

Ransomware for the holidays

Dread the holidays? If you work in cybersecurity emergency response, you have good reason to.

Ransomware criminals began seizing on holiday weekends this year to strike big. They crippled Colonial Pipeline for Mother's Day, meat processor JBS Foods for Memorial Day, software supplier Kaseya for the 4th of July and Howard University for Labor Day. Folks in retail and transportation are especially nervous as Thanksgiving and Christmas loom.

For insight into how ransomware has wrecked weekends and holidays, the cybersecurity firm Cybereason surveyed more than 1,200 security professionals in the U.S. and eight other countries who suffered such attacks



over the past year. More than a third said they had lacked a specific contingency plan to mount a response — and nearly a quarter still don't have one, even given that they've been victimized. One in four said their outfit had to shut down to recover, although Cyberreason said it didn't have data on the length of the forced shutdowns.

How to prevent a recurrence? That varies, but 41% were adding more weekend/holiday staff. One advantage to being on the clock: security personnel were more apt to be sober. In the study, 70% of respondents admitted to having been intoxicated while responding to a weekend/holiday ransomware attack.

Holiday and weekend ransomware attacks

May 2021	Mother's Day Weekend	Colonial Pipeline
May 2021	Memorial Day Weekend	JBS Foods
July 2021	Fourth of July Weekend	Kaseya Limited
Sept 2021	Labor Day Weekend	Howard University
October 9, 2021	Saturday	Ferrara Candy Company
October 18, 2021	Saturday	Sinclair Broadcasting
October 23, 2021	Saturday	Schreiber Foods in Wisconsin

