CIO BAROMETER — HEALTHCARE CYBERSECURITY

DATA AT RISK

"As attacks and threats rise, privacy and security enforcement also is rising sharply. Regulators in Australia, the U.S. 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

Healthcare and Cybersecurity: The Pressure's On

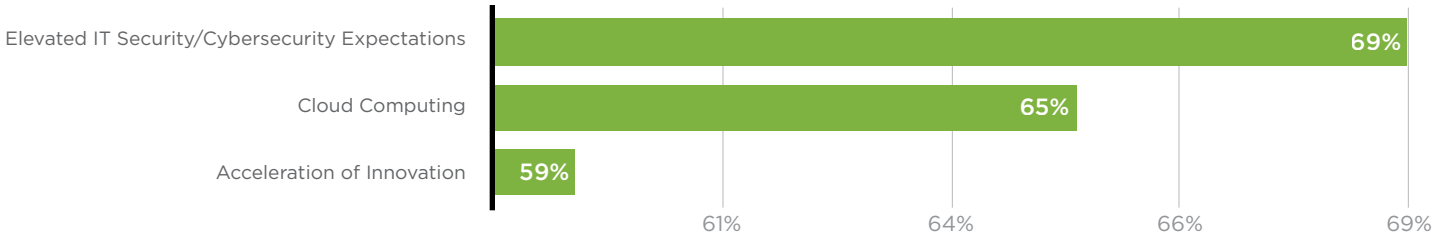
As major security breaches continue to top the news, governments and organizations respond with new regulations, increased oversight and stiffer penalties. Public tolerance is slipping, too. Simultaneously, increased demand for mobility and expanding supply chains, along with a desire to link IT systems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

CSC
BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

The fifth annual CIO Barometer represents the views of more than 680 IT managers, directors and officers working for organizations spread 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%, followed notably by "cloud computing," at 65%, and "acceleration of innovation," at 59% — both of which bring their own security challenges.

Healthcare: Significant Developments in IT Department



"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 cyber-espionage units, for example, continue to infiltrate pharmaceutical companies in order to steal their 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 cyber thieves, 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.

"Once you have access to a medical record system, you have access to tens of thousands of individual records, which makes theft a very lucrative prospect. Thieves can walk off with millions, and it often takes months before a provider or payer discovers the theft."

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, and are encouraged, to improve coordination of care by sharing data with other providers, but by doing that they increase their security exposure tremendously. Their cyber defense posture is based upon a fortress principle, and now they have more doors in the fortress walls open to partners than they have guards to watch them."

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 U.S. 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 non-compliance fines to up to 100 million euro, or 5% of an organization's global annual turnover — whichever is the greater. In the U.S., 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 in the U.S., also has made senior executives more attentive and apt to drive more of their focus, and budgets, to security.

Healthcare respondents to the CIO Barometer study reported "cybersecurity and IT security costs," at 36%, as the most "costly element" in their overall budgets for the previous year.

"Healthcare by and large didn't have discrete cybersecurity budgets until recently; instead security was just a part of overall IT funding," says Staynings. "Now discrete cybersecurity budgets are appearing across the industry, eating up a much larger percentage of overall IT spend."

MANAGING CYBERSECURITY 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% reported it as "very important," while only 3% 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%, a "high priority" at 24% and a "priority" at 27%.**

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

"Healthcare organizations have procured all kinds of different security technologies, and now they need to run and manage them," says Staynings. "That's very costly to do, and they're still not staying up with all the current threats. Typically they're addressing yesterday's requirements and not solving any of the big challenges. It's a big problem.

"Managed security services help healthcare offload a lot of 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."

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%, second only to "budget constraints," at 48%.**

BYOD, BIG DATA AND SECURITY

While game-changers such as BYOD and big data analytics carry challenges, their adoption seems certain. **For example, only 10% 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% responded that it is "very important."**

"Today it's a lot more difficult to get on people's networks or access their databases. The simplest approach is to find a vulnerability in an application and exploit it to gain access to the data that application can access or, even more concerning, to change that data, which could cause some very real harm."

Richard Staynings, CSC global coordinator, Healthcare Cybersecurity

New big data analytical capabilities also offer the potential to solve some of healthcare's biggest challenges — 40% of healthcare respondents reported "harness big data" as "very important," whereas only 2% 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, in order to improve 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 a vulnerability in an application and exploit it to gain access to the data that application can access or, even more concerning, to change that data, which could cause some very real harm.

"The majority of healthcare applications are ancient by today's standards and have been up and running in a traditional client/server environment for a long time," he adds. "Employees expect to access them from smartphones and other personal devices. At the same time increasing numbers of other clinical applications also need to access these old iron systems and their data for the meaningful exchange of information. However, they weren't built to do that securely."

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 medicines, care and patient data, will be met as well.

CIO Barometer 2013 is the fifth annual survey reported by CSC in collaboration with market research institute TNS Sofres. Based on a quantitative analysis of the trends and outlooks for IT directors, the survey relied on CIOs from major European, North American, Brazilian, Australian and Asian companies and public institutions. To see the full report, go to http://www.csc.com/townhall/insights, or email securitysolutions@csc.com.

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

WORLD CSC HEADQUARTERS

THE AMERICAS
3170 Fairview Park Drive
Falls Church, VA 22042
United States
+1.703.876.1000

ASIA
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

AUSTRALIA
Level 6/Tower B
Macquarie Park, NSW 2113
Sydney, Australia
+61(0)2.9034.3000

EUROPE, MIDDLE EAST, AFRICA
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

ABOUT CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC leads with an informed point of view while still offering client choice.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."