Target exec's departure puts spotlight on CIOs

March 6 2014, by Bree Fowler

This undated image provided by Target Corp shows Chief Information Officer Beth Jacob. Jacob is resigning effective Wednesday, March 5, 2014, as the retailer overhauls its information security and compliance division in the wake of a massive pre-Christmas data breach. (AP Photo/Target, Mark.Williams)

The departure of Target's chief information officer in the wake of the company's massive pre-Christmas data breach highlights the increased pressure facing executives who are charged with protecting corporate computer systems from hackers whose attacks are on the rise and becoming more sophisticated.

CIOs from companies in all walks of business —from retail to banking and drug discovery— are using the Target breach as a rallying point to call attention to their struggle and garner additional funds and manpower to fight digital threats.

Cyberattacks were on the rise long before Target's news that hackers had stolen 40 million debit and credit card numbers, along with the personal information belonging to as many as 70,000 people. A 2013 Hewlett-Packard Co.-sponsored study by the Ponemon Institute found that the average annual cost of cybercrime incurred by a benchmark sample of U.S. organizations was $11.6 million per organization, a 26 percent increase from the previous year.

For a host of companies, the Target breach was a pivotal event that permanently altered the way they approach data security. Many CIOs say they're receiving more support, but they say the trade-off is that they're facing increased scrutiny from their CEOs and other executives. If their fortress walls fall to hackers, their jobs will be on the line.

Ken Grady, CIO of life sciences company New England BioLabs Inc., says the increased attention to data security has been a good thing for him. It has prompted much needed support from colleagues. But that backing comes at a cost.

"If I have a breach in spite of all that, I need to be able to say that we did everything we could to prevent it," Grady says. "If I can't do that, then it would have a negative effect on me."

Analysts believe the Target data theft couldn't have had a positive effect on Beth Jacob, who had served as the company's CIO since 2008. Target said Wednesday that Jacob's resignation was her decision, but analysts say Jacob took the fall amid a slew of bad publicity for the Minneapolis-based company.

Target is in the midst of overhauling its information and compliance division and plans to look outside the company for a chief information security officer and a chief compliance officer, two newly created positions. Before the overhaul, information security functions were split among a variety of executives.

Tim Scannell, director of strategic content for the CIO Executive Council, a professional trade group, says companies have come to realize the importance of security. The result: boosted budgets and staffing increases. According to a recent CIO Executive Council survey, computer security professionals say they expect an average increase of 8 percent in their budgets this year.

"I think CIOs are getting more respect," Scannell says. "They're winning a seat at the table. But along with that, we have a heightened security risk, so they're under pressure to do something about it."

Scannell notes that even if a company isn't a retailer that deals directly with consumers, most now have some kind of e-commerce operations, which makes them a potential target for an attack.

The new era of cybersecurity was a hot topic at the recent RSA tech security conference in San Francisco. Daniel Ives, an analyst for FBR Capital Markets, says many of the data security professionals in attendance said they are increasing security spending in light of recent high-profile data breaches. He predicts that data security spending could rise as much as 15 percent this year.

Ives says that while retailers, financial and health care companies have the most to lose in the event of a cyberattack, any company that so much as uses mobile phones or puts customer data on their networks is also at risk.

"Getting on the cover of The Wall Street Journal in some cyberattack is a CIO's worst nightmare," he says. "They're the bodyguard and the linchpins of the companies they work for more today than ever before, because of the amount of data that's out there."

And companies aren't the only entities at risk for data breaches. Universities also handle vast amounts of personal information.

Gerry McCartney, Purdue University's systems CIO, says public universities also face the challenge of remaining transparent while protecting everything from student social security numbers to the research of its professors.

"If you lock data up like Fort Knox people can't use it," he says. "It's like locking your car up in the garage so you can't get into an accident, but then what's the point of having a car? You want your people to have access to data."

Ed Brandman, CIO of the private equity firm KKR & Co., says his company focuses on advising its portfolio companies, which range from payments processor First Data Corp. to retailer Academy Sports, on the best practices for protecting data.

He says a major task CIOs face is balancing data security spending with the perceived potential for an attack, noting that CIOs also have to decide how much to spend on other technology related investments such as computers and mobile devices.

"And no matter how much you're spending, you never have 100 percent confidence that you're safe," Brandman says. "It's an always evolving state."

Mark Popolano, CIO of ProSight Specialty Insurance, agrees. His company's commercial insurance business is all about weighing risks against costs.

"If you want to spend an infinite amount of money on security you can," he says. "But the government does and they're not 100 percent foolproof."

It's for that reason that Grady says New England BioLabs paid particular attention to how Target and Neiman Marcus, which also recently reported a data breach, handled their situations in terms of costs and transparency.

He says the fact that the breaches happened to those two companies shows that they can happen to anyone. The important thing is to know how to respond if the worst does occur.

"What we don't want is to be unprepared and not have a plan, heaven forbid we have such an issue," Grady says.

Citation: Target exec's departure puts spotlight on CIOs (2014, March 6) retrieved 21 June 2024 from https://phys.org/news/2014-03-exec-departure-spotlight-cios.html