Georgia Municipal Association lawyer: In-house attorney, CIO must work in tandem on cyber threats

SUBSCRIBER CONTENT:
Jan 21, 2018, 6:00am EST

No longer is the chief information officer (CIO) a company's sole defense in the battle to keep information safe. Today, the in-house counsel is at the forefront of protecting organizations from cyber threats internally and externally.

SPECIAL/CAROLINE JOE
Alison Earles is an in-house attorney at the Georgia Municipal Association.

The technical aspects of cyber security still fall to a company's information technology (IT) department, but the in-house attorney and CIO must work in tandem, said Alison Earles, an in-house attorney at the Georgia Municipal Association, a non-profit state organization that represents municipal governments. Laws related to cyber security must combine with protective measures implemented by the IT staff, she said.

Sid Harris, former dean of Georgia State's J. Mack Robinson College of Business and a board member of two financial technology companies, agreed.

"More than ever, in-house counsels are working across the enterprise," he said. "With cyber [security] being a significant business risk, they must work with the chief information security officer or CIO to make sure the corporation is protected."

Protecting information begins with knowing what information you have, where it is and where it goes, Earles added. "Information not needed should be destroyed," she said.

Training around cyber safety is essential, according to corporate legal experts. Not only are employees of the Georgia Municipal Association trained regularly in conjunction with the Carl Vinson Institute at the University of Georgia, but so are elected officials and city employees, said Earle. The sessions cover information privacy and security laws, preventing breaches and responding when a breach does occur.

General counsels need to determine the value their companies put on cyber security, as well as the type and sensitivity of their data, said Will Fagan, general counsel and corporate secretary for the insurance brokerage firm Sterling Seacrest Partners, Inc. These legal leads also must make sure they attend corporate meetings that involve cyber security issues, he added, so their expertise can be acknowledged.

How do many cyber security attacks happen?

"In the largest number of data breaches," Fagan explained, "the vector of attack is some employee clicking on an email and opening up malware."

For example, he said, if a company president authorizes wiring money, cyber thieves could potentially create a phony order sent from the president to the accounting department. If the breach is not discovered, the money is then wired to the thieves. This "phishing" scheme is one of the most common used by cyber criminals, Fagan said. Frequently, these criminals are able to access a company's computer system from outside and "watch" traffic for months before striking, he added.

However, Earles said, "not all hackers are that good," so employees must learn common red flags to a cyber security attack.

"Usually you can see in the email if something is off: a URL not spelled right, a blank subject line or a dubious image," she said. "We always train our people not to open things that look suspicious."

Responding to cyber crises is crucial. According to Harris, reacting quickly is key.

"You need a lot of people making an analysis of the situation, but an internal team can take too long, because they don't always have specialized expertise to get the answer," he said.

A team from outside the organization, including counsel with cyber expertise, should be on standby to assist, Harris added.

"The last thing you want," he said, "is to have a partial solution [to the breach] that results in the same problem happening again."

To keep organizations from concealing breaches, some governments have implemented regulations requiring a time limit on notification to customers. The European Union (EU) was the first to implement a 72-hour notification policy that covers all data residing in the EU, regardless of the company's location. New York was the first state to enact a similar rule, also with a 72-hour limit to notify authorities.

While preventative measures are a must, companies also must be insured against cyber risks. Fagan said while most policies such as worker's comp or general liability are based on a set form, cyber has no such form. "Cyber is such a new and emerging field, the industry has not gotten to the point of having a set playbook," he said, adding that in-house counsel can assist in securing an experienced insurance broker who understands the company's business and its inherent exposures. "Insurance carriers are writing it as they go."

Considering all that can happen to a company, Fagan said, this issue is near or at the top of the list of concerns.

"Cyber security is one thing that can really keep you up at night," Fagan said.

Cyber security tips for in-house counsel

Stay abreast of cyber security rules and regulations.
Work closely with your CIO.
Know what information the company has and where it goes.
Dispose of documents no longer needed.
Insist on attending C-suite meetings.
Conduct regular employee training on cyber security.

Report breaches immediately (and involve your PR team).
Have outside cyber experts, including counsel, available on quick notice.
Assure proper insurance coverage is in place.
Encourage employees to report cyber breaches, even those they may have caused, without fear of punshiment.

Gary McKillips
Contributing Writer
Atlanta Business Chronicle