# Report says workers are biggest data-security threat

9 October 2019, by Neal St. Anthony

Credit: CC0 Public Domain

Headlines about cybersecurity breaches and data theft from government agencies and companies such as Caribou Coffee, Target and Medtronic in recent years can inspire fear of bad guys exploiting the internet from dark places on the web.

However, most of the online swiping comes from insiders.

"Organizations are overlooking the most harmful data-security threat: their own employees," said Code42 CEO Joe Payne.

The Minneapolis-based data-security firm commissioned the 2019 Global Data Exposure Report of 1,028 information security leaders and 615 business decision-makers by Sapio Research of the United Kingdom.

"Fifty years ago, if you were going to leave General Motors, you couldn't take the plant with you," Payne said last week. "And the critical information about the production line was locked in a cabinet."

Now, the ideas and other proprietary information is all digital. Companies have done a good job of sharing the information across the workforce, using tools such as Google Drive, Drop Box, Slack and e-mail to improve collaboration.

"The problem is that now our most important information, whether it's sales prospects or customer lists or source code ... is spread across the organization and is highly portable on a thumb drive or e-mail," Payne said. "Information is less 'siloed.' But there are unintended consequences. Our study basically shows that 63% of people admit that they took data from their last job and brought it to their current job. Our work indicates it's closer to 100 percent."

To be sure, Code42 has a vested interest in this one.

The company sells data-loss protection products that are designed to detect insider threats, satisfy regulatory compliance and help investigators respond quickly to loss incidents.

It also has a good point. In the increasingly digital workplace, people and data are fluid. Job tenure is declining. There's more work from remote locations, and employers empower employees and spur productivity with easy-to-use data-sharing platforms.

"Although many companies have traditional prevention tools in place, data loss, leak and theft, particularly among insiders, continues to happen at an alarming pace," the Sapio Research study said. "Information security teams need to find new ways to secure data. Without urgent action, insider threats will become increasingly disruptive."

There's an ongoing federal court case that highlights the issue.

U.S. Bancorp last year sued Michael Cole, the

former president of U.S. Bancorp's Ascent Private Capital Management, which serves clients worth at least $75 million. U.S. Bancorp alleges Cole swiped proprietary data about strategy, services and clients on the way out the door to take a top job and ownership position with Cresset Capital Management, a fledgling competitor.

"This is potentially a big deal for both USB and Cresset," Ben Anderson, an independent securities lawyer, said last year. "It reflects the intense competition among large asset managers to hire consistently profitable investment teams, who in turn can attract institutional investors."

It also reflects the growing use of forensic technology to track access by employees to computers where high-value data is retained.

U.S. Bancorp alleges that in addition to using its confidential documents as the basis for the strategic plan he prepared for Cresset, Cole continued to misappropriate related data until the time he departed U.S. Bancorp in June 2018. This is a high-stakes case being watched in the industry.

Most cases of alleged employee theft don't make it to federal court. Regardless, the Sapio Research study found:

- 69% of organizations say they were breached due to an insider threat, despite preventive measures.
- Nearly two-thirds of survey respondents admit to bringing data from past employers to their news jobs.
- Most employees feel entitled to personal ownership of their work.

About 25% of the people in the U.S. changed jobs last year, Payne said.

"When they leave one job, they often go to work for a competitor or start something in their own industry," he said. "Insiders have more access to information than ever. And they have a lot less loyalty. And that's half the breaches."

Code42 and others make products that react quickly to all kinds of events and anomalous behavior, such as files being called up in the wee hours of the morning, particularly by folks headed out the door soon.

"We're seeing companies empower their employees without the proper security programs in place," said Jadee Hanson, the chief information security officer at Code42.

The study found 38% of info security offices admit that their company suffered a breach of intellectual property in the last 18 months. Warning employees, alerting them to "phishing" expeditions and prevention measures aren't enough.

By and large, security teams' data-security investments haven't kept up with competing factors.

Failing to act will result in "catastrophic data loss" and higher legal bills, Sapio Research predicted.