NTT Security

Global Overview

Cybersecurity Expertise in Private and Public Healthcare

Healthcare providers have been addressing information security risk for many years and cybersecurity remains a primary focus for both private and public healthcare providers globally.

As organizations continue to innovate and rely increasingly on the interconnectivity of systems and data, the sector has become a primary target for cyber threats. It's no longer a question of if, but when a cyber attack will occur.

Globally, healthcare providers face some unique threats with an increasing number of connected medical devices and vendor-owned equipment in use. These include information kiosks, connected heart monitors, infusion pumps, Wi-Fi for patient and guest access, bring your own device (BYOD) requirements, imaging systems and a myriad of other connected devices.

Securing this wide range of devices within an organization's infrastructure is a challenge, with the added complexity of demonstrating regulatory compliance. In addition to this, Gartner estimates that by 2020, the number of medical devices requiring security hardening by a healthcare provider will increase by 45 percent.[1]

Cybersecurity challenges in public and private healthcare provision

Today's healthcare providers face a number of challenges and information security concerns:

- A constantly-changing threat landscape – with new threats emerging and existing threats becoming more sophisticated
- The growing number of connected medical devices on the network increases privacy and security risks
- The attack surface is growing – IoT devices, PCs and legacy systems are all being connected and are potentially incompatible with new security defenses, providing perfect entry points for hackers
- Fear of the big breach – not every healthcare sector breach makes the headlines, but some do and one day it might be yours
- Concerns surrounding the repercussions of a breach – could it have been prevented and how it did happen?
- Weak links – the healthcare sector relies heavily on contractors and temporary staff who may not rigidly follow your security processes
- Vendor-owned systems reside on healthcare provider networks
- Tightening regulation from regulatory authorities
- Patient privacy concerns – in the US for example, patients need better assurances of protected health information (PHI) and health data security before opting into a health information exchange or other patient data-sharing models

75.7% of respondents indicated that their organizations experienced a significant security incident in the past 12 months. 61.9% identified email as the initial point of compromise.

2018 HIMSS Cyber Security Survey

Our unique capabilities

We have a broad range of managed security, risk and compliance services we can deliver to your organization.

Our experts have global reach and local resources, and understand the specific challenges that you face in private and public healthcare provision.

Working with a network of trusted partners and NTT Group companies, we enable your cyber resilience using a combination of consulting, managed, cloud, and hybrid security services.

NTT Security's end-to-end security services for the healthcare sector

Continuous compliance and consulting

Healthcare providers face legislative challenges every day and CISOs are spending more time than ever thinking about compliance. Most of these regulations are in place to ensure that hospitals protect their patients' health records, putting the healthcare industry under immense pressure to comply or run the risk of onerous fines. In the US alone, healthcare providers need to capture exhaustive information on patients in the form of electronic health records (EHRs), encrypt and protect patient information, render information "unusable, unreadable or indecipherable" to unauthorized individuals, notify different parties if an information breach occurs – and pay steep penalties of up to USD 1.5 million for wilful neglect in terms of sending out breach

1. Gartner, Top Three Security and Privacy Impacts of Connected Medical Devices on Healthcare Providers, Saniye Burcu Alaybeyi, Marc-Antoine Meunier, Gregg Pessin, September 2017

notifications. Add to this HIPAA, HITECH, CMS, ASTM and IEC requirements and there's a lot that could go wrong.

In the UK, organizations will want to make sure they handle notification of personal data breaches correctly. If the breach is subsequently found to be a serious infringement of the General Data Protection Regulations (GDPR), very large fines may be imposed by the Information Commissioners Office (ICO). And in Germany, the German Data Protection Amendment Act (GDPAA) has substantially changed the current German Federal Data Protection Act in order to align it to the GDPR.

Knowing about your compliance commitments and gaps is one thing – effectively filling them is another.

When you engage with NTT Group companies, you can be assured that NTT Security healthcare experts will help shape each governance, risk and compliance policy and process from a strategic and technical standpoint. This ensures that you are able to create a security infrastructure with the right security policies, processes, architecture, and expertise in place.

External advice can be invaluable to evolve a comprehensive security strategy and, using our proven Global Enterprise Methodology consultancy delivery approach, we will enable you to understand your risk exposure and make informed risk management decisions.

Our compliance expertise covers: log data mining for efficient security and compliance incident investigations, PCI, regulatory assessments, IT governance, risk and compliance (GRC), executive security and CISO risk advisory.

Managed Security Services

The threat landscape is evolving, with threats becoming more frequent and sophisticated, leaving many healthcare providers struggling to manage all aspects of cybersecurity in-house. Partnering with NTT Security as your Managed Security Services provider gives you access to our world-class specialist organization and healthcare security experts. We're here to provide you with end-to-end 24/7 monitoring, management, and support of your IT and security assets. What really sets our Global Managed Security Services apart are our unique threat detection, advanced analytics, and unrivalled threat intelligence capabilities focused on your industry – leaving you with peace of mind and the convenience of being able to engage with one global provider for all your secure digital transformation needs.

Our Managed Security Services also allow you to easily fulfil any recommendations made by our consulting services and ensure you receive a unique end-to-end cybersecurity service relevant to your industry.

Risk:Value 2018 findings

The 2018 NTT Security Risk: Value research reveals that:

- Over 40 percent of public and private healthcare providers don't yet have a formal information security policy in place
- Of those with a policy, only 42 percent believe that all employees are aware of the policy
- Only half of public and private healthcare providers have an incident response plan in place
- Loss of patient confidence would be a key issue for organizations if they lost information in a security breach
- 38 percent of private providers and 28 percent of public healthcare providers believe that they will never be breached
- Only 8 percent of private providers and 12 percent of public providers rule out the use of third party managed security service providers to support the in-house team.
- Contractors and temporary staff are seen to be the weakest security link for 66 percent of public and private healthcare providers

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.