RISK & INSURANCE

An Inevitable Threat

Critical Condition

The interconnectivity of medical devices could spur catastrophic consequences.

By: Michelle Kerr | April 7, 2014 • 7 min read

Topics: April 2014 Issue | Cyber Risks | Emerging Risks | Health Care

It's the stuff of futuristic daydreams. Implantable sensors that can detect signs of a potential health problem and send alerts to your smartphone, like a "check engine" light for your body. A straight-out-of-Star-Trek handheld medical scanner you can use to diagnose your own problems and alert your physician. A capsule-shaped sensor you can swallow so your doctor can perform your annual physical via phone or tablet, even while you're at work or — better still — out on the links.

Only these aren't daydreams at all. These are just a small sampling of the health care innovations that will be market-ready in the near future. Health-related mobile apps are booming as well, growing at a rate of 25 percent a year.

These technologies will become a part of the increasingly interconnected environment of health care devices, which already includes common technology such as radiology equipment, dialysis machines and the smartphone in the pocket of every practitioner.

The Looming Cloud

The Internet of (medical) Things is part of the push toward modern, patient-focused health care. It is at the core of the telemedicine movement and it is poised to expand access to care at a crucial point in the evolution of health care reform. But there is an ominous cloud hanging over all of this progress.

Health care systems are under siege like never before. Experts report a worsening trend in the frequency and complexity of cyber attacks on health care networks, with a sharp increase over the past year.

“The advanced persistent threats that we’ve been fighting on behalf of our clients in government and defense for the past five years have now shifted into the health care arena,” said Tom Patterson, director of global cybersecurity consulting with CSC.

Tom Patterson, director of global cybersecurity consulting, CSC.

“Companies are being targeted; adversaries are spending more than a year breaking in, escalating their privileges, looking around, customizing specific malware to defeat their specific defenses, and then either exfiltrating data or doing the damage they wanted to do. That type of attack is light years ahead of most health care companies’ defenses.”

A report published in February by the SANS Institute painted an overwhelmingly dire picture of cyber threats in health care. Between September 2012 and October 2013, researchers identified 375 U.S. health care organizations that were compromised — many of whom are still unaware that they’ve been compromised. HIPAA and the HITECH Act forced health care organizations to take comprehensive measures to protect patient data or face heavy fines. The trouble is that compliance doesn’t necessarily equal security, and systems unrelated to protected health information (PHI) are getting less attention.

The SANS study found that hackers were infiltrating devices such as radiology imaging software, conferencing systems, printers, Web cameras and mail servers. With each new device and application connected to health care networks, security experts warn, a new window opens for hackers to exploit, widening the available attack surface.

“There are two types of companies, those that have been hacked, and those that don’t know they’ve been hacked,” said Kurtis Suhs, vice president and national technology and privacy product manager for Ironshore.

Unfortunately, the ones that don’t know about it yet could be in deeper trouble than they could ever imagine.

While much ado is made of the cost of data breaches in the retail sector, the impact of a disruption to the health care delivery system could be far more chilling. Imagine hackers taking control of the life-support devices in every critical care unit of a 25-hospital health care system. Imagine if they could gain control of every medication-delivery pump in the network, delivering lethal doses to dozens of patients.

What if malware from a random smartphone could infect every diagnostic device across the network, scrambling readings and making it impossible for doctors to treat patients? These scenarios are already possible — more possible than most would care to think about.

“The health care ecosystem is one of the most critical infrastructures for any country,” said Andrea Fiumicelli, vice president and general manager of healthcare and life sciences for CSC. “Preventing health care delivery from working for even a few hours could have a massive impact on a national level.”

“Both terrorist groups and hacktivist groups spend a lot of time trying to disrupt other parts of critical infrastructure,” added CSC’s Patterson, “but the easier it becomes to disrupt the actual health of the target humans, the more we’re going to see them slipping into that arena as well.”

The ability to commandeer medical devices makes health care systems a prime target for extortionists as well, experts said.

This Technology Outlook 2020 looks at global megatrends and technologies affecting the health care sector.

Beth Berger, national director of Arthur J. Gallagher’s health care practice, used the example of how equipment servicing can be done
remotely via Internet-based diagnostics.

“What if somebody hacked into that and recalibrated [equipment] ... ? What if I told this hospital that unless you wire me X amount of dollars, I can shut down the life support on all the people in your hospital? And let me show you for two minutes.”

Strategy Shift

The prevailing opinion among experts is that the health care industry lags far behind most other industries in terms of making real improvements to cyber security. However, it’s fairly easy to understand why.

“You really have to have empathy for health care providers these days,” said Kathleen Keefe, breach response services director for the Beazley Group.

“They’re facing so many changes and cyber is just one of them. They’ve got dwindling reimbursements, changing payment methodologies, increased regulation and heightened expectations about providing care to more people who [now] have insurance under the health reform act. ... I feel like we just have to help them.”

Help is coming, albeit slowly. CSC's Patterson said the FDA is moving toward classifying certain medical devices as industrial control (IC) devices, which will subject them to stringent security controls.

Meanwhile several web-based medical apps and programs are getting certified by Underwriters Laboratories, according to **Dr. Bill Bithoney, senior adviser at BDO Consulting and a member of the health care practice.**

But health care organizations need to look inward and start changing the way they think about cyber security, beginning with the way they think about the growing network of peer-to-peer devices.

"Everything is going to be connected in the health care space very quickly and it's going to come from multiple different vendors," said Patterson. "It's all going to start talking to each other on its own. ... The health providers aren't necessarily going to have a single point of control for all these devices. So if you don't have a security scheme that takes that into account, you're at real risk."

"Years ago, it was all about perimeter security," said Ironshore's Suhs. "It was, 'You've got to buy our firewall and antivirus to prevent the bad things from happening.'

"The security paradigm has changed today. I don't think there's a way you can prevent a data breach.

"It's a matter of how do you detect it. Those that can quickly detect are those that can probably cost contain the breach in an effective way. ... From an underwriting standpoint, that's the paradigm I have."

Kevin Kalinich, cyberrisk global practice leader for Aon Risk Solutions, warned against trying to solve the problem by throwing more money at IT.
Before deciding on a strategy, health care entities would be well served to take an enterprise risk management approach to protecting their systems, he said.

Identify Vulnerabilities

Organizations must ask themselves, "How do we check in the patient? How do we collect their information? How do we decide who has access to patient information?" Armed with a better understanding of how the system works together as a whole, then they can begin to identify their vulnerabilities.

"It's crucial to balance IT security with appropriate policies and procedures," said Kalinich. "It's about knowing what you should be doing and what you should not be doing with Internet-connected medical devices. Each department needs to be on the same page about what they should be doing and that includes their third-party providers. It's a culture issue.

"Insurance and cyber security go hand in hand," he added. "The underwriters will give you more comprehensive coverage for a cheaper price if you have good ERM."

Patterson added that insurance companies also need to look inward, and think about creating cyber products that deliver real value to insureds.

"Cyber insurance hasn't been tied to real security — it's always been actuarially based.

“What I want to see the industry evolve to is, ‘Here’s the probability of this happening. So if you take these tangible steps, it will make you more secure, so the probability goes down, so your risk goes down, your insurance [premium] goes down.’ It becomes much more of a useful policy,” he said.

“That makes all the sense in the world and I think that’s what companies would love to buy today if they believed in it,” Patterson said.
Beazley’s Keefe agreed.

“The folks in the markets who can deliver solutions that make sense and add value and really make a difference are the ones that will be the leaders.

Michelle Kerr is associate editor of Risk & Insurance. She can be reached at mkerr@lrp.com