cybereason

ORGANIZATIONS AT RISK

Ransomware Attackers Don't Take Holidays

INTRODUCTION
CEO Insight

The holidays are a crucial time for businesses, but there are a number of factors that may make this year more challenging. With the world still dealing with the COVID-19 pandemic, store shelves are empty, manufacturing is delayed, supply chains are stalled, and staffing shortages are leading to cancelled flights.

Organizations have another challenge to deal with as well. Ransomware is a serious and growing threat around the world. One source projects that the global cost of cybercrime will hit $6 trillion—with a "T"—in 2021. That is double what it was just 5 years ago, and much of that financial impact is the result of ransomware.

So, how well do organizations understand the risk from ransomware attacks, especially those that occur during the weekends and holidays, and how prepared are they to address this risk?

HOLIDAY RANSOMWARE CRISIS

Ransomware is a threat everyday, but a concerning trend is that major attacks tend to occur on weekends and holidays when fewer staff are around to detect and respond to them because a majority of the security team is trying to relax with family and friends. The Colonial Pipeline attack occurred over Mother's Day weekend. JBS was attacked over Memorial Day weekend. The Kaseya attacks happened over the Fourth of July weekend. The list goes on.

In fact, there have been over 200 ransomware attacks that have made headlines in 2021 so far—and those are just the ransomware attacks that have been acknowledged publicly. Tech giants Acer and Apple were each hit with $50 million ransom demands, and the Colonial and JBS attacks impacted critical infrastructure supply chains in the United States and disrupted the economy. While all verticals are at risk, the upcoming holiday season makes the Retail and Transportation industries high-value targets given the potential for revenue loss and supply chain disruptions--factors ransomware attackers are likely to consider when selecting targets most likely to pay a huge extortion demand.

Combine that with the fact that the average ransom payment is up more than 500% over 2020 to $5.3 million, and that 83% of organizations end up paying the ransom, and it is easy to see that this is an ongoing crisis. It is even more concerning when you consider the fact that 80% of organizations that have paid a ransom have been hit with a second attack.

"This research highlights the fact that it takes longer to assess, mitigate, remediate and recover from an attack that hits on the weekend or holidays - an adversary advantage that attackers are quite aware of.

Cybereason partners with defenders to reverse the adversary advantage. This report offers insights into the risk and guidance on mitigation so defenders are better prepared to prevent a ransomware attack this coming holiday season."

LIOR DIV
CEO, CYBEREASON

HOUSE OF CARDS

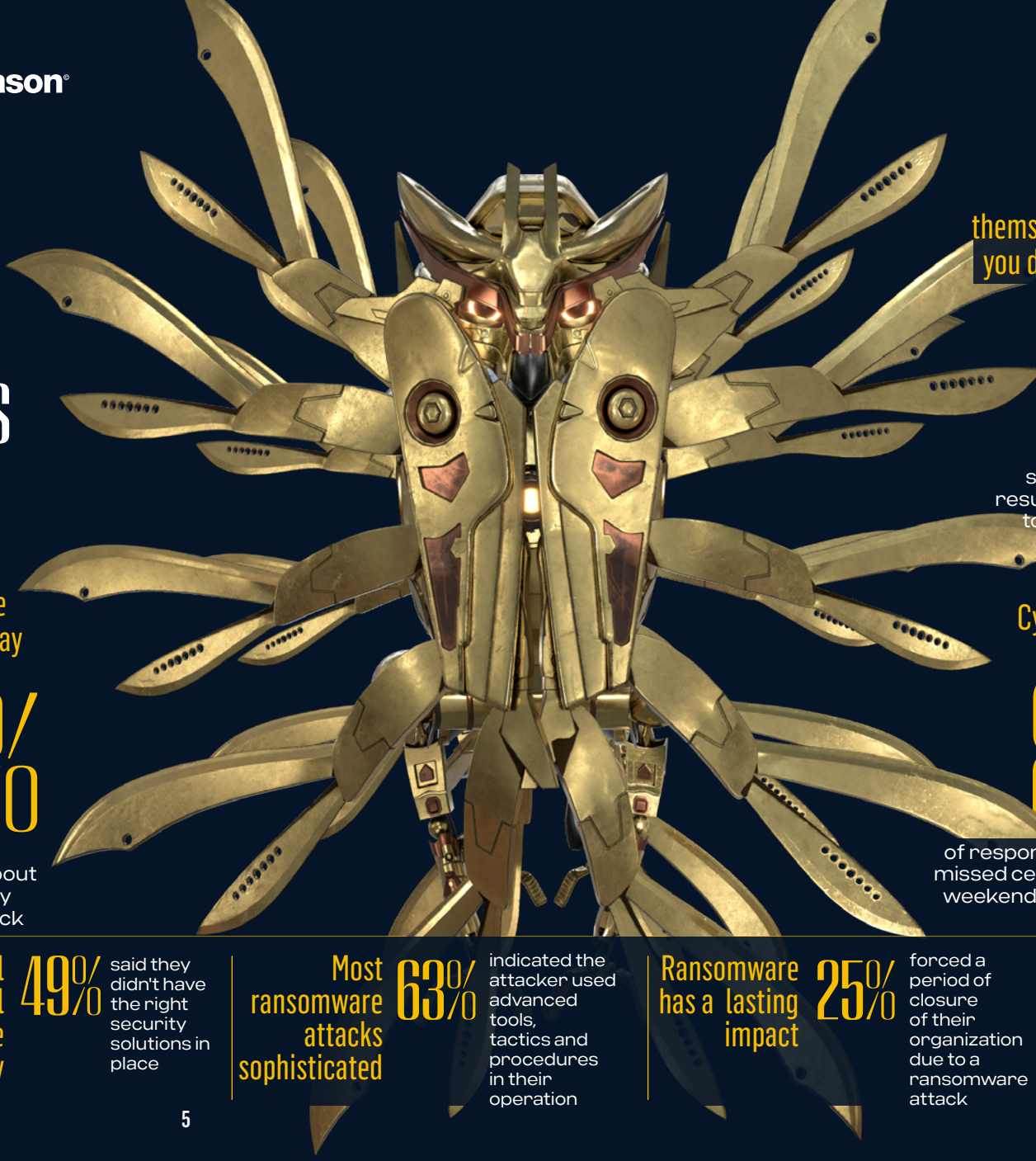
Stress and burnout are very real challenges for cybersecurity professionals. Security teams are understaffed and overwhelmed as they attempt to protect an increasingly complex attack surface against a constantly expanding threat landscape using outdated tools that can't detect or stop modern threats.

Combine that with a fragile economy, struggling supply chain logistics, and the likelihood of a significant ransomware attack during the upcoming holidays and we have a "house of cards" scenario that could collapse if anything bumps the proverbial table.

If a significant ransomware attack occurs over the upcoming holidays, it may have devastating consequences for organizations caught off guard. Cybereason conducted this research to provide insight into the **disconnect between the perceived risk from weekend and holiday ransomware attacks and the actual risk to organizations.**

cybereason

Key Global Results



Attackers embed themselves deeper when you don't rapidly detect

60% said weekend/holiday resulted in longer period to assess the scope of the attack

Attackers do the most damage while you are away

89% indicated they are concerned about a weekend/holiday ransomware attack

Cybereason let's you leave work at work

86% of respondents indicated they missed celebrating a holiday or weekend activity because of a ransomware attack

Many feel unprepared to deal with ransomware effectively

49% said they didn't have the right security solutions in place

Most ransomware attacks sophisticated

63% indicated the attacker used advanced tools, tactics and procedures in their operation

Ransomware has a lasting impact

25% forced a period of closure of their organization due to a ransomware attack

66% suffered significant revenue loss due to a ransomware attack

As we approach the end of the year,

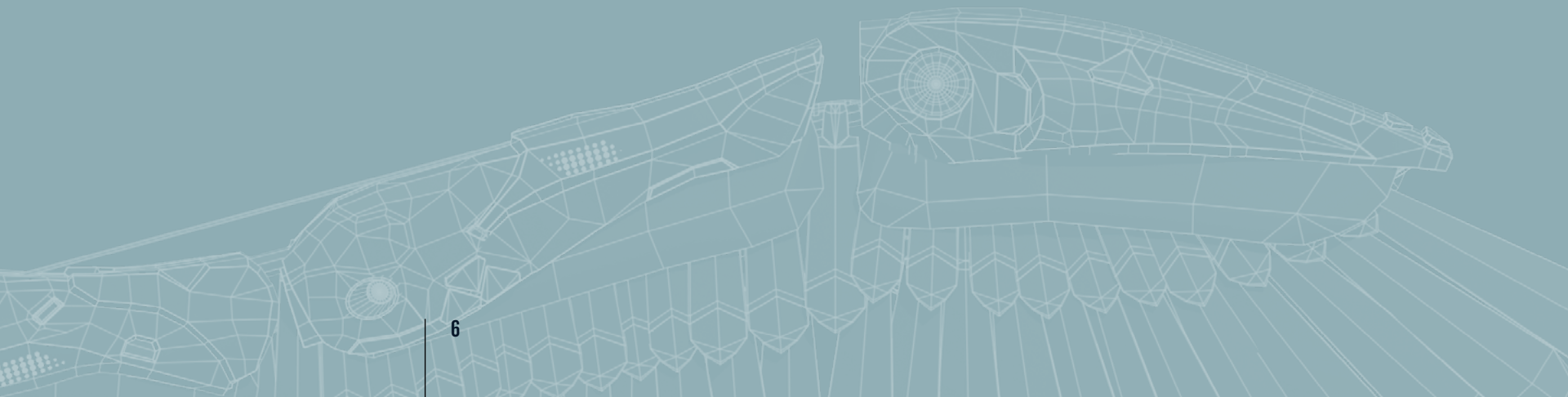
businesses and consumers alike shift into holiday mode. The holiday season infuses billions of dollars into the economy as people shop for gifts, attend or host holiday events, and travel to spend time with family and friends—reflecting on the year gone by and preparing for a fresh start in the new year.

Unfortunately, cybercriminals will also shift into holiday mode. Cybereason conducted a global research study to better understand the real risk of ransomware attacks during the holiday season and on weekends.

Understanding this research will help guide defenders to take action and organizations to get the processes and tools in place to effectively detect and stop these attacks.

> 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.

ANDREW
SECURITY ANALYST
LEGAL INDUSTRY



Complex RansomOps

Successful RansomOps, a term that best describes the more complex ransomware operations so prevalent today, employ low-and-slow, APT-like tactics designed to infect as much of the target network as possible in order to generate ever larger ransom demands--some of which now exceed the $50 Million dollar mark.

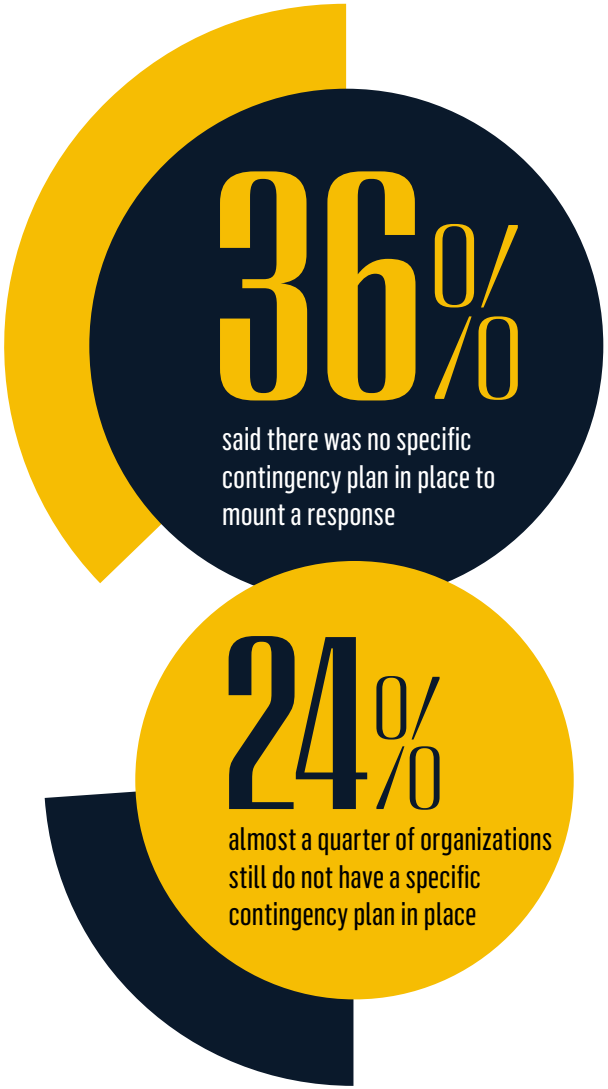
What's most important to understand about RansomOps is that prior to that actual ransomware payload delivery, the attackers have engaged in weeks or even months of detectable activity on the target network.

This is where strategies to detect and disrupt them early in the kill chain can turn what would have been a potentially devastating ransomware security event into a less disruptive intrusion and/or data exfiltration attempt.

PERCEPTION VS. REALITY:

Are Organizations Prepared?

In June of 2021, Cybereason published a global research report, titled Ransomware: The True Cost to Business, which revealed that the vast majority of organizations that have suffered a ransomware attack experienced significant impact to the business as a result.



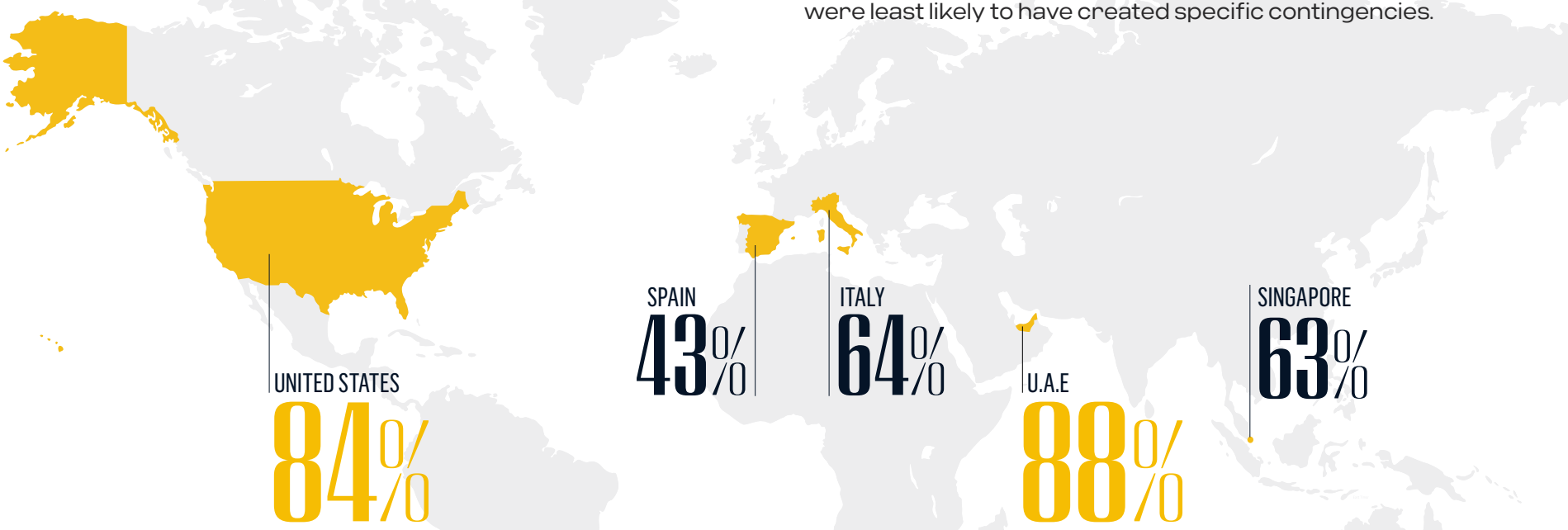
This latest ransomware holiday study looked more specifically at the business impact from ransomware attacks that were orchestrated to hit organizations when they may be at greatest risk with regard to mounting a successful defense: weekends and holidays. All of the study participants worked at organizations who have previously been the victim of a ransomware attack.

Despite having already been a victim -as well as the spate of highly publicized and extremely disruptive ransomware attacks that occurred over weekends and holidays during 2021 like the attacks that crippled the likes of Colonial Pipeline, JBS meat packers, managed services provider Kaseya and more- **more than a third (36%) said there was no specific contingency plan in place to mount a response** to the ransomware attack their organizations suffered.

The study also revealed that **almost a quarter (24%) of organizations still do not have a specific contingency plan in place** despite having been the victim of a successful ransomware attack.

The study revealed that the Construction (81%) and IT/ Telecoms (84%) industries were most likely to have prepared for ransomware attacks on the weekends and holidays, while Healthcare (65%) and Manufacturing (67%) -arguably two of the biggest target verticals for ransomware attacks because of the potential for significant revenue losses or the loss of life- were among the industries least likely to have developed specific contingencies.

Similarly, organizations with 2000 or more employees -where company size is often a targeting factor used by attackers to facilitate larger ransom demands- were also significantly below average, with just over two-thirds (69%) indicating they have specific plans or policies in place. Organizations in the U.S. (84%) and UAE (88%) were most likely to have specific incident response plans and policies in place, while those in Spain (43%), Singapore (63%) and Italy (64%) were least likely to have created specific contingencies.



Percentages show organizations per country likely to have specific incident response plans and policies in place

20%

One in five (20%) believed their organization would never be a target of a ransomware attack

63%

Two-thirds believed the attackers were a sophisticated nation-state threat actor (Advanced Persistent Threat)

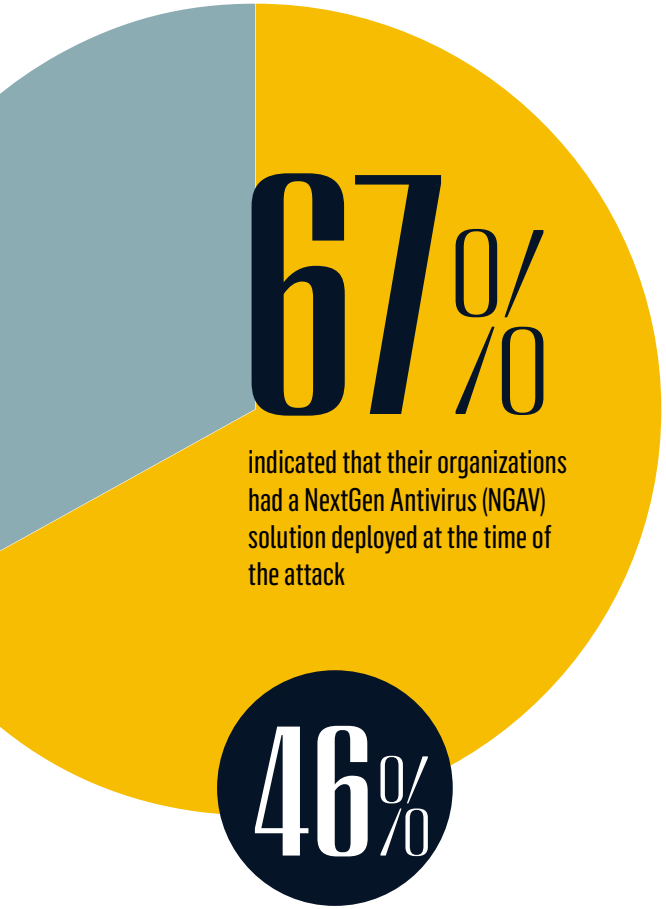
49%

Said the attack was successful because they didn't have the right security solutions in place

All of these indicators point to a **significant disconnect between the perceived threat and actual risk to the organization.** This disconnect is demonstrated in the results that **one in five (20%) believed their organization would never be a target of a ransomware attack.** The reasons for this false sense of security may include small company size or inclusion in a particular vertical that they felt offered them some immunity. Whatever the reason, the findings here clearly show that some organizations do not have a clear understanding of the potential risk posed by ransomware attacks.

Another perceptual disconnect revealed in the study is that **63% of respondents said they believed the attackers were a sophisticated nation-state threat actor (Advanced Persistent Threat)** despite the fact that the overwhelming majority of documented ransomware attacks are conducted by cybercriminal organizations and not nation-state actors, with the exception being cash-strapped North Korea in limited instances. The Transportation sector (64%) was in line with the overall average while the Retail sector (46%) showed well below average.

Additionally, even though **89% of all respondents said they are concerned about the prospect of ransomware attacks** during weekend and holiday periods, **nearly half (49%) said the attack their organization already experienced was successful because they didn't have the right security solutions in place**—another key indicator of the disconnect between the perceived risk and organizational preparedness to address it. For the Retail (69%) and Transportation sectors (68%) the response was significantly higher--something of particular concern as we approach the holiday season.

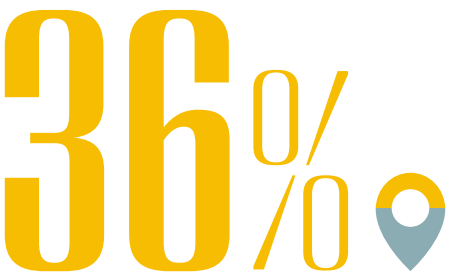


Furthermore, **only 67% indicated that their organizations had a NextGen Antivirus (NGAV) solution deployed at the time of the attack,** a class of solutions that includes Artificial Intelligence/Machine Learning capabilities that have proved to be highly effective against both known and never before seen malware variants, exploitation of zero-day vulnerabilities, and more advanced operations that leverage tactics like fileless attacks or malicious macros, among others. The Retail sector (57%) was slightly below that average, while the Transportation sector (84%) was significantly higher.

NGAV solutions have been highly effective against these approaches, especially in networks that need to remain air gapped or otherwise isolated, because these solution rarely need to be updated to be effective. But they also have some deficits in prevention capabilities when not part of a multi-layered solution beyond the machine learning detection models alone.

The study also revealed that ***46% of respondents said their organizations had traditional signature-based antivirus (AV) in place*** when they were hit by a ransomware attack. The traditional AV approach has been around for several decades and continues to be reasonably effective against already known commodity malware strains. Unfortunately, its effectiveness is dependent on a long process that requires human analysis and continuous delivery of new signatures for detections, so traditional AV is not effective against novel, polymorphic or repacked malware strains. It also offers no protection against fileless attacks, malicious macros or other advanced techniques.

EDR solutions are designed to address the attacks that prevention tools cannot stop, **as well as augment proactive threat hunting and post-event forensic investigations.**



said their organization had an Endpoint Detection and Response (EDR) solution in place

Furthermore, **only 36% of respondents said their organization had an Endpoint Detection and Response (EDR) solution in place** when they were attacked. The Retail sector (46%) was higher than average, while the Transportation sector (28%) was considerably lower. This is concerning given the growing body of research and continued media coverage of recent high-profile ransomware attacks that clearly demonstrate attackers are employing more complex "low and slow" attack sequences designed to remain undetected by traditional and NextGen antivirus solutions. These more sophisticated RansomOps can often only be surfaced through behavioral detections and/or proactive threat hunting that leverage an EDR solution.

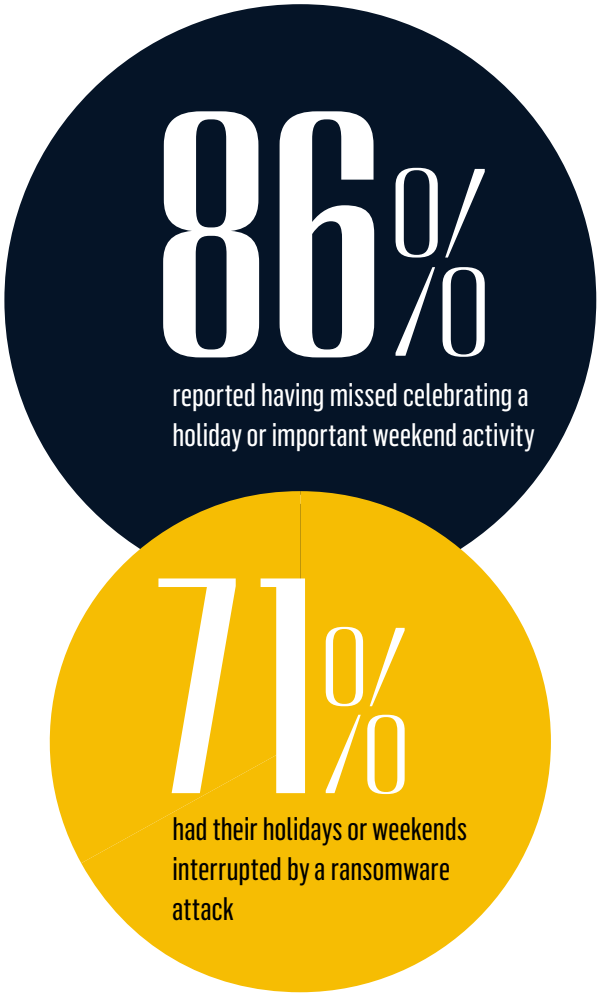
The advent of EDR tools came in response to the shortcomings of both traditional and NextGen AV and the corresponding paradigm shift where defenders acknowledged that if an attacker is skilled enough and has sufficient time and resources, they will eventually be successful in penetrating any target. EDR solutions are designed to address the attacks that prevention tools cannot stop, as well as augment threat hunting and post-event forensic investigations.

EDR solutions have proven so effective that a recent Presidential Executive Order requires federal agencies to "deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents," as well as for "active cyber hunting, containment and remediation, and incident response."

UNMITIGATED RISK:

The Human Element

While we have covered processes and technologies, the third and arguably most important aspect of every security framework involves people. Although this includes employees across every business unit, our focus here is solely on the defenders. By now it is no secret that the security field is suffering from an extreme talent shortage, and this shortage is one of the major factors leading to stress and burnout for security professionals. The 2020 (ISC)2 Cybersecurity Workforce Study estimated there were some 3.1 million security staff positions that needed to be filled, with 879,000 open spots in the U.S. alone.



In this Cybereason study, **responding to a ransomware attack resulted in 86% of respondents missing holidays or weekend activities with family and friends.** Of these respondents, defenders in the Financial Sector were the biggest outlier, with a lower than average 71% indicating they had their holidays or weekends interrupted by a ransomware attack. This may result from the fact that organizations in the Financial Sector generally have the most mature security programs due to regulatory requirements, and they have more resources available to mount better defenses.

One of the more surprising findings in the study was that **70% admitted to having been intoxicated while responding to a ransomware attack on the weekend or during a holiday,** a risk factor for organizations that may not have been accounted for by incident response and business continuity plans. The Retail sector (73%) was slightly higher than average, while the Transportation sector (80%) was significantly higher.The

Construction (91%) and Legal (81%) sectors also had the highest instances of staff reporting intoxication, while Media (60%), the Financial Sector (63%) and Manufacturing (67%) reported the lowest. Staff with the least seniority were least likely to be intoxicated while engaging in a response to a ransomware attack, while senior staff were most likely to have been intoxicated.

Regionally, Spain and Singapore were the biggest outliers with 47% and 54% of respondents confessing to being intoxicated during a ransomware incident response, respectively. Furthermore, organizations in the highest revenue brackets were most likely to have staff who admit to being intoxicated during a ransomware incident response.

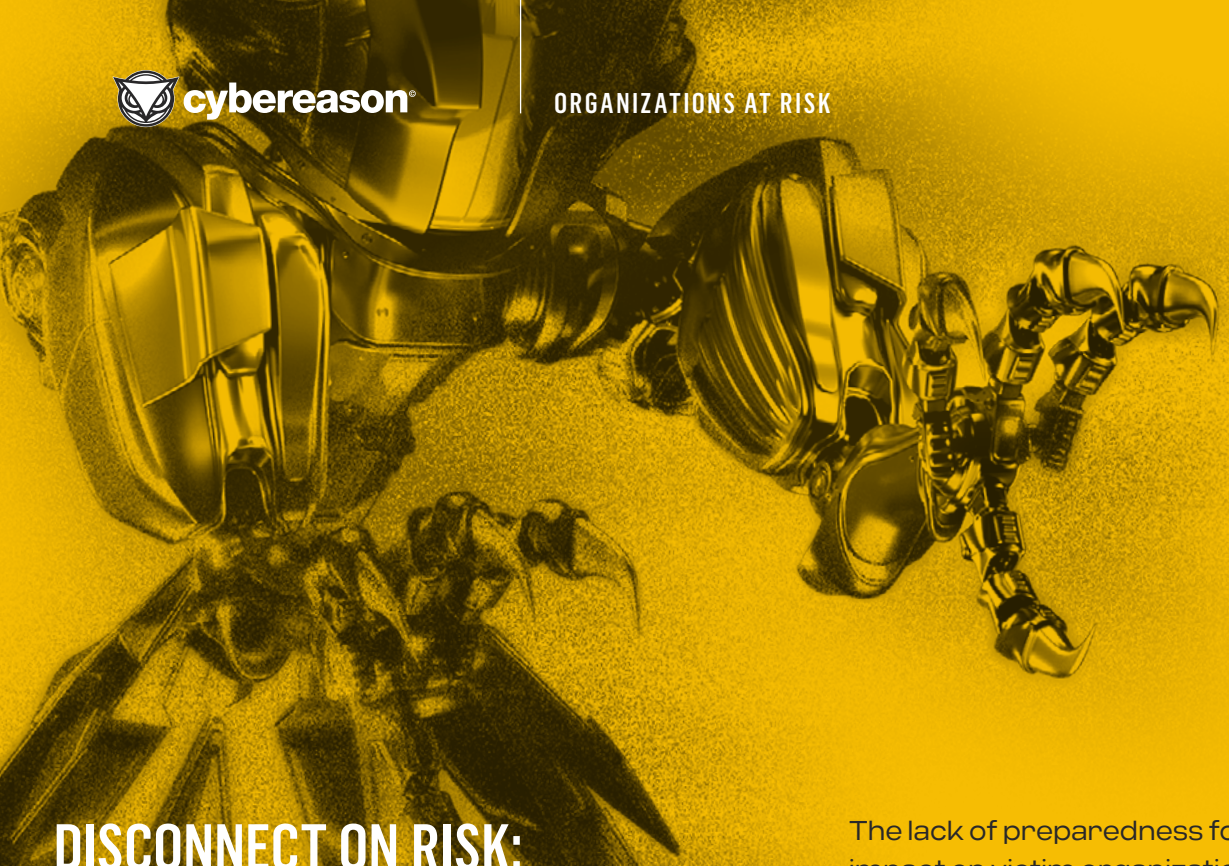
SECTORS WITH THE HIGHEST INSTANCES OF STAFF REPORTING INTOXICATION

70% admitted to having been intoxicated while responding to a ransomware attack on the weekend or during a holiday

LEGAL
81%

MANUFACTURING
67%

FINANCIAL SECTOR
63%



DISCONNECT ON RISK:

Impact to the Business

The lack of preparedness for ransomware attacks has a significant impact on victim organizations, with **60% of respondents saying weekend and holiday attacks result in longer periods to assess the scope of the situation.** Furthermore, **50% said it required more time to mount an effective response,** and **33% said it resulted in a significantly longer period of time to fully recover** from the attack.

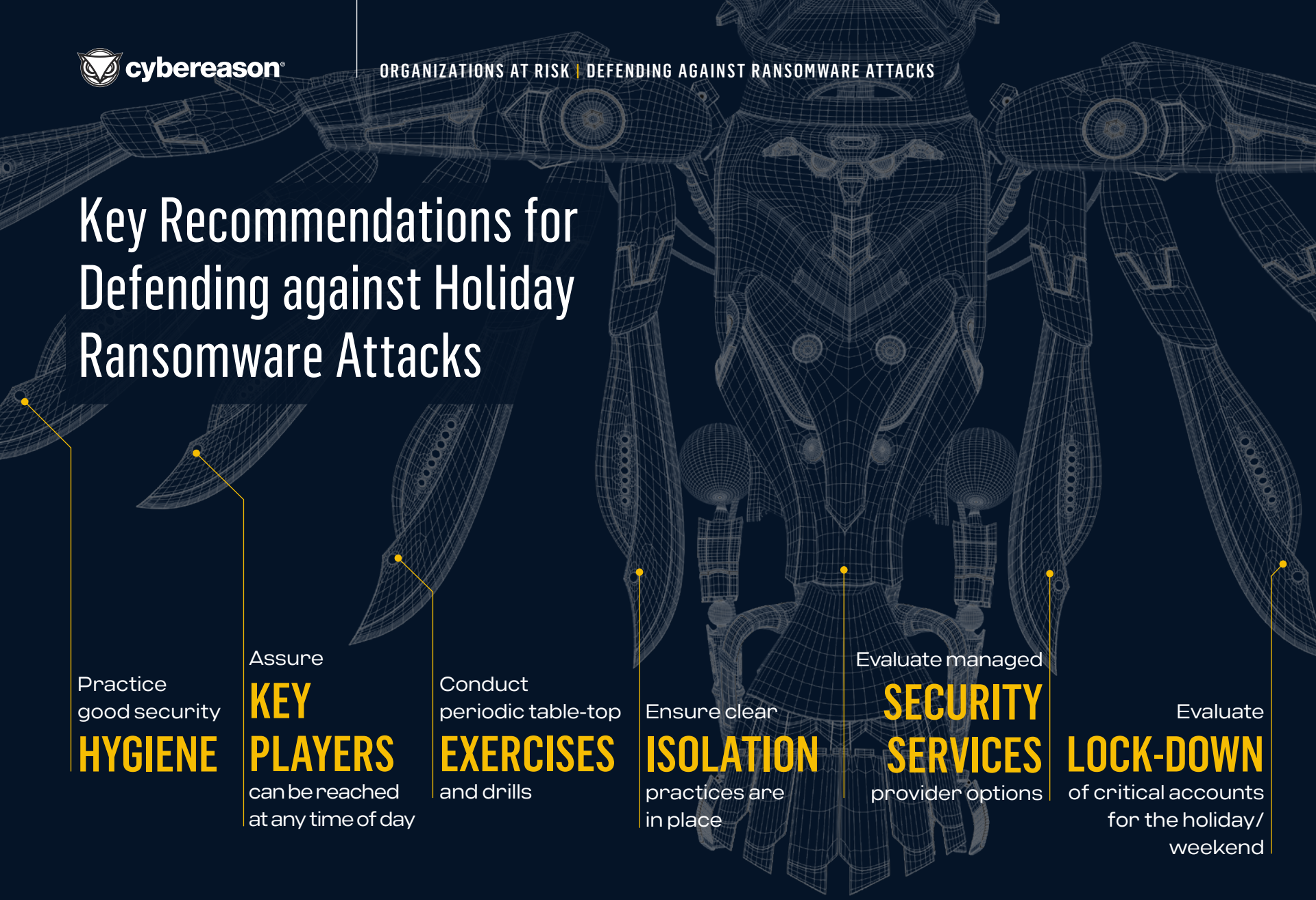
One key factor in the inability to mount a timely response was revealed by **35% of respondents saying that a ransomware attack during a weekend or holiday made it harder to assemble the right team to mount a response.** These delays in responding to an attack on the weekends or holidays correspond to **12% of study participants who said their organizations lost more revenue as a result,** with IT/Telecom, Legal and the Transportation sectors most significantly impacted.

The **business impact** from a ransomware attack can include loss of revenue, damage to the organization's brand, unplanned workforce reductions, and disruption of business operations

Defending Against Ransomware Attacks

For attackers, it does not take much in the way of deductive skills to understand that most organizations are likely to be more vulnerable to attack on the weekend and during the holidays, so it's a solid assumption that threat actors will continue to attack high-value targets during these periods. So how are organizations planning to address the threat?

Key Recommendations for Defending against Holiday Ransomware Attacks



Practice good security **HYGIENE**

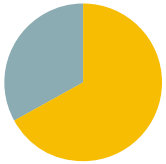
Assure **KEY PLAYERS** can be reached at any time of day

Conduct periodic table-top **EXERCISES** and drills

Ensure clear **ISOLATION** practices are in place

Evaluate managed **SECURITY SERVICES** provider options

Evaluate **LOCK-DOWN** of critical accounts for the holiday/ weekend



68%

indicated their organizations are planning to or are in the process of adding new technologies to address the risk

To better prepare for ransomware attacks, the **majority of respondents (68%) indicated their organizations are adding new technologies** to address the risk. **Just over half (51%) said they are or will be implementing a specific contingency plan or policy,** with Retail (45%) coming in a bit below average and Transportation (60%) well above. **Nearly half (41%) said they are adding more staff during these periods**--but there is more that can be done to reduce the risk from weekend and holiday ransomware attacks:

Practice good security hygiene like implementing a security awareness program for employees, assuring operating systems and other software are regularly updated and patched, and deploying the best-in-class security solutions on the network.

Assure key players can be reached at any time of day as critical response actions can be delayed during weekend/holiday periods. It may be the case that the right people are not getting their emails due to system issues from the attack, or are not answering their phones because there is no set expectation they need to monitor communications in case of an event. Having clear on-call duty assignments for off-hours security incidents is crucial here.

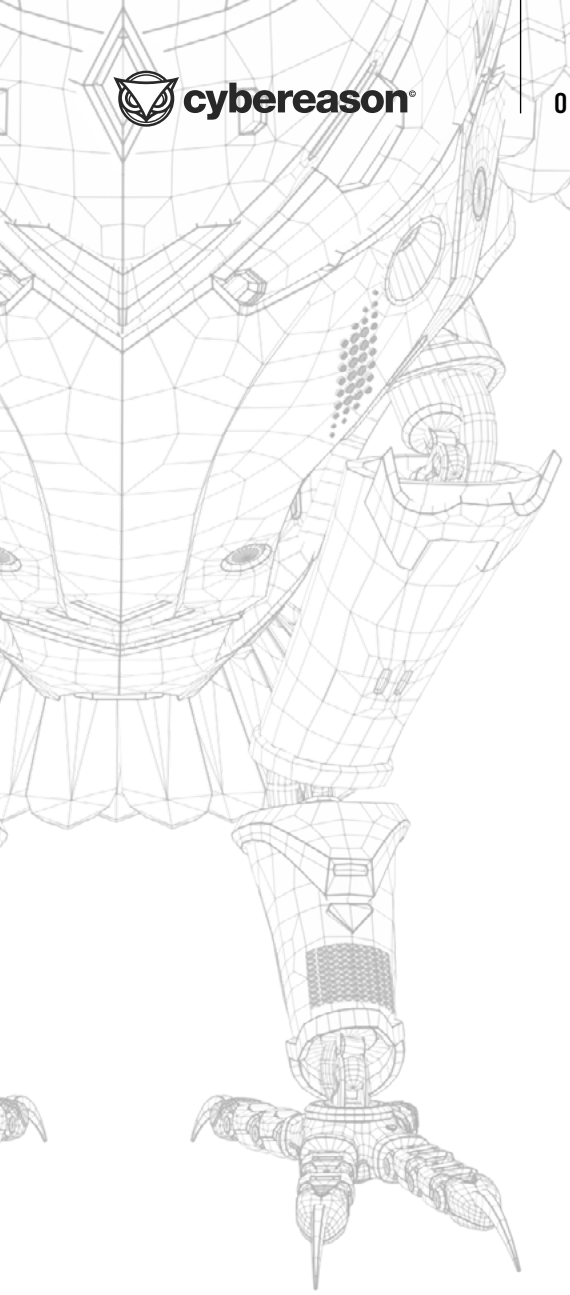
Conduct periodic table-top exercises and drills that include staff beyond the security team like Legal, Human Resources, IT Support and all the way up to the Executive Suite to ensure a smooth incident response.

Teams
should be proficient at
disconnecting a host,
locking down
a compromised account,
blocking
a malicious domain.

Ensure clear isolation practices are in place to stop any further ingress on the network or spreading of the ransomware to other devices. Teams should be proficient at things like disconnecting a host, locking down a compromised account, and blocking a malicious domain, etc. Testing these procedures with scheduled or unscheduled drills at least every quarter is recommended to make sure all personnel and procedures work as expected.

Evaluate Managed Security Services Provider options if your organization has staffing or expertise shortage issues and establish pre-agreed response procedures with them so they can take immediate action following an agreed upon plan.

Evaluate lock-down of critical accounts for the weekend/holiday when possible. The usual path attackers take in propagating ransomware across a network is to escalate privileges to the admin domain-level and then deploy the ransomware. Those highest privilege accounts in many cases are rarely required to be in use during the weekend or holiday breaks. Teams should create highly- secured, emergency-only accounts in the active directory that are only used when other operational accounts are temporarily disabled as a precaution or inaccessible during a ransomware attack.



The strategy relies on the assumption that the chances of these accounts' credentials being compromised should be extremely low given the accounts are almost never in use so they have less exposure to potential threats. The SOC can use these accounts to disable all the other domain admin accounts for the weekend/holiday and re-enable them for regular work periods or if needed in an emergency. It may seem like a cumbersome process, but it is nothing compared to the process of decrypting or reimaging hundreds or thousands of encrypted endpoints following a successful ransomware attack. There are also options to take similar precautions with VPN access in limiting its availability during the weekend depending on business needs.

Enjoy Your Holidays In Peace

Cyber attacks and ransomware come in all shapes and sizes. Some attacks are simple, and some are sophisticated and complex. Some threat actors are average cybercriminals, and some are nation-state adversaries with considerable resources. The reality is that none of that matters. Defenders must defend against all attacks—regardless of the threat actor or level of sophistication.

You need a multi-layered platform that uses **Indicators of Behavior** (IOBs) to identify and stop the ransomware attack chain

Once your data is encrypted, there are no good options. The only effective way to fight ransomware is to prevent it from occurring in the first place. Most tools rely on Indicators of Compromise (IOCs)—which implies by its very name that it is not being detected until a compromise has occurred. You need a multi-layered platform that uses Indicators of Behavior (IOBs) to identify and stop the ransomware attack chain regardless of whether it has been seen before—and before the damage is done.

That starts with having the right tools. Cybereason is undefeated against ransomware. The ability to recognize IOBs, combined with an operation-centric approach that provides visibility across the entire malicious operations—or MalOpTM—enables Cybereason to detect ransomware attacks earlier and respond more quickly to shut them down.

You need downtime. You deserve to be at your child's birthday party, spend time with family, and enjoy holiday celebrations. Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere—including modern ransomware. We will help make sure you can enjoy your weekends and holidays in peace.

RESEARCH METHODOLOGY

This research was conducted by Censuswide in September of 2021 and spans cybersecurity professionals around the world asking key questions about their experience with and preparation for holiday or weekend ransomware attacks. The study surveyed 1,206 cybersecurity professionals working in organizations with 700 or more employees from across the United States, UK, France, Germany, Italy, Singapore, Spain, South Africa, and UAE. All study respondents have been victims of a ransomware attack during a holiday or weekend in the last 12 months, making them ideal for providing insight about the impact experienced and what they plan to do differently moving forward.

cybereason

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders, providing operation-centric attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense Platform combines the industry's top-rated AI-powered detection and response (EDR and XDR), next-gen antivirus (NGAV), Anti-Ransomware Protection and Proactive Threat Hunting to deliver context-rich analysis of every stage of a MalOp™ (malicious operation). Cybereason is a privately held, international company headquartered in Boston with customers in more than 50 countries.

Learn more at **www.cybereason.com**