PHILIPS

Services and solutions delivery

Operational Intelligence

Enterprise-wide cybersecurity

Executive briefing

Enterprise-wide cybersecurity

"Cybersecurity is front and center in the transition to connected care."

Jeroen Tas, Chief Innovation & Strategy Officer, Philips

Operational technology attacks surged

2,000%

year-over-year. Threat actors continue to shift their sights to attack vectors including IoT, OT and connected industrial and medical systems.

8.5 billion records breached in 2019, giving attackers access to more stolen credentials. Securing credentials and access controls is more important than ever.

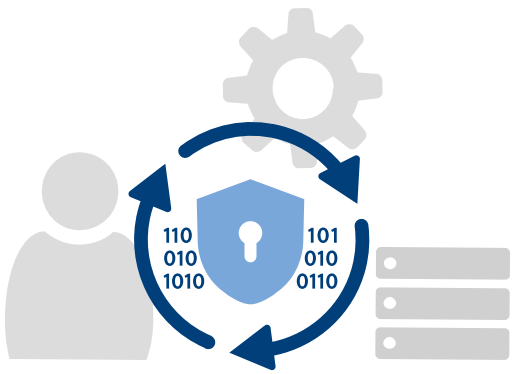
150,000 vulnerabilities disclosed to date. Patching vulnerabilities is still a problem for many organizations and cybercriminals know that.

Source: IBM X-Force Threat Intelligence Index 2020

With so many complex quadruple aim demands on C-suite level time, many healthcare organizations have tended to afford responsibility for cybersecurity to the technical experts, assuming that the CTO or CISO (chief information security officer), if there is one, will take ownership. And yet, many CTOs or CISOs will only have visibility over a limited part of the enterprise, making board level knowledge and budget allocation, critical.

Healthcare is the tenth most targeted industry by cyber criminals. And so, with CEO and COOs' remits spanning the full organization, change maker senior leaders are importantly positioned to develop and deploy enterprise-wide cybersecurity. In fact, the commitment to managing effective cybersecurity needs to be horizontal, breaking down silos to forge an ongoing collaboration between healthcare operations and technology personnel.

In this quick read, we explore the must-knows and must-deploys for managing healthcare cybersecurity as a senior level, pose the key questions all C-suite changemakers need to be asking themselves and outline top tips for preventing a healthcare data breaches and cybersecurity threats.



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

Cyber security management and the healthcare organization

With healthcare the tenth most targeted industry by cyber criminals, discover the top 5 insights for preventing a healthcare data breaches and cybersecurity threats.

Insight 1:
No longer tech only

Insight 2:
Relationships and collaboration are key

Insight 3:
Arm with knowledge and ask the right questions

Insight 4:
Plan for the worst case scenario

Insight 5:
Talk to Philips about its industry-leading cybersecurity solutions

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

Insight 1: No longer tech only. Cybersecurity is an evolving, complex operational challenge
The advent of the Internet and interconnectivity has opened up many formerly closed-loop networks within hospital systems, bringing new risks to hospitals. Legacy IT equipment and old security measures – passwords, encryption, and other abilities – may not meet the required standard for today's IoT world.

Healthcare providers also face serious shortages of skilled IT professionals who can properly deal with cyber intrusions[1] and every day new cyber threats emerge, varying in sophistication. The most destructive have brought whole IT systems down, compromising patient medical records and crippling a hospital's operations.

The 2017 ransomware strain known as WannaCry led to more than $4 billion[1] in damage and clinicians were forced to use pencil and paper to record clinical data, and attempt medical care without access to patient records.

Insight 2: Relationships and collaboration are key
The endpoint for any discussion on healthcare cybersecurity and medical information privacy ultimately comes down to one word: trust. In an ecosystem that is composed of multiple stakeholders – industry regulators, healthcare leaders, clinicians, patients and manufacturers of health IT equipment such as Philips Healthcare – each party has a role to play.

An area of industry consensus is the need for continued co-ordination between healthcare providers and manufacturers to deal with security concerns. Among healthcare providers, steps are being taken to incorporate cyber security into the technology and network architecture upfront, increase investment in cyber security teams, and take a broader view of the security value chain.[2]

Through collaborating across the healthcare ecosystem, the industry can build on advances made by other critical infrastructure industries, supporting the advantages that digital connectivity will bring for patient care. "There is no one golden solution. Instead of it being a burden, we have to embrace security and privacy into our organizations," says Dirk de Wit Head of Global Product & Security Services, Philips. "Every one of us within this ecosystem needs to play our role in mitigating this threat."

1 Reuters, 'More Disruption feared from Cyberattack', 2017
2 The Cyber-resilient enterprise, Accenture, 2018

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

Insight 3: Arm with knowledge and ask the right questions
As Accenture's paper, "The Cyber-resilient enterprise" states, C-Suite leaders "are ramping up their engagement in cybersecurity— to a point where they are assuming accountability for the cyber risks facing the company. But, with security programs only covering 67 percent of the organization on average, most have much more to do." Accenture recommends that all COOs and changemaker senior levels ask themselves the following questions to determine full engagement in the cybersecurity threat:

1. Does the CTO/CISO have oversight of more than just the corporate office— of functions, subsidiaries, joint ventures, labs? Put another way, over which areas of the business does the CTO/CISO not have oversight?
2. For new business initiatives that will increase cyber-risk, have you involved the CTO/CISO in discussions to advise, coach and address the risk?
3. When considering the adoption of new technologies, have you consulted the CTO/CISO to identify and develop solutions for security concerns?
4. In discussions with the CTO/CISO, do you feel you are speaking the same language?
5. Does the CTO/CISO understand where you are taking the business?
6. What is the nature of discussions between the CTO/CISO and business leaders—do they focus on technical and compliance issues or on the risk implications for business success?

According to Accenture, the CTO/CISO must partner up with the COO to become a business advisor to leadership. Together, they can prepare business leaders to think differently about security, because they set the tone for the whole company.

Insight 4: Plan for the worst case scenario
Healthcare organizations are valuable and sensitive infrastructures, but they are having to deal with ever-growing and increasingly sophisticated cyber threats.
It is a significant challenge for healthcare organizations to maintain good cyber security because many institutions possess such complex, layered networks with fragmented healthcare IT systems.

Healthcare data is extremely valuable too. Healthcare information has all of your most sensitive data all in one place making it very popular for identity theft, billing and insurance fraud, and extortion. Unlike credit card data, which you can change and replace, you cannot change your healthcare data easily.

2 The Cyber-resilient enterprise, Accenture, 2018

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

Preparation is key. In its 2019 Cyber Security Breaches Survey, the UK government reported that around half (46%) of UK firms had reported that they experienced a cyber attack or data breach in 2019 – up 39% from 2018. With this in mind, Philips cybersecurity experts recommend the following recommendations for preventing healthcare data breaches and improving healthcare data security.

Five tips for preventing healthcare data breaches and better healthcare data security

1. Have a clear overview
Clearly understand what products and assets are in your environment.

2. Focus on legacy products
Work with technology partners on any legacy types of products and solutions that might not have the capability to be updated, patched and secured.

3. Develop best practices
Make sure that you are working with an understanding of what are best practices from an industry perspective.

4. Manage cyber security across the entire supply chain
It is important to work on your procurement processes and understand the components within the bill of materials of the solutions you provide.

5. Partner with manufacturers, vendors
Consider involving your core vendors (e.g. in imaging informatics) in managing and mitigating your security risks by security standards and leverage the experience and capacity available from medical device manufacturers to help healthcare organizations fulfill their responsibilities in cybersecurity and privacy, e.g. HIPAA.

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

Insight 5: Talk to Philips about its industry-leading cybersecurity solutions

At Philips, Security By Design is an end-to-end mindset: infusing security principles begins with product design and development, through testing and deployment – followed up with robust policies and procedures for monitoring, effective updates, and where necessary, incident response management. Our solutions solve many customer challenges but security is always inherent in everything we create and connect. In a medical devices industry "first", Philips established a Security Center of Excellence (SCoE) to develop products that are "cyber-resilient".

With this mindset and as a leading health technology company and medical device manufacturer, 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.

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.

The Philips Healthsuite digital platform also 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.

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).

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

Overview of the Philips medical grade cybersecurity suite of services

Medical grade cybersecurity consultancy services

Philips cybersecurity consultancy services help customers with regulatory compliance, risk & vulnerability assessments of medical systems, including advice on implementing organizational processes that seamlessly integrate security response & recover workflows with all suppliers. We advise and help devise strategies and frameworks for customers, run security workshops and provide cybersecurity consultants across provides to ensure trusted IT environments are created.

Medical grade cybersecurity protection services

Philips Protection services help customers keep their systems secure through coordinated vulnerability disclosures, medically validated patching, network segmentation.

Medical grade cybersecurity detection, respond and recover services

Philips detection, respond and recover services help customers to identify their medical assets, and monitor the security posture of their medical systems 24x7 and, where needed, trigger response & recovery workflows, as well as helping with recovery from cybersecurity events.

Medical grade cybersecurity access and audit services

Philips access and audit services help customers keep control over who (vendors & employees) accesses their systems and allows for streamlined & compliant auditing of procedures and access to systems and data.

Medical grade cybersecurity secure lifetime extension services

Philips secure lifetime extension services help customers maximize the lifetime usage of their medical devices, by providing mitigating controls to maintain acceptable security postures.

Managed medical grade cybersecurity services

Philips Managed security services complement its managed technology services solution, by managing the full security services portfolio.

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