FINANCIAL TIMES
THURSDAY 12 AUGUST 2021
FT.COM

Cyber Security

Workers increasingly steal company data during ‘turnover tsunami’

Rise in insider threats comes as disgruntled employees quit in record numbers as lockdowns ease

HANNAH MURPHY – SAN FRANCISCO

Employees are taking sensitive computer code from their own companies at three times the rate they were a year ago, according to new research into so-called insider threats, as record numbers of disgruntled workers quit their jobs with pandemic restrictions easing.

An analysis of data of 700,000 company devices by the cyber security group Code42 found that there were about 65m attempts made by staff to exfiltrate source code from their corporate network in the three months to the end of June, up from about 20m in each of the previous three quarters.

The jump is part of a broader rise in employees exposing company data, either by unwittingly moving it outside of workplace networks or by deliberately taking it, according to Joe Payne, Code42’s chief executive.

“We’re just seeing a huge increase in employees taking source code from their companies,” Payne said. “It’s highly correlated to turnover . . . We’ve seen more job changes this quarter than we’ve seen in a couple of years now.”

The percentage of workers quitting their jobs in the US rose to an all-time high in April, as those who had been staving off leaving their role during the pandemic departed as soon as restrictions loosened, a phenomenon known as the “turnover tsunami”.

Source code is the set of instructions created by software developers writing a computer program, and often constitutes highly sensitive or proprietary data. In cases where such data is knowingly taken, this may be motivated by financial opportunity, a grudge against an employer, blackmail from an outsider — or simply a sense of pride.

590m
the total number of exposure events in the three months to the end of June, up from 365m in the previous quarter

“When we talk to employees, they say ‘It’s my code.’ [But] you’re not allowed to take the source code that your company pays you to create,” Payne said, adding: “Taking source code can have massive consequences for businesses — it can be the end of your business.”

The total number of exposure events — instances where any kind of data was taken outside company networks either accidentally or maliciously — reached almost 590m in the second quarter, up from 365m in the previous three months. Source code exfiltration as a proportion of the overall number of those events rose to 11 per cent from 6 per cent.

Removable media — such as USB sticks —were the most widely used method for taking company data, followed closely by uploads to Gmail and Dropbox, the report found.

As the shift to remote working has made it more difficult for employers to keep tabs on their employees and opened up companies to new vulnerabilities, many have employed cyber security groups that wield machine learning and analytics to flag suspicious activity.

However, some argue that such systems, known colloquially as bossware, constitute Big Brother-style surveillance and an intrusion of privacy.