PHILIPS

Executive Insights

Protecting data, securing systems

February 2018

Protecting data, securing systems

“Product and information security is a combination of education, policies and procedures, physical security and technology.”

Michael McNeil,
Head of Global Product & Security Services, Philips

A collaborative approach by all stakeholders can protect healthcare providers and patient data from cyber threats.

Healthcare organizations are valuable and sensitive infrastructures due to their support for people’s well-being and safety[1] but they are dealing with ever-growing and increasingly sophisticated cyber threats. Personal health data is extremely valuable and tends to be the most prized by cyber criminals[2]. Unlike credit card data, which you can change and replace, you cannot change your healthcare data easily. Healthcare information has all of your most sensitive data all in one place. This makes it very popular for identity theft, billing and insurance fraud, and extortion.

The challenge for healthcare IT leaders grows with each new data breach the healthcare industry suffers. Attacks on healthcare systems persist not just because hospitals are viewed as easy to penetrate, but because cyber crime is a rewarding business model:[3] a low cost endeavor with the promise of high returns. Conversely: the higher the importance of security and privacy, the higher the cost for the organization hosting sensitive data.

In this paper we will explore the challenges facing healthcare IT leaders and discuss the multi-faceted approach required by all stakeholders in the healthcare ecosystem to manage and mitigate this pervasive threat.

[1] Independent Security Evaluators, ‘Securing Hospitals: A research study and blueprint’
[2] Reuters, ‘Your medical record is worth more to hackers than your credit card’
[3] McAfee, ‘Health Warning Cyberattacks are targeting the health care industry’

2 billion personal records were stolen in the US in 2016, 100 million of them were medical records.

65% of victims of medical identity theft pay out-of-pocket costs averaging $13,500 per victim.

Accenture, IBM
X-Force Threat
Intelligence Report
2016

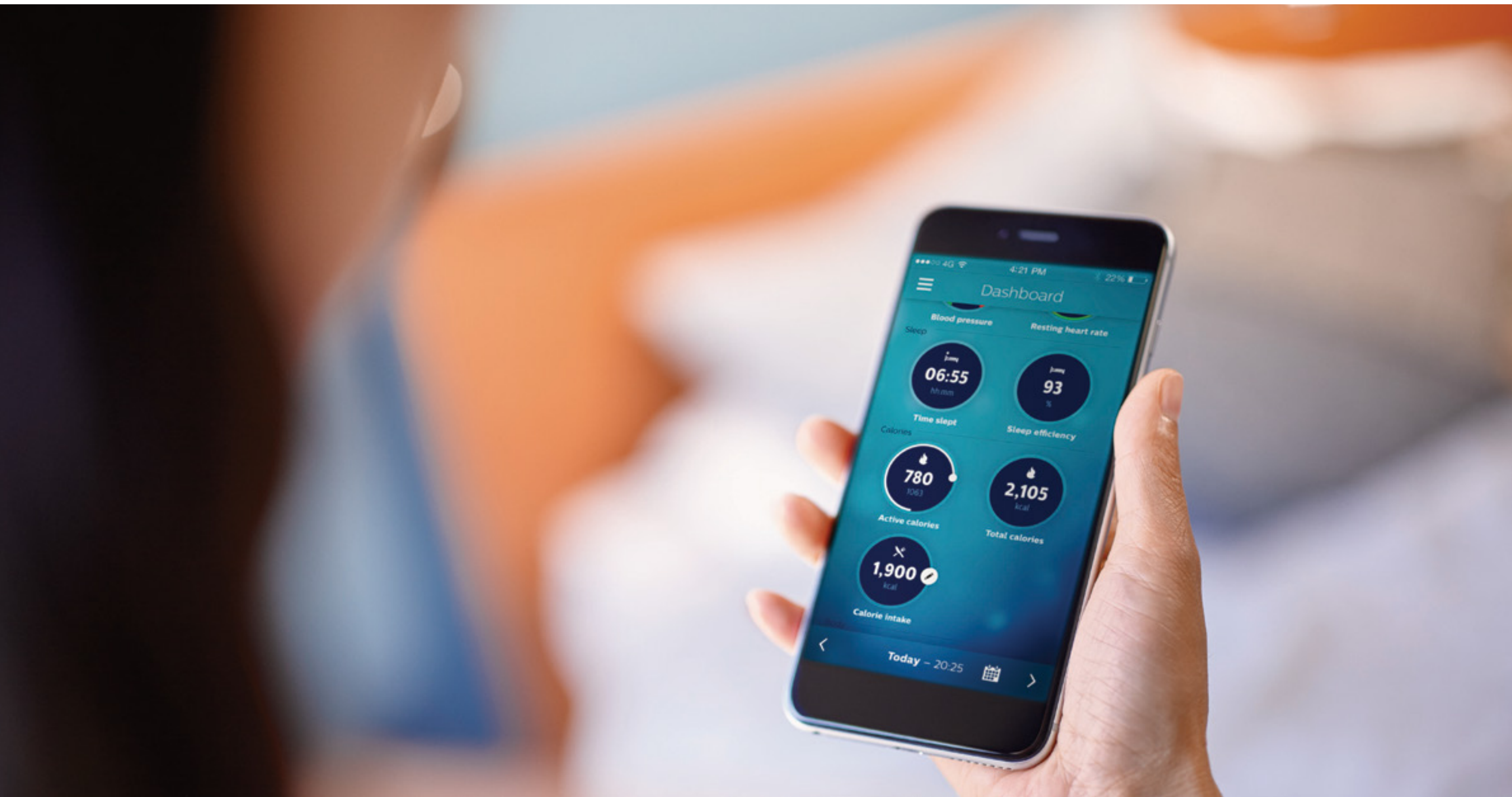
An evolving, complex problem

The healthcare industry is challenged to maintain good cyber security because many institutions have complex, layered networks with fragmented healthcare IT systems. Within hospital systems many of what used to be closed-loop networks, because of the advent of the Internet and interconnectivity, has now opened up, 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[4] and every day new cyber threats emerge, varying in sophistication. The most destructive have brought whole IT systems down, compromising patient records and crippling a hospital's operations.

The 2017 ransomware strain known as WannaCry led to more than $4 billion in damage[5] and clinicians were forced to use pencil and paper to record clinical data, and attempt medical care without access to patient records.

[4] Curran & Hinde, 2016
[5] Reuters, 'More Disruptions feared from Cyber Attack'



The privacy security paradigm

Traditionally, cyber security has been viewed within the healthcare industry as an IT burden[6] to be dealt with in a reactionary way, rather than as a solution that can help protect the patient and their data.

"Hospitals are used to considering cyber security as a burden[6] and a cost to their organization, instead of viewing it as an added value in supporting quality patient care," says Mr.McNeil.

The onset of the European General Data Protection Regulation (GDPR)[7], Europe's new framework for data protection laws, will allow people to have easier access to the data organizations hold about them. GDPR also outlines a new fines regime and clear responsibility for organizations to obtain the consent of people they collect information about.

> "Hospitals are used to considering cyber security as a burden and a cost to their organization, instead of an added value in supporting quality patient care."
>
> **Michael McNeil,**
> Head of Global Product & Security Services, Philips

Data protection

Similar to HIPAA in the US, data concerning healthcare, specifically 'data concerning health,' 'genetic data' and 'biometric data' will be subject to a higher standard of protection than personal data under the GDPR. "The current view is that around 75% of GDPR requirements translate into security related actions and investments," says Stef Hoffman, Chief Information and Security Officer, Philips. "As such, new privacy legislations worldwide drive complexity and investments in security."

One of the most important changes under the GDPR is mandatory data breach reporting. Breaches must be reported to a data protection regulator within 72 hours, and those affected by the breach must also be informed. Healthcare providers could face penalties of up to €20m or 4% of the previous year's annual global turnover[8] for not reporting data breaches or unlawful processing. For health IT leaders this means they will have to put in place clear procedures.

[6] US Healthcare Industry Cybersecurity Taskforce, 'Report on Improving Cybersecurity in the Healthcare Industry''

[7] WIRED, 'What is the GDPR?'

[8] FT, 'Businesses failing to prepare for EU rules on data protection'

"Security – like safety and quality – is a prerequisite for confidence in the Philips brand, and cannot be solved through technology alone. Comprehensive information security requires focus in three domains: People, Processes and Technology."

Gal Gnainksy,
VP, Chief Security Officer, Philips

'The Three Deadly Sins'

Handling increasing amounts of health-related data, one of the most sensitive types of personal data, requires increasingly high levels of assurance for customers, regarding the security and privacy protection measures Philips has in place. Regular security plans have the goal of ensuring the confidentiality, integrity and availability of critical data and the systems that house that data.

"Security – like safety and quality – is a prerequisite for confidence in the Philips brand, and cannot be solved through technology alone. Comprehensive information security requires focus in three domains: People, Processes and Technology," says Gal Gnainksy, VP, Chief Security Officer at Philips.

The concept "end-to-end security by design", which means to imbed security from initial design to production to support, is key to the long-term success of our products, services and solutions. Philips promotes consistent adoption of strategies to proactively address risks and threats, including what are often referred to in the area of cyber security as 'The Three Deadly Sins':

- **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.

A multi-faceted response

"In healthcare we have the ability to accelerate our execution based upon some of the knowledge and learnings of other industries."

Michael McNeil,
Head of Global Product & Security Services, Philips

The starting point for any discussion on security and 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 – 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 made to incorporate cyber security into the technology and network architecture upfront, a bigger investment in cyber security teams, and a broader view of the security value chain[9].

More sophisticated internal processes are being developed in hospitals – increased monitoring of threats and security incidents, impact assessments about how an attack might affect the daily hospital workings and the delivery of care, training and education to ensure staff know what steps to take to keep their organization secure.

[9] KPMG, 'Healthcare and Cyber Security: Increasing Threats Require Increased Capabilities'

Transparency and compliance

For manufacturers like Philips, compliance with data protection and privacy standards and regulations is critical. Healthcare is one of the most heavily regulated industries in the world and the regulation of medical devices includes regulatory agencies such as the US Food and Drug Administration, which require hardware and software releases and changes be subjected to rigorous verification and validation methods.

“Patient safety in today’s connected care environment is a task we all take very seriously,” says Mr.McNeil. “As we all evolve our cyber security programs, transparency, accountability and responsiveness must be priorities we continue to maintain.”

Philips ensures compliance with data protection and privacy standards and regulations, and is open and transparent in reporting and remediating vulnerabilities as part of a robust Coordinated Vulnerability Disclosure process (previously defined as Responsible Disclosure).

Critical industry learnings

Philips is also one of two member medical device manufacturers participating on the U.S. Health and Human Services (HHS) Cybersecurity Taskforce. “One of the first lessons learned in developing the taskforce recommendations was interviewing other critical infrastructure industries,” says Mr. McNeil. “In healthcare we have the ability to accelerate our execution based upon the knowledge and learnings of other industries.”

A Philips Security Center of Excellence (SCoE) develops products which are ‘cyber-resilient’, deploying a dedicated team of ethical hackers, or ‘security ninjas’, which engages in continuous vulnerability and penetration testing to identify product weaknesses. The SCoE shares information with leading cyber security researchers and test facilities around the world, assisting them to rapidly eliminate, reduce, and mitigate cyber threats.

Privacy and data protection at Philips

Privacy and data protection are integrated into General Business Principles, whereby we submit ourselves to a number of commitments such as:

- The implementation of Binding Corporate Rules (BCRs) that provide a baseline for privacy protection within Philips worldwide and allow international data transfer between Philips group companies.
- Implementation of a privacy program and governance structure which embeds privacy and data protection in the company.
- Limiting collection of data, and where appropriate, obtaining consent from individuals.
- Notifying individuals as to how collected data will be used, and allowing them to exercise their rights.
- Taking appropriate steps to maintain the accuracy and relevance of the data. Protecting personal data using appropriate security safeguards.

No silver bullet

> “There is no one golden solution. Instead of it being a burden, we have to embrace security and privacy into our organizations. Every one of us within this ecosystem needs to play our role in mitigating this threat.”

Michael McNeil,
Head of Global Product & Security Services, Philips

It is unlikely that data breaches will subside in the months and years ahead. As healthcare continues to become more connected, new security threats will emerge.

With old systems and through more connected health equipment and devices the reality is that as long as the expected rewards are greater than the cost of performing an attack, the threat will continue and grow.

However, through collaborating across the healthcare ecosystem, the lessons the industry learns now 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 Mr.McNeil. “Every one of us within this ecosystem needs to play our role in mitigating this threat.”

www.philips.com
February 2018