315 W. 11TH AVE., DENVER, CO 80204 | 720–328–1418 | www.LAWWEEKCOLORADO.com VOL. 16 | NO. 22 | $6 | MAY 28, 2018

LAW WEEK COLORADO

Businesses Now Better at Protecting 'Crown Jewels'

Law firm study shows improvement in security for knowledge assets

BY **TONY FLESOR**
LAW WEEK COLORADO

The world of cybersecurity is changing. While many businesses have been fixated on protecting their consumers' information from breaches, their own data had gone unprotected. Now, though, a new report published by Kilpatrick Townsend & Stockton and the Ponemon Institute suggests that many companies are thinking more about protecting the "crown jewels."

"WE'RE LOOKING UNDER THE LAMP POST FOR THE KEYS WE LOST IN THE DARK ALLEY BECAUSE THE LIGHT IS BETTER."

— Jonathan Neiditz, cybersecurity expert

The study focuses specifically on knowledge assets — those pieces of information that are most important to a business, excluding consumer data. The study is the second produced by Kilpatrick and Ponemon Institute, and the newest report shows that not only are cyberattacks changing, but businesses' awareness and the way they think about those breaches are changing as well. Threats are increasing, but so is business awareness of the threats.

Jonathan Neiditz, a partner at Kilpatrick in Atlanta and co-leader of the firm's cybersecurity privacy and data governance practice, said the dramatic changes in this year's results came to him as a shock. "I didn't expect there would be so much change," Neiditz said.

The study was created to focus on those pieces of valuable information for businesses, such as trade secrets or intellectual property. Through his work doing data classification policies for clients in order to help them follow regulations to protect consumer data, he found that many companies weren't doing much to safeguard their own data. "Companies were protecting cardholder information and SSNs and things like that but when I would ask them what their most important digital assets were, they wouldn't be able to identify that," Neiditz said. "And then I'd ask how are they protecting that; they'd say not so much."

The first year of the study — which was completed in late 2016 — found that the issue was not even on most companies' radar. When the study was initially conceived, it was "the rise of the targeted data breach," Neiditz said. The market for personal identifying information was saturated, and even though breaches of Ashley Madison, Experian and the IRS made headlines, companies were more frequently being targeted for DDOS and ransomware attacks.

By focusing a study on security of valuable information, Neiditz said he and Ponemon sought to help organizations focus their security tools on defending against those attacks. Within a year's time, the awareness has changed dramatically.

According to the study, companies are more frequently making the protection of knowledge assets an integral part of their IT security strategy, requiring assurances that knowledge assets are managed and safeguarded appropriately and addressing the risk of human error in creating leaks.

That last component is a major part of security. Neiditz said that among high performers and companies within the general population, the careless employee is the most common cause of a breach.

"The malicious outsider is the performer, but the careless insider is the way they get it," Neiditz said. "What [this data] tells me is we're still at the beginning of this."

The human error comes through again in the chink in most companies' armor. "We asked respondents where their most valuable information was located, and they said private communication." It is also the most difficult to secure and the worst secured. "The way I put it is we're looking under the lamp post for the keys we lost in the dark alley because the light is better," Neiditz said. "We're not necessarily looking in the right places. This tells us where to look, what to secure and what the priorities should be."

In order to correct these security weak spots, Neiditz suggested companies address the human component by providing more effective training programs, limiting access to information to a need-to-know basis and changing incident response plans to include lawyers when company information is involved that might have a significant impact on the organization, such as a major ransomware or DDOS attack.

According to the study, best practices among the highest-performing companies include requiring assurances to senior management or a board that knowledge assets are safeguarded adequately, conducting third-party audits to ensure their practices and policies that safeguard knowledge assets are being followed and conducting regular training and awareness programs and audits and assessments of areas most vulnerable to employee negligence.

High-performing companies are the ones that are more likely to know when a breach happens and that have reached a high level of "digital transformation," using technologies to share information freely internally while also using technologies to keep that information secure as well.

Neiditz also recommends that companies consider what their organization is within the digital world — something many companies don't think about, he said. For instance, a company involved in containers might realize it's actually in the location-tracking business.

Once the company recognizes those core assets, those are crown jewels or knowledge assets," Neiditz said. "You want to protect that with cybersecurity. That has competitive value. If it were taken away from you, it would cripple you." •

— Tony Flesor, TFlesor@circuitmedia.com