CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | July 14, 2021

How GCs Should Respond to Worsening Threat of Ransomware Attacks

"A lot of GCs are realizing that this is something that really does fall into their laps," said Ronald Sarian, former GC at eHarmony, which was the victim of a major data breach in 2012.

By Phillip Bantz

What You Need to Know

- GCs need to play a central role in orchestrating cyberattack planning and response.
- Building an incident response team is a key part of the planning process.
- In-house leaders should regularly monitor their cyber insurance policies.

When Ronald Sarian took his first in-house job as the Los Angeles-based general counsel at eHarmony in 2013, he inherited a bit of a mess. Before his arrival, hackers had infiltrated the dating website and made off with passwords for millions of users.

As Sarian settled into the GC seat after having spent more than 20 years in the vastly different world of business and real estate litigation, he decided to immerse himself in all things cybersecurity.

He set out to understand how eHarmony stored and protected data for some 60 million users. He learned about firewalls and phishing attacks. He had lunch once a week with his information technology staffers. They had his cell number and he had theirs.

Photo: Chris Carlson/AP

The entrance of Colonial Pipeline Co. in Charlotte, North Carolina. Pipeline operators were directed to conduct a cybersecurity assessment under a Biden administration directive issued in May in response to the ransomware hack that disrupted gas supplies in several states.

"I thought to myself, 'This is going to be incredibly important for me to start getting into and really understanding how we work and what we're doing to make sure things are in order,'" said Sarian, who was an outlier in the in-house realm at the time.

"Most GCs had absolutely no clue about cybersecurity," he recalled. "I'd talk to them and they'd say, 'That's something that somebody else does.'"

That mindset has shifted over the past decade, as cyberattacks have become more common and hackers have developed increasingly aggressive and sophisticated methods of targeting companies of various sizes and in a broad cross section of industries.

"More and more GCs I talk to now have a better understanding of cybersecurity. A lot of GCs are realizing that this is something that really does fall

into their laps. Your job as the GC is to protect and enable the company," said Sarian. He's now a senior counsel at Constangy, Brooks, Smith & Prophete in Los Angeles.

If any in-house leaders were still sleeping on their cybersecurity responsibilities, the recent wave of high-profile ransomware attacks on major companies, including Colonial Pipeline Co., Acer Inc. and the National Basketball Association, to name only a few, should be a cold splash of water to the face.

"This is a comprehensive and existential risk to almost any company," said Tedrick Housh, a Kansas City-based partner at Lathrop GPM who leads the firm's cybersecurity team. "I think it is a bit of a false hope to treat this as an IT problem and not an organizational issue that GCs need to quarterback."

Prepare to have 'key pieces in place'

Outside counsel and cybersecurity experts cringe when they think of corporate clients who call in a panic in the midst of a cyberattack, knowing only that something bad has happened. They have no clue about how it happened or exactly which data and systems have been breached and are scrambling for a fix without a coherent response plan.

In-house leaders who want to avoid that chaotic and potentially devastating scenario need to be working regularly with their chief information and security officers, C-suite members, boards of directors and other stakeholders within their companies, including the public relations team, to craft step-by-step responses for various types of cyberattacks.

Establishing relationships with expert ransomware negotiators, outside counsel who specialize in cybersecurity and key contacts in law enforcement and regulatory agencies long before an attack occurs is another smart move.

"Coming from a legal perspective, there's an understanding and discussion that can be had in advance to put all of the key pieces in place," said Rocco Grillo, managing director at Alvarez & Marsal in New York, where he advises major corporations on cybersecurity matters.

Ransomware attacks have risen to the top of the list of concerns for in-house counsel, who most likely won't, and probably shouldn't be, negotiating directly with cyberattackers. Leave that to the experts.

But they should be a part of the discussions to get to that point and advise on the legal implications of paying a ransom to regain control of a company's data.

"These are difficult business decisions and I think the GC needs to be involved with the C-suite, board members and the negotiator," Sarian said. "It's critical."

'It's operational, it's legal, it's public relations'

While leading crisis teams in prior in-house legal roles, Theresa Robbins Shea, who recently took over as the legal chief at Utz Brands Inc. in Hanover, Pennsylvania, ran cyberattack simulations as part of her prep work for cyber-related snafus.

"I think the GC plays an integral role on that team. And it isn't just for privilege reasons. It's for purposes of thinking about all the legal implications that are related to all of these decisions that are made when you're dealing with any sort of crisis, whether it be cyber or COVID or otherwise," she said.

The IT team typically takes the lead on preventative cybersecurity measures, but "no matter how good your systems are, hackers are also good. So you

also have to have a structure in place for what will occur if and when some sort of breach happens," Shea noted.

"That structure is simply having the team members identified in advance, knowing what everyone's role is and the factors that will trigger the team being put into active mode. For us, that meant daily meetings with the team, assessing what's happening with the situation, deciding what steps need to be taken legally and otherwise," she said.

"It's operational, it's legal, it's public relations—it's all of that together and really formalizing a structure whereby that team is dealing with the updates that are occurring in real time, as opposed to trying to create that team after the problem occurs," Shea added.

At Uber Technologies Inc., the legal team also works closely with the cybersecurity team, board and audit committee to plan responses for various types of cyberattacks. The planning includes regular reviews of the San Francisco-based ride-hailing and gig economy company's cybersecurity posture, according to Keir Gumbs, the firm's former deputy GC.

"A CLO, as a senior leader of an organization, has a shared responsibility for ensuring that a company is prepared to deal with cyber-related threats," added Gumbs, who recently left Uber to become chief legal officer at Broadridge Financial Solutions Inc.

Doing the cyber insurance do-si-do

Cyberattack prep is incomplete without regular reviews of a company's cybersecurity insurance policy, especially as more insurers move to tweak coverage provisions in response to the rapid increase in costly ransomware incidents.

"It's just a very fluid situation," said J.A. "Jay" Felton, a corporate litigator and partner at Lathrop in Kansas City. "But every general counsel should be able to answer the questions, 'What are we doing to protect ourselves, and what do we do if we are hacked, and how are we going to pay for this? Do we have insurance?'"

Some insurers are now insisting on more intense underwriting, wanting companies to show that they have strong cybersecurity measures in place to help thwart attacks, noted Housh, Felton's fellow law partner.

"If you're looking at buying insurance, that seems rather intrusive," Housh said. "It's an intricate dance that's going on right now as the market tries to figure out how to deal with this."

Other insurers have decided to revoke ransomware-related coverage entirely. In May, for example, French insurer AXA declared that it would stop covering ransomware payments. The company's subsidiaries in Asia were subsequently hit with ransomware attacks.

Another major insurer, CNA Financial Corp., also fell victim to a ransomware attack earlier this year and reportedly paid a whopping $40 million to regain access to its data and network systems.

"So now the insurers themselves are under attack because they have important information about companies as well," Housh said. "More and more, those who are attacking a company have already gone in and done their reconnaissance work and not only know their financial situation and ability to pay but whether they have a policy that will likely pay."

He added, "If the bad guys know it before the company does, that's definitely not a recipe for success."