MiBiz®

FEBRUARY 14, 2022
VOL. 34 • NO. 9

SERVING WESTERN MICHIGAN BUSINESS SINCE 1988

INSIDE THREAT:

Experts warn of growing data exfiltration from company employees

By JAYSON BUSSA | MiBiz
jbussa@mibiz.com

As business owners face a complex set of external cybersecurity threats, industry professionals caution them to remain diligent about their inner workings, as companies face an equally dire threat from inside their organizations and workforce.

Cases involving current or former employees that have either intentionally or accidentally leaked data continue to represent a big chunk of data breaches.

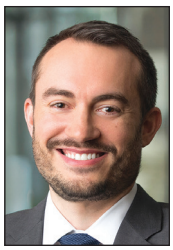
"I think the threat is greater inside the company just based on the access that certain people have," said Nathanael Dick, an I.T. manager at Grand Rapids-based technology firm **DornerWorks Ltd.**

What's known as the exfiltration of data from sources inside a company is a growing problem, according to Traverse City-based **Ponemon Institute**, a research organization that focuses on information management.

In its most recent "Cost of Insider Threats Global Report," researchers reported that insider threat incidents have risen 44 percent over the last two years. The cost to organizations of theft by people who are credentialed to access sensitive information increased from $2.79 million in 2020 to $4.6 million at the present time.


Dick


Reiffer


Rolecki

San Jose, Calif.-based computer security software firm McAfee Corp. also probed the topic extensively with a 2015 report called "Grand Theft Data," and featured a follow-up study in 2019 called "Grand Theft Data II."

The initial study showed that internal actors were responsible for 43 percent of all corporate data loss. Half of those instances were intentional while the other half were accidental.

For Dick and his role at DornerWorks, the constant threat from inside of his own office is a problem he diligently monitors.

Continued on next page

"We haven't had an event here, but I've seen cases where people have stolen some pretty major company secrets, and that's a big deal," he said. "There are a lot of easy ways to take that data and copy it down, whether it's plugging in an external hard drive or just downloading it."

Keeping tabs on information, and where employees go with it, has also grown into a more complex problem with the spike in remote work during the COVID-19 pandemic.

"With the rise of remote work, it's been a big deal with people not understanding that we have to use the tools and systems that work provides," Dick said. "We have to keep it on our content management systems or version control systems so we can make sure that our company can still see that data."

Intentional vs. accidental

The nature of data breaches triggered by sources inside a company vary greatly. Many of these occurrences happen by accident through what Dick labels "cyber sloppiness." This is when employees disregard proper protocols when handling data.

"For example, if you let your users use a personal laptop, you're opening the door for them to have proprietary documents right on their computers," Dick said. "Or, maybe they'll transfer files using things like Google Drive or DropBox."

There can be a more nefarious, intentional side of these events, though. This might include employees who purposely access and download information to pass it on to another party or entity. Or, a former employee might lock, steal or export data as a means of exacting revenge against a company.

In other cases, employees who have spent significant time with a company developing proprietary digital tools might feel entitled to bring that information to another company, which should be remedied via appropriate contractual measures such as non-disclosure agreements and either a non-compete or non-solicitation agreement for outgoing employees.

"We haven't had an event here, but I've seen cases where people have stolen some pretty major company secrets, and that's a big deal."

—NATHANAEL DICK
I.T. Manager, DornerWorks Ltd.

"There has been a definite trend upwards (in illegal data exfiltration) throughout the course of 2021 and 2022. The year is still young and we have already seen a lot of both intentional and not intentional," said **Varnum LLP** Partner John Rolecki, who specializes in data privacy and litigation.

Many instances of illegal data exfiltration go unnoticed, which makes routine checks of a company-wide network vital. These can be regularly scheduled check-ins, but it's also important when any individual with close ties to sensitive information leaves a company.

"It's always a good idea — when you have someone at a certain level of involvement with the network leave — to make sure there is no irregularity," Rolecki said. "That kind of routine scan can ultimately lead to uncovering illegal exfiltration when you might not have known until it was too late or it becomes more complex."

And when company officials are able to identify forms of exfiltration, and the person behind it, Rolecki said they should provide a written notice to that person to inform them that what they are doing can come with civil and potentially criminal ramifications.

"Demand clarity, demand more information and demand the return (of the data)," Rolecki said.

Access denied

Richard Reiffer, vice president of strategic initiatives for Grand Rapids-based **Fusion IT LLC**, offered a variety of solutions and strategies designed to mitigate the risk of illegal data exfiltration.

Reiffer said that when a company relies on just one or two people to manage their network, it can more easily be held hostage.

"They have to quit relying on one person," he said. "We see that in so many small to medium companies, where they have a single I.T. person and if something happens to that I.T. person — even if they get hit by a bus — all of a sudden all that information went with that individual.

Reiffer also subscribes to the Zero Trust approach to cybersecurity, in which access to information is granted as it's needed.

"It is a practice where, by default, you don't trust anybody," he said. "It sounds terrible, but you slowly give access as access is needed. You don't just deny it blindly, but they have to say, 'This is why I need access.' The person that's gaining access to the manufacturing database on the floor doesn't need access to the QuickBooks database."

Keeping tabs on who has access to what information is vital, and Reiffer said companies can use applications to automatically analyze this dynamic.

"A lot of companies really fall short when it comes to that," Reiffer said. MiBiz