Cymulate
Extended Security Posture Management

Ransomware Study: Unexpected Reasons for Optimism

Concern Drives Enterprises to Turn the Tables

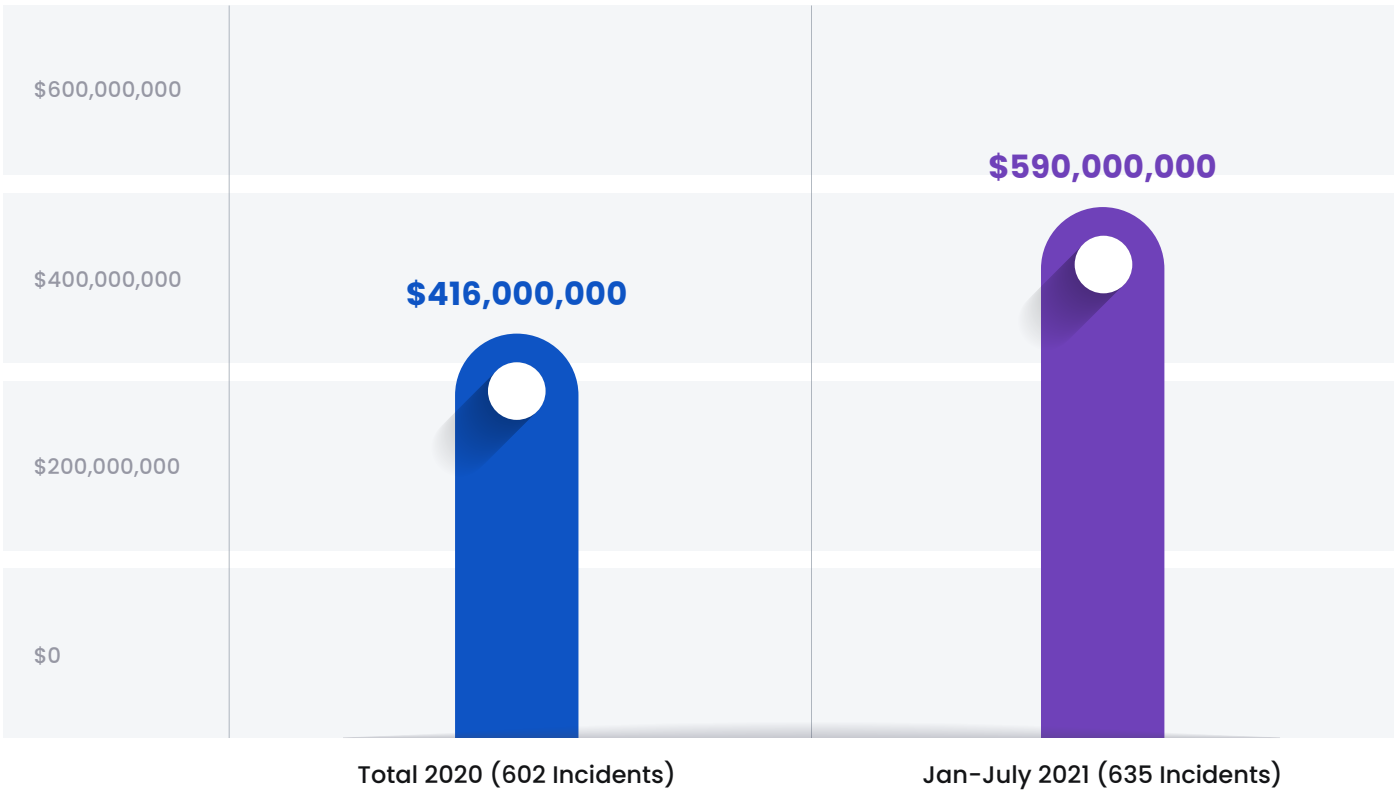
Table of Content

01 Executive Summary

As we approach the final quarter of 2021, there is no doubt about what this year's "attack of the year" contest winner is. Ransomware was by far the top cybersecurity crime bothering everyone's minds this year. And for a good reason – the cost is devastating! The US Treasury Financial Crimes Enforcement Network found that, during the first half of 2021, ransomware victims paid out over $590 million. This is more than the entire amount paid out in 2020 whole year.[1]

News stories on successful ransomware attacks like Colonial Pipeline, which took down critical US infrastructure, and Kaseya – a combined Ransomware/Supply Chain attack that took down over 1500 companies in a single attack, were everywhere.
Cymulate has commissioned a global survey among enterprise professionals globally to get a deeper understanding of the effect these attacks are having on organizations worldwide, their level of confidence in defensive infrastructure and what steps they are taking to improve their defensive line.

Cost of Ransomware



US Dept. Of Treasury, Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 – July 2021

[1] US Treasury, Financial Crimes Enforcement Network, Financial Trend Analysis, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021. https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

02 | Key Findings

01

Companies of all sizes, industries, and regions have been affected by ransomware directly.
High awareness, up to the business/ board room levels prevails.

02

Considerable anxiety over future attacks affects nearly everyone, whether they experienced a ransomware attack or not. These rather bleak statements hide the surprisingly optimistic findings uncovered when looking at the attacks' outcome: In Latin America and Asia, enterprises face a slightly higher risk (5-6% over the average). North America, Europe, and Australia, have a very slight advantage, with a 3% less than average probability of being targeted.

03

Increased adoption and integration of EDR and MFA defensive tools.

04

Increased level and quality of preparation. Most companies, whether ransomware victims or not, have allocated additional budget and headcount as a direct consequence to ransomware risk awareness. Most have created new and modified incident response plans – with some even spending time practicing them.

05

Massive increase in the incorporation of offensive cybersecurity testing methods. On this last point, we uncovered that most respondents preferred advanced offensive cybersecurity testing methods like continuous security validation, attack surface management, and attack-based vulnerability management over less advanced techniques like breach attack simulation and pen testing.

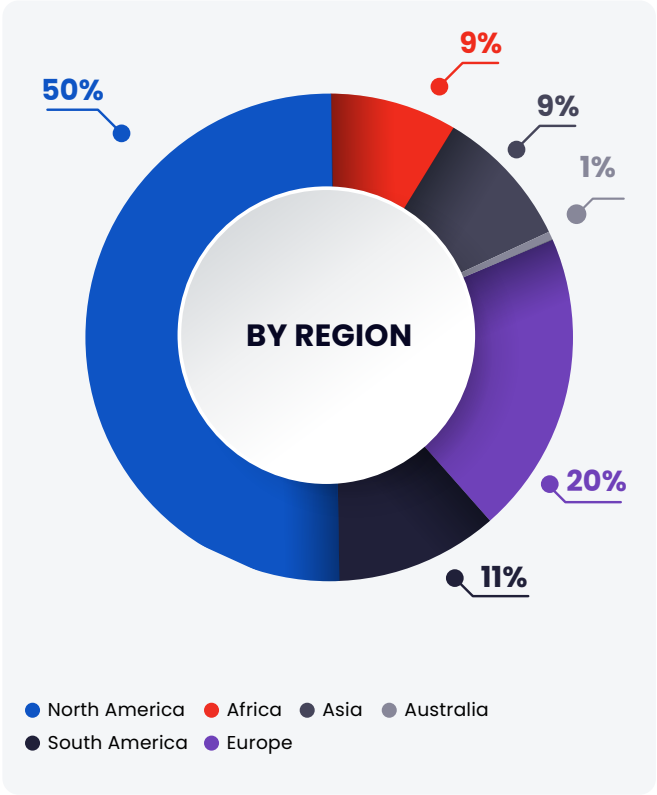
The Unexpected Cause for Optimism:

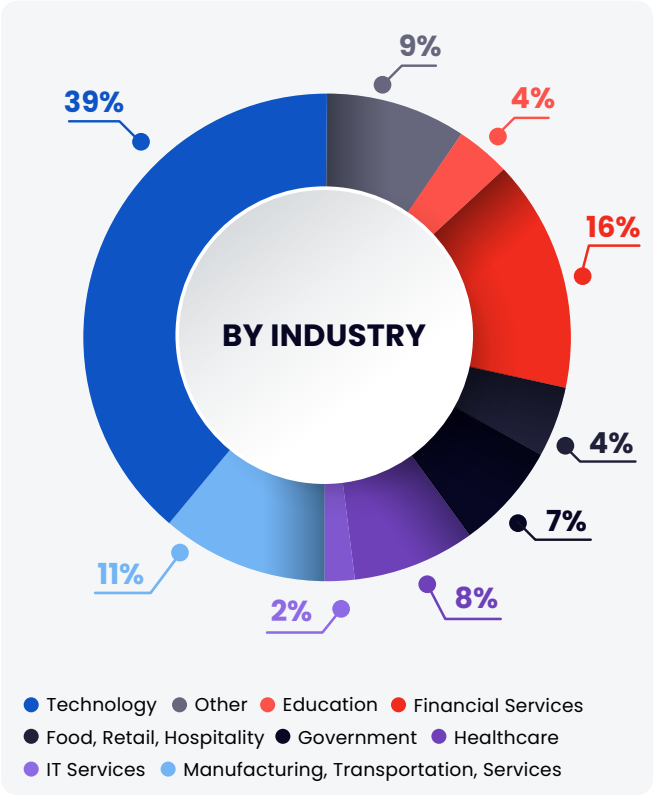
The attacks outcome in duration and severity: the majority of respondents who experienced an attack reported minimal damage – only affecting a few servers/workloads, and minimal duration – a few hours to a few days at maximum.

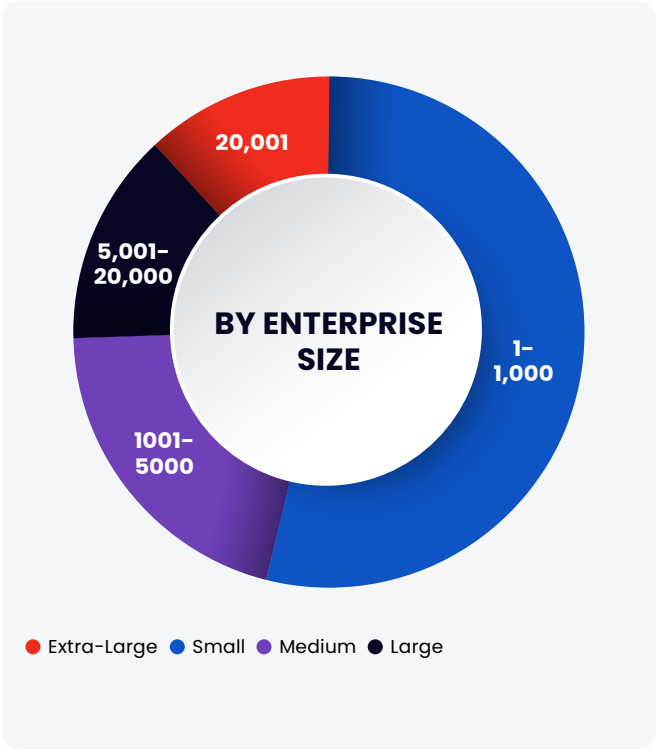
At the root of these positive findings lie: Increased level of understanding of ransomware risk at business and board level, resulting in increased anxiety across all industries globally, anxiety that spurs action.

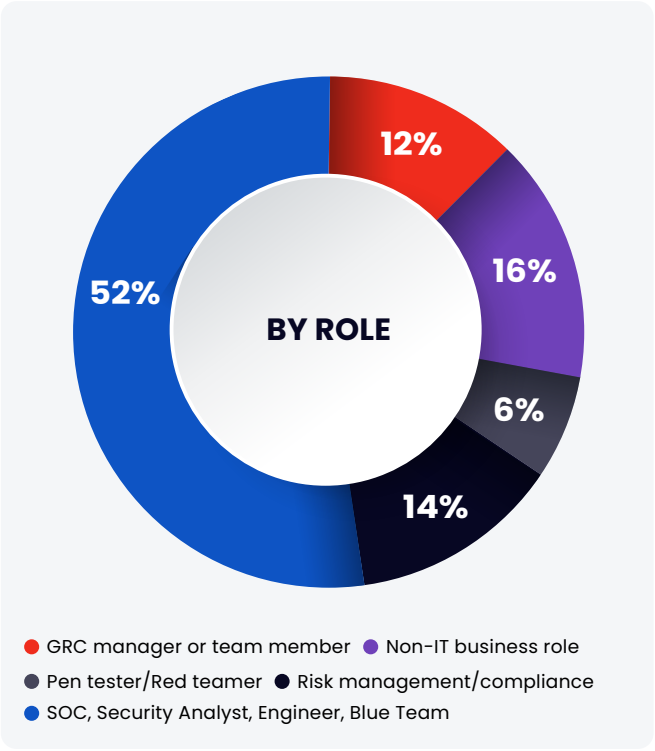
03 | Methodology

Cymulate's ransomware survey gathered 881 responders globally, working across 14 verticals, in various roles and in companies of all sizes, making it a well-rounded sample of participants.







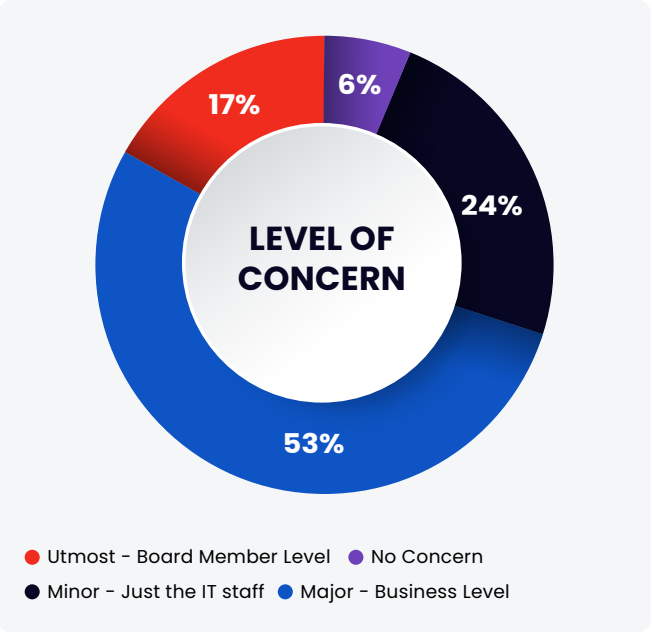


04 The Rise of Ransomware Awareness Across Industries

Before digging into the factual reasons for hope uncovered by this survey, it is interesting to get a feeling of the respondents' general ransomware awareness and their perceived ability to defend their enterprise from attack.

Ransomware awareness has risen in the enterprise to the business and the board levels

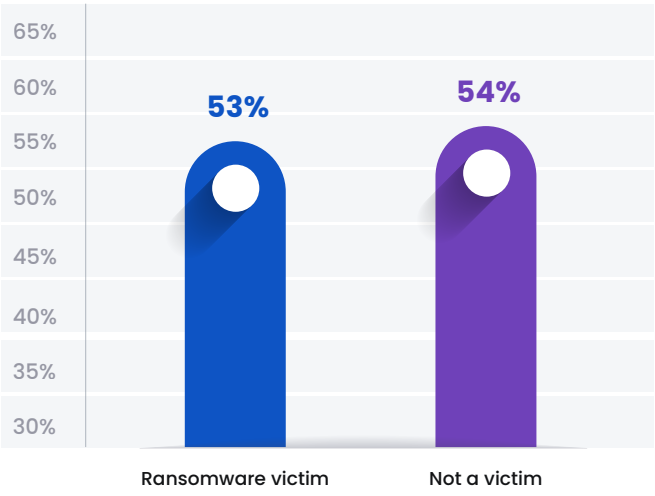
Testimony to ransomware's rising ill-gotten fame, concern about exposure to ransomware reaches 90% of the respondents, spread equally between those who have been hit and those who have not, and is not limited to the IT level. In fact, 70% of the respondents report that concern has reached the business management level, with a slight uptick at the board level for those who experienced an attack.



The level of confidence in the ability to fight ransomware remains low

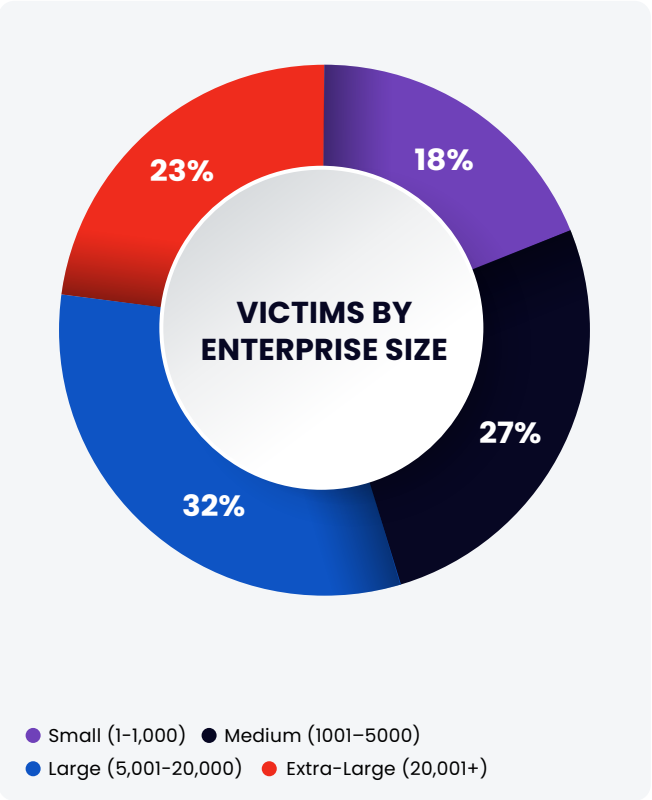
Yet, awareness alone does not translate into a similar level of confidence in the reliability of the defense. Confidence about the ability to fend off a ransomware attack is equally between victims (53%) and non-victims (54%). A third (28%) of all respondents had been hit by a ransomware attack.

Confidence About the Next Attack



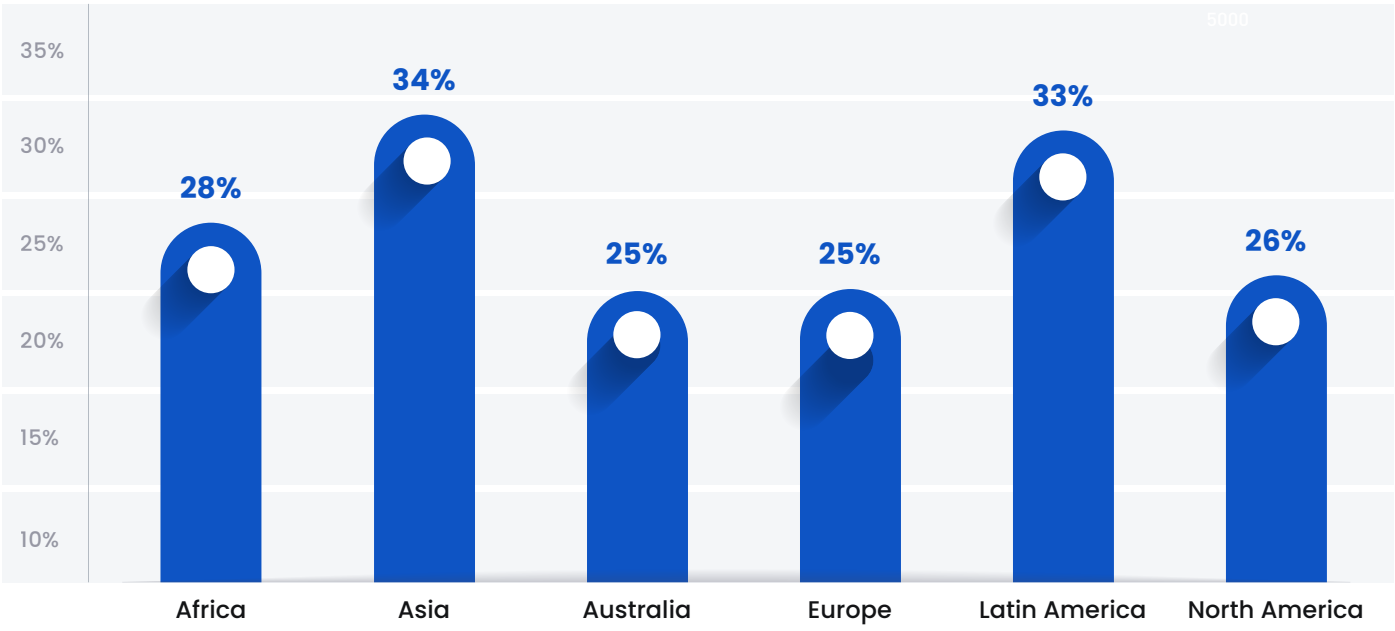
Ransomware is targeting businesses of all sizes, wherever they are

28% of survey responders said their business had been hit by ransomware. Past statistics claim the majority of these occur in businesses between mid-sized (1,001 and 5,000 employees), and large companies (5,001 - 20,000 employees).
What we uncovered is that, in fact, everyone is targeted. While the mid-size and large groups had a relatively higher than average hit rate (33% and 39% respectively), the surprise is that smaller businesses (1 – 1,000 employees), with a 23% hit rate, is barely 5% less than the average, and that the largest businesses (20,001+ employees) were hit at the 28% average survey rate. Size-wise, the probability of experiencing a ransomware attack is 39% and 33% for large and medium companies, the "lower risk" ones, extra-large (>20k employees – 28%) and small (<1k – 23%) companies still having a one-in-four chance of being hit. In and of itself, that is unsurprising. The surprise is extra-large companies, thought to have the most resources and largest cybersecurity teams, actually scored worse than other sizes with 32% of respondents saying they were hit by a ransomware attack.



Ransomware Victims by Region

In Latin America and Asia, enterprises face a slightly higher risk (5-6% over the average).
North America, Europe, and Australia, have a very slight advantage, with a 3% less than average probability of being targeted.



05 | The Unexpected Cause for Optimism – Most Ransomware Victims Are Far From Helpless

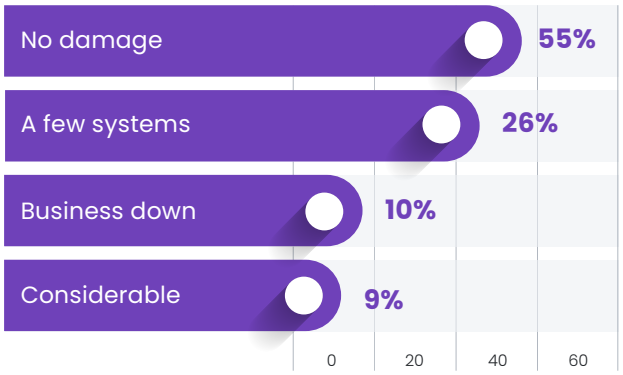
It seems hackers and the press have given ransomware such infamous notoriety that potential victims have improved their level of preparedness. The survey data indicates that, while everyone may be a target, most of those who are hit are doing an excellent job defending themselves and recovering gracefully. When taking a closer look at the damages incurred by the respondent victims of an attack, overall, they suffered limited damage both in severity and duration, with over half the respondents proactive enough to stop the attack before it could cause any damage, and the vast majority of those even before it could cause any downtime.

01 Severity

Business impact is minimal to nil for the vast majority of the respondents who experienced a ransomware attack

- Only 19% of the respondents experienced major damages and an interruption of business or production
- 26% of the respondents reported that damages were relegated to a few systems
- 55% of the respondents stopped the attack close to entry without experiencing any damage

Damages to Business

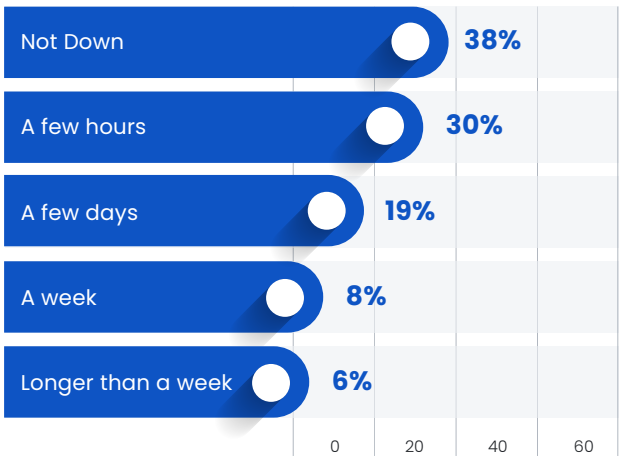


02 Duration

Ransomware attacks failed to significantly impair normal business services

- 38% of the respondents' services were not down
- 49% of the respondents' services were down for only a few hours to a few days
- Only 14% of the respondents' services were down for a week or more

Business Disruption Duration



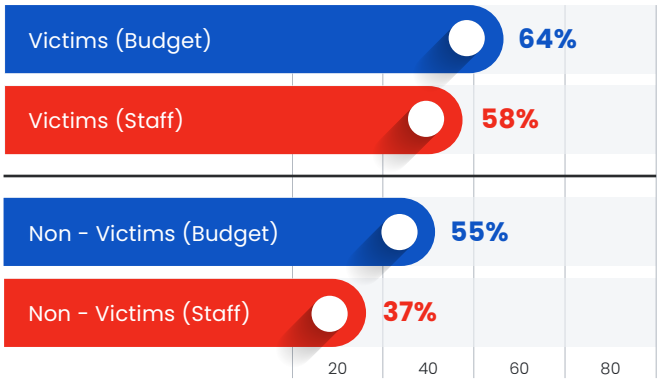
06 | Learning from the Most Resilient Respondents

When all is said and done, the most interesting part of this survey was uncovering the techniques used by those who were most resilient against ransomware attacks. After all, as ransomware attacks are likely to continue unabated, the best option for potential victims is to efficiently improve their preparation level.
So, what are the steps taken by the best performers?

01 Increasing Resources

The looming threat of ransomware is having a positive effect on the entire spectrum of security posture management. From budget and staff increases to changing and practicing IR plans, ransomware is seen as the driver behind these improvements, with a mild uptick for respondents hit by a ransomware attack.
Regardless of whether they were hit by ransomware or not, the pervasive ransomware threat caused respondents to increase their budget and staffing.

Budget & Staff Increases

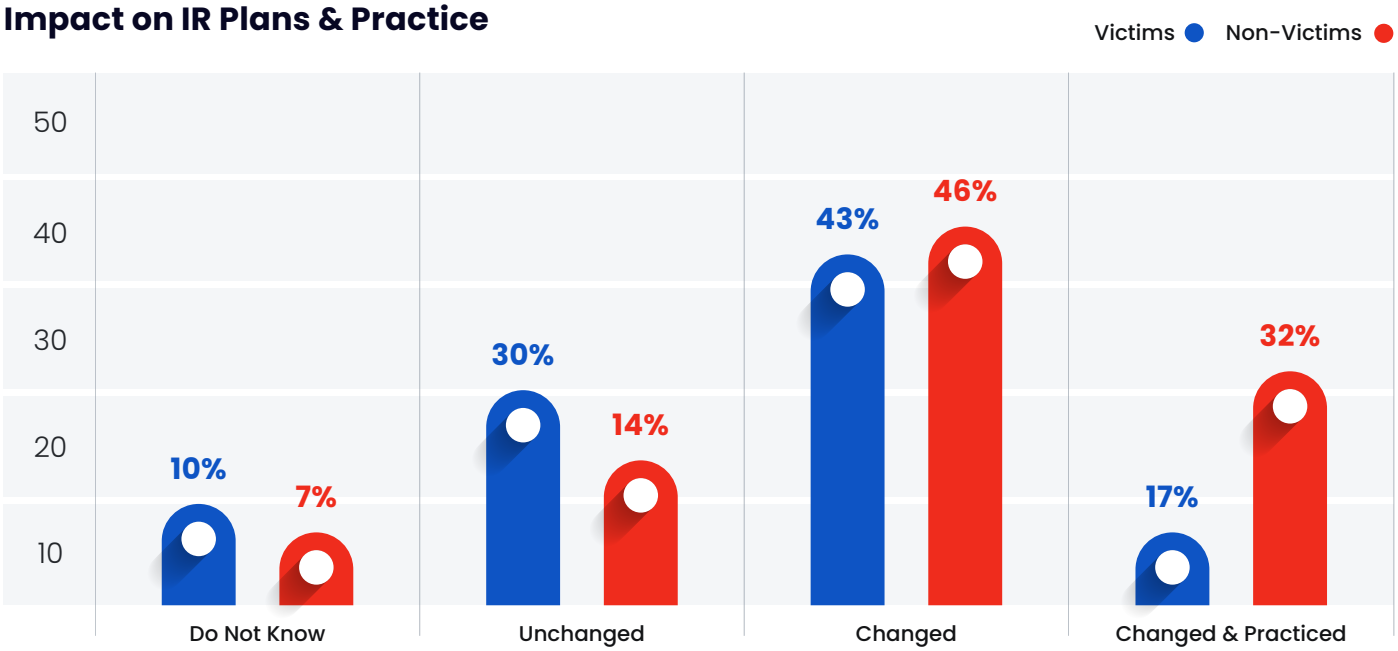


02 Upgrading Incident Response Planning and Practice

In addition to increasing the budget and staff, a large minority of the respondents opted to improve their Incident Response (IR) readiness.
He proportion of those opting to upgrade their IR plans is quite similar between victims and non-victims of ransomware attacks, which is encouraging.

If there is one lesson to be learned from this survey about IR, it is that the importance of practicing IR plan is still vastly underappreciated by those who have not experienced an attack. Those who did are twice as likely to run practice of their improved IR plans.

Impact on IR Plans & Practice



03 Investing More Resources in Security Solutions and Procedures

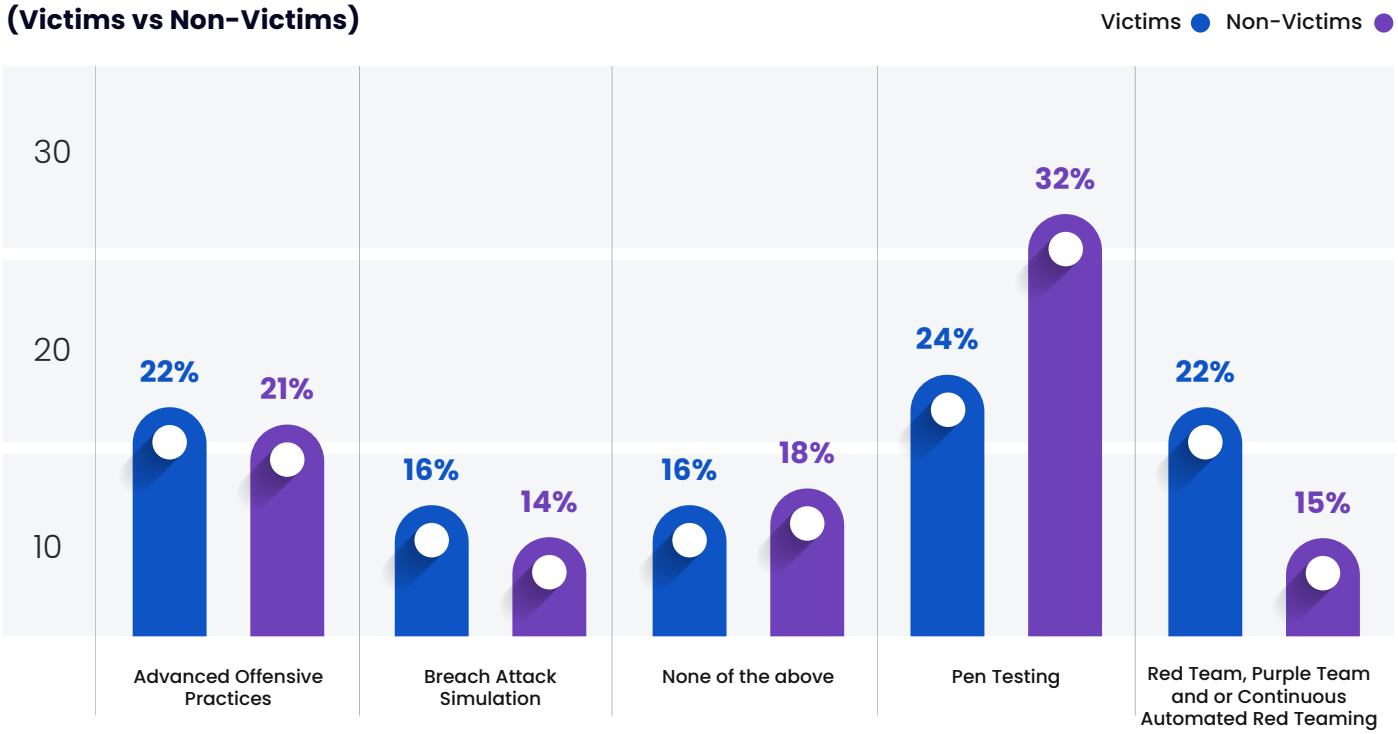
Finally, budget increases resulted in investment in security solutions and the incorporation of procedures. A closer look at how these funds were allocated is quite informative as it shines a light on the difference experiencing a ransomware attack makes in selecting a specific technology. This is true both when looking at defensive and at offensive solutions. Amongst defensive solutions, Multifactor Authentication (MFA) is clearly identified as an effective defensive measure by those who experienced an attack (37% victims/34% non-victims), as opposed to Endpoint Detection and Response (EDR)(30% victims/39% non-victims), the relative importance of which seems to shrink after experiencing a ransomware attack. This must say something about what the post-mortem forensic analysis revealed!

04 Incorporation of Offensive Cybersecurity Solutions

Most respondents, over 82% across the board, are now adopting offensive solutions. Not all of them are already on board with the Extended Security Posture Management (XSPM) comprehensive umbrella, but the tendency to incorporate elements of it is on the rise, and overall adoption is likely to rise with the increase in awareness of advanced offensive security techniques.

Though 24% of the respondents still use manual pen testing, 22% already adopted advanced pen testing techniques such as Red Team, Purple Team and or Continuous Automated Red Teaming (CART), and 22% adopted partial security posture management technologies such as Attack Surface Management (ASM) and/or Posture Security Validation, and 16 % included Breach and Attack Simulation (BAS). Only 16% of the respondents have yet to incorporate any offensive solution in their basket. As testing cyber resilience is now part of most compliance regulations, this is quite a worryingly high number. Let us hope that, when made aware of that grievous shortcoming in their security posture management, they will skip the outdated manual pen testing step and immediately adopt advanced offensive solutions.

Additional Offensive Practices (Victims vs Non-Victims)



Cymulate

07 | What Else Are We Curious About?

Analyzing the results, we would have loved to dig deeper into the nitty-gritty details of how respondents implemented offensive and defensive tools.

These pending questions and more, some of which stem from this survey's answers, will be addressed in our next survey, so stay tuned.

Key Takeaways

Fear Spurs Effective Action

Paradoxically, ransomware's ill-gotten fame might be pushing the development of security measures covering other potential dangers. Concern about ransomware is felt by all, and the result of fear is increased budget and resources that are invested in improving security posture management.
Though ransomware is at the source of these security posture improvement, the end-result s a better defense against all types of attacks.

Offensive is Effective

Most notably, advanced offensive cybersecurity solutions are seeing increased adoption and are efficient against ransomware threats.
This increased adoption of offensive techniques will lead to the early identification of additional potential entry vectors and, eventually, to an overall security posture hardening.

Our suggestions for you

- Use continuous, automated offensive testing to get a security posture baseline against ransomware and optimize your cybersecurity defenses, people, and incident response plans against it.
- Continuously track your trending risk and keep it low
- Use actionable data to rationalize your cybersecurity tool stack and optimize your cybersecurity spend

Want a free ransomware evaluation right now?

Click here

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Start Your Free Trial

Contact us for a live demo, or get started with a free trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632