

ORGANIZATIONS AT RISK 2022 Ransomware Attackers Don't Take Holidays



Contents

EXECUTIVE SUMMARY	3
FINANCIAL, OPERATIONAL AND PERSONAL IMPACT OF WEEKEND/HOLIDAY RANSOMWARE ATTACKS	4
WEEKEND/HOLIDAY STAFFING LEVELS	6
ENDPOINT PROTECTION TECHNOLOGIES	7
TYPES OF INCIDENTS SECURITY TEAMS ARE MOST OFTEN TRYING TO RESOLVE	8
STEPS ORGANIZATIONS ARE TAKING TO ADDRESS RANSOMWARE	9
TIME IT TAKES TO RESOLVE RANSOMWARE ATTACKS	10
RECOMMENDATIONS	11
METHODOLOGY	12



Executive Summary

Ransomware actors strike when companies are most vulnerable: on Holidays and Weekends

cybereason°

In 2021, Cybereason launched its inaugural global study of the impact of ransomware attacks that occur on holidays and weekends. The findings were alarming. Our research revealed that most companies were unprepared for a ransomware attack during "non-business" hours, largely because they didn't have contingency plans in place to address them and because they cut staffing levels during these times. Consequently, these attacks took longer to investigate and resolve, and cost companies more money.

This year, we conducted a similar study to see if anything had changed. We found that many organizations remain unprepared to handle a ransomware attack on a holiday or weekend, as they continue to operate with a skeleton crew at these times. It's no wonder SOC teams operate so lean on holidays and weekends: security professionals are experiencing record-levels of burnout compounded by a protracted global talent shortage and relentless adversaries.

But there's no reason organizations can't have contingency and incident response plans in place to quickly mobilize their SOC teams, IR teams, and partners when a holiday or weekend attack occurs.

On the pages that follow, we share the findings from this year's global study, compare them to last year, and provide recommendations to help companies optimize staffing and combat the ransomware threat, no matter when actors decide to strike.

Describe the impact of a holiday/ weekend attack compared to an attack occurring on a weekday?

34% It took us longer to

assemble our team

Cybereason[®]

37%

It took us longer to stop the attack

36%

It took us longer to recover from the attack

The business lost more money

It took us longer to assess attack scope

3/%

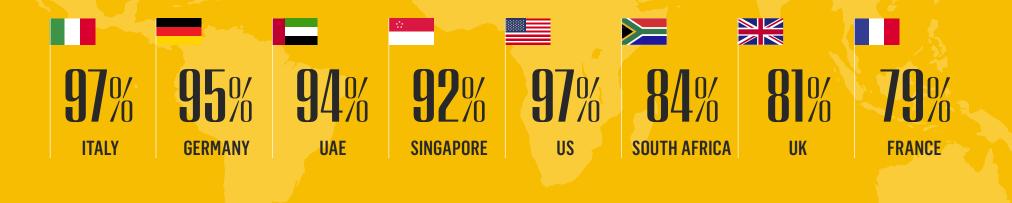
By Industry ►	Education	Finance	Healthcare	IT & Telecom	Manufacturing & Utilities	Retail, Catering & Leisure	Travel & Transport
It took us longer to assess the scope of the attack	54%	39%	30%	35%	38%	41%	33%
It took us longer to respond/ stop the attack	42%	40%	31%	31%	37%	40%	43%
The business lost more money	42%	24%	34%	24%	32%	31%	38%

Respondents were asked to select all applicable answers



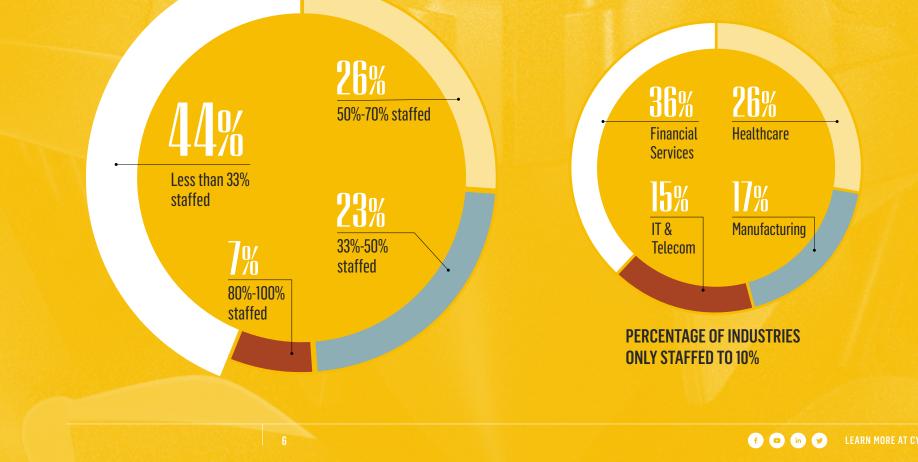
Have you ever missed celebrating a holiday or participating in a weekend event because of a ransomware attack?

B B O/ **B O**/ **V E**S



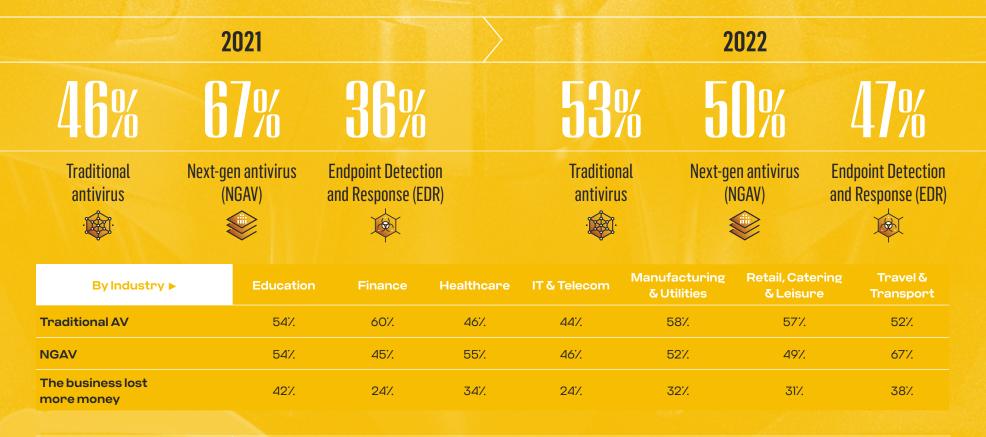


How is your organization staffed on holidays and weekends?



What endpoint protection technologies does your company have in place?

O cybereason°



🕐 💿 🐽 🌚 🛛 LEARN MORE AT CYBEREASON.COM

What type of security incident is your SOC team most frequently trying to resolve?

Cybereason[®]

BIOS TARGETED ATTACK ATTACK ATTACK ADDISONAL

By Country ►	US	UK	Germany	France	UAE	Singapore	Italy	South Africa
Ransomware	66%	45%	40%	41%	50%	45%	37%	44%
Supply chain attack	47%	54%	30%	33%	48%	38%	51%	45%
Targeted attack	34%	29%	25%	31%	27%	29%	33%	35%



What steps is your organization taking to address the heightened ransomware threat?

We are planning to implement new detection capabilities specifically for ransomware, that have better detection efficacy .____



so we can respond faster

We're pursuing automation to accelerate attack detection and response



We're learning to negotiate with ransomware actors

A

38%

We're setting up crypto wallets in the event we decide to pay

Cybereason[®]

On average, how long does it take your organization to resolve a ransomware attack?



By Industry ►	All	Education	Finance	Healthcare	IT & Telecom	Manufacturing & Utilities	Retail, Catering & Leisure	Travel & Transport
1-2 hours	3%	8%	4%	37.7.	3%	2%	3%	5%
3-4 hours	26%	8%	44%	18%	32%	23%	28%	5%
5-6 hours	18%	17%	19%	14%	36%	16%	17%.	10%
7-23 hours	14%	8%	9%	15%	12%	19%	14%	38%
1-2 days	16%	25%	13%	19%	8%	16%	19%	14%
3-6 days	13%	28%	8%	21%	5%	14%	12%	14%
lweek	6%	8%	3%	8%	2%	7%.	47.	10%
2-3 weeks	2%	0%	٦X.	2%	1%	4%	2%	5%



Recommendations



cybereason°

EXPLORE DIFFERENT STAFFING MODELS FOR SOC ANALYSTS AND INCIDENT RESPONDERS

Look to hospital emergency rooms and other emergency response organizations for models.



IDENTIFY OPTIMAL Staffing for Weekends and Holidays

What's the least amount of coverage you can get away with and still reduce risk?



PURSUE A MANAGED DETECTION AND RESPONSE (MDR) STRATEGY

Augment your existing staff with expert, third-party 24x7x365 coverage.



LOCK DOWN PRIVILEGED ACCOUNTS DURING OFF-PEAK Hours

Highest privilege accounts are rarely used on weekends and holidays.



IMPLEMENT CLEAR ISOLATION PRACTICES

This will prevent attackers from making any further ingress on the network and from spreading the ransomware to other devices.



REPLACE TRADITIONAL ANTIVIRUS PRODUCTS WITH NGAV AND EDR

Look specifically for behavior-based tools capable of identifying ransomware attacks in their earliest stages, based on suspicious behaviors the tools are seeing across the organization's network.





METHODOLOGY

Censuswide conducted a global survey of 1,203 cybersecurity professionals working in companies with more than 700 employees in the U.S., U.K., Germany, France, Italy, UAE, South Africa, and Singapore. The survey was conducted online between September and October 2022. Survey respondents worked at organizations that had experienced one or more ransomware attacks during a holiday or weekend in the last 12 months.

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason Al-Driven XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOptm instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.