Services and solutions delivery

Operational Intelligence

Your medical device cyber security strategy

Executive briefing

Exploring the security challenges of medical devices and how to address them

> “Cybersecurity is front and center in the transition to connected care.”
> Jeroen Tas, Chief Innovation & Strategy Officer, Philips

Today, many medical devices are designed like specialized computers. Add directives such as Meaningful Use and the desire of clinicians to access patient data from a variety of devices and locations, and it is no surprise that medical devices are occupying an increasing number of nodes on the typical healthcare IT network.

As the requirements to ensure patient safety, provide clinicians with convenient access to information and images, and provide medical device security converge, healthcare IT professionals and changemaker senior leaders are facing new challenges. These challenges include:

- How do we ensure medical device security as care providers access patient information and images on a wide range of devices - including mobile devices?
- What are the most likely sources of cyberattacks and highest risks to data – and how do we protect against them?
- How can we meet our goals to drive down operational costs by minimizing “one-offs” in our enterprise architecture when interfacing with regulated medical devices?
- With varied adoption of security best practices by manufacturers, how can we evaluate our device and system providers and determine where they stand?
- Effectiveness and data and system security for our networked medical devices, as indicated in IEC 80001-1?

Why is security such a big challenge when it comes to medical devices?

As a medical device, security updates, patches and potential virus signatures need to be properly assessed by the device manufacturer before they can be safely used. This validation process takes at least 3 months from the time the security update is released. These security updates are also often analysed by hackers to see if vulnerabilities can be exploited. This combination of long procedural time scales and intense hacker visibility of the security updates makes it difficult to keep the security mitigations up to date enough in real time, increasing the likelihood of security incidents. Securing and safeguarding medical devices is therefore a 24/7, round the clock endeavour.

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

How to safeguard medical devices and take steps towards creating an enterprise-wide resilience strategy?

To secure and safeguard medical devices, the NHS (the UK National Health Service) recommends the following steps. It's important that they apply to all network connected devices irrespective of operating system

Step 1: Identify the enterprise's medical devices

Define all of the devices in the estate, including full details along with operating system information. This audit should result in the drawing up of a complete network topology that shows how the in scope devices communicate with associated devices and services and also how access can be enabled for remote updates to be delivered if this is appropriate for the device in question. Examples of devices may include MRI scanners, handheld vital signs monitoring and syringe drivers; you may wish to refer to the European Council Directive 93/42/EEC, which lays out the definition of a medical device.

Step 2: Develop and apply a mitigation plan

Create an effective mitigation plan that combines the following approaches:

Reduce the of compromise by preventing the devices from accessing untrusted content (effectively making it hard for malicious content to reach the device and exploit it)

Reduce the impact of compromise by preventing access to sensitive data or services from vulnerable devices (so even if the devices are compromised, the damage will be minimised.

Step 3: Reduce the likelihood of a compromise

Prevent access from untrusted services

Prevent or reduce access to removeable media

Constrain network access

Remove unnecessary services

Constrain remote access

Remove access to services (limit access levels)

Zone networks and air gap

Put in place effective and proactive protective monitoring

Ensure proper anti-malware and intrusion detection

Step 4: Apply user management

Manage user accounts carefully throughout the lifecycle. For example, deleting accounts when staff leave or change jobs.

Create an incident response procedure

Step 5: Collaborate with third parties and properly understand connections

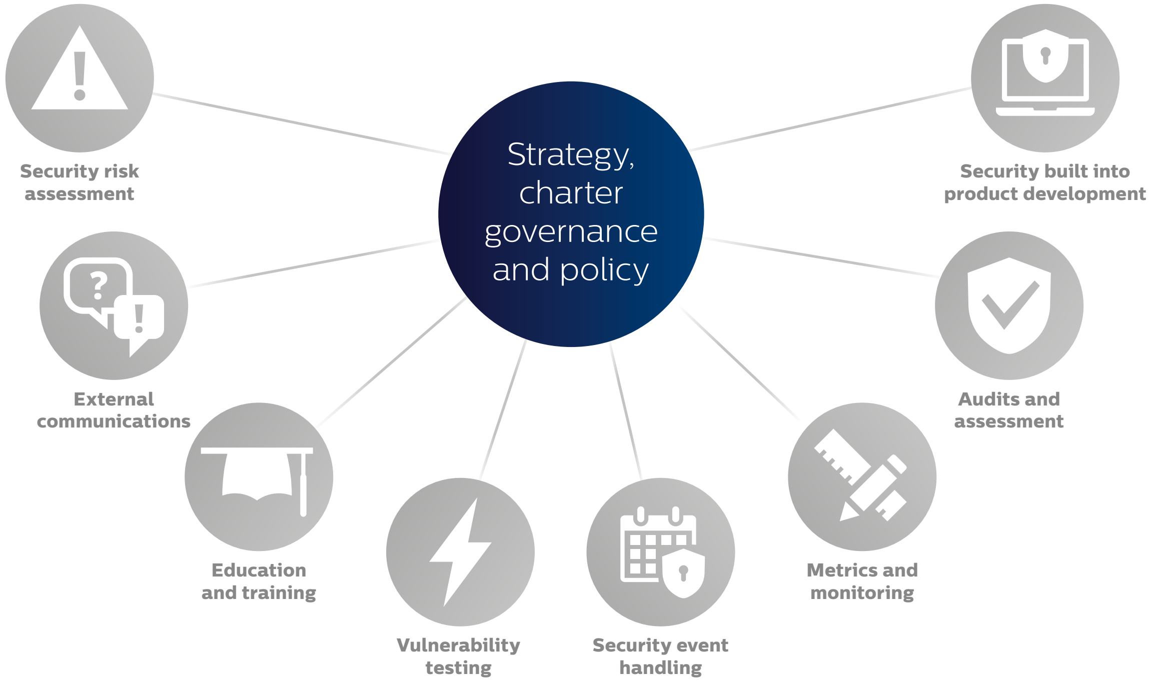
Consider the security of third party organizations and, when procuring contracts, prioritise support and security. For example, in the event of a security incident how quickly should you have support engineers on site to apply mitigations? Similarly, once a patch has been released and tested, how quickly should it be applied to any medical device it concerns? Getting these statements into contracts will make it easier to stay on top of your own security requirements.

Step 6: Periodically review your medical device estate

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

Why partner with Philips to define and implement a state of the art cybersecurity strategy?

Manufacturers' security programs are critical to ensure that security and privacy are a focus from the start. Recently, the FDA issued a recommendation that medical device manufacturers and health care facilities put safeguards in place to reduce the risk of cyberattacks, further underscoring the need for well-designed programs. Security programs must include some key foundational elements to achieve success:



Strategy, charter governance and policy

Security risk assessment

Security built into product development

External communications

Audits and assessment

Education and training

Metrics and monitoring

Vulnerability testing

Security event handling

Philips promotes consistent adoption of strategies to proactively address risks and threats, including what are often referred to in the area of cybersecurity as 'The Three Deadly Sins':

Security from the start

Password risk:
the risk from a lack of strong identity and permission management, e.g. multifactor authentication

Encryption risk:
the risk from a lack of strong end-to-end data encryption – from the source where data is generated, over the network and when resting in a data center – and/or effective data-loss prevention solutions

Patch management risk:
the risk from a lack of effective patch management, creating vulnerabilities in, for example, legacy operating systems.

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

Informed by the guiding principles of ‘Security by design’

Philips holistic strategy is based on the guiding principles of ‘Security by design.’ We unite the power of our people, processes and technologies to protect the confidentiality, integrity, and availability of critical clinical and personal data across the entire care lifecycle. We understand that your cybersecurity is only as strong as its weakest link, so our goal is to make sure that Philips patient monitoring clinical networks and systems are not an entry point for an attack.

The Philips security program approach cover all eight foundational elements and begins with solid strategy, governance, and policy. Ongoing education and training are required, as are audits and assessments.

Additionally, Philips medical device product development includes detailed risk assessments and vulnerability testing that mimics your environment. Because threats are evolving and ongoing, we have programs in place for event handling, as well as metrics , monitoring, and communications to keep you informed.

Gal Gnainsky from Philips Group Security explains:
“We’ve spent years building and investing in a robust end-to-end ‘Security by Design’ program, embedding security principles and best practices throughout a product’s life cycle. We understand that our customers have high and growing expectations for the security of the solutions that they rely on. In addition, global regulatory authorities have also increased the scope and scale of product cybersecurity compliance requirements to help protect patients and consumers. We look forward to continuing to meet these critical commitments.”

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

Comprehensive services for a comprehensive cybersecurity strategy

Security by design goes beyond products and networks. With Philips 'Security by design' solution, you can choose from a comprehensive range of services to keep your monitoring network, systems and devices up to date, performing at peak capacity, and shielded from the constant threat of cyberattacks. These include and span:

Philips Security Center of Excellence

The Philips Security Center of Excellence was launched in 2015 to develop cyber-resilient products and services through security-by-design, risk assessment, vulnerability and penetration assessment, specialized trainings, and incident response.

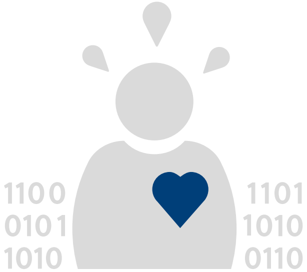
Underwriters Laboratories certified

Philips has also recently been named the first medical device manufacturer to receive a new Underwriters Laboratories (UL) product cybersecurity testing certification. Underwriters Laboratories (UL) is an independent global safety certification and testing company with locations worldwide.

The UL IEC 62304 certification was designed by Underwriters Laboratories to provide an overall framework to evaluate the robustness and maturity of a medical device manufacturer's cybersecurity controls and capabilities for product development.

In support of the successful Philips firm registration for the security option of IEC 62304, UL performed a comprehensive audit of the Philips Security Center of Excellence. The audit reviewed and verified core Philips Security Center of Excellence product security processes, including security risk management and risk control measures, software security verification planning, change management and continuous improvement, and the Center's laboratory quality management system.

The UL certification combines cybersecurity testing elements of the established UL 2900-2-1 standard for Software Cybersecurity for Network-Connectable Products, which focuses on the demanding requirements of healthcare and wellness systems, as well as security principles from international standards (ISO 13485 and ISO 14971).



Philips Patient Monitoring

Philips Patient Monitoring is a regulated medical IT system that provides continuous monitoring and communication of patient vitals while meeting manageability, serviceability and security requirements. The following medical devices are included in our security solution:

- Patient Information Center iX (PIC iX) B.02 and higher
- IntelliVue Bedside Monitors Release M and higher
- IntelliSpace Critical Care and Anesthesia (ICCA)
- CareEvent B.01 and higher
- IntelliSpace Perinatal (Integration Test only)
- CompuRecord (Integration Test only)

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

The Philips Patient Monitoring Systems approach to protecting patients, medical devices and information spans:

Lifecycle Management

When new software or an operating system releases, we publish the end of support dates for the legacy product you are using. This allows you time to budget, plan for upgrades and prevent the risk of unsupported medical devices and operating systems.

Securing clinical network

We provide best-practice, product-specific security recommendations to effectively secure IntelliVue Patient Monitoring System's wired and wireless devices.

System hardening

Includes planning, testing, implementing and auditing patch management software and protecting against vulnerabilities disclosed by the manufacturer. Generate confidence with IT stakeholders Philips PIC iX System implements security hardening based on the US Department of Defense (DoD) Security Technical Implementation Guides (STIGs). The applicable STIGs, includes, but is not limited to: Windows® operating system, .NET, SQL and Internet Explorer.®

Security assessment and penetration testing

Using two types of testing, we access system vulnerability and measure which flaws will leave the system open to the most risk. Includes productspecific NESSUS® scans and penetration testing.

Active Directory authentication and authorization

By leveraging Active Directory PIC iX inherits customer authentication and password policy settings. This improves authentication and authorization.

Strict configuration management process Integrity assurance through a product's lifecycle by making the development and deployment process controllable and repeatable.

Remote enablement

Our remote enablement solution, powered by PerformanceBridge Focal Point, enables you to assess the performance of your Philips clinical and network devices. It helps to speed diagnostics, drive performance, and keep your operating system and device software up to date. Philips experts watch over your device inventory and manage software revisions remotely to simplify the deployment of the latest cybersecurity updates.

Network management

Our management system consists of authentication, authorization and accounting (or AAA) and includes the following recommendations:

- Employ logging methods for global network configuration access/change audits. These methods track not only configuration change times, but also the user ID making the change. Utilize AAA services, such as TACACS+ or RADIUS.
- Configure all user accounts to automatically time out.
- Enlist secure protocols (HTTPS, SSH, SNMPv3, etc.) for system management and disable unsecured protocols (HTTP, Telnet and SNMP) where possible.

Philips Remote Support (PRS)

To maintain and protect your systems remotely.

Technology solutions

Support the highest security standards and best IT practices.

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