ASN
Kidney News
May 2018 | Vol. 10, Number 5

Health Institutions At Risk From Repeat Ransomware Attacks

By Bridget M. Kuehn

The high profile WannaCry and Petya ransomware attacks in 2017 brought institutions—including major health systems—around the world to a screeching halt and drew attention to the rising cybersecurity threats facing healthcare.

In fact, the nonprofit ECRI Institute named ransomware and other malicious software its top health technology hazard for 2018. Hackers use these computer programs to infiltrate an organization's network and prevent the organization from accessing its electronic medical records or online systems. The attackers then demand a ransom to stop the attack. These attacks can bring normal hospital operations to a halt causing delays in patient care that could threaten patient safety, said Juuso Leinonen, senior project engineer in the ECRI Institute's Health Devices Group.

"This is a problem and there's probably no hospital that's completely immune to it," Leinonen said.

Healthcare has become the top target for such attacks, according to a survey of 2700 Internet Technology (IT) managers by network security company Sophos. Three-quarters of healthcare institutions that responded to the survey had been victims of ransomware attacks, even though more than half had systems in place to prevent them. Across sectors, the average cost of an attack was $133,000 and affected organizations often face repeat attacks.

Vulnerable systems

Healthcare organizations often are easier targets than organizations in other industries that have worked to harden their defenses, explained James Scott, senior fellow at the nonprofit Institute for Critical Infrastructure Technology (ICIT) in Washington, DC. Hospitals may not have leaders who are well versed in cybersecurity and their frontline information technology staff may not have the right expertise and training to ward off attacks, he said.

"The nature of 24/7 patient care also makes routine IT maintenance tasks more difficult to achieve," said Andrew Mundell, a security architect at Sophos.

Growing use of networked medical devices is another challenge, Leinonen noted. These expensive devices may have lifespans that stretch for a decade, he said. Some hospital devices may still require manual updates; others may be so old new security patches are no longer available.

"The reality is that there are thousands of medical devices in most healthcare institutions from hundreds of different vendors and potentially each one of those devices

Continued on page 3

KidneyX Accelerator Holds Promise for Fostering, Speeding Innovations in Kidney Care

A new effort to foster the development of innovative technologies and therapeutics in the kidney space is on the horizon.

A signed Memorandum of Understanding between ASN and the U.S. Department of Health and Human Services (HHS) established the Kidney Innovation Accelerator (KidneyX), a public-private partnership. KidneyX aims to prevent kidney diseases while improving the lives of the 850,000,000 people worldwide who are currently affected by accelerating innovation in the prevention, diagnosis, and treatment of kidney diseases. KidneyX will award prize funding to promising companies, enabling and accelerating the commercialization of more products to benefit people with and at risk for kidney diseases. Building off the success of similar public-private accelerators, KidneyX will engage a community of researchers, innovators, and investors to bring breakthrough therapies to patients.

With KidneyX, "HHS sends an important message to investors and innovators regarding the desire and demand for new therapies," said HHS Chief Technology Officer Bruce D. Greenstein, who announced HHS's commit-

Continued on page 3

Inside

Speeding Innovations

Continued from page 1

ment to launching KidneyX in partnership with ASN and the broader medical community at ASN Kidney Week 2017.

KidneyX will use a three-pronged approach to address the barriers innovators commonly identify as they look to bring new drugs and technologies in kidney care to market, bridging the gap between research and market-ready products.

First, the Accelerator will provide merit-based, non-dilutive funding to promising innovators selected through a competitive process. This funding will incentivize the accelerated development and commercialization of disruptive technologies in kidney care, such as a next-generation kidney.

Second, KidneyX will encourage better coordination across HHS with the National Institutes of Health (NIH), Food and Drug Administration (FDA), and Centers for Medicare & Medicaid Services (CMS) in order to help clarify the path toward commercialization.

The third prong of KidneyX's approach to accelerate innovation in kidney care is to create a sense of urgency to develop new therapies, much like the sense of urgency associated with other areas of healthcare including oncology, neuroscience, heart disease, and diabetes. An important part of this effort will be increasing interactions with the venture capital community and other investors who have previously shied away from the kidney space.

By opening pathways of collaboration among science, engineering, finance, and other disciplines, KidneyX aims to bring that same sense of urgency to innovators and investors.

"The urgency to develop better therapies and, ultimately, cures, is palpable to patients and their families on a daily basis. ASN applauds the commitment of HHS to fight kidney diseases, and is proud to partner with them in launching KidneyX and generating real change within the kidney community," noted Mark D. Okusa, MD, FASN, ASN President.

The Kidney Health Initiative's (KHI) *Development of a Roadmap for Innovation in Renal Replacement Therapy* project will serve as a resource for KidneyX. The KHI project aims to describe scientific, technical, and regulatory milestones needed to achieve the goal of creating a bioartificial or bioengineered alternative to dialysis as renal replacement therapy.

KidneyX's first round of prize funding will focus on accelerating the commercialization of next-generation dialysis products and will begin accepting applications in late summer 2018. Individuals who are interested in learning more about KidneyX are encouraged to visit www.kidneyx.org and join our mailing list.

What is the Kidney Innovation Accelerator?

Mission: Accelerate innovation in the prevention, diagnosis, and treatment of kidney diseases

KidneyX Principles

- **Patient-Centered** Ensure all product development is patient-centered
- **Urgent** Create a sense of urgency to meet the needs of people with kidney diseases
- **Achievable** Ground in scientifically driven technology development
- **Catalytic** Reduce regulatory and financial risks to catalyze investment in the kidney space
- **Collaborative** Foster multidisciplinary collaboration including innovators throughout science and technology, the business community, patients, care partners, and other stakeholders
- **Additive** Address barriers to innovation public/private sectors do not otherwise address
- **Sustainable** Invest in a diverse portfolio to balance risk and sustain KidneyX

Ransomware Attacks

Continued from page 1

could have their own security requirements or patching requirements so that definitely makes it a significant problem and very difficult to manage," Leinonen said.

Smaller healthcare organizations like physicians' offices or dialysis centers may be at even greater risk, said Mundell.

"[Small organizations] are likely to have smaller IT and security teams working to combat the latest threat," he said.

Once an organization has been compromised, they are likely to face repeated attacks, according to the Sophos report. They may be re-infected by the same malicious software if the organization fails to properly remove it from the system, Mundell said. After an organization pays a ransom, attackers may increase the number or sophistication of their attacks in the hopes of securing another ransom.

Very sophisticated hackers may use a ransomware attack as distraction, so they can establish remote access to medical records or other data that they can later extract undetected, Scott said. Patient information such as Social Security numbers, credit card numbers, or health insurance credentials can be sold to would-be identity thieves for $20-$1300 depending on how much information is offered, according to an ICIT report.

"The fact that there is a lot of sensitive data in a healthcare institution makes it inherently risky and appropriate controls need to be in place to make sure that data is protected both on your medical devices as well as in your other systems," Leinonen said.

The reality is that there are thousands of medical devices in most healthcare institutions from hundreds of different vendors and potentially each one of those devices could have their own security requirements.
—Juuso Leinonen

Data defenses

There are many steps that healthcare organizations of all sizes should be taking to protect against ransomware and other online threats. Some may require substantial time and financial resources, but experts say they are essential.

"You are investing for the future," said Michelle De Mooy, director of the Privacy & Data Project at the Center for Democracy and Technology. "You are protecting your patients' privacy and the integrity of your data."

Organizations should do a risk or security audit to help them identify their vulnerabilities, De Mooy recommended. Institutions should encrypt their data and have backup systems in place, she said. They should also ensure that all employees are adequately trained to recognize potential threats, such as suspicious links in e-mails or files ending in .exe.

They should also have a complete inventory of all networked medical devices, the software they use, and records of system updates, Leinonen said. He and his ECRI colleagues frequently field questions from hospitals hit by ransomware attacks about which devices may be vulnerable. Too often these facilities don't have the information they need to quickly identify devices at risk.

"Knowing what you have is almost a requirement to protecting them effectively," he said.

They should consider security when they purchase new medical devices, Leinonen said. These decisions should be made with input from frontline medical staff, IT staff, and the Chief Information Officer.

Facilities should aim to have a multi-layered defense against attacks, Scott said, so that attackers "give up and move on." He emphasized the importance of investing in qualified IT staff and hiring an in-house or outsourced threat-hunting team that can proactively test for weaknesses, seek out hackers in the system, and patch vulnerabilities.

Leinonen emphasized the need to adequately budget for data and systems security in order to preserve smooth operations.

"The reality today is that things are going to get more and more connected and this is going to be more of a significant concern as time goes on," he said. "This is not solely an IT problem, this is something where anybody, everybody from C-Suite to frontend clinicians can and should have a role to positively contribute overall to managing the security risks that may exist within the organization."