No Holidays for Hackers: Higher Revenue Losses for Non-weekday Cyber Events

MSV INSURANCE AGENCY

Ransomware events that occur on holidays and weekends cause much higher revenue losses than cyber incidents occurring on weekdays—primarily due to lower staffing levels—according to a survey of over 1,200 cybersecurity professionals.

Security firm Cybereason found that nearly half (44%) of organizations drop security staffing levels on holidays by as much as 70% andnder a quarter of respondents reduce their security staff by 90% from normal weekday levels. Just 7% of organizations have at least 80% of their security professionals available on holidays and weekends.

The impact is clear: one-third of respondents said they saw a much greater financial toll from weekend and holiday attacks, up from 13% in 2021's study. The losses were even higher in the transportation and education sectors, where the number of respondents reporting higher revenue losses jumped to 48% and 43%, respectively.

"Ransomware actors tend to strike on holidays and weekends because they know companies' human defenses often aren't as robust at those times," said Lior Div, Cybereason CEO and co-founder. "It allows them to evade detection, do more damage and steal more data as security teams scramble to mobilize a response."

The study also revealed slower risk assessment times during breaks, with 60% of respondents saying it took them longer to fully understand the scope of the attack. This, in turn, slows down recovery time and adds costs.

Cybercriminals already know holidays and weekends are prime attack times, especially as the strain of relentless cyber events takes its toll on security professionals. In fact, multiple high-profile cyberattacks have occurred on holidays. In 2021, hackers made headlines on Mother's Day weekend (Colonial Pipeline), Memorial Day weekend (meat supplier JBS Foods) and the Fourth of July (software vendor Kaseya). This year might be even worse, according to a few respondents.

"This November/December is going to be particularly rough, as it's going to be the first time some people have been able to see their families since the pandemic began. All of that means that people will be further from the office and less likely to check alerts," said one security analyst in the legal sector.

The survey indicated a few areas where organizations can improve their resilience to off-hours cyber events. More than a third (36%) of organizations said they had no business continuity plan, despite observing other companies' struggles to bounce back. Of those firms that have already experienced a ransomware event, nearly a quarter (24%) still don't have a ransomware-specific contingency plan.

Some industries are better prepared than others. Specifically, the IT/telecommunications sector and construction firms were most likely to be prepared, with 84% and 81% of respondents indicating they have plans in place for weekend and holiday events. Manufacturing (67%) and health care (65%) were less prepared, despite these sectors' potential for high revenue losses or loss of life.