Cyber crime against the healthcare sector

With cyber crime the fastest growing criminal activity in the world, attacks on healthcare providers are becoming more prevalent. Post, in association with Kennedys, hosted a roundtable to find out the scale of the threat –and what the industry can do to combat it

By Ryan Hewlett

Neil Arklie, vice-president of financial lines, cyber, media and technology, Axis Insurance

Andy Barber, business development manager, cyber security, Ideal Health

Stephanie Crowther, healthcare and cyber underwriter, Hiscox

Philip Dearn, practice leader, UK healthcare, Marsh

John Douglas, technical director, First Response Europe

Christopher Malla, partner, Kennedys

Deborah Newberry, head of public affairs, Kennedys

Martin Overton, cyber risk specialist, AIG and an ethical hacker

Jillian Raw, partner and head of global cyber offering, Kennedys

Cyber crime is the world's fastest growing criminal activity, estimated to cost businesses more than £286bn a year. And cyber attacks focus on healthcare more than any other industry, with exposures ranging from security breaches to human errors, viruses and hacking, all of which present a new challenge to the insurance sector.

According to a recent report published by IBM, the rate of cyber attacks against the healthcare sector climbed to the highest level of all industries studied. In 2016 alone, almost 30 NHS trusts were targeted by ransomware attacks.

A *Post* roundtable, in association with Kennedys, looked at the challenges posed by cyber threat in the healthcare sector as a result of new technologies. Bringing together experts from healthcare, cyber engineering and insurance, it sought to find ways to minimise the risks.

In October 2016, ransomware was to blame for an attack which saw an NHS Trust in Lincolnshire forced to cancel almost 3000 appointments and operations over a period of four days. In a statement, Northern Lincolnshire and Goole NHS Foundation Trust said that a ransomware variant called Globe 2 was to blame for the incident.

These trends are in no way isolated to the UK. In the US, healthcare data breaches accounted for 35% of all reported data breach incidents last year, according to recent survey findings from Beazley.

At the roundtable, Philip Dearn, practice leader for UK Healthcare at Marsh, explained how technology is proving to be a disruptive force in healthcare.

"Everything involving technology in the healthcare world has grown at such a rapid pace over the last decade. In hospitals it is commonplace to find software-driven equipment, to telemedicine, to online booking systems and electronic patient records. All of these things, 10 years ago, were not in use, they simply didn't exist.

Richard Sawyer, director and head of North American terrorism, Aon Risk Solutions

Mike Shen, head of cyber innovation, Novae

Matt Sumpter, underwriting manager, CNA Hardy

"Innovations such as wearable devices are bringing about a completely new world in terms of healthcare delivery," added Dearn. "Technology is growing all the time, bringing with it all of the different applications and functions that technology is able to deliver."

All of this technology is allowing the healthcare sector to boost efficiency, according to Christopher Malla, partner at Kennedys and a specialist in medical malpractice.

> **As technological innovation ushers in a new era of care within the health sector, it also brings with it new risks and challenges that need to be addressed**

Malla commented on the recent announcement that the Royal Free Hospital had teamed up with Google Deep Mind, an artificial intelligence platform, to develop an app named Streams, aimed at improving the identification and treatment of patients at risk of acute kidney injury.

"This is precisely the kind of innovation that will deliver efficiencies. The team behind the app is predicting 500,000 hours saved by a healthcare professional. That's the equivalent of 150 nurses," Malla said.

"It is a major development in relation to economic savings for an NHS hospital, but also for the private sector. It should deliver improved patient safety. The intention is that when the app is rolled out, it will save 10,000 avoidable deaths. This is a massive impact to patient safety."

But as technological innovation ushers in a new era of care within the health sector, it also brings with it new risks and challenges that need to be addressed.

"Technology has certainly helped on the efficiency side, but it's also a double-edged sword. It brings efficiencies, but also brings new risks," said Martin Overton, cyber risk specialist at AIG and an ethical hacker.

"The threat landscape has morphed hugely in the last 10 years," said John Douglas, technical director at First Response Europe.

"The threat used to be bored teenagers sitting in their bedrooms with a laptop and a broadband connection; this is no longer the case."

Douglas said that "bored teenagers" only account for 5% of the current threat. Now the trend has shifted towards eco-terrorism and groups such as Anonymous, best known for hacking into US government sites, including the Pentagon.

According to him, "the biggest single threat for the healthcare sector comes from nation state intelligence services, and organised criminal networks stealing data".

Douglas added that the main reason for the breaches is financial gain. Criminal organisations attempt to steal data in order to sell it on to other criminal networks.

Close to home

Matt Sumpter, underwriting manager at CNA Hardy, pointed out that many threats come from much closer to home.

"We all talk about these big scary issues such as nation hacking," Sumpter said. "In reality it is operational error, the people factor, a lack of investment in IT and security, which are the big exposures that these hospitals and healthcare providers are facing."

NHS IT systems are increasingly vulnerable to attacks by cyber blackmailers trying to extort ransoms from hospitals. As the threat of cyber risk is becoming more evident, hospitals need to question how best they can protect themselves and respond to the threat most effectively.

The financial gain available from such attacks has resulted in a rapid increase in attack activity within the UK. A recent freedom of information request from the I newspaper found that at least 28 NHS trusts in England have been victims of ransomware incursions in the last 12 months.

Jillian Raw, a partner at Kennedys and head of the firm's global cyber offering, said the rise in such cases is due to medical records being viewed as "data gold mines", providing hackers with a treasure trove of personal data that can be used for identity theft and fraud.

> 30

< 29

"Medical data sells for a high price on the black market and up to 10 or 20 times the price of stolen credit card numbers," Raw said. "For the nation states and organised criminal gangs, medical records are much more valuable than stolen credit card numbers.

"It's an enormous source of material that an attacker could get from one single attack on a hospital."

Attractive static data

Mike Shen, head of cyber innovation at Novae, said that one of the qualities which makes medical records so attractive to attackers is that it's static data. "Medical records don't change," Shen said. "You can take a credit card number, which gets less valuable by the second because the card owner is going to cancel the card as soon as a problem is discovered."

It isn't only data loss that is an issue. Internet-enabled and connected medical equipment is also vulnerable to malicious hacks, potentially enabling a hacker to cause physical harm to a patient while under care, said Overton.

"We've seen it with things, like insulin pumps that are accessible via wifi, and with other drug infusion systems."

Connected equipment does pose a risk, especially those with hard-coded passwords in firmware as this means that the user can't change them.

Overton added that such devices should be read only, thus limiting the effect of potential attacks; if a hacker could gain control of medical equipment, the hacker would only be able to view information but not control the item, therefore reducing the chances of harm to a patient.

Hospitals are faced with a double threat; externally, there is the threat of data hacking and the disruption of medical equipment, and externally there is the internal threat of human error from within the hospital itself. How then are hospitals to mitigate this risk internally?

Overton believed from a technical point of view, a lot of these issues can be resolved through "normal security hygiene".

"A good security framework, having backups, training your staff and making sure you test them against phishing scams are all cyber security basics; 80% to 90% of the incidents that I've ever dealt with could easily have been solved just by doing good security hygiene."

Training staff, developing adequate threat scenarios and procedures and driving change from the top down are of paramount importance, according to Andy Barber, business development manager for cyber security at Ideal Health.

Barber said that hospitals already have plans in place to deal with large catastrophic events such as plane crashes and terrorist attacks. As such, it would be very simple to put the same level of procedure together for a data breach scenario.

"The training has to be for everybody, these issues are not just for the IT side of things. It has to be driven from the boardroom, and hospitals must make sure there is governance in place and training awareness," Barber said.

Internet-enabled and connected medical equipment is also vulnerable to malicious hacks, potentially enabling a hacker to cause physical harm to a patient while under care

The challenge will be imparting the same level of security practices across the 40,000 organisations that make up the NHS, as one weak link is enough to cause substantial problems.

Overton agreed the need for change has to be driven by the board. "Change needs to be driven from the top down. It needs to be board-led," he said. "You need to have the chief strategy officer or chief information officer talking directly to the board, or as a member of the board. If you're trying to push

the stuff uphill, it's harder work than trying to trickle it down from the top."

The challenges are not only for the hospitals. Cyber threat in healthcare presents a complex and difficult to read picture for insurers. In the underwriting sphere, the lack of claims data adds further difficulty when pricing cyber risk for a hospital. As such it can be hard to know precisely what the impact of a cyber event may be.

Pricing interruption

Stephanie Crowther, healthcare and cyber underwriter at Hiscox, said that it is possible for insurers to accurately cost the downtime and the extra expense that a cyber leak or hack on a hospital would have. The trouble comes when trying to price the interruption of patient care.

"The biggest danger for healthcare institutions is the possibility that patient care is impacted and interrupted. Insurers don't yet know what that looks like on a financial and human life level. The pricing is yet to be quantified. The industry hasn't seen a breach that's sufficiently caused patient care to drop to a point where it becomes an issue."

Axis Insurance vice-president of financial lines, cyber, media and technology Neil Arklie noted that current loss estimates for catastrophic cyber attacks on hospitals put them on a par with the most destructive natural disasters.

"There are University of Cambridge studies written in conjunction with RMS and Lloyd's that estimate that catastrophic losses for these events could run into tens of billions of dollars."

did you know?

19%

of healthcare breaches were caused by hacking or malware in 2016

Healthcare data breaches accounted for

35%

of all reported data breach incidents in the US during 2015

Human error and unintended disclosure represented

40%

of all industry cyber incidents in 2016

Source: Beazley

Despite the potentially vast loss figures, Arklie said that a single, significant cyber event would be easily absorbed by the insurance industry.

"The insurance industry should be able to absorb one major loss," Arklie said. "The problem will be if the industry suffers two of three of these losses, then it may find itself with a major erosion of capital."

Arklie said that a change of thought in the insurance sector is in order. Insurers need to adapt their thinking when it comes to complex cyber claims; they will need to shift focus from a reactive, claims-first approach towards a proactive focus on threat resilience.

Response to an incident

"Insurers should work on the basis that every organisation will be hacked at some point," added Arklie. "It must be about resilience and the way the organisation responds to a cyber incident.

"In cyber, you are likely to have an incident that may lead to a claim, and the insurer needs to determine how to respond and structure its programmes and adjust its mindset to a new paradigm."

Richard Sawyer, director and head of North American terrorism at Aon Risk Solutions, called on all interested parties to work together, arguing that this paradigm shift presents a big opportunity for the insurance sector.

"We're seeing a lot of people in the insurance sector innovating within this gap in the market. There's an opportunity to find out what keeps risk managers up at night, and fill the void with adequate insurance products.

"The threat is changing overnight, it's evolving at a rate that no one can keep up with. Policy wordings and contracts are almost out of date a week later. This makes it the responsibility of the hospitals, risk managers, brokers and the underwriters to work together and produce policies that are up to the task." ■