APRIL 2014

CSC WORLD

HOW BIGGER GOT better

Inside the Bank's
Post-Merger Transformation

INSIDE

HEALTHCARE AND CYBERSECURITY

THE PRESSURE'S ON

by Jenny Mangelsdorf

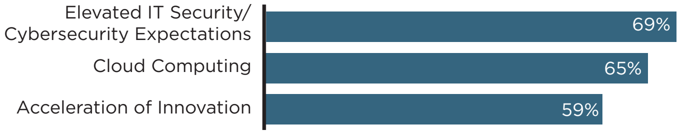
> "As attacks and threats rise, privacy and security enforcement also is rising sharply. Regulators in Australia, the United States and European Union have increased their vigilance, and a number of other governments, such as Singapore, have or will soon have new privacy laws."
>
> — Richard Staynings, CSC Global Coordinator, Healthcare Cybersecurity

As major security breaches continue to top the news, governments and organizations respond with new regulations, increased oversight and stiffer penalties. Simultaneously, increased demand for mobility and expanding supply chains, along with a desire to link IT systems to industrial control systems, adds to risk. Cybersecurity has taken center stage for healthcare CIOs, as evidenced by responses to CSC's 2013 *CIO Barometer* survey.

The fifth annual *CIO Barometer* represents the views of more than 680 IT managers, directors and officers working for organizations across 18 countries. For those operating in the healthcare sector, cybersecurity consistently appeared as a priority and challenge, regardless of whether the subject was innovation, management or cost.

Overall, healthcare respondents reported "elevated IT security/ cybersecurity expectations" as the most significant development in their IT departments, at 69 percent, followed notably by "cloud computing," at 65 percent, and "acceleration of innovation," at 59 percent — each of which brings its own security challenges.

Healthcare: Significant Developments in IT Departments



"Most of the life sciences industry is having its intellectual property stolen left, right and center," says Richard Staynings, CSC global coordinator, Healthcare Cybersecurity. "Nation-funded cyberespionage units, for example, continue to infiltrate pharmaceutical companies in order to steal intellectual property so their nations can better compete in the global pharmaceutical space."

As the life sciences industry battles theft of intellectual property and works to better secure its supply chains, medical providers and insurers focus on securing personal healthcare information.

"Unlike life sciences organizations, which are being targeted by Asian state-sponsored cyberthieves, payers and providers are being targeted by cybergangs mainly from Eastern Europe," Staynings says. "These criminals increasingly target medical records, which can bring $20 – $40 per record compared to, at most, $2 for a credit card record.

Regulations and risk

"Some very opposing forces are making cybersecurity much more challenging for healthcare providers," adds Phil Hemmings, CSC director, Global Industry Marketing, Healthcare and Life Sciences. "For example, providers want to improve coordination of care by sharing data with other providers, but by doing that they increase their security exposure tremendously."

Regardless of whether a healthcare organization is providing care or developing new medicine, evolving regulations play a key role in driving the focus on cybersecurity, especially considering the associated risks, including class-action lawsuits, jail and loss of reputation.

"As attacks and threats rise, privacy and security enforcement also is rising sharply," says Staynings. "Regulators in Australia, the United States and European Union have increased their vigilance, and a number of other governments, such as Singapore, have or will soon have new privacy laws."

Penalties and associated damages also have been increasing. Last October, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs approved new EU data protection and privacy regulations, including increasing noncompliance fines to up to €100 million, or 5 percent of an organization's global annual turnover — whichever is greater.

In the United States, starting in 2014, patients who are harmed by a data breach will be able to collect a portion of the penalty money as damages. The possibility of jail time, up to 10 years, also has made senior executives more attentive and apt to drive more of their focus, and budgets, toward security.

Managing a challenge and priority

With cybersecurity costs escalating, and some say becoming unsustainable, healthcare executives cite management as a priority. When asked about "management of expanding IT security/cybersecurity," 43 percent reported it as "very important," while only 3 percent reported it as "not important at all."

Healthcare respondents also ranked "more effective management of IT security/cybersecurity" as a "very high priority," at 36 percent, a "high priority" at 24 percent, and a "priority" at 27 percent.

With both management and budgets an issue, an overwhelming percentage of healthcare respondents say they are looking to managed security services for help, with 27 percent reporting that the "adoption of managed security services" is a "very high priority," and 20 percent and 38 percent reporting it as a "high priority" and "a priority," respectively.

"Managed security services help healthcare [organizations] offload the mundane operational work, providing a huge opportunity to free limited internal staffs for higher-value security tasks, lower their security costs and obtain much better results," Staynings says.

Lowering healthcare costs overall, regardless of region or industry, also continues to drive the industry, and many look to innovation to help alleviate the issue.

However, innovation carries its own security challenges. Healthcare respondents, when asked about the "main issues limiting the IT department's leadership in terms of innovation," cited "concerns in effectively managing IT security/cybersecurity risks," at 44 percent, second only to "budget constraints" at 48 percent.

BYOD, big data and security

While game-changers such as bring your own device (BYOD) and big data analytics carry challenges, their adoption seems certain. For example, only 10 percent of healthcare respondents reported that "allowing the business to use BYOD/consumer technology in the workplace" was "not important at all" or "didn't apply" to their companies, whereas 39 percent responded that it is "very important."

New big data analytical capabilities also offer the potential for solving some of healthcare's biggest challenges — 40 percent of healthcare respondents reported "harness big data" as "very important," whereas only 2 percent said it "doesn't apply to my company." However, securing and managing that data also presents major security and privacy issues.

"The innovative technologies the healthcare industry wants to use and explore create additional security challenges," says Staynings. "For example, improving a population's overall health requires huge systems and massive amounts of data, which in turn creates more security issues."

As healthcare organizations adopt new technologies, they also need applications to support them. Sixty-one percent of healthcare CIOs reported that they believe their role is perceived to be centered on "energizing and promoting the applications portfolio." However, applications can present major risk.

"If you want to steal information, compromising an application is the easiest way to get it," says Staynings. "Today, it's a lot more difficult to get on people's networks or access their databases. The simplest approach is to find the vulnerability in an application."

Fortunately, the healthcare industry thrives on challenge, as seen by its many accomplishments. New challenges, such as managing aging populations and increased rates of chronic diseases, along with securing critical infrastructure and intellectual property, and securely delivering medicine, care and patient data, will be met as well. ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

To see the full report, go to csc.com/cio_barometer.