Executive Summit 2018

Digitalizing healthcare: Building trust in the digital age

SIEMENS
Healthineers

Advances in digital technologies are generating increasingly sophisticated tools for prevention, diagnosis, and treatment. They can lead to improved record keeping and back-office performance. Yet the healthcare industry's dependence on these devices and instruments makes it vulnerable to hackers.

Text: Bill Hinchberger

Daniel Nigrin, Senior Vice President of Information Services and Chief Information Officer at the Boston Children's Hospital

Digital technologies will transform the nature of how we manage health and well-being. Many current developments seem to come right out of science fiction, whether they are unimaginable opportunities or potentially dystopian threats to be combatted. Over 100 leaders of the global healthcare community at the Siemens Healthineers Executive Summit in Frankfurt, Germany, heard about an exciting example of the former – the creation of a "digital twin" to help physicians choose more personalized treatments – in addition to tips about how to combat hacking.

Cybersecurity to the rescue

Hackers can have numerous motives, including politics, money, and recreation. Daniel Nigrin, Senior Vice President of Information Services and Chief Information Officer at the Boston Children's Hospital, and Nicolas Krämer, Chief Executive Officer of Lukaskrankenhaus Neuss in Germany, talked about getting hacked. Sandro Gaycken, Founder and Director of the Digital Society Institute, and Melissa Hathaway, President of Hathaway Global Strategies, provided expert analysis. While no strategy can be failsafe, the speakers outlined a series of tips for how healthcare industry executives can adopt best practices.

At the Executive Summit 2018, a panel of distinguished guests discussed all things digital.

"We have experience taking care of viruses, but not computer viruses."

Nicolas Krämer, Chief Executive Officer of Lukaskrankenhaus Neuss

Boston Children's Hospital was hit by Anonymous, a nebulous "hacktivist" group, in 2014. The barrage started with a distributed denial-of-service attack and a flood of incoming messages that overloaded the system, disabling Internet capabilities. Then came numerous attempts to penetrate the system. Without email, the hospital "used old-fashioned sneaker power" to deliver messages and documents, Nigrin recalled.

Forewarned by an Anonymous video online, Nigrin and his team had time to prepare. They convened an incident response team, including people from the marketing department. They notified authorities, including the Federal Bureau of Investigation (FBI), which only reacted once the attack had started. Losses reached almost seven figures in US dollars. The insurance company balked at first, but paid up after the hospital appealed. The culprit was arrested and convicted.

Known in Germany for its state-of-the-art digital technology, Lukaskrankenhaus Neuss was forced to embark on a "long-lasting digital fast," as Krämer put it, by a 2016 cyberattack. First, members of staff noticed that their instruments seemed sluggish. Then came a blackmail message. "It was obviously a virus," said Krämer. "We have experience taking care of viruses, but not computer viruses."

To prevent the virus spreading, they shut down the system, took measures to protect patient data, and called the German federal police – and they did not pay the ransom. They discovered and eliminated the virus, and traced it to a phishing email (disguised as legitimate) opened by an employee. Krämer cited cryptographer Bruce Schneier: "Amateurs hack systems. Professionals hack people." He added, "The opposite of artificial intelligence is human stupidity." Damages rang in at EUR 1 million. The hospital had no insurance. The case is ongoing.

Gaycken called hacking "an unsolved problem that goes back 40 years." Hackers used to need nine months on average to get into a system; now it takes three days. IT systems should be patched every two years, but they are designed to last for 15 years.

While the threat looms large ("most militaries are hacked daily"), there are few really good hackers – only about 30 to 40 in Germany, Gaycken estimated. They can earn salaries of EUR 500,000 to 1.5 million a year. Those on the dark side tend to prefer financial targets, such as banks and stock markets. However, Gaycken said that "a new business model" based on mass attacks is emerging. For example, one hacker disseminated a report about how pacemakers could be disabled. That forced a company to recall 500,000 units. The hacker made a bundle on the stock market by anticipating investor reactions. "It is much easier to do a mass attack than an individual one," Gaycken said. "It is easier to hack into 10,000 cars than just one."

Hathaway stated that "the digital transformation is introducing new risks" to systems, data sets, and devices. The emphasis on efficiency leads people to say: "We'll do it now and patch it [for security] later." But that can be dangerous. "What are the new governance mechanisms that need to be put into place?" she asked.

"It is easy to find your vulnerabilities on the Internet," according to Hathaway. And you don't need to be a top-notch hacker. With a one-dollar gadget, an average computer geek can gain entry. It usually takes 197 days on average to find the problem and 67 solve it. She added that 90 percent of the healthcare industry is affected to the tune of USD 6.2 billion a year. In the United Kingdom, 81 of 236 hospitals were hit hard by an attack which rendered some hardware – that was running on the operating system of a leading software supplier – permanently useless.

Patient data and other information "is being stolen because it is valuable," said Hathaway, with health insurance companies at particular risk.

Sandro Gaycken, Founder and Director of the Digital Society Institute

Melissa Hathaway, President of Hathaway Global Strategies

Dorin Comaniciu, Vice President of Artificial Intelligence at Siemens Healthineers, projected his "digital twin" and showed how AI can help practitioners to predict and plan for potential treatments.

> *"We need to eliminate unnecessary interventions, prioritize better healthcare, and advance precision medicine."*

Dorin Comaniciu, Vice President of Artificial Intelligence at Siemens Healthineers

Meet your digital twin

In his keynote speech, Dorin Comaniciu, Vice President of Artificial Intelligence at Siemens Healthineers, described how he used artificial intelligence (AI) to make a prototype digital model of his own heart. He demonstrated how it can be used to help practitioners test potential treatments in advance of the possible real thing.

"The focus needs to be on doing what is right for the patient," he said. "We need to eliminate unnecessary interventions, prioritize better healthcare, and advance precision medicine." As it becomes more sophisticated, AI will be at the center of this, Comaniciu predicted.

He outlined four layers in a hierarchy of AI systems in healthcare based on three factors: integration, access, and complexity. From low to high, they are as follows:

1 Scanner/Instrument: Workflow automation through reconstruction and advanced physics
2 Reading/Reporting/Guidance: Measurement and quantification for detection, diagnosis, and guidance
3 Patient-centric Approach: A "digital twin" to predict, plan, and prescribe
4 Patient Cohort: Population health management with outcome analysis, quality care, and meaningful use

As an example of advances within the second category, Comaniciu introduced DeepReasoner, described as a multitask network for prediction and risk assessment. It can take a myriad of patient data and compress it into a fingerprint that can be used to analyze risk and potentially help devise the right drug therapy.

The main part of his talk focused within the third layer, the digital twin. Comaniciu described how he merged manifold data from multiple sources to create a highly sophisticated model of his own heart. It has similar dimensions and can mimic things such as electrical signal activation, muscle contraction, ejection fraction (blood pump rate), and pressure dynamics. If and when it becomes widely available, cardiologists will be able manipulate these "twins" to test and prescribe the best therapies for their patients. Similar models can be made for other parts of the body, as Comaniciu demonstrated with examples from orthopedics and knee replacements. ●

Conclusion

Hacking is here to stay, and healthcare organizations can be attractive targets. "You can never be completely secure, but [adding security] is better than leaving your doors open," Nigrin said. Meanwhile, executives and practitioners should pay attention to developments in artificial intelligence as new tools are likely to emerge in the coming years.

Takeaways

- A good place to start is to "realize that you have a problem," said Gaycken. "And that you cannot solve it alone."
- Remember that it is an organizational problem, not an IT problem, Nigrin said.
- Gaycken outlined three useful steps: make a risk assessment, determine your priorities, and look for alternatives to your main IT systems.
- In doing a risk assessment, decide "what you can live with and what you cannot," said Hathaway.
- "Once you know the risks," added Hathaway, "set up new governance mechanisms according to your risk tolerance."
- "Buy differently and build differently" – in ways that will reduce risk, said Hathaway.
- "You need to have multiple modalities" for storing electronic medical records, said Nigrin. Don't depend only on Internet-based systems.
- Never pay a ransom. That's what law enforcement officials told Nigrin.
- Make sure that your public information strategy is based on the truth, said Krämer.
- Have a good insurance policy.
- In the aftermath of its attack, Lukaskrankenhaus Neuss took a number of steps, including:
  - Investing more in IT security
  - Setting up a sandbox system, which separates applications from critical system resources, for email attachments
  - Improving employee awareness

Bill Hinchberger is a Paris-based independent journalist.

Speakers

- Daniel Nigrin, MD, MS, Senior Vice President of Information Services & Chief Information Officer, Boston Children's Hospital, Boston, Massachusetts, United States
- Melissa Hathaway, President, Hathaway Global Strategies LLC, Great Falls, Virginia, United States
- Nicolas Krämer, PhD, Chief Executive Officer, Lukaskrankenhaus GmbH, Neuss, Germany
- Sandro Gaycken, Founder and Director, Digital Society Institute, ESMT Berlin, Germany

Siemens Healthineers
Headquarters
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen, Germany
Phone: +49 9131 84-0
siemens-healthineers.com