cybereason | PRESIDIO

RANSOMWARE: THE TRUE COST TO BUSINESS

PreventID

A Global Study on
Ransomware Business Impact

INTRODUCTION
CEO INSIGHT

In May of 2021, Colonial Pipeline announced that it had fallen victim to a devastating ransomware attack that shut down operations and cut off fuel supplies to millions, causing massive economic disruption across the Eastern United States. The FBI confirmed the attacks were executed by the DarkSide ransomware gang, a relatively new threat actor that Cybereason has been tracking since August 2020.

It is estimated that there is a ransomware attack on a business every 11 seconds on average, with global ransomware damage losses projected to reach $20 billion this year. The FBI reported an increase of more than 225% in total losses from ransomware in the U.S. in 2020 alone.

Dealing with the aftermath of a ransomware attack is complicated and costly. Key findings in this new research reveal that the vast majority of organizations have experienced significant business impact due to ransomware attacks, including loss of revenue and damage to the organization's brand, unplanned workforce reductions, and even closure of the business altogether.

This research underscores that prevention is the best strategy for managing ransomware risk and ensuring your organization does not fall victim to a ransomware attack in the first place.

LIOR DIV
CEO, CYBEREASON

This research also reveals that the majority of organizations who chose to pay ransom demands in the past were not immune from subsequent ransomware attacks, often by the same threat actors. In addition, having cyber insurance coverage in place does not guarantee an organization will be able to recoup losses associated with a ransomware attack.

A key benefit of this report is that it provides insight into the business impact of ransomware attacks across key industry verticals and reveals data that can be leveraged to drive better ransomware defense approaches. This research underscores that prevention is the best strategy for managing ransomware risk and ensuring your organization does not fall victim to a ransomware attack in the first place.

Cybereason is dedicated to exposing emerging threats and delivering actionable intelligence to better defend organizations against disruptive ransomware attacks. Together, we can reverse the adversary advantage and return the high ground to the defenders.

KEY GLOBAL RESULTS

The Concern is Real

81% are highly or very concerned about the risk of ransomware attacks

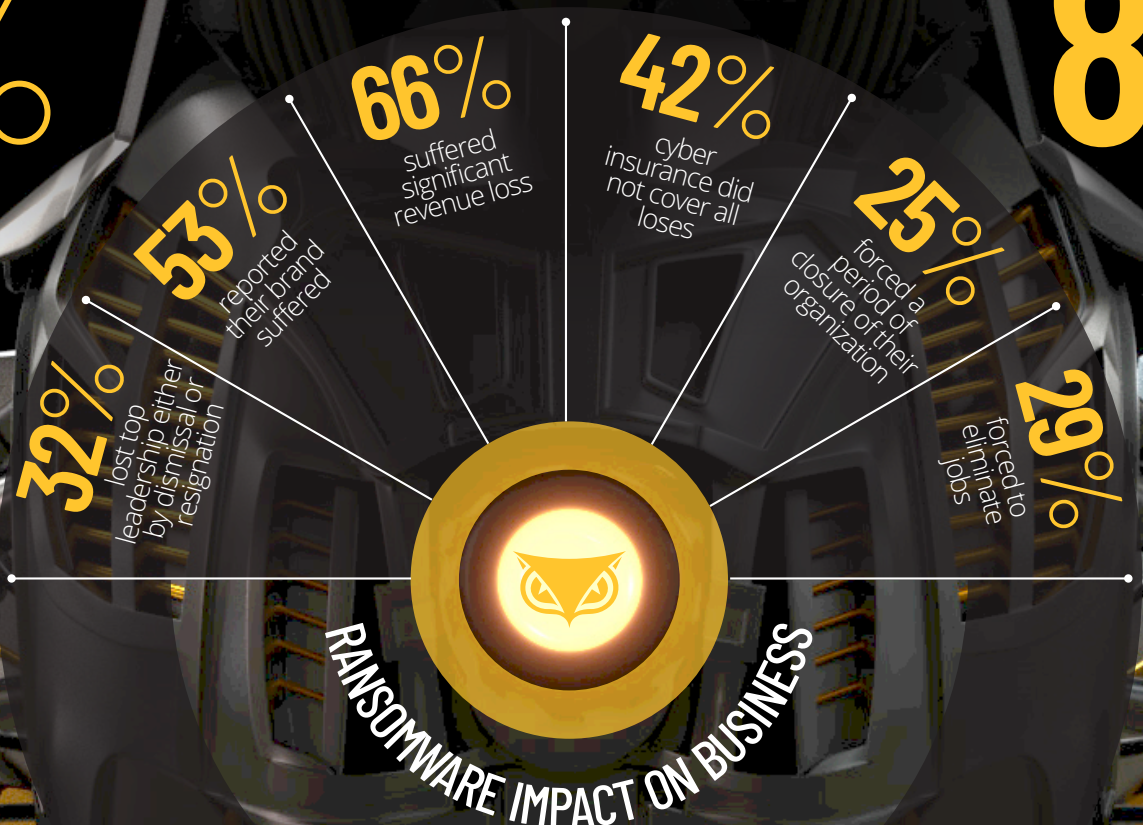
73% have a specific plan or policy in place to effectively manage a ransomware attack

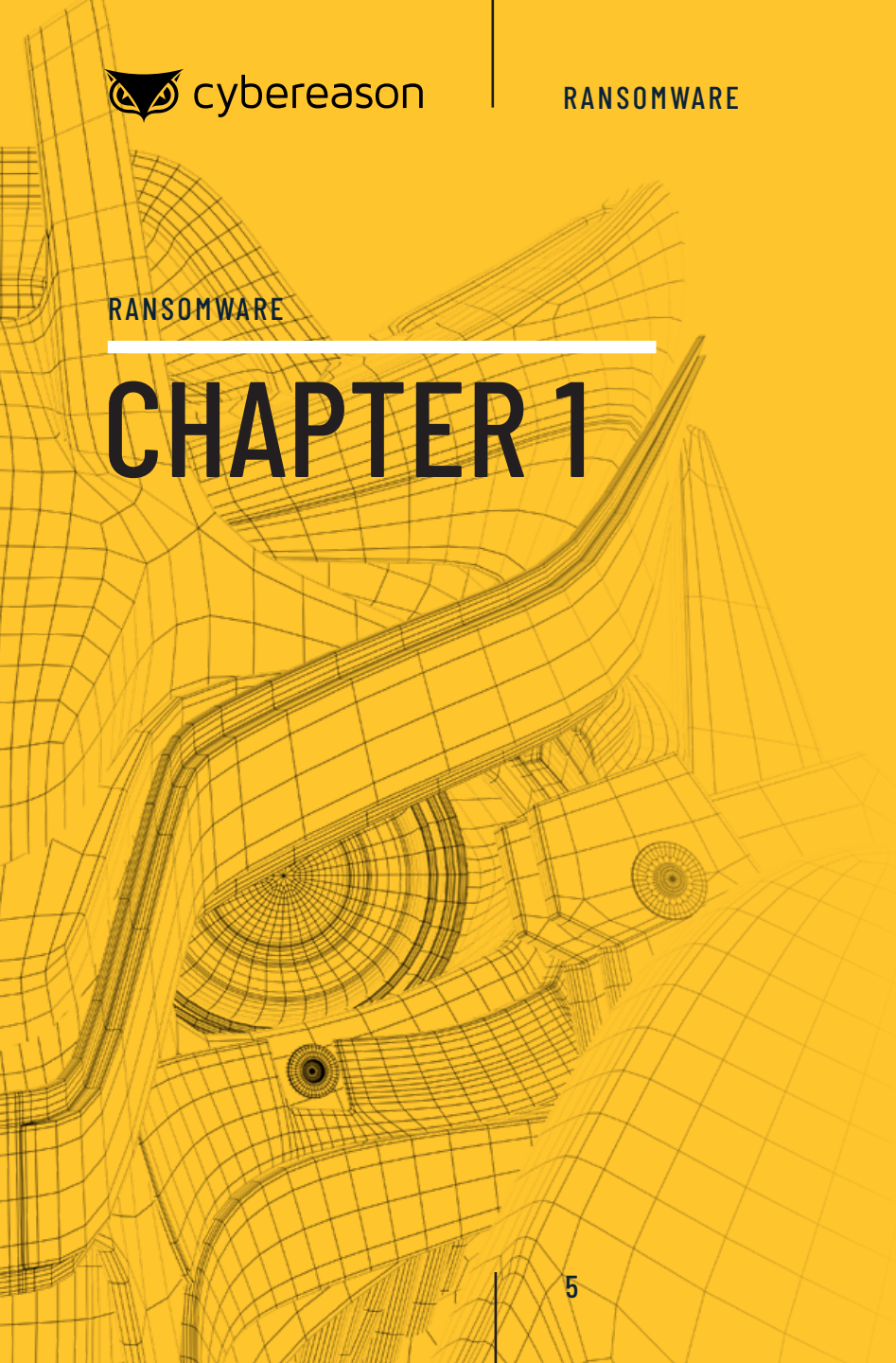
42% believe they have the right people in place to get the job done

Doesn't Pay to Pay

80% of those who paid a ransom experienced another attack

46% regained access to their data following payment, but some or all of the data was corrupted





RANSOMWARE

CHAPTER 1

IMPACT OF RANSOMWARE ON THE BUSINESS

Ransomware attacks can negatively impact an organization in a variety of ways, with combined losses potentially reaching tens or even hundreds of millions of dollars. Short term impacts can include disruption of critical business operations due to the inability to access data, costs associated with incident response and mitigation efforts, interruption of system processes, lost productivity, and the ransom payment itself if the organization chooses to acquiesce to the extortion demand, among others.

Longer term impacts can include diminished business revenue, damage to the brand reputation, loss of key executives and employee layoffs, loss of customers and strategic partners, and –in some circumstances– can even impact the viability of the business altogether.

Of the 1263 respondents in the survey

66%

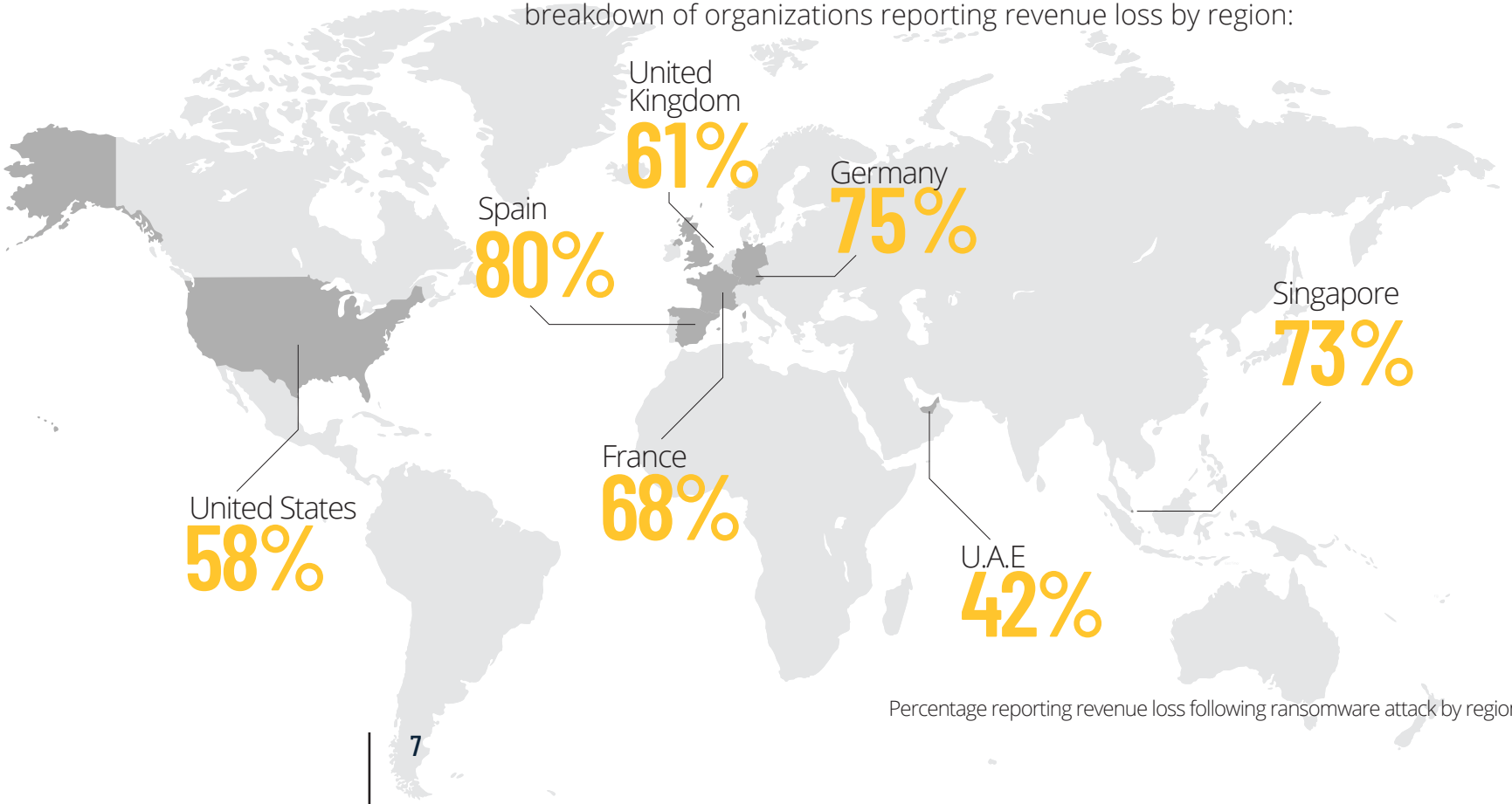
suffered significant revenue losses

LOSS OF REVENUE

FedEx reported losses of around $300 million as a result of the NotPetya ransomware attacks back in 2017, and the city of Atlanta reportedly spent more than $2.6 million to recover from a SamSam ransomware attack in 2018. The City of Baltimore reportedly spent more than $18 million to rebuild its entire IT network after refusing to pay in yet another SamSam ransomware attack, and Cognizant Technology Solutions reported diminished earnings in 2020 due in part to fallout from a Maze ransomware attack.

REVENUE LOSS BY REGION

Of the 1263 respondents in the survey, fully two-thirds (66%) reported that their organization suffered significant revenue losses as a direct result of a ransomware attack. According to the survey responses, company size appears to have very little impact on revenue loss. The following chart shows the breakdown of organizations reporting revenue loss by region:



Percentage reporting revenue loss following ransomware attack by region

ORGANIZATIONS REPORTING REVENUE LOSS BY INDUSTRY VERTICAL:

75%
Government

Financial Services
73%

Retail
74%

Healthcare
64%

Technology
64%

Automotive
58%

Manufacturing
51%

Legal
50%

These results emphasize the fact that every industry vertical is vulnerable to a statistically significant chance of revenue loss following a successful ransomware attack due to disruption of business processes, system downtime, diversion of resources and people power to recovery, brand damage and more.

Percentage reporting revenue loss following ransomware attack by industry

DAMAGE TO BRAND AND REPUTATION

No company wants to be the next TJ Maxx, Target, Equifax, or Microsoft--following the recent widespread compromise of their Exchange Server offering. However, even those infamous attacks pale compared to SolarWinds, where the brand has become synonymous with the attack itself.

Ransomware attacks can and certainly do sully brands associated with them. For example, the U.K.'s National Health Service (NHS) is still reeling from the massive WannaCry ransomware attacks in 2017, which cost the organization more than $100 million in combined losses and resulted in more than 19,000 cancelled appointments. This level of service disruption no doubt had a negative impact on how NHS customers view the reliability of their healthcare provider.

In this research, more than half (53%) reported that their organizations' brand suffered as a result of a ransomware attack. Respondents in Singapore (40%), Spain (44%) and France (49%) reported the least number of organizations suffering reputational damage following a ransomware attack. More than half of the respondents in Germany (51%), the U.A.E. (54%), the U.S. (56%), and the U.K. (63%) reported their organizations' brand was negatively impacted.

Organizations may think that they are fully prepared to address the impact from a ransomware attack if they are covered by cyber insurance, have data backups available, and are able to complete recovery efforts in short order. But the reality is that no matter how prepared an organization is to respond to a ransomware attack, their brand is at risk of significant damage regardless of all other factors.

C-LEVEL RESIGNATIONS AND DISMISSALS

The CISO is, unfortunately, one of the most consistent casualties of security events. The average tenure for a CISO has continued to drop over the years and is currently somewhere around 18-26 months. Despite there being a capital C at the beginning of the title, most CISOs do not hold traditional C-level positions in their organizations.

Does that mean the C-level is immune from fallout after a major security event? Not at all. CEOs at Target, Home Depot, Sony, and TalkTalk were either forced out, resigned, or retired early following major security breaches.

Ransomware attacks also pose a risk for C-level executives, as evidenced in 2020 when ERT CEO and President Jim Corrigan was likely pressured to step down following a ransomware attack that delayed the company's COVID-19 vaccine trials. To that end, nearly one-third of the respondents in our survey (32%) indicated that they had lost top leadership following a ransomware attack either by dismissal or resignation.

Simply put, having the right prevention, detection and response capabilities in place to assure an attempted ransomware attack is not successful can have a direct impact on the tenure of executive teams. These survey results make it clear that a major security event like a successful ransomware attack will rise to the level of a boardroom discussion given the impact to victim organizations is significant.

EMPLOYEE AND STAFF LAYOFFS

C-level positions are not the only ones at risk from ransomware, as rank and file employees can also be casualties as organizations seek to regain stability in the aftermath of an attack. In 2020, steel manufacturer Evraz announced sweeping layoffs for their production and pipefitting crews following a ransomware attack that devastated the company's North American operations.

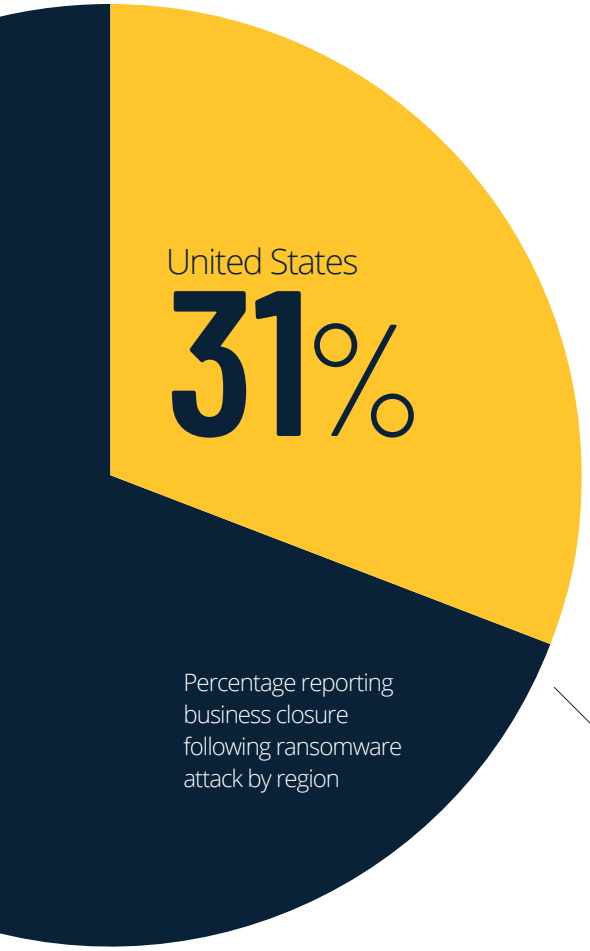
This latest research bears out this sad consequence of ransomware attacks, with nearly one-third (29%) of respondents saying their organization was forced to eliminate jobs following a ransomware attack. Respondents in Singapore (13%), Germany (19%) and the U.A.E. (29%) reported average or below that average, while the U.K (31%), Spain (31%), and the U.S. (33%) reported slightly higher than the average. France was the outlier, reporting that 39% of organizations were forced to eliminate jobs following a ransomware attack.

Based on industry vertical, respondents in the Government sector reported no job losses while the Automotive, Retail and Legal sectors had significantly more instances of job loss following a ransomware attack. The key takeaway here is that while the public sector may be insulated to a degree from having its workforce impacted by a ransomware attack, the private sector is at risk of a workforce reduction following a successful ransomware attack regardless of industry vertical:

INDUSTRY VERTICAL	PERCENTAGE REPORTING LAYOFFS
Legal	50%
Retail	48%
Automotive	42%
Manufacturing	29%
Technology	29%
Healthcare	24%
Financial Services	23%
Government	0%

Percentage reporting layoffs following ransomware attack by industry

PERCENTAGE REPORTING BUSINESS CLOSURE



FORCED TO CLOSE THE BUSINESS

Finally, we come to the ultimate impact an organization can suffer at the hands of ransomware attackers, the demise of the business itself. Telemarketing firm The Heritage Company informed 300 employees that they were ceasing operations and that the workforce should seek new employment options following a ransomware attack that shut down their production servers for an extended period - the announcement came just days before the Christmas holiday.

While the complete loss of a business due to a ransomware attack might seem like the ultimate edge case, it is actually a more immediate risk than most business leaders might assume. More than one-quarter of survey participants (25%) reported a ransomware attack had forced the closure of their organization for some period of time. The following chart shows further breakdown by region:

REGION	PERCENTAGE REPORTING BUSINESS CLOSURE
United Arab Emirates	42%
United Kingdom	34%
United States	31%
France	22%
Germany	21%
Singapore	20%
Spain	5%

When evaluating results of the survey by the number of employees, results were mixed. Notably organizations with 250-500 employees self-reported the greatest impact at nearly one third (27%), while by vertical industry the automotive and retail verticals were most impacted at 42 and 33 percent respectively. These results clearly demonstrate that no business sector is immune to potentially catastrophic outcomes following a successful ransomware attack.

WILL CYBER INSURANCE COVER THE COSTS?

According to a study produced by one of the largest providers of cyber insurance in North America, ransomware attacks spurred nearly half of all cyber insurance claims (41%) that were filed in the first six months of 2020. But does cyber insurance always cover the wide range of costs associated with a successful ransomware attack? The answer is not necessarily.

The City of New Orleans was the victim of a successful ransomware attack that reportedly resulted in losses estimated to exceed $7 million dollars. Despite the fact that their insurance policy covered losses as a result of ransomware attacks, the city was ultimately only able to recoup about $3 million dollars of the losses from their insurer.

This scenario was also borne out in our research results, where 54% of respondents indicated their organization purchased a cyber insurance policy that covers ransomware in the last 24 months, versus 21% who said their organizations took out a cyber insurance policy but it did not cover losses incurred from ransomware attacks.

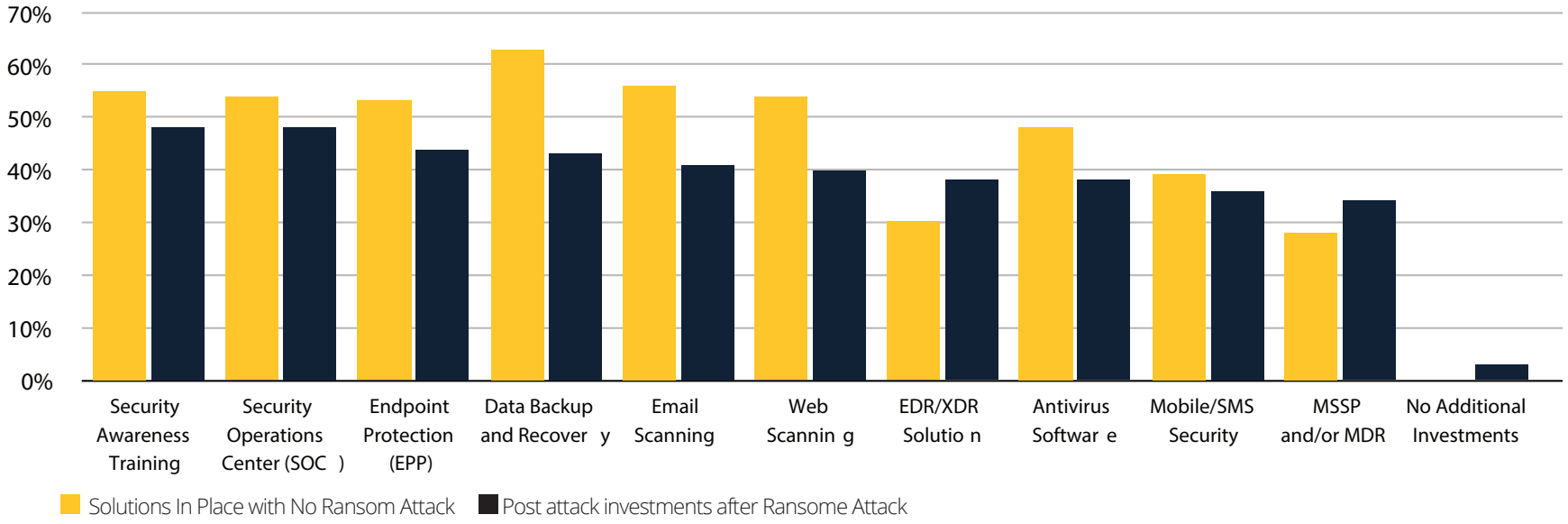
Of the organizations who had cyber insurance policies in place and were subject to a ransomware attack, a full (42%) said their insurer only covered a portion of the losses. These results suggest a major impact to those who don't have the proper insurance, and the potential for significant impact to the business even if they do. The moral of the story here is if you have cyber insurance, take the time to ensure you will be properly covered.

SECURITY INVESTMENTS POST-RANSOMWARE ATTACK

There is a long standing conundrum in security where communicating the success of the program is often an exercise in proving a negative: if there are no major security events, do we need to continue to invest in security solutions and operations at the same level? Unfortunately, it often takes a major security event to spur additional investments in the security program, tools, and staffing.

We asked the portion of our survey respondents who indicated their organization had been subject to a ransomware attack in the last 24 months to share which security solutions they invested in following the attack in order to further protect their networks from any future events.

The table below compares those investments against the solutions already in place at organizations where the survey participants indicated they had not suffered a ransomware attack in the last 24 months. This view provides a side-by-side comparison of which solutions were in place that may have protected organizations from a ransomware attack and the investments made by organizations after an attack:



TOP 5 SOLUTIONS IMPLEMENTED AFTER A RANSOMWARE ATTACK

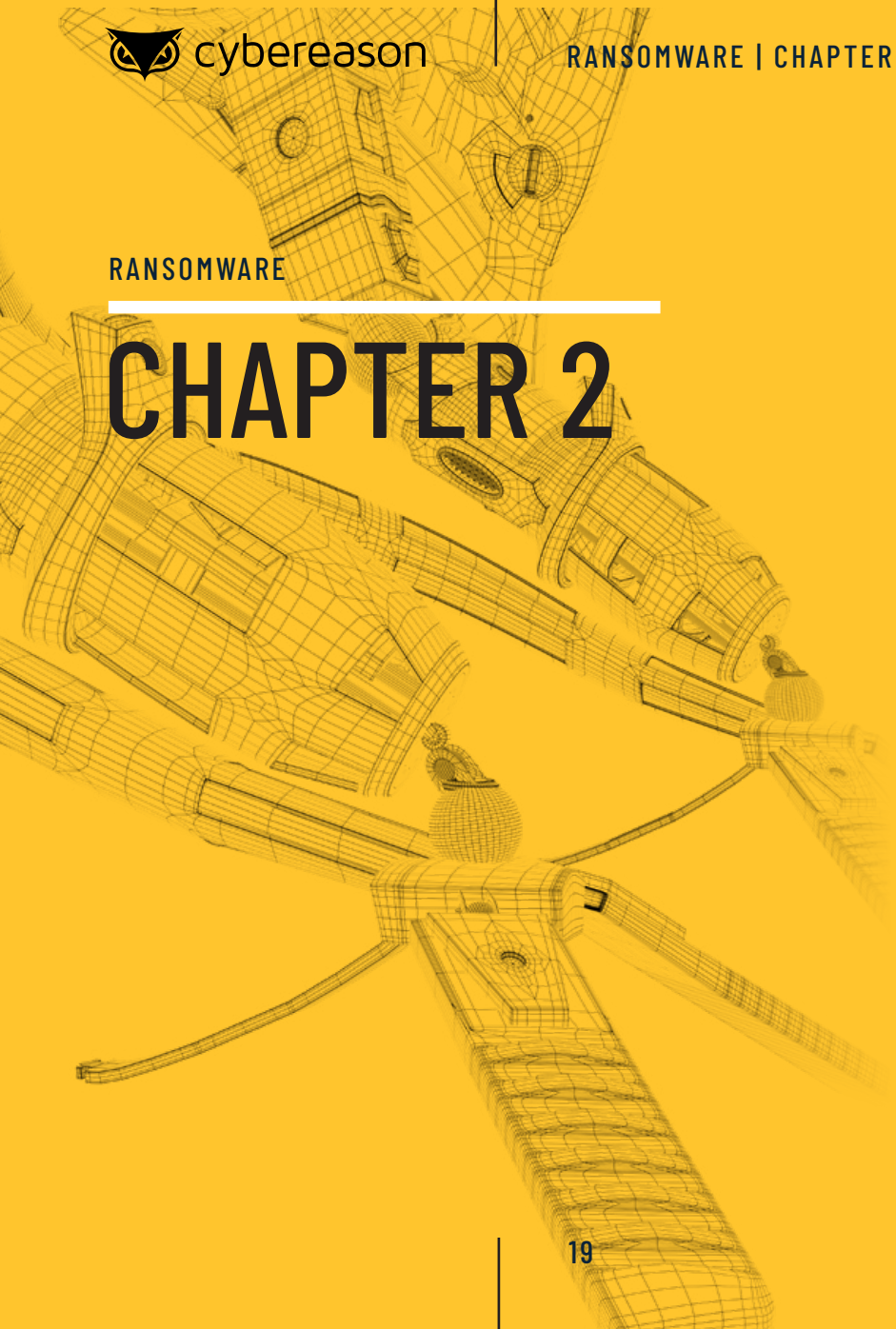
EMAIL SCANNING
41%

DATA BACKUP AND RECOVERY
43%

ENDPOINT PROTECTION
44%

SECURITY OPERATIONS CENTER (SOC)
48%

SECURITY AWARENESS TRAINING
48%



RANSOMWARE

CHAPTER 2

RANSOMWARE: WHO IS CONCERNED? EVERYONE

One of the biggest takeaways from this research is simultaneously concerning and encouraging. When we asked, "How concerned are you about the risks associated with ransomware?" more than four out of five respondents (81%) indicated that they are highly or very concerned about the risk of ransomware attacks. That result is concerning for two reasons. It shows what a pervasive threat ransomware is and illustrates the urgency of addressing the ransomware crisis. If you work in cybersecurity today and you are not at least somewhat concerned about ransomware, you're just not paying close enough attention.

Nearly
75%
of survey participants stated that they have a specific plan or policy in place to effectively manage a ransomware attack

The reality is that the vast majority acknowledge how serious the risk is from ransomware. However, our data shows there may be a bit of a disconnect or a false sense of confidence when it comes to how prepared organizations are to defend against ransomware attacks. Nearly 75% of survey participants stated that they have a specific plan or policy in place to effectively manage a ransomware attack, and just under 60% believe they have the right people in place to get the job done. If organizations have a plan and they have the right people in place, why are most still worried?

Interestingly the United States stood out as having a higher number who believe they have the right people (69%) than the number that indicated they have a plan or policy (58%). It suggests that there are some companies in the U.S. who are so confident in their IT security team, THEY BELIEVE that will be enough to protect them even without a process in place.

Meanwhile, the U.S. continues to bear the brunt of the most significant ransomware attacks, so research like this should help to close that gap and provide a clearer view of the potential implications to the organizations from ransomware. In countries like the United Kingdom, Germany, Spain, and France between 73% and 87% have a plan or policy, while the percent indicating they have the right people ranged from 45% to 66%, in contrast to the U.S. results.

A DOUBLE EXTORTION ATTACK FIRST EXFILTRATES SENSITIVE DATA AND INTELLECTUAL PROPERTY. THE ATTACKERS THEN THREATEN TO EXPOSE OR SELL THE STOLEN DATA IF THE RANSOM DEMAND ISN'T MET,

WHICH DATA BACKUPS CAN NOT PROTECT AGAINST.

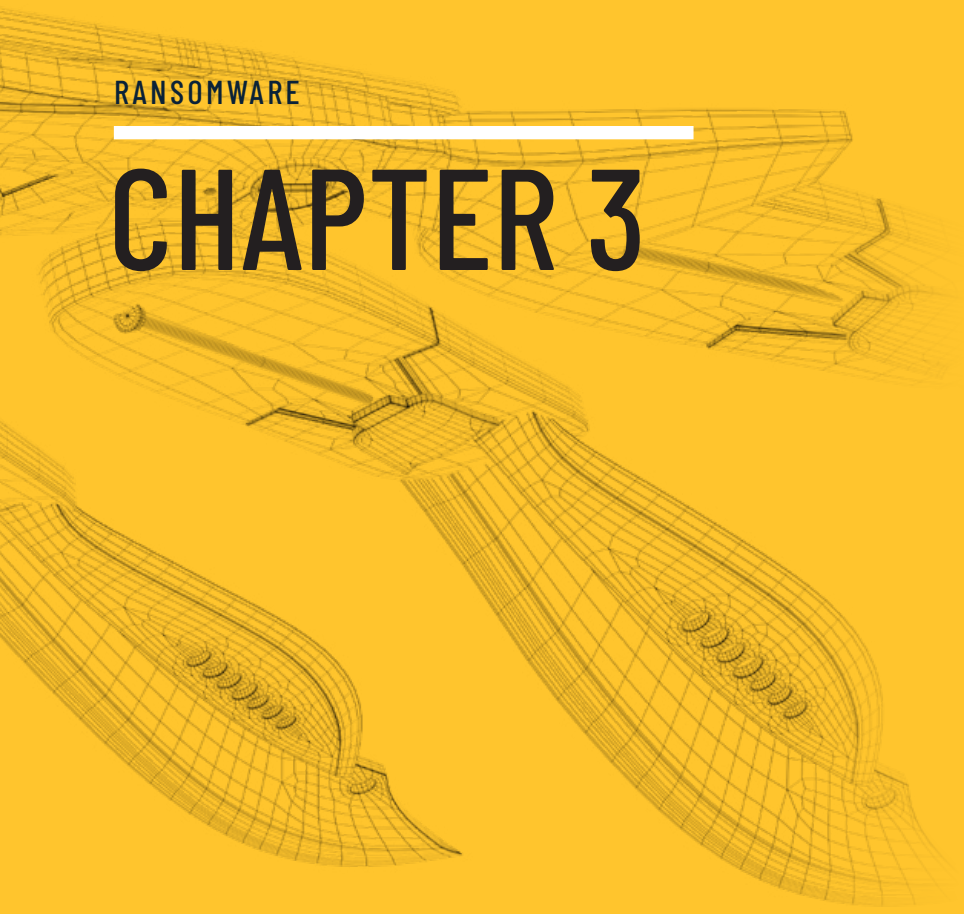
Even with a large percent of organizations indicating they have the policies and people in place to defend against ransomware, the last year has been unusually challenging. Cyber criminals recognized an opportunity to capitalize on the chaos and confusion as companies around the world struggled to deal with the COVID-19 pandemic—with many businesses shifting to a completely remote, work-from-home model overnight. It created significant challenges for IT security teams—expanding the attack surface and making visibility more difficult. Ransomware also enables attackers to continue compromising systems and collecting ransoms while safely quarantining at home and respecting social distancing protocols themselves.

The overall volume of ransomware attacks seems to be decreasing, but the attacks that are out there are more sophisticated and have a more devastating impact. Businesses improved backup processes and technologies in response to the rise in ransomware attacks. In the event of a ransomware attack, they could simply ignore the ransom demand and restore systems from backup and resume normal operation. Cybercriminals adapted, though, and created Double Extortion malware attacks. Rather than just encrypting data, a Double Extortion attack first exfiltrates sensitive data and intellectual property. The attackers then threaten to expose or sell the stolen data if the ransom demand isn't met, which data backups can not protect against.

At the same time, the ransom demands have skyrocketed. The average ransomware demand in 2018 was reportedly $6,000. That number increased 14X in 2019 to $84,000, and then more than doubled again in 2020 to $178,000. We have seen a number of attacks in 2021 that dwarf that ransom amount. Colonial Pipeline reportedly paid a ransom of $5 million to DarkSide, and both Acer and Apple have been hit with ransom demands of $50 million.

Working together with public and private industry is a step in closing the gap between perception of preparedness and concern. The United States government has formed a Ransomware Task Force—which Cybereason is participating on. It is composed of representatives from various government agencies and public and private sector organizations—working together to collaborate on addressing the ransomware crisis.

THE EFFORTS OF THE RANSOMWARE TASK FORCE FALL INTO THREE PRIMARY CATEGORIES—PREPARATION, DISRUPTION, AND RESPONSE. RANSOMWARE IS A GLOBAL ISSUE AND IT CONCERNS EVERYONE, SO IT IS IMPORTANT FOR US TO WORK TOGETHER TO DISRUPT RANSOMWARE OPERATIONS AND REVERSE THE ADVERSARY ADVANTAGE.



RANSOMWARE

CHAPTER 3

IN MOST CASES IT DOESN'T PAY TO PAY

One of the biggest issues organizations grapple with when subject to a ransomware attack is whether they should pay the ransom demand. While expediency is certainly a major factor, there are many things that need to be considered, and there are definitely risks involved with a decision to make the payment.

Should the organizations contract with a specialist to negotiate the terms of the payment? Will the attackers honor their end of the bargain and return access to all of the data? What if that data is corrupted in the process? What if the attacker is located in a country that is subject to sanctions that may deem a payment a criminal violation? Will payment encourage threat actors to follow on with yet another ransomware attack? What are the risks to the organization if the ransom payment is not made?

It is a difficult predicament for any organization to be in, and there are no clear cut "best practices" to follow, as each infiltration, attack group, victim organization, jeopardized data set, and potentially impacted third-party is somewhat unique. There are numerous factors that need to be weighed in considering whether to make a payment or not, so most ransomware attack scenarios need to be evaluated on a case-by-case basis.

DOUBLE EXTORTION

With Double Extortion, attackers first exfiltrate sensitive data and threaten to release it publicly if the ransom demand is not met. This means the target is still faced with the prospect of having to pay the ransom regardless of whether or not they employed data backups as a precautionary measure.

In recent developments, some ransomware purveyors have adopted other Double Extortion approaches to increase the likelihood they will receive their ransom demand. For example, in April, 2021, it was reported that the DarkSide ransomware gang was putting additional pressure on their targets by threatening to provide insider information based on exfiltrated data to stock traders so they could take short positions against publicly traded companies should they refuse to meet the ransom demand.

NEARLY
HALF OF RESPONDENTS (46%) INDICATED
THEY REGAINED ACCESS TO THEIR DATA FOLLOWING PAYMENT, BUT EITHER
SOME OR ALL
OF THE DATA WAS CORRUPTED.

WHAT IF WE DECIDE TO PAY?

With so much at risk, does it pay to just pay? Among survey respondents who indicated their organizations paid the ransom demand following an attack, nearly half of respondents (46%) indicated they regained access to their data following payment, but either some or all of the data was corrupted.

Other organizations were more fortunate. More than half (51%) said they were able to successfully regain access to the encrypted data without any data loss. Only 3% indicated that they did not regain access to any of the encrypted data.

But does payment of the ransom make the organization more vulnerable to follow-on ransomware attacks? That may depend on the actions they take to understand and mitigate the vulnerabilities that allowed the first attack to be successful.

An unnamed organization that was the target of a successful ransomware attack and paid a ransom demand reported to be in the millions of dollars apparently was targeted in a second ransomware attack by the same threat actors just two weeks later because they did not take the necessary steps to understand how the first attack occurred and implement additional measures to assure the attack vector was remediated.

This research revealed that of the organizations that opted to pay a ransom demand, 80% incurred another attack. Of those who did get attacked again, nearly half (46%) said they believed it was at the hands of the same attackers, while just 34% said they believed the second attack was perpetrated by a different set of threat actors.

DEFENDING AGAINST RANSOMWARE

Once an organization has been compromised with ransomware, there is no good option available. If the ransom is not paid, business may grind to a halt for days—or even weeks—as data is restored from backups and systems are restored. In the case of a Double Extortion attack, not paying the ransom also means accepting the risk that sensitive data or intellectual property may be exposed publicly or sold to the highest bidder on the Dark Web. Again, the financial impact of lost business and productivity, combined with the cost of recovery efforts can often exceed the ransom demand.

The alternative is to pay the ransom, but that comes with issues and risk as well. As noted earlier, many organizations that pay the ransom are able to regain access to their data but find that some or all of it has been corrupted. The decryption tool provided by ransomware attackers is often buggy or slow, forcing companies to restore from their own backups even after they have paid the ransom. There is also no guarantee that your data won't still be sold online after you have paid the ransom.

3 TIPS FOR DEFENDING RANSOMWARE

1 **Follow security hygiene best practices** -timely patch management, offsite data backups and employee security awareness training

2 **Deploy multi-layer prevention capabilities** on all enterprise endpoints across the network

3 **Implement extended detection and response solutions** across the environment for visibility to end advanced ransomware attacks before they can gain footing on the network

The only good option is to avoid getting compromised with ransomware in the first place. Traditional cybersecurity tools and next-gen endpoint solutions are inadequate because they rely on recognizing previously identified attacks and indicators of compromise.

Organizations need cybersecurity with comprehensive visibility across the environment, and the ability to analyze indicators of behavior in addition to indicators of compromise. Behavior provides clues about what is happening now, or what may happen soon, as opposed to compromise which focuses on reacting once a malicious action has occurred.

It's important to view the entire malicious operation—or Malop—to understand the scope of the attack and to connect the dots between actions and behavior that may seem innocuous when viewed alone. The Malop provides a more comprehensive understanding of what is going on, and gives you the visibility, context, and intelligence necessary to detect and prevent ransomware attacks before the damage is done.

Conclusions and Takeaways

The lessons to be learned here are fairly straightforward: the impact of a successful ransomware attack to both an organization's top and bottom line are significant regardless of region, industry vertical, or company size. Ransomware attacks can have far-reaching ripple effects that can shake an organization to its core. Often, the outcome is damage to reputation, loss of jobs, loss of revenue, and even the loss of the business itself in worst case scenarios.

While good risk management requires organizations to have contingency plans in place for dealing with the aftermath of a ransomware attack on all levels, the most prudent strategy to avoid significant losses for your organization is always going to be a strong effort around prevention strategies. Even with robust prevention capabilities in place that can block the majority of ransomware attacks, some will inevitably slip by prevention defenses, so organizations must also invest in comprehensive detection and response capabilities as well.

Data backup solutions are also highly recommended, as they can ease some of the pain of recovery efforts, but organizations need to keep in mind that attackers have strategies to render backups all but moot in some circumstances. Similarly, the right level of cyber insurance coverage can mean the difference between recovering all losses associated with a ransomware attack versus recouping only a portion of the costs - or none at all.

Organizations need to be sure they have the right personnel with the prerequisite skill sets and the right security solutions in place to assure that ransomware attacks are either blocked outright with effective security solutions and controls, or at a minimum are detected at their earliest stages and mitigated before the attack can escalate to the point where serious damage is done to the business.

SURVEY METHODOLOGY

The survey was conducted by Censuswide in April of 2021 on behalf of Cybereason. 1,263 cybersecurity professionals took part in the survey—with participants from the United States (24%), United Kingdom (24%), Spain (12%), Germany (12%), France (12%), United Arab Emirates (8%), and Singapore (8%). There is diversity in the survey regarding how long participants have worked at their company, and how long they have worked in their current role.

The survey sample includes responses from an array of industries. Technology is the most represented industry in the survey at 44%, followed by Manufacturing (16%), and Finance (11%). The rest of the survey participants came from Healthcare, Automotive, Government, Legal, or other industries.

There is a range of different size companies represented. The largest group is 500 or more employees (30%), but we also received responses from companies with 250-500 employees (23%), 100-249 employees (25%), 50-99 employees (11%), 10-49 employees (10%), and fewer than 10 employees (1%).

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders providing future-ready 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 detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a Malop (malicious operation). The result: defenders can end cyber attacks from endpoints to everywhere. Cybereason is a privately held, international company headquartered in Boston with customers in more than 30 countries.

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