Issue 2

Securing the Internet of Things

Internet-connected medical devices are transforming the health system-playing critical roles in such tasks as patient care, medical records and billing-but each connected device is a potential gateway for cybercriminals. Following a year marked by major, industrywide cybersecurity breaches and a 525 percent increase in medical device cybersecurity vulnerabilities reported by the government, hospitals must take quick, decisive action to maintain data privacy, secure connected medical devices and protect patients (see Figure 1).

Hospitals have become a victim for so-called "ransomware" attacks, such as WannaCry, in which intruders gain access to files, encrypt them and demand payment in cryptocurrency in return for access to the files. In 2017, at least two US hospital systems experienced problems after being hit by WannaCry, and 16 hospitals in the UK were unable to access internet-connected devices.

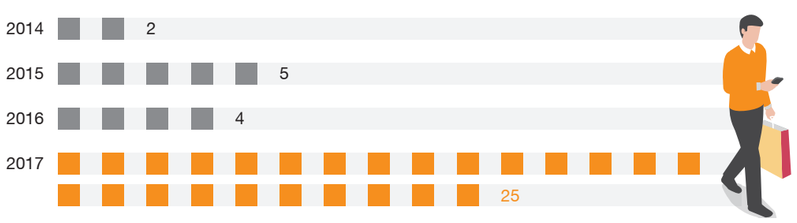
People's Daily has also reported similar incidents happened in China. PwC's Global State of Information Security Survey (GSISS) found that 16 percent of all healthcare institutions suffered a ransomware attack in 2016. Eleven manufacturers of medical devices issued warnings about the potential for the WannaCry event to affect their devices, and several were confirmed to have been affected.

Many hospitals have thousands of medical devices connected to their networks. Some, lacking purchasing controls or strict network policies, don't even know how many such devices they have, let alone how secure they are. PwC's GSISS survey found that just 64 percent of healthcare institutions said they have performed a risk assessment of connected devices and technologies to find potential security vulnerabilities, and only 55 percent of those said they have put security controls in place for these devices.

Staff training, too, remains a critical problem. Only 31 percent of healthcare institutions plan to train their employees on security practices for the Internet of things this year. Another 31 percent say they plan to establish policies for Internet-connected devices this year.

"Everyone is rethinking their security practices in the wake of WannaCry," said Chantal Worzala, vice president of health information and policy operations at the American Hospital Association. The problem, she said, is that "hospitals literally deploy thousands of devices, and trying to remediate all of those devices is a pretty daunting challenge in the heat of the moment if there's a cybersecurity attack. This is particularly true when many device companies do not provide information about potential vulnerabilities or updates and patches to fix vulnerabilities. "Another problem is that regulators can be slow to alert the public. It took more than a year for the FDA to issue a warning about a critical device vulnerability after researchers discovered it in late 2014.

Figure 1: Device vulnerabilities are being reported at record rates
Medical device cybersecurity vulnerabilities reported by the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, by year



Source: PwC Health Research Institute analysis of Department of Homeland Security ICS-CERT security publications. Data current as of Sept. 25, 2017

Ramesh Moosa
Cybersecurity and Forensics Partner
PwC China

"

Due to the growing aging population and increasing demand for medical services in China, Internet-connected medical devices present a great opportunity to raise efficiency, lower medical costs and improve patient care and experience.

Glucose monitoring device is a great example of utilizing Internet-connected medical devices. China has the highest rate of diabetes in the Asia-Pacific region. Healthcare professionals in China are adopting digital healthcare systems for maintaining electronic health records for patients and managing health programs. Advancement in technology such as the introduction of smart, wearable gadgets in the market has helped to increase market penetration of glucose monitoring devices. More than 80% of the population in China has adapted to the new technologies introduced using digital technology. Approximately about 40% of the population uses health applications to track regular activities.[1]

Lifesaving Internet-connected medical devices such as pacemakers and infusion pumps have opened the gateway for data and cybersecurity attacks and incidents. The increasing risks will have a great impact on the way hospitals and medical professionals manage and operate the delivery of safe and secure medical services in the era of Internet-connected medical devices.

Thankfully, more institutions and enterprises globally have now realised the seriousness of the problem and are starting to actively formulate defensive measures.

On this issue, PwC has the following recommendations:

Firstly, understand the potential risks to your organisation. A cybersecurity breach can render medical devices inoperable or result in the loss of sensitive patient information. At its worst, a cyber breach may cripple an entire healthcare institution and may pose severe risks to patients' safety.

Secondly, adopt enhanced prevention measures and be fully prepared to respond to incidents. It never hurts to be fully prepared for the worst case scenario. Healthcare institutions need to invest in precautionary measures, and ensure that their employees are well trained to handle any potential threats that might cripple the organisation.

Lastly, embrace and enforce security and safety standards. Comprehensive security testing should be carried out in advance of procuring or installing systems. In addition, define clearly what device manufacturers are responsible for, including security updates and security support and other post-sale maintenance activities, to ensure adequate service levels for critical support functions.

No organisation is immune to the cyber storm and threats that is brought about by the benefits and convenience of digitisation. The only way to stay safe and resilient is to be very well prepared.

PwC is here to be your partner.

"

Implications

Hacks are like a "non-natural" disaster.

Hospitals and life sciences companies should prepare for cybersecurity incidents to happen more often and invest in the planning, defensive measures and personnel required. They can do so by preparing as they would for a natural disaster. They should create and test cybersecurity breach and remediation plans. Facilities should be prepared to respond if their devices go down, or even if they suspect that their network has been breached. And they should create business continuity plans that are accessible offline. In a bid to lower costs when facing cybersecurity incidents, medical institutions should take serious consideration to purchase relevant insurances.

Understand the risks to your organization.

Security failure can mean devices rendered inoperable, critical patient records being stolen or unavailable, and even facilities being shut down as a precaution. The financial and reputational cost of a breach affecting patient health can far exceed the lost revenue from business disruption. Twenty-six percent of consumers affected by a hacking incident say they've decided to change doctors, hospitals, insurers or medical organizations because their medical information had been stolen in a hacking incident. Thirty-eight percent say they would be wary of using a hospital associated with a hacked medical device. The increasing use of connected devices in EHR systems means companies' value-based payments also could be at risk if there's concern about the collected data's integrity.

Healthcare institutions should strategically consider how they manage internet-connected devices.

Cybersecurity risks can be managed using a layered approach, including limiting who has access to devices and limiting what the devices can do. While 95 percent of healthcare executives think their practice is secure against cybersecurity threats, just 36 percent have access management policies in place, and 34 percent have a cybersecurity audit process in place. Many companies also lack in-house cybersecurity expertise and will need to find it externally. Companies can also use language in vendor contracts to establish what device manufacturers are responsible for, including security updates and security support. More and more medical institutions requires their vendors to adhere to security standards before purchasing their products, as well as ask a third-party to undergo security check or provide cybersecurity report.

[1] Arizton Advisory & Intelligence, "Glucose Monitoring Devices Market - Global Outlook and Forecast 2018-2023" (2018), http://www.arizton.com/public/market-reports/glucose-monitoring-devices-market (仅有英文版)