INSIDER FEATURE

Attracted to disaster: Secrets of crisis CISOs

In the aftermath of a security incident, new CISOs are often appointed to take over and lead through the chaos. Here are the skills and traits experts say these crisis CISOs need—and how to prepare yourself to rise to the occasion.

By Mary K. Pratt
Contributing Writer, CSO

Stephanie Benoit-Kurtz spent much of her career taking jobs where the priority is crisis cleanup.

“I’m brought in when organizations don’t have what they need and they need someone to figure that out,” she says. That means assessing cybersecurity capabilities, pinpointing problems, and closing gaps. The work makes her, in her words, “a nicely paid janitor.”

Benoit-Kurtz and other security experts like her have plenty of opportunities for work, with high-profile breaches and hacks pushing CEOs and boards to hire new leadership, hoping that the top-level switch-up will set their organizations on a better course in the aftermath of a disaster.

SolarWinds, for example, hired former CISA chief Chris Krebs and former Facebook CSO Alex Stamos as consultants in early 2021, shortly after the discovery that Russian hackers had compromised the company’s software and used it as a pathway to launch other attacks.

Twitter hired Rinki Sethi as its new CISO in September 2020, following the high-profile breach the social networking site had suffered in July.

And a few years earlier, in 2017, Equifax took similar action, naming vice president of IT Russ Ayers as interim CISO before hiring veteran CISO Jamil Farshchi.

They’re all part of a niche class of CISOs who take on the difficult challenges that come in such crisis-fueled environments.

Leading through crisis

“Crisis CISOs—people who have been there, done that—are very much in demand,” says Paul Wallenberg, director of technology services at the recruiting firm LaSalle Network.

Enterprise executives often want new security leadership in the aftermath of a significant incident, believing that their organizations will benefit from the particular skills and the fresh perspective that a new appointee will bring, say Wallenberg and other experts.

And in many cases those executives are right: They do indeed gain something by bringing on new security chiefs.

“You see in history organizations where there was an incident or some significant regulatory action bringing in new CISOs, and some have made a night-and-day difference,” says Neil Daswani, a veteran cyber security leader and co-author of Big Breaches: Cybersecurity Lessons for Everyone.

But Daswani and others don't discount incumbent CISOs, noting that they, too, can add value in crises. In fact, in a world where security breaches are considered a matter of when, not if, management advisors say all CISOs should be developing the skills and temperament it takes to lead through a crisis to ensure that, one, their organizations can successfully navigate the post-breach challenges and, two, that their own careers can weather the storm.

"There is the need for due diligence after an incident to determine whether there were gaps, and there should be repercussions; everyone should be accountable for the job they're hired to do," says Deborah Golden, Deloitte Risk & Financial Advisory's US Cyber and Strategic Risk leader. "But it's not always a clear-cut decision on [whether to bring in a new CISO]. What's most important is how quickly the CISO and other executives can respond."

After the fall

Publicly traded companies that suffer a breach are most likely to hire new CISOs, and they typically look for security leaders who have experience handling a crisis, Wallenberg says.

"These companies are changing faces no matter what. Whether it's a placebo effect or not, it's a way of alleviating concerns going forward," he adds.

Government agencies likewise have a history of dismissing presiding CISOs during crises and appointing a new CISOs to take over, at least in part because "[t]here's often blame that needs to be laid at someone's feet," Wallenberg says.

Private organizations often seek out new CISOs at such times, too, according to industry insiders, although they frequently make the switch quietly to avoid bringing further attention to any security concerns.

CEOs have good reasons for wanting to bring in a new CISO to handle a crisis, Daswani and others say.

To start, a new CISO generally brings to the position needed skills—whether deep industry knowledge to appropriately align controls to risks or experience with new zero trust security protocols—that the incumbent CISO lacked in ways that contributed to the incident.

"You may need to bring someone on who can see what their predecessor couldn't see or help the leadership see what they couldn't understand previously," says Daswani, co-director of the Stanford Advanced Security Program and the former CISO of Lifelock and then Symantec's consumer business unit.

The new CISO, for example, may be more capable of identifying gaps and persuading the C-suite to make the investments needed to close those gaps, he explains.

Furthermore, crisis CISOs can help post-incident by signaling to the security department and to the enterprise overall that leadership is serious about making changes and improvements, Wallenberg says.

"It's not just the CISO who adjusts when a crisis happens; the whole security department and the whole organization does as well," he explains. "Companies have to make big shifts."

The case for incumbents

To be fair, a CISO hired during a crisis often has an advantage in advancing his or her agenda. First, the new CISO won't have to convince others that security needs attention, as that fact is already evident thanks to the incident that took place. Second, the rest of the C-suite is eager to demonstrate a commitment to security initiatives.

"When there's a new security leader brought in, I think everyone is going to be open-minded and have open ears again," Daswani says.

Despite the benefits that a crisis CISO can bring, Daswani says not all post-incident scenarios call for such leaders.

Daswani says chief executives and their C-suite leaders need to consider the incident's nature and severity, early indicators of how and why it happened, and the existing CISO's capabilities when determining whether to keep or dismiss the incumbent CISO.

"A company hit by a ransomware attack, which maybe means it needs a better anti-malware suite and a better backup strategy, could be the kind of incident best dealt with in a very straightforward way with no need to change leaders," Daswani says. "It may be better to keep the security leader in place with a goal of reducing risk quarter by quarter."

On the other hand, an organization that experienced a persistent attack from a nation-state hacker could very well need a more seasoned CISO than the one they had.

"Those are very different kinds of incidents, very different kind of threats," Daswani says.

It's important to note, too, that security leaders say incumbent CISOs provide their own value in a crisis.

Assuming they're qualified, they know the technology, the business processes and the industry as well as the threats and the risks that are unique to their own organization.

Given all that, they could possibly identify the root causes of the security incident more quickly than even a CISO brought in specific for that task.

Chaos junkies needed

Still, industry leaders say that not all CISOs have the full range of business, leadership, and security skills required to work through that critical post-incident period, when there's a spotlight on the enterprise and tensions run high.

"We don't want someone always complaining about the house being on fire; that's not going to help," Daswani says.

Daswani has taken on the post-incident CISO job during his career, and he says the job requires someone who will take charge yet demonstrate empathy to those impacted by the attack.

He says organizations benefit from someone who has had prior experience working through a security event.

Benoit-Kurtz says she, too, has learned from experience what traits are needed to succeed as a crisis CISO.

There's the ability to work through the turmoil—a trait she believes most CISOs in general already have. "In order to be in cybersecurity, you really have to be a chaos junkie because every day is something new that you didn't expect," says Benoit-Kurtz, who is currently the director of cybersecurity at Station Casinos and lead faculty chair for cybersecurity programs at the University of Phoenix.

They must be able to formulate a strong forward-looking security strategy, articulate it and then advocate for it—forcefully if needed. "The organization needs to have someone willing to challenge the other executives, because you can't throw Band-Aids on [the problems] and be done," she says.

At the same time, the crisis CISO needs to be calm in that chaos and possess the ability to communicate in ways that elicit in others the appropriate level of concern; they should know how to talk about security without alarming others while still impressing the need for remediations.

"You have to have astute communication skills to calm nerves and navigate the crisis calmly. And you have to be a bit of a politician. You have to be able to navigate a lot of stakeholder relationships," Wallenberg says, pointing out that these CISOs often work closely with regulators and lawyers to handle the government probes and lawsuits that often follow cyberattacks.

Additionally, such CISOs must have the technical chops, the security expertise, and the cultural fit.

“The job can be adversarial and tough because you’re telling vendors and the organization that the environment isn’t good, so you need someone who has the tenacity to stay tough but the skill to be build consensus,” Benoit-Kurtz adds.

These CISOs must also be skilled at quickly assessing workers’ skills and bring together those with the needed capabilities, a high level of commitment, and a willingness to speak up. “You need people who will challenge traditional approaches. So CISOs need to have team members who will challenge them, and the CISO needs to be secure enough to deal with that,” Benoit-Kurtz says.

A growth opportunity

CISOs experienced in crises management and willing to take on the task are in a growth profession.

But, then again, given the number of cyberattacks happening, every CISO will have those growth opportunities in the years ahead. Experts say many CISOs will indeed find themselves handling a significant incident at some point in their careers; some will handle more than one—even without seeking out such positions.

Golden has faith they’ll rise to the occasion.

“I do think that the majority of security leaders are well-suited to handle a crisis,” she says. “But you have to build that muscle; you have to train it.”

She says CISOs should prep for such events, perfecting the skills they’ll need as they build the incident response plans they’re already expected to develop as part of their regular duties.

“It’s understanding what the pressures are and knowing how to handle them in a crisis,” Golden adds, noting that wargaming is particularly effective at honing crisis management skills.

Daswani agrees, saying that CISOs should be studying the history of breaches and hacks as well as their root causes so they can incorporate that knowledge into their security plans to reduce the probability of an incident and the severity of a successful attack and up their chances of a quick, full recovery.

https://bit.ly/3rBv0Y6