PHILIPS

Services and solutions delivery

Operational Intelligence

Healthcare and medical device cybersecurity

Executive briefing

The healthcare and medical device cybersecurity challenge

Hospitals and similar healthcare organizations typically have **300%** to **400% more** medical equipment than IT devices[1].

The danger of healthcare security breaches is ever-present and costly. In 2018, there were 365 reported healthcare data breaches involving 500 or more records, an increase of 83% from 2010, according to HIPAA Journal.

Evidence indicates that financially-motivated cybercriminals are the primary attackers against healthcare industry networks and medical devices. These hackers aim to steal and then sell medical records on the dark web, or to encrypt network connected devices to disrupt activity and hold companies for ransom. By disrupting hospital and nursing home networks, they have, in past years, been able to pressure healthcare organizations to pay for ransomware attacks in order to restore their operations sooner, thereby protecting lives.

Through 2020 and beyond, the healthcare sector will have to continue to evolve its security strategies to go beyond protecting data to the prevent downtime of compromised devices and ensure patient safety 24/7. In view of frequent ransomware attacks and with budgetary pressures intensified by covid-19, hospitals have to strengthen medical device cybersecurity but have very limited resources to do so.

As a 2019 survey by CynergisTek revealed one-third of executives considered medical device security one of the top five risks facing healthcare, yet most reported they lack an effective strategy to assess the risks posed by medical devices. Notably, more than a quarter said they don't have any risk assessment process in place at all.

1 Medical Device Security, HIMSS.org

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

Collaboration is key to effective medical device cybersecurity

With industry-leading cybersecurity strategies for both its own products and the third-party software in its systems, Philips has a policy of proactive cybersecurity with collaborative information sharing. Far from being a device manufacturer issue alone, effective medical device cybersecurity demands collaboration between hospitals, manufacturers, regulatory agencies such as the FDA, and the research community are essential to successful end-to-end protection of hospitals and their patients.

Gal Gnainsky from Philips Group Security explains how Philips is committed to proactively addressing the security concerns of its customers and is forging partnerships to put in place its visionary medical device cybersecurity strategies:

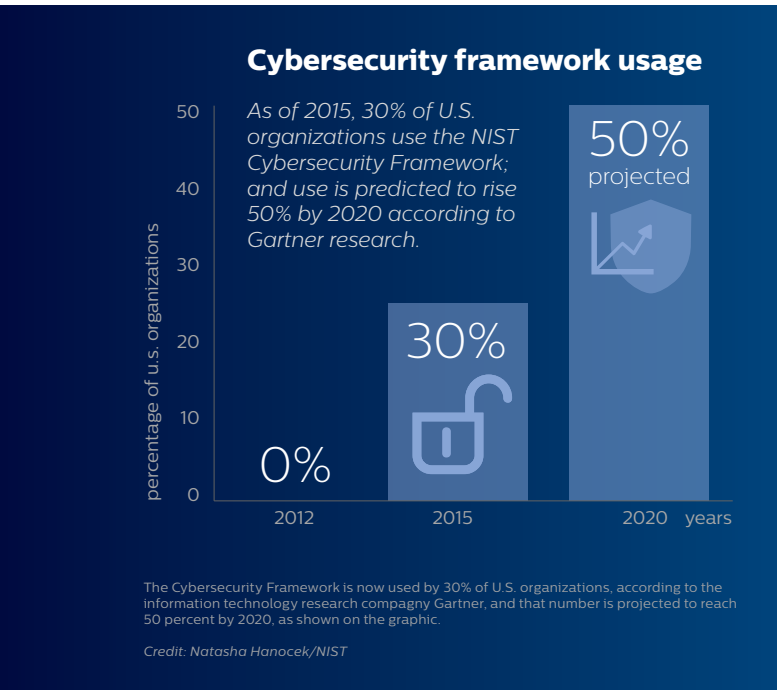
“We view healthcare as the delivery organ to which we need to introduce core cybersecurity and medical domain cybersecurity functions. This is a complex process though because, unless organized efficiently, it will cause operational challenges, such as increased downtime and overheads. To counter this, our solutions align operational technical maintenance workflows and cybersecurity workflows wherever possible. Our cybersecurity services align with technical services and cover all of the connected equipment in the medical domain.

At Philips, as a medical device manufacturer and health technology company, we work in partnership with our healthcare provider colleagues to define and implement comprehensive medical device cybersecurity and data security strategies. To guide our efforts, we have created a global policy to address the evolving nature of security in medical technology, including product feature requirements, security threat assessment and tracking, and compliance with local government standards.”

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

NIST-based services help meet the challenges of medical device cybersecurity

Philips offers healthcare providers a full suite of medical grade cyber security services to help manage their cybersecurity risks in connected medical devices and manage their critical assets. Our solutions have been designed to align with global cybersecurity best practice and are based on the NIST cybersecurity framework, covering the whole spectrum of identify, protect, detect, respond and recovery.



The Cybersecurity Framework is now used by 30% of U.S. organizations, according to the information technology research compagny Gartner, and that number is projected to reach 50 percent by 2020, as shown on the graphic.

Credit: Natasha Hanocek/NIST

Additionally, as the privileged access that is necessary for remote maintenance services can be a significant risk to healthcare providers, Philips also provides high resolution auditing of our remote access and provide possible integration with top remote service access management solutions. And taking into account that many healthcare providers have economic incentives to keep using legacy systems, Philips secure lifetime extension services help customers maximize the lifetime usage of their medical devices, by providing upgrade paths and mitigating controls to maintain acceptable security postures.

Integrating people, process and technology, Philips consultancy services help customers with regulatory compliance, risk and vulnerability assessments of medical systems. We implement security standards that meet, or exceed, current regulatory requirements and industry best practices, including:

- Philips' product security risk assessments are aligned with the FDA recommended standard ISO/IEC-800001 standard, and numerous other standards including NIST 800-53 Rev 4, ITIL v3.1.24 and ISO/IEC-27000 series standards.
- Philips is also compliant with ISO 14971, EU Directive 95/46/EC and both HIPAA Security and Privacy Rules.
- Creation of customer-facing information such as the industry-standard Manufacturer Disclosure Statement for Medical Device Security (MDS2).
- Support for FDA guidance on Premarket Management on Cybersecurity in Medical Devices, and FDA Postmarket Management of Cybersecurity in Medical Devices.
- Trained Philips professionals have considerable cybersecurity and medical device expertise and credentials like ISO27001, SOC 2, HIPAA aid in building thought leadership and credibility in medical device cybersecurity.

And of course, the Philips Healthsuite digital platform (HSDP) provides the basis and framework for security and privacy in the connected cloud. Within the Philips connected cloud HSDP this framework is the Information Security Management System (ISMS) which governs design for security and privacy in platform product and services creation, as well as risk assessment and incident response processes.

Security controls are embedded at various levels – application security, computing security, data security, information security, network security – as well as administrative and operational safeguards. Security and privacy controls are mandated in the initial designs to ensure effective data protection across all platform capabilities.

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

Philips also takes the lead in collaborating with regulatory agencies such as the FDA and international regulators, industry partners and healthcare providers, among others, to close security loopholes and implement safeguards. The organization also actively participates in key industry groups that have a security or privacy focus, including AdvaMed, MITA, and many others worldwide, engaging in best practices for identifying, addressing and publicizing potential vulnerabilities. Philips cybersecurity officers have taken leading roles in helping create global standards as part of cybersecurity task forces, including the International Cybersecurity Guidance initiative by the International Medical Device Regulation Forum (IMDRF).

How to safeguard medical devices and manage critical assets

When developing a device - or assessing the risks associated with using a device, Philips Group Security applies the NIST cybersecurity framework for Improving Critical Cybersecurity Version 1.1. This voluntary framework consists of standards, guidelines and best practices to manage cybersecurity risk. While the primary stakeholders of the Framework are U.S. private-sector owners and operators of critical infrastructure, its user base has grown to include communities and organizations across the globe.

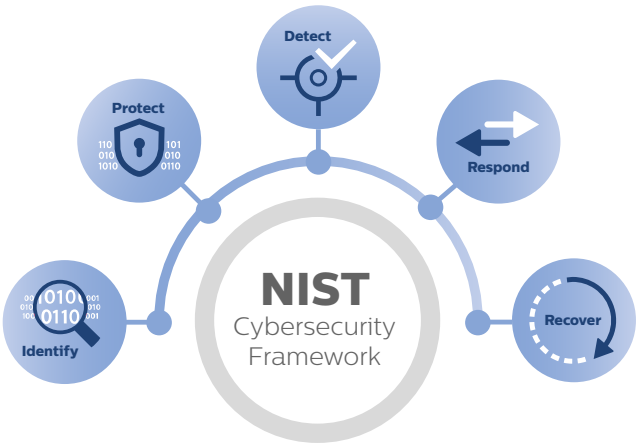
The framework core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. An example of Framework outcome language is, “physical devices and systems within the organization are inventoried.”

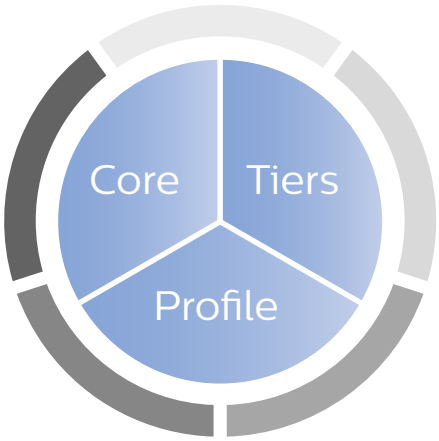
The core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/ operations level.

The NIST cybersecurity framework

The NIST cybersecurity framework core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The NIST cybersecurity framework core then identifies underlying key categories and subcategories for each function, and matches them with example Informative References, such as existing standards, guidelines, and practices for each subcategory.

The NIST cybersecurity framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks. NIST worked with private-sector and government experts to create the framework, which was released in early 2014 and NIST was ratified by the US Congress ratified it as in the Cybersecurity Enhancement Act of 2014.





The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

The framework implementation tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the NIST cybersecurity framework core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

Aligned with our Philips focus on Operational Intelligence and collaboration, the NIST cybersecurity framework provides guidance relevant for the entire organization. The full benefits of the Framework will not be realized if only the IT department uses it. The framework balances comprehensive risk management, with a language that is adaptable to the audience at hand. More specifically, the function, category, and subcategory levels of the framework correspond well to organizational, mission/business, and IT and operational technology (OT)/industrial control system (ICS) systems level professionals. This enables accurate and meaningful communication, from the C-Suite to individual operating units and with supply chain partners. It can be especially helpful in improving communications and understanding between IT specialists, OT/ICS operators, and senior managers of the organization.

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

How to reach us
Please visit www.philips.com
healthcare@philips.com