CSO

INSIDER FEATURE

Caught in the breach: How a good CSO confronts inevitable bad news

Breaches are inevitable, but those tasked with detecting and responding to them say there are ways to avoid becoming the 'Chief Scapegoat Officer'.

By Taylor Armerding | Follow

CSO | Sep 15, 2014 6:36 AM PT

What goes through the mind of a CSO/CISO upon being told by his or her team that their organization has been breached?

This is not an idle or theoretical question. It seems that almost every day brings news of yet another breach of a high-profile organization, with the potential number of consumer victims running into the tens of millions, and the costs to the company running into hundreds of millions, or even billions when the long-term cost of brand damage is included.

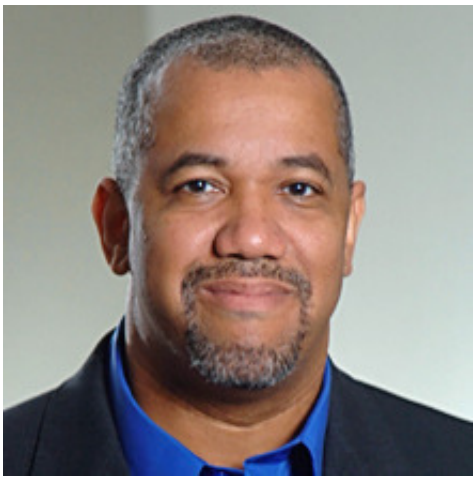
So it makes sense that C-level executives with "Security" as part of their title would be the ones facing questions about how it happened and what to do about it, not to mention accountability for it.

[How to survive a data breach]

Martin Fisher, CISO at Northside Hospital, admits that the immediate reaction for the typical CSO/CISO will probably include, "a few minutes of panic/denial, then some terror."

He gets no argument on that from Kim Jones, senior vice president and CSO at Vantiv, who adds "anger" to the list. But both say that for a professional, those initial feelings quickly turn to calmness and resolve.

> "The organization is going to look to the CISO to figure out what is going on and provide the quality information needed to respond effectively to the breach event" Fisher said. "Whether 'at fault' or not, the CISO owes the best possible leadership to the organization at that critical moment."



Kim Jones, senior vice president and CSO, Vantiv

Jones agreed. “The real issue is how long do the non-constructive mindsets last,” he said, adding that that can depend on several factors – whether a CSO has set proper expectation regarding breaches; what has been done in advance to improve security in the infrastructure; and whether the IT program has been built with security as a focus.

“My anger and resolve are focused on stopping the bad guys as early and quickly as possible,” he said, “but I have the luxury of that mindset because I have a leadership team that views security as a brand-enabling value proposition.”

Peter Chronis, CSO of EarthLink, said whatever emotions are running through a CSO’s mind after a breach, resolve is the one to project. “In times of any crisis, leaders set the tone for how organizations behave, prioritize and react,” he said.

“As security leaders, it is our job to have a tactical plan prepared for the worst circumstances, but we’re also responsible for building a strong strategy to reduce the likelihood that plan will be needed.”

The panic/terror feeling is understandable, however, given the prevailing attitude toward CSOs and CISOs in many organizations. According to a recent survey by ThreatTrack Security titled, “No Respect. CISOs Misunderstood and Underappreciated by their C-Level Peers,” 74% of the 200 executives responding said they thought CISOs should not be part of organizational leadership teams.”

And 44% said the primary role of the CISO is to be held accountable for any organizational data breaches – another way of saying “scapegoat.”

Fisher, joking that the findings should be filed under, “dog bites man,” said the serious point is that in the past, some CSOs, “were more of a pain in the rear to C-levels than anything else.”

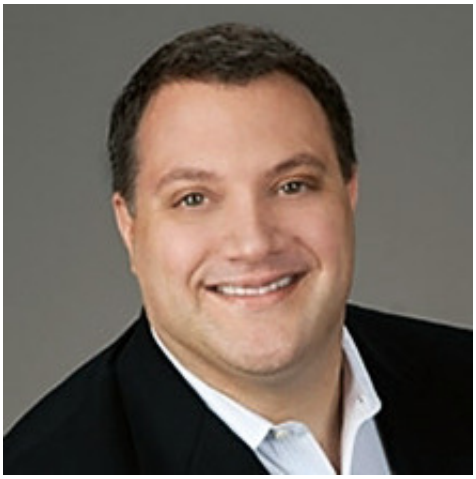
To change that, he said, CSOs need to demonstrate business savvy and be willing to, “subordinate the tactical desires of the security team to the strategic/operational goals of the organization.”

Jones has a similar message, noting that in many companies, “CSO stands for ‘Chief Scapegoat Officer’ even to this day. It really creates a perception/morale issue and worse, an efficacy issue.”

Jones said that kind of pressure on CSOs, “forces them to think extremely tactically about issues and problems as they live in fear of the breach, which only exacerbates the perception of CSOs as lower-level wrench turners versus strategic enablers.”

If that perception is going to change, he said, it will likely take efforts by other C-level executives to encourage CSOs to think strategically, and more effort by CSOs to, “link ourselves to the business.”

Chronis said CSOs should stop viewing themselves as “victims of circumstance.” Those who, “build long-lasting credibility and are partners in solving complex business problems will find themselves at the table more often than those who don’t.”


Peter Chronis, CSO, EarthLink

Whatever the view of CSOs, they are very likely to deal with breaches. Numerous experts agree that it is impossible to prevent them all, given the skill and sophistication of attackers, and that the entry point may have nothing to do with a technology weakness, but simply a careless employee who clicks on something like a malicious link in a phishing email.

As Jones put it, “I can make it harder for someone to get in, and I can make it harder to get to me versus my competitor, but I can’t absolutely guarantee that we’ll never be breached, even given infinite time and infinite resources.”

At that point, the mindset is on detection and response. An effective response can often prevent attackers from accomplishing their mission. The real disasters – and there are many examples – come when detection fails, and a company learns from a third party weeks or months after the fact that it has been breached and the attackers are still inside their system.

For any CSO without a plan, there are a number available online. One, from Experian, presents a “first 24-hour checklist” that includes securing the premises, documenting everything known about it, stopping additional data loss, reviewing protocols, starting an investigation and notifying law enforcement if needed.

Beyond that is a list of tasks that include fixing the vulnerability that caused the breach, identifying legal obligations and reporting regularly to upper management.

Fisher called the Experian plan, “as good a draft/generic template as any. But the key to any effective IR plan is customizing it to your organization. You have to take organization culture, process, leadership, and capability to build a plan that is actually actionable when the incident happens,” he said.

In general, Chronis said that, “knowing the warning signs, having a response plan and being prepared to adjust it on the fly is your most valuable asset during a potential security event.”

Jones agreed. “My focus for breaches at the tactical and operational levels needs to be on detection and containment. In other words, find the breach earlier, isolate it and kill it before it gets to the crown jewels.”

Taylor Armerding