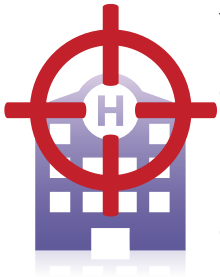
# Cyber Crime: A Growing Threat

**By Staff Writer, GE Healthcare**

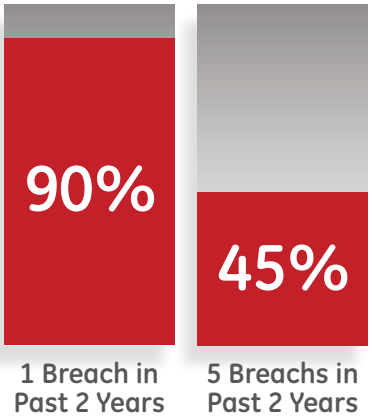
The headlines are sobering. In May, a Wichita, Kansas, hospital was affected a second time by ransomware-wielding cybercriminals who were dissatisfied by the first payment it made to unlock computer files.



The Kansas Heart Hospital incident came after a string of ransomware strikes on hospitals, including the February 2016 attack on Hollywood Presbyterian Medical Center that netted $17,000 for the criminals holding its data hostage.[1, 2, 3, 4]

Ransomware is just the latest method cybercriminals are using against hospitals, and it likely won't be the last. Data breaches could be costing the healthcare industry $6.2 billion, estimates the Ponemon Institute in its "Sixth Annual Benchmark Study on Privacy and Security in Healthcare Data." Nearly 90 percent of the 91 healthcare organizations and 84 business associates in the study had a data breach in the past two years, and 45 percent had more than five data breaches, the majority of which contained fewer than 500 records.[5]

Cybercriminals are constantly probing for weaknesses and building on successful techniques. "It's totally cat and mouse,"




says Lee Kim, director of privacy and security for the Healthcare Information and Management Systems Society.

In recent years, cybercriminals have begun targeting hospitals in much the same way they strike the retail and banking industries. The reason is the same — they hold valuable information that criminals can use or sell on the black market.

But hospitals are different. In addition to holding credit card information and personal identification numbers that can be used for financial fraud and identity theft, hospitals have patient medical information. Each medical record may be worth 10 – 20 times the value of a credit card number to cyber thiefs.[6]

When people think of data breaches, they often think of raids against big companies, for example the 2013 attack on Target that exposed 40 million customers' debit and credit card numbers.[7]

But small- and medium-sized businesses — and hospitals — are targets, too. Kansas Heart Hospital has 54 beds. Cybercriminals go after these targets because they believe these organizations often have fewer resources and less know-how to protect against threats and are viewed as easier, quicker marks.

"Time is money even for hackers," Kim says. "It's safe to say that whether you're small or large, there are cyber-crime campaigns that have been sketched out. All kinds of entities have been attacked."

Another difference between hospitals and other industries is that hospitals have so many entities that legitimately have to connect to their system — doctors, health insurers, patients accessing their own records. "Trying to distinguish the legitimate actors from the illegitimate actors is hard," says Mary Ellen Callahan, chair of the law firm Jenner & Block's Privacy and Information Governance Practice.

Another complication is that the number of routes criminals can take to get into hospitals' systems has grown as healthcare has become more digitally interconnected. Increasingly, physicians, vendors and even patients are able to access the system remotely. "Anything that is internet-enabled is vulnerable," Callahan notes.

Sometimes, a hospital employee unwittingly causes a breach by surfing on a website laden with malware or by falling for an email phishing scheme, says Richard Seiersen, general manager for cyber security and privacy at GE Healthcare.


Phishing scams are getting increasingly sophisticated and difficult for people to recognize. Callahan points to a scam targeting finance department employees with spoof emails that look like they come from the company's CEO and ask the employee to make a wire transfer. An FBI alert issued in April 2016 estimates this scam has cost organizations more than $2.3 billion over the past three years.[8]

Cybercriminals use social media to determine who the CEO is and the best person to target with the fake email, Callahan notes. They might even use social media to discover an executive's hobbies or interests and use that information to make their malicious email look legitimate.

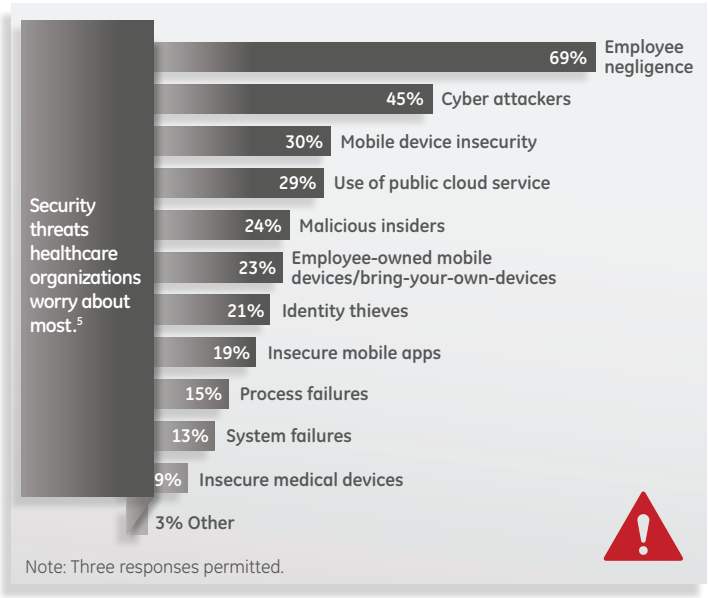
Phishing emails, a common route for ransomware, include a link to a convincing-looking but fake website or an attachment that is laden with malware. Clicking on the link or attachment delivers the malware that gives the criminal entry into the hospital network. Because many hospitals run information networks in which virtually all systems — from administrative to clinical — are connected without barriers, the virus is able to spread.

The infection doesn't necessarily have to enter the hospital through an in-house computer. Imagine a physician whose personal laptop or mobile phone is infected with malware because the doctor surfed on a malware-containing website or fell for a phishing scam. If the physician logs into the hospital network from the infected device, the virus could enter the hospital's system.

Hospital employees and medical staff aren't the only way into a hospital's network. Vendor relationships can be exploited, Callahan notes. The Target breach began when hackers stole credentials from an HVAC vendor; that vendor had indirect access to Target's credit card information.

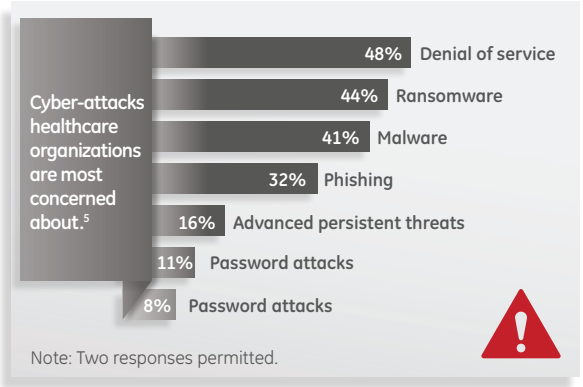
"Bad actors only need to be successful once," Callahan says. "The legitimate companies need to defend 100 percent, and that's the hard part."

Medical devices may be another access point for cybercriminals. Some types of devices may be connected to the internet and, depending on the connection, can be hacked directly to gain access into the hospital system. Another route is via the network connection between the hospital and the compromised medical device. The connected medical device may be an entry into the hospital network, if it is not segmented, and may be used as a means to get additional information available via the network and other connected systems.




The danger isn't just that patients' financial and personal health information could be stolen. Patients' actual health could be at risk. Healthcare organizations are too focused on protecting health records and not focused enough on the potential for patient harm, concludes a February 2016 report by Independent Security Evaluators. So far, there have been no reports of a breach harming patients, but the potential exists.[9]

"By use of any or all of these malicious techniques, a coordinated attack by a single individual, group, entity or government could create widespread fear and concern regarding the safety of the medical and health system in general," the report's authors add.



The impulse in reaction to these alarming scenarios could be to batten down the security hatches and severely restrict network access. But, again, hospitals are unlike many other industries in that immediate access to data is necessary for many users. Finding the right balance between security and usability is a major topic for hospitals right now, Seiersen says. If hospitals make it too difficult for clinicians to quickly access patients' medical information, it could jeopardize care, he adds.

In healthcare, the patient always has to come first, Kim says. The information must be kept confidential and steps need to be taken to ensure its integrity. But the healthcare provider should not be fighting with IT applications or other IT infrastructure that does not work, such that the provider is addressing a technical problem with the software, for example, instead of taking the patient, she adds.

When a system is too secure, employees are likely to find a way to circumvent it, Callahan says. "That makes it more vulnerable and exposes it," she adds.

Callahan points to the case of Pfc. Bradley Manning, an Army intelligence analyst, convicted in 2013 of copying and disseminating classified communications, including State Department cables. He was able to access the information because the Department of Defense, worried that tight State Department individual security controls were hindering communications, copied the State Department's secured data base and made it available wholesale to secured DOD users, explains Callahan, formerly the chief privacy officer of the U.S. Department of Homeland Security.[10, 11]

The news surrounding hospital privacy breaches has placed the issue high on hospitals' radar screens. As a result, hospitals are investing more in technology tools and health information security personnel, Kim says. Many hospitals are appointing chief information security officers to work full time on the task, rather than information security being just a part-time IT role, she notes. A shortage of people trained specifically in information security in the hospital environment could hinder hiring, however.

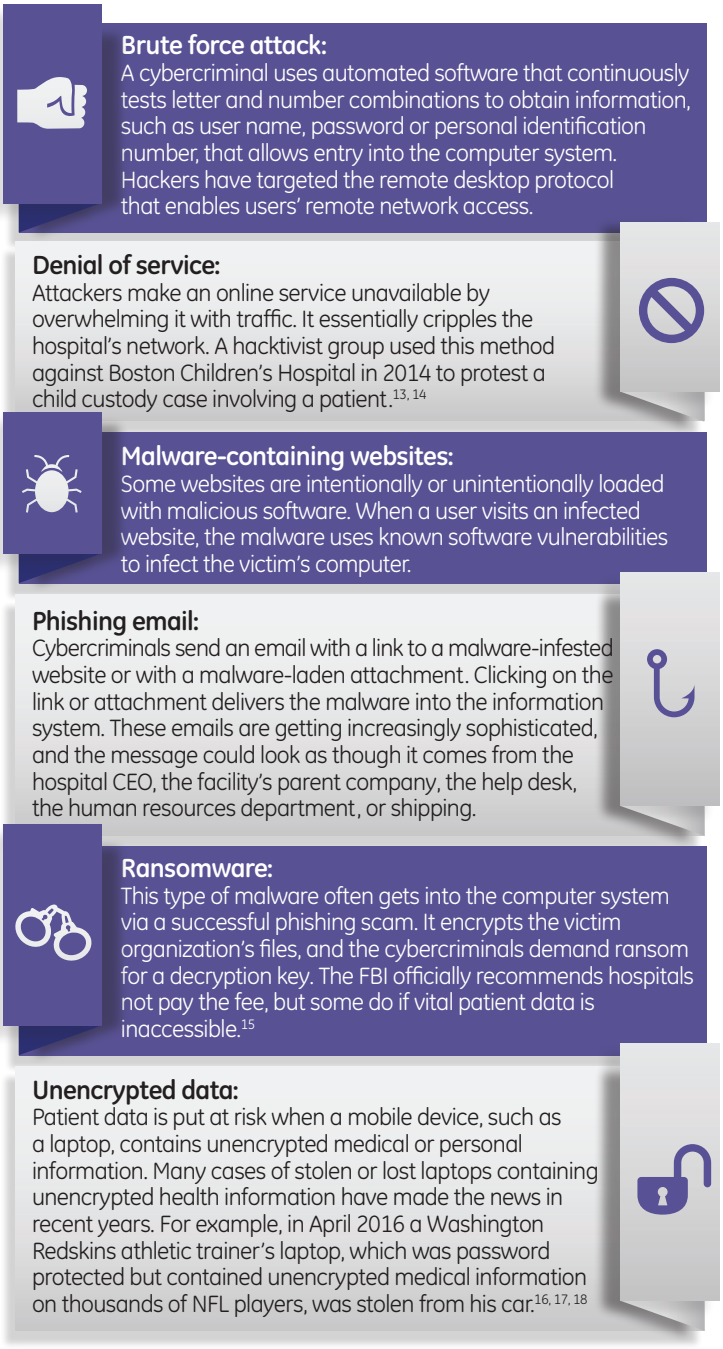
Cost pressures on hospitals also can hamper efforts. While cybersecurity is a top priority, other organizational goals, such as maintaining overall hospital financial viability and ensuring delivery of high-quality care, compete for budget dollars, notes a survey by the research firm KJT Group Inc.[12]

The enormity of the problem and the complexity of hospital cybersecurity can make the task seem impossible. "Some people say it's too intimidating; it's too overwhelming," Callahan says. "You've got to triage it. You have to go step by step and go down the priority progression."

Healthcare organizations may never be able to achieve perfect cybersecurity, Seiersen says. But, he adds, "we have to make the stakes difficult enough that the attacker goes somewhere else."

Seiersen predicts that cybersecurity innovations increasingly will be driven by healthcare. "Necessity is the mother of invention. I think other industries will begin looking to us because they have privacy risks, too."

## Cyber-threats 101



[1] Siwicki, Bill. Healthcare IT News. Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money. http://www.healthcareit-news.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom. May 23, 2016.

[2] Sun, Deedee. Hackers demand ransom payment from Kansas Heart Hospital for files. http://www.kwch.com/content/news/Hackers-demand-ransom-payment-from-Kansas-Heart-Hospital-380342701.html. May 20, 2016.

[3] Stefanek, Allen. President and CEO. Hollywood Presbyterian Medical Center. Memo from CEO. February 17, 2016.

[4] Winton, Richard. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html. February 18, 2016.

[5] Ponemon Institute LLC Ponemon Institute Research Report. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. May 2016.

[6] Humer, Caroline and Jim Finkle. Your medical record is worth more to hackers than your credit card. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN-0HJ21I20140924. September 24, 2014.

[7] Olavsrud, Thor. CIO. 11 Steps Attackers Took to Crack Target. September 2, 2014.

[8] FBI Warns of Dramatic Increase in Business E-mail Scams. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams. July 26, 2016.

[9] Independent Security Evaluators, LLC. Hacking Hospitals. https://securityevaluators.com/. July 26, 2016.

[10] Vergun, David. Manning guilty of 20 specifications, but not 'aiding enemy'. https://www.army.mil/article/108143/Closing_arguments_heard_in_Pfc_Manning_tri-al/. July 26, 2013.

[11] Tate, Julie. The Washington Post. Bradley Manning sentenced to 35 years in WikiLeaks case. August 21, 2013.

[12] A propriertary study on Cyber Security for GE Healthcare by The KJT Group, Inc.

[13] Farrell, Michael B. Justina Pelletier case: Hacker group Anonymous targets Children's Hospital – The Boston Globe. https://www.bostonglobe.com/business/2014/04/24/hacker-group-anonymous-targets-children-hospital-over-justina-pelletier-case/jSd3EE5V-VHbSGTJdS5YrfM/story.html. July 26, 2016.

[14] Miliard, Mike. FBI arrests Massachusetts man for Anonymous 2014 cyberattack on Boston Children's Hospital. http://www.healthcareitnews.com/news/fbi-arrests-massachusetts-man-anonymous-2014-cyberattack-boston-childrens-hospital. Feburary 19, 2016.

[15] Incidents of Ransomware on the Rise. https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise. July 26, 2016.

[16] Clarke, Liz. The Washington Post. Redskins employee's laptop stolen; NFL trying to determine extent of the breach. June 1, 2016.

[17] Knoblauch, Austin. Redskins: Laptop containing player data was stolen. http://www.nfl.com/news/story/0ap3000000666134/article/redskins-laptop-containing-player-data-was-stolen. June 1, 2016.

[18] Petchesky, Barry. Deadspin. Thousands of NFL Players' Medical Records Stolen from Skins Trainer. June 1, 2016.

**Staff Writer, GE Healthcare**

**For more information on this topic, please contact Forward.Thinking@ge.com**

**www.gehealthcare.com/forwardthinking**



Please visit www.gehealthcare.com/forwardthinking.

JB21249US (1)b
August 2016