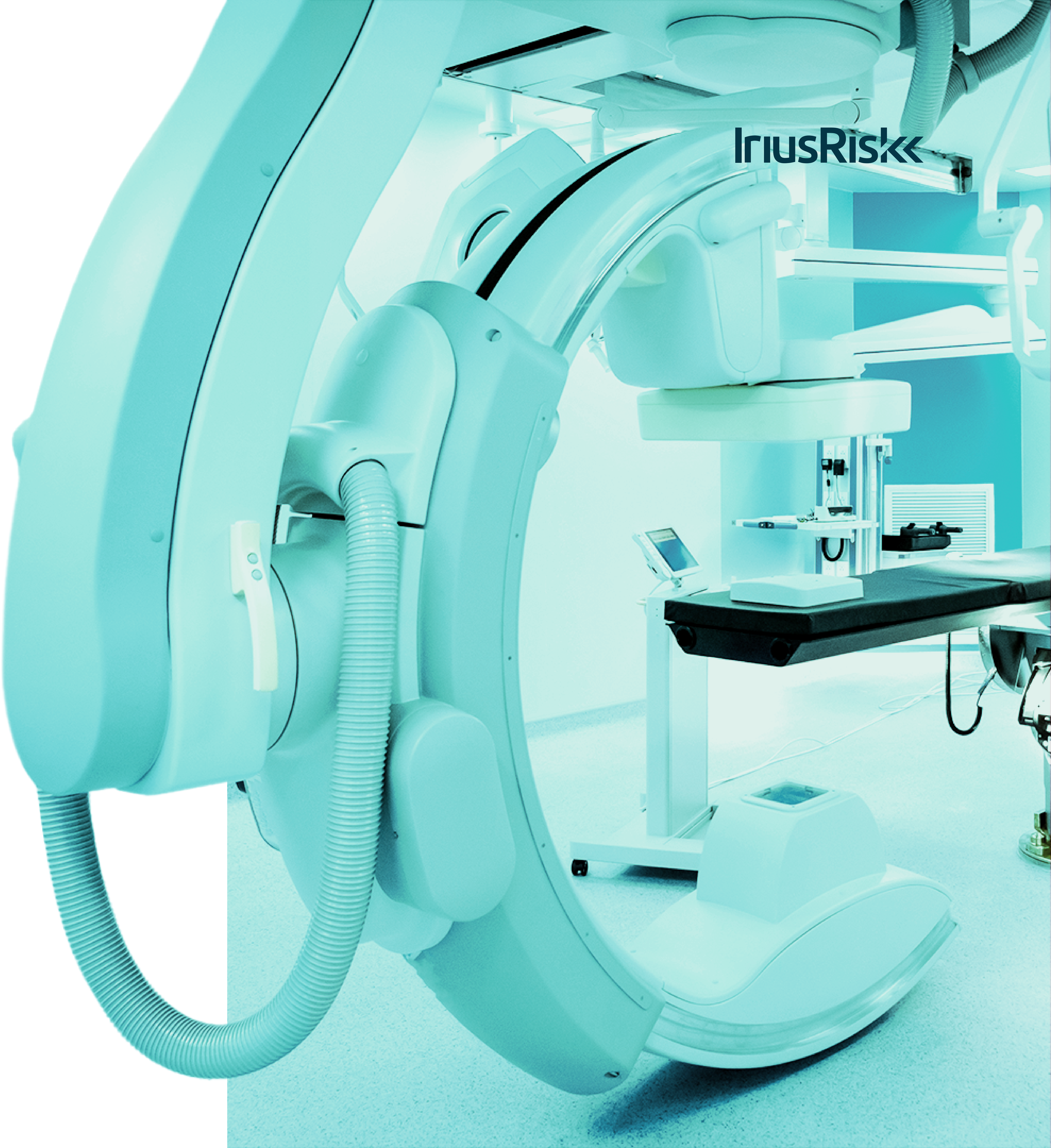
Cybercriminals now place the medical and healthcare industry at the top of their hit list. For them, there's a perfect storm of easy targets in the form of vulnerable equipment and rich pickings from stealing valuable patient records and data.

There's also money to be made from ransomware for hackers able to connect the digital dots from a vulnerable medical device to a broader facility network.

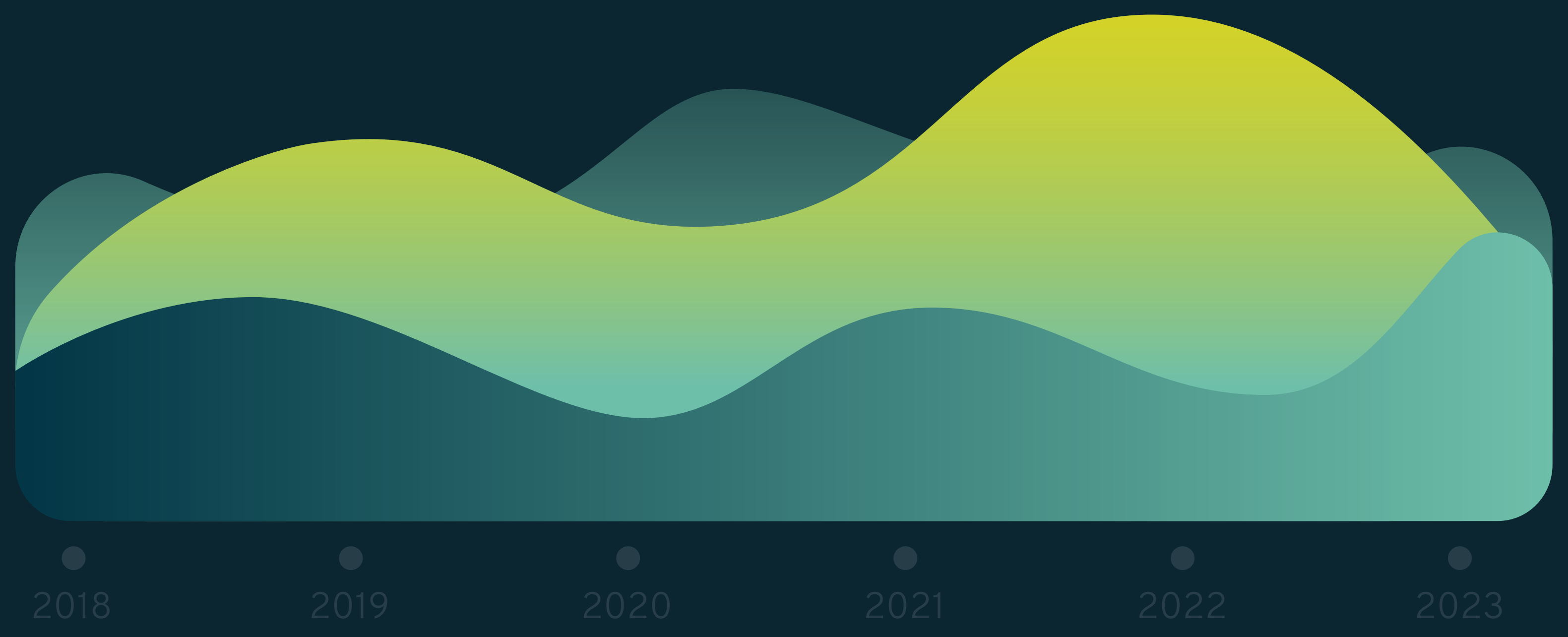
According to Statista, the average cost of a healthcare data breach is over $10 million, which will continue to rise. This hefty sum puts healthcare at the top of the league table for breach cost, above even the financial sector.

But of course, there is also a human price to pay. Patients suffer the indignity of personal data being stolen. In the worst-case scenarios, their healthcare is impacted as a hacker tampers with a device's functionality or the equipment goes out of service. There is then downtime while code fixes are found and deployed.

Patients can also become targets of fraud based on their medical history because it's unique and cannot be "stopped" and changed, like, for example, stolen credit card information.



Stats can't be ignored



22.5 million healthcare records were breached in the US in the first half of 2022

of medical devices are at the end of their life using older, more exploitable tech

of healthcare IT professionals worry that patient information is exposed, lost, accessed, or stolen

If you think the threat of data breaches is overplayed, consider this: according to GlobalData, 22.5 million healthcare records were breached in the US in the first half of 2022 alone.

GlobalData's Cybersecurity in Healthcare 2022 report also highlights that spending on cybersecurity in the medical device sector will soar to $1.2 billion by 2025, up from $869 million in 2020. While seemingly rising alarmingly, the costs can be controlled by efficient threat modeling offered by IriusRisk.

But while the threats remain real, 86% of healthcare IT professionals worry that patient information is at risk, as stated in the A Critical Investment: Taking the Pulse of Technology in Healthcare report by SOTI.

Further, more than half of healthcare IT professionals (56%) thought that interconnected medical devices at their facility were not adequately secure. Their concerns are justified since a vast 70% of organizations have suffered a breach, either accidental or malicious.

The problem worsens as medical devices age. According to Cisco, 60% of medical devices in healthcare are reaching the end of their useful life. That makes for an ageing set of equipment that might become increasingly exposed to hackers with ever-sophisticated illegal techniques.

New device breakthroughs pose a risk

As new medical devices and innovations emerge, so does the risk for those manufacturers who do not use automatic cyber threat modeling in the critical development phases.

With remote, cloud-connected equipment like pacemakers or arm monitors for diabetics, which link with mobile device apps hosted in the cloud, sending information to and from a central healthcare database becomes an open territory for hackers. But similar technologies are used for IV pumps and other medical devices.

In fact, IV pumps make up 38% of a hospital's IoT footprint, according to a study by Cynerio, and well-publicized breaches of IV pumps in recent years have confirmed that the threat is real. Fortunately, a breach of Alaris pumps in February 2023 was not denoted as critical. But it came only months after Baxter pumps were found to be at medium risk.

Regulatory recommendations for Threat Modeling

US directives

The US Food and Drug Administration (FDA) first raised concerns about medical device security in 2014. As you might imagine, the risk has grown exponentially since then.

In 2019, the FDA funded the Medical Device Innovation Consortium to raise awareness about threat modeling. And in 2022, it published an updated outline of best practices for threat modeling to strengthen cybersecurity resolve as part of a collaborative effort within the industry. It covers four areas:

- Understanding how a medical device operates
- Uncovering organizational weaknesses and vulnerabilities
- Understanding how to eliminate, mitigate or transfer the risk of a threat
- Accepting that threat modeling is a continuous process

The Playbook for Threat Modeling Medical Devices stresses that a diverse team at a medical device manufacturer should be involved in cyber threat preparedness and response. The process is part of what the FDA demands before approving devices for public use.

But while the playbook focuses on general threat modeling principles, it does not recommend one particular approach. This might leave some medical device manufacturers needing clarity about the best path to take.

EU directives

The EU has toughened up its stance on medical device regulation (MDR). New rules from 2021 tighten the safety of devices from a clinical standpoint, and state devices should use a robust cyber-secure approach.

But like the FDA's Playbook, the MDR, and the updated regulations for in vitro diagnostic devices (IVDR), these do not detail how manufacturers should guard against cybercrime.

As in the US, it means the best solution for European manufacturers is to seek third-party expertise and reassurance – like that provided by IriusRisk. Those that do not, might be vulnerable to multiple ransomware attacks, which have recently included a French hospital (2022), the UK's National Health Service (2022), the Irish Health Service Executive (2021), and a Finnish mental health facility (2020).

Trust in IriusRisk

IriusRisk provides an unequivocal automated threat modeling platform to protect your new devices from even the most persistent cyber criminals.

Federal/public sector organizations, financial institutions, and medical device manufacturers trust our platform. They recognize that threat modeling is part of the design process as recommended by The Open Web Application Security Project (OWASP) and the National Standard Institute of Technology (NIST), among many other notable bodies.

NIST says: “*We recommend using threat modeling early to identify design-level security issues and focus verification. Threat modeling methods create an abstraction of the system, profiles of potential attackers, including their goals and methods, and a catalogue of potential threats.*”

With IriusRisk, which can be delivered on-premises or over the Cloud, you incorporate security analysis from the start of a project rather than viewing security as something carried out at the end of a development lifecycle.

IriusRisk

What we do

The IriusRisk automated threat modeling platform fits your existing SDLC to secure design right from the start. It helps multiple teams to manage security risks at any one time. It analyzes weaknesses and vulnerabilities in coding no matter how many Infrastructure as Code descriptors are generated. And with DevOps routinely configuring code during a medical device's development lifecycle, it's easy to see why an automated threat modeling platform is needed.

The model helps prioritize investment and unblocks potential security bottlenecks that delay end delivery. For auditors and reviewers, IriusRisk outlines assets, controls, potential attack surfaces, trust-zone boundaries, and accepted risks.

Importantly, our threat modeling platform brings stakeholders together so multiple teams collaborate on security work throughout the design process. Working together encourages shared considerations of compliance, risks, and usability. It helps educate team members and potentially causes less friction on subsequent projects.

Above all, it encourages agile behaviour during the development process. It bonds security together with Dev Ops to create "DevSecOps," and there can be no better proponent of the Shift Left paradigm.

Key Benefits

Are you still wondering how automated threat modeling can help your medical device manufacturing operations?

Consider these key takeaways

- Threat modeling improves time to market for new medical devices
- Helps organizations remain secure, save costs and reputational harm
- Generate a threat model in minutes
- Import from your Infrastructure as Code
- Create a culture of collaboration between security and development teams
- The platform enables regulatory compliance and full auditing trails and reports
- NIST references it as the first step in the Recommended Minimum Standard for Developer Verification Code

IriusRisk case study

Customer

$10 million revenue US medical equipment manufacturer

Challenge

The client previously used a combination of manual threat modeling and the Microsoft Threat Modeling Tool. Its approach did not match best practices, and manual work meant the process could not be scaled, leading to potential risk.

The business needed more teams to have access to the threat modeling process.

Solution

IriusRisk solved the key issues. One person was assigned to manage the platform across the business, ensuring risk was centralized at a library level so multiple teams could assess and deal with each challenge efficiently as it emerged.

The client was able to customize IriusRisk to suit its needs fast, creating a comprehensive automatic threat model.

Results

IriusRisk demonstrates superior capabilities for scalable threat modeling that is easily understood by all teams, from security architects and devs to security engineers.

One huge benefit over the Microsoft Threat Modeling Tool is the ability to introduce product components to models and how these impact overall security risk.

There’s no better time to learn more about IriusRisk and how our platform can transform your organization’s development processes.

Simply click on the button below to get started with a platform demonstration.

Book now

IriusRisk