ADVISEN FPN
FRONT PAGE NEWS

Health Care CIOs Boosting Security in the Wake of Breaches

Publication Date **08/20/2014**
Source: **Dow Jones News Service**

By Clint Boulton

A recent string of high-profile data breaches is leading some health-care CIOs to modify their approach cybersecurity.

The new approach is partly influenced by executive boards demanding more communication from IT on security efforts. CIOs say they are implementing new security software and processes, hiring staff and meeting with their boards more regularly. But the industry may need to up its security spending to get results. Health-care providers generally have smaller IT budgets than private-sector companies.

The shift comes with an awareness that health-care is lagging behind other industries in security efforts. A May study from BitSight Technologies, ranked health-care cybersecurity below retail and other industries. A U.S. Department of Health and Human Services' database of breach reports has tracked 944 incidents affecting personal information from about 30 million people. The devastating impact of last year's Target Corp. breach further tuned health care attitudes towards cysbersecurity.

In this context, health-care CIOs have adjusted their security posture. Marc Chasin, CIO of St. Luke's Health System, said IT hosts quarterly cybersecurity briefings with senior executives. Mr. Chain said he is also planning to detail St. Luke's cybersecurity efforts at a meeting with a new audit committee set up this year to assess risks.

Improved communication with the board was most evident on Monday following news that a cyberattack against rural hospital operator Community Health Systems Inc. resulted in the data theft of 4.5 million people . Mr. Chasin said the news resulted in a flurry of questions from senior executives and board members about the hospital's defenses. They asked: whether the organization was susceptible to such breaches; what the network defenses are; and what the company's remediation steps were in the event of such a breach.

St. Luke's security efforts, which includes a program teaching employees on how to recognize email-based threats, has been complicated by the industry's federally-mandated push towards digital health records. Unlike the financial industry, which has the time to build out sophisticated digital security systems, health care has "been on paper until recently," Mr. Chasin said. St. Luke's and other health-care providers are still playing catch-up.

But hackers are not waiting. Health-care organizations make fine targets because they possess payment data, as well as detailed patient records that are used to collect reimbursement for health-care services, said Judy Hanover, an IDC analyst who covers health care. She said that criminals steal patient data to fraudulently file an insurance claim for services that haven't been rendered, or impersonate patients to receive health care services.

The recent Community Health hack, which resulted in the theft of patient names, addresses, birth dates, telephone numbers and Social Security numbers, has helped drive home the point that health-care remains a major target. "We've not been on the front lines as long as defense or finance... but I'm slowly starting to see that shift as I talk to my peers," said Reid Stephan, director of IT security, who joined St. Luke's after serving as a security manager for Hewlett-Packard Co.

Darren Dworkin, CIO of Cedars-Sinai Medical Center, said health-care providers have long focused on preventing data loss from within -- such as when an employee loses a laptop -- rather than defending against external threats. Citing the April incident in which Anonymous allegedly crippled Boston's Children's Hospital with a denial-of-service attack, he said that he is acquiring new cybersecurity technologies and improving governance. "Now that people are coming at us, we... are revisiting security in a new way," said Mr. Dworkin. "There's a lot we need to do."

To start health-care organizations can increase their security spending, Ms. Hanover said. Health-care providers generally have smaller IT budgets than private-sector companies. U.S. health-care providers' spending on security software and services will account for only 1.8% of their total IT spending in 2014, she said.