Hospital cyberattack highlights health care vulnerabilities

March 30 2016, by Tom Murphy

In this Thursday, Feb. 5, 2015, file photo, the Anthem logo hangs at the health insurer's corporate headquarters in Indianapolis. A lawsuit filed against Anthem over its massive database breach in 2015 rips the insurer's cybersecurity and casts a spotlight on the vulnerability of health care information. The insurer cautions that the lawsuit's claims are merely allegations. (AP Photo/Michael Conroy, File)

A cyberattack that paralyzed the hospital chain MedStar this week is serving as a fresh reminder of vulnerabilities that exist in systems that protect sensitive patient information.

That attack came a month after a Los Angeles hospital paid hackers $17,000 to regain control of its computer system and more than a year after intruders broke into a database containing the records of nearly 80 million people maintained by the health insurer Anthem.

In Anthem's case, only a single password stood between hackers with a stolen employee ID and a chance to plunder the Blue Cross-Blue Shield carrier's database, according to a federal lawsuit filed by customers over the breach.

Cyber criminals also have staged high-profile attacks in recent years against the federal government, retail chains and the adultery website Ashley Madison, among many other targets. But security experts say health care companies make especially inviting targets for a number of reasons.

The information they protect is more valuable on the black market than a credit card number stored by a retailer. Health care cybersecurity also can lag behind measures taken in other sectors like banking.

This can stem in part from a business emphasis on tight budgets and convenience over security. Health care companies also have to deal with an additional headache: Multiple entry points into a system, with security quality varying among clinics, labs, hospitals that may have access.

In this Monday, March 28, 2016, file photo, a sign designates an entrance to the MedStar Georgetown University Hospital in Washington. Hackers crippled computer systems at hospital chain MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The hack is one of several high-profile breaches that have riddled the health care sector. (AP Photo/Molly Riley, File)

Cybersecurity experts note that government guidelines for health care data protection also are light on details and standards. The federal law known as HIPPA tells health care companies when they can disclose a person's records and to whom. It also requires them to protect the information.

But it doesn't come with a lot of specific mandates for that protection, said Lee Kim, director of privacy and security for the nonprofit Healthcare Information and Management Systems Society.

Intruders cracked Anthem's database sometime between the end of 2014 and the start of 2015 in a hack that is still under investigation. They gained access to Social Security numbers, birthdates and employment details for customers as far back as 2004, all key ingredients for stealing someone's identity.

Anthem, the nation's second-largest health insurer, has said that hackers staged a sophisticated attack that evaded multiple layers of security to reach its database. But a lawsuit filed last year by customers who say they were affected by the breach paints Anthem as a ripe target.

It says the insurer allowed wide employee access to its database and didn't train employees how to handle "phishing" emails, which can bait a recipient into revealing a password.

Investigators have said they think hackers may have used a phishing scheme to compromise the credentials of several workers.

A partially redact complaint filed in the litigation also said the company failed to employ common defenses like encryption, which can scramble data and make it useless.

"Stealing this much data takes time, and there were numerous steps along the way when any company following standard IT security practices would have foiled the hackers," the complaint states.

An Anthem spokeswoman said the details in the federal lawsuit were merely allegations, and the company could not comment on pending litigation.

"At Anthem, securing our member, provider and client data is a top priority," spokeswoman Jill Becher said in an email.

Hackers cracked Anthem's database by stealing the credentials of an employee whose job didn't require access to the database, according to the complaint, which was based in part on a security assessment Anthem commissioned after the breach.

A failure to restrict access to sensitive information is one of the biggest security weaknesses hackers exploit, said Michael Zweiback, an attorney and former federal prosecutor. Allowing widespread access gives hackers many chances to try to trick a worker into divulging a password.

"This is something that happens in hospitals, it happens in Fortune 500 companies right now, every day," he said.

Companies hesitate to restrict access because they want to make it easy for employees to move from network to network and do their jobs, Zweiback said.

"When security becomes the emphasis, employees start to complain because maybe they don't get access as quickly," he said.

The lawsuit also states that Anthem only required a single password for those who wanted to get into its database from a remote location. Experts say two-factor authentication is the more common practice. This basically involves an employee entering a user name and password and then a separate password or identification number that can change.

Only about 10 percent of health insurers use two-factor authentication and encryption to protect data, said Avivah Litan, a cybersecurity analyst for the information technology adviser Gartner. Litan works as a consultant in several sectors, including health care.

Anthem has said it normally encrypts data it exports, but that practice would not have helped because the hacker used high-level security

credentials to get into its system.

Experts say encryption can be tuned so that even authorized users can view only one person's account or a portion of a record at a time.

Litan and other consultants say health care companies have started showing more interest in cybersecurity, and top executives of these companies have begun to pay closer attention to it. But Litan hasn't seen the actual investment from these companies yet.

"I'm sure Anthem has made some changes, but the other ones are waiting until they get budgets, and they won't get budgets until they get breached," she said. "That's just the way it works."

Anthem has said in regulatory filings that it quickly fixed a security vulnerability it discovered after its breach and has continued to improve security since then.

Ultimately, no security plan is perfect against a determined hacker, noted John Gunn, vice president for VASCO Data Security. But companies that drop several layers of security between an intruder and sensitive information can convince a hacker to try elsewhere.

"The more systems that companies put in place, the more attractive other targets are based on what a hacker has to invest and what they will get for it," Gunn said. "Companies make this cost-reward decision, so do hackers."