Cymulate

Data Breaches Study: **Methods, Implications, and Prevention**

June 2022

Table of **Contents**

Introduction and Key Findings

Introduction & **Methodology**

Cymulate commissioned a global survey which took a deep dive into the impact of ransomware on today's businesses and found that despite the growing threat, there are reasons to be optimistic. Companies are moving from a reactive stance to a more proactive approach to cybersecurity. They are focusing on business impact and risk reduction, optimizing their defenses, and incorporating new best practices, such as offensive testing.

This report is the next step in Cymulate's research, taking a broader look at the state of the industry and the attacks today's organizations are facing. We wanted to understand how companies are being breached, the origins of initial attacks, and the kind of damage and duration today's businesses are experiencing.

What we found shines a light on the true state of cybersecurity readiness today. At a time where the threat of ransomware is raising its head once again, where the war in Russia and Ukraine threatens western security posture on a daily basis, and as regulators and governments alike are encouraging organizations to become increasingly proactive – this report paints a picture of the number of breaches today's businesses are facing, the cost of those breaches, and critically, their readiness and response.

Methodology

We commissioned a survey of 858 senior decision-makers from North America, EMEA, APAC and LATAM, 36% of whom work in the technology industry, and the remainder spread across other industries including banking, finance and government. The survey was completed by Global Surveyz, an independent survey company, and took place during April 2022.

The respondents work in roles including cybersecurity, IT, developers, business and risk management, in companies which range from less than 100 employees to more than 100K. The respondents were recruited via Cymulate's in-house list of customers, prospects and followers, and invited via email to complete the survey. The average amount of time spent on the survey was 6 minutes and 21 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key **Findings**

01 How do attacks get in? Employees, followed by partners

Fooling employees via phishing scams is still the number one way that attackers make it through the front door, at 56%. However, in 37% of cases, attacks are coming from connected third parties. When most enterprises are deeply interconnected between their partners, vendors, customers, suppliers and shared applications, this is an especially interesting result. If they can't breach your employees, the hackers will turn to your partners and supply chain. Interestingly, 29% of attacks come from insider threats, which can often be unintentional due to human error. Despite the difficulties of managing the remote working landscape, it's clear that education is key.

02 Once hit, it is more likely that you will be hit again

Cyberattacks are part of today's reality, and it was no surprise to see that 39% of respondents have suffered breaches over the past 12 months. While there is a common misconception that lightning doesn't strike in the same place twice – this couldn't be further from the truth. In fact, if we look at the companies who have been hit by cyber-crime this year, 67% of these have been hit more than once, with almost 10% experiencing 10 or more attacks.

03 All sizes get hit, but smaller businesses experience worse business damage for longer

The majority of large companies (57%) reported that the disruption to their business processes after their worst cyberattack lasted a short time, and 40% reported a low amount of damage to the business overall. In contrast, medium-sized companies with less than 2,500 employees had a worse time recovering, with just 33% claiming the time to recover was short, and only 27% reporting low levels of damage. The larger the company, the more resources they are likely to have to recuperate.

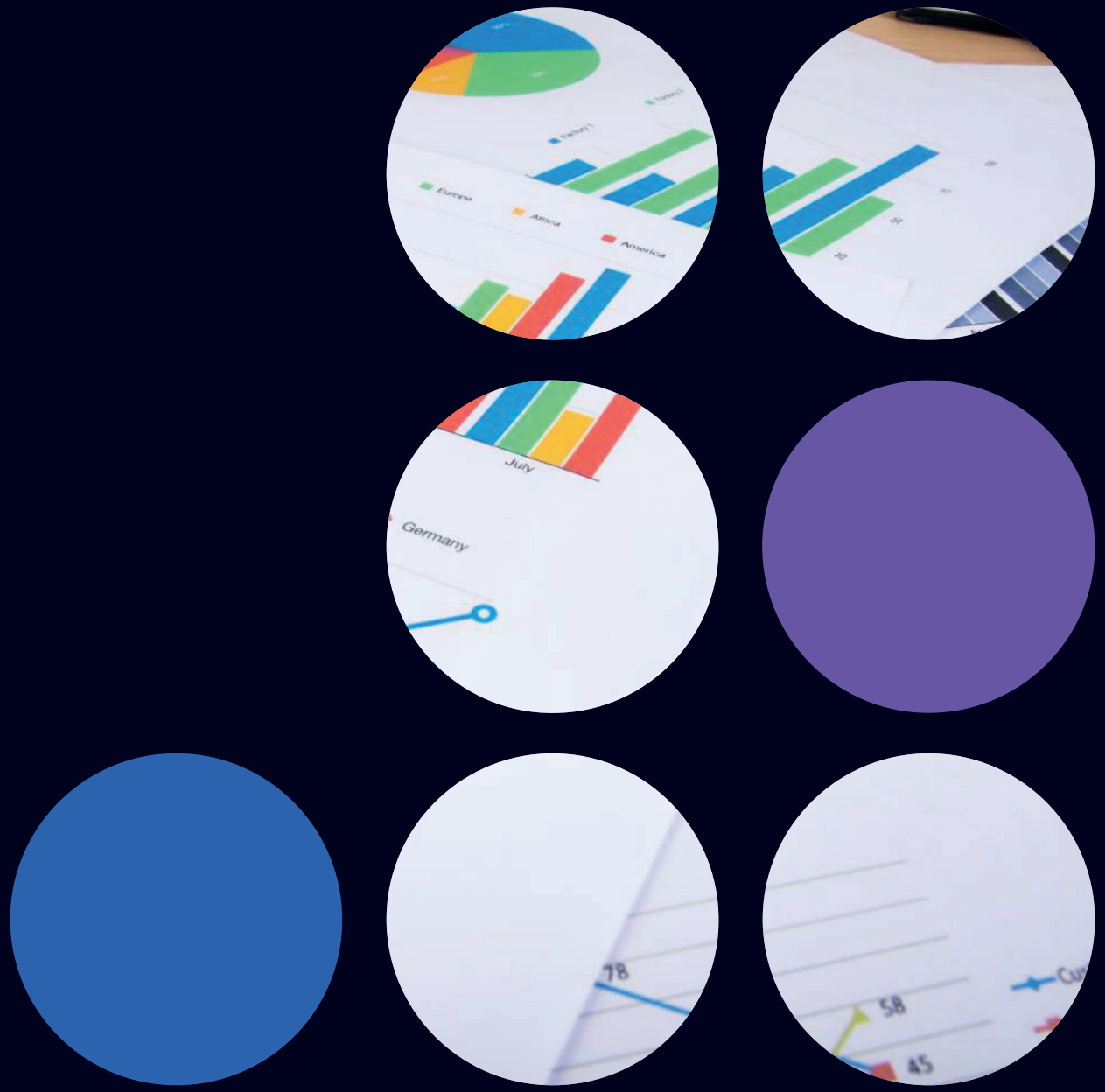
04 A reactive approach is a costly gamble

In the wake of a cyberattack, there are a lot of moving parts. In 39% of cases, security teams need to bring in legal, finance and executive staff to handle the fallout, and in 35% of cases, a third-party consultant will need to be instructed. Finally, 22% of the time, businesses will have to handle the regulatory mandate of public disclosure, which can cause even greater damage if it isn't handled with sensitivity and expertise. Being proactive about cybersecurity could eliminate this added cost altogether.

05 The more you meet, the less likely you'll be breached

The benefits of proactivity and cybersecurity readiness are proven by the data we collected on how often leadership and cybersecurity teams meet to discuss risk reduction. Of our respondents, those who met the most frequently (15 times a year, more than once per month) had zero breaches. In contrast, those businesses who suffered 6 or more breaches were the ones who met the least often, under 9 times per year on average.

Cyberattacks Breaches and Impact



Number of Breaches Over the **Last 12 Months**

Almost 40% of survey respondents admitted to being breached over the past 12 months.

On average, the companies reported being breached 1.3 times.

These numbers are not surprising to us at Cymulate, and minor incidents are likely to happen at any company.

However, if we look at only the companies who were breached, 67% were attacked more than once, showing that if an attacker hits your infrastructure, you are more likely to be attacked again.

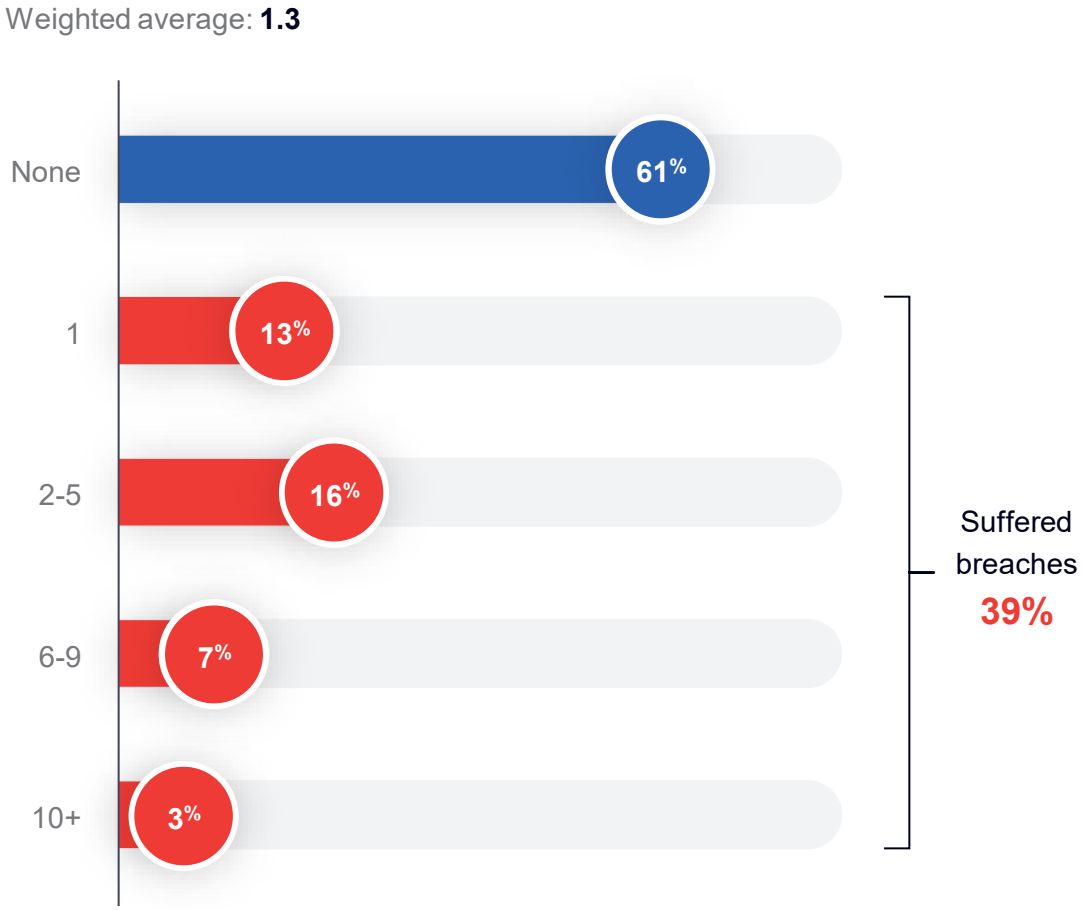


Figure 1 Number of Breaches, Last 12 Months

Type of **Cyberattacks Experienced**

The top types of cyberattacks companies experienced were malware attacks (55%), ransomware (40%) and DDoS (32%).

Malware can be a component of many of the other kinds of attacks, including ransomware, application attacks, insider threat, botnets, crypto-jacking, and wiper attacks. We also need to consider that these reported attacks are only the attacks that the companies are aware of. There may be more instances of cyberattacks that businesses do not know have happened.

Ransomware is one of the most devastating types of attacks out there today, and this data shows that it's a large problem for today's businesses.

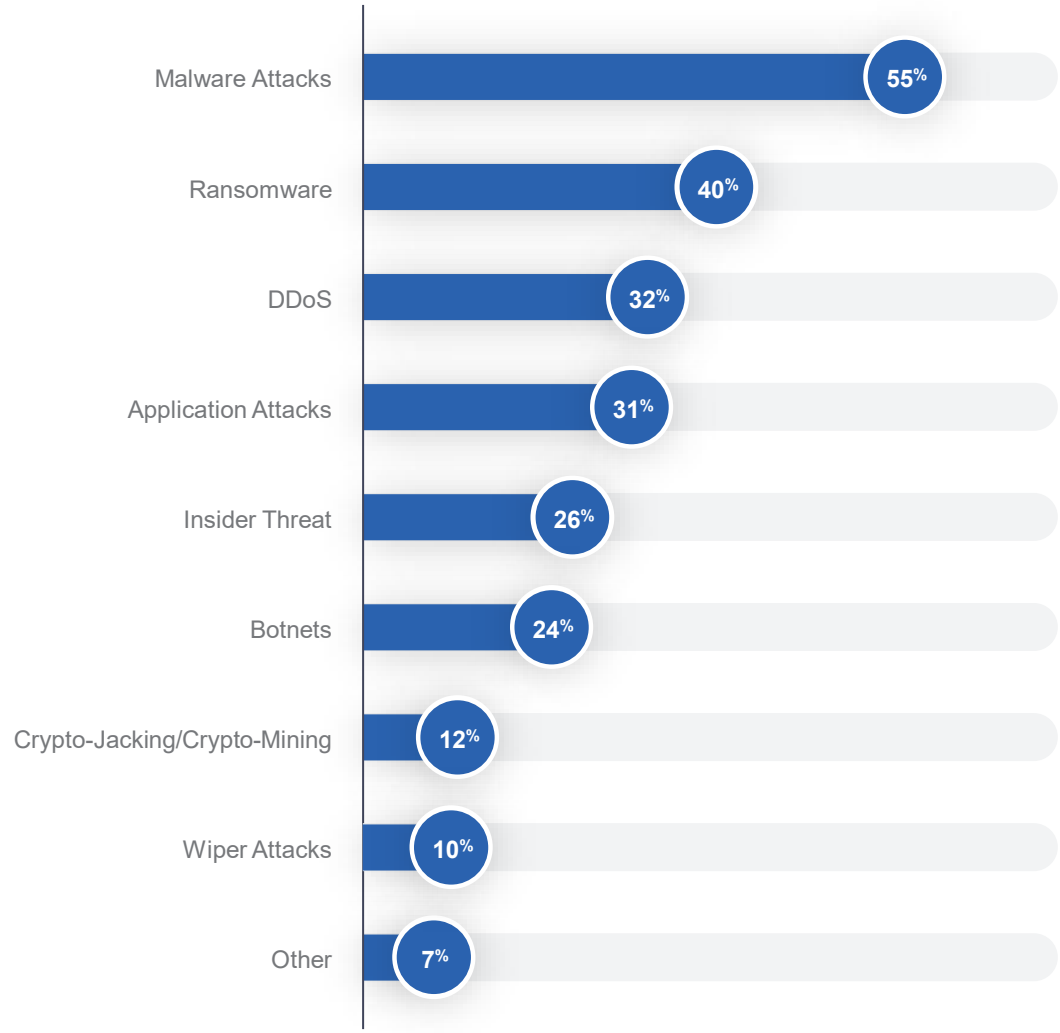


Figure 2 Type of Cyberattacks Experienced

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Cyberattack **Sources**

The top source for cyberattacks is end-user phishing (56%). This is followed by 3rd parties connected to the enterprise (37%), direct attacks on enterprise networks (34%), and insider threats (29%).

We are familiar with concept of attackers trying to gain an initial foothold by targeting your employees, encouraging them to click on malicious links or attachments. However, the second most common attack source today is third parties – your digital supply chain. Businesses are increasingly connected, and partners need access to your systems to enable business continuity. This means that your weakest link might not be under your own roof at all, which is a worrying thought.

Another concerning statistic is the level of insider threat, which is defined as an action originating from your own employees, either maliciously or through human error. This means we must double our efforts on employee awareness, beyond merely end-user phishing education.

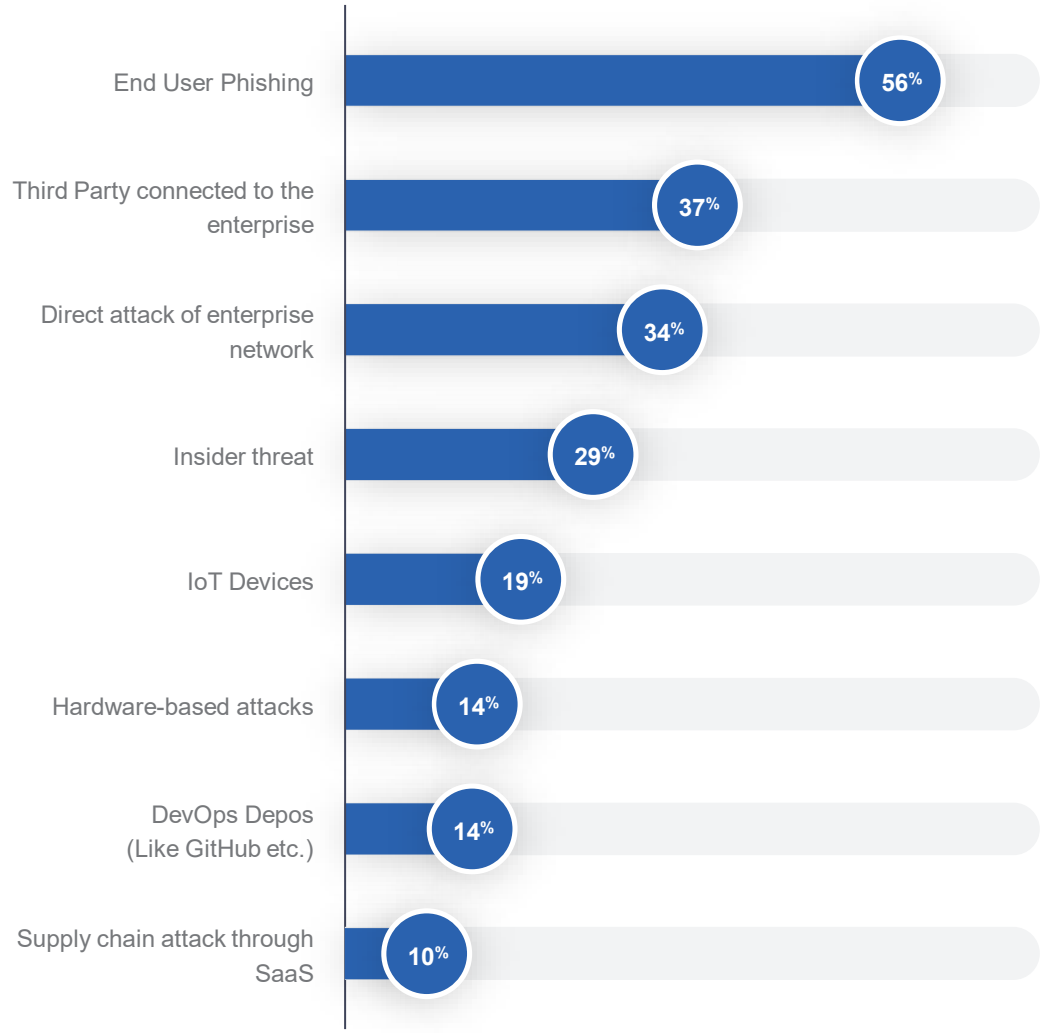


Figure 3 Source for Cyberattacks

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Impact on IT Systems from **Most Powerful Cyberattacks**

We spoke to respondents about the damage and duration of their most impactful cyberattack, both from a business and an IT perspective.

When it comes to IT, 27% of companies reported high damages to their IT systems from their most powerful cyberattack and 25% reported a long time to remediate for the most powerful cyberattack.

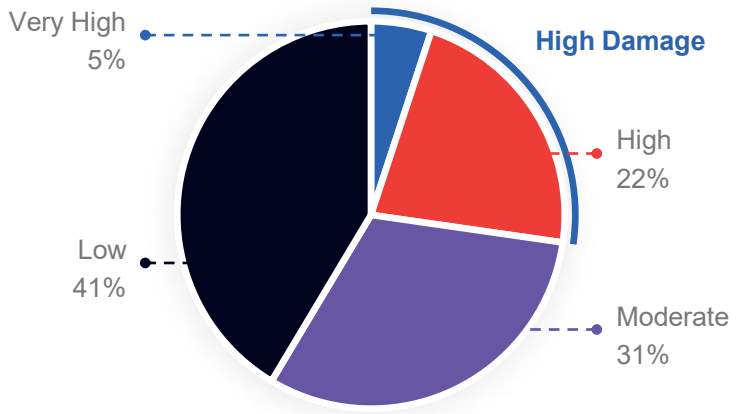


Figure 4 Damage to IT Systems from Most Powerful Cyberattack

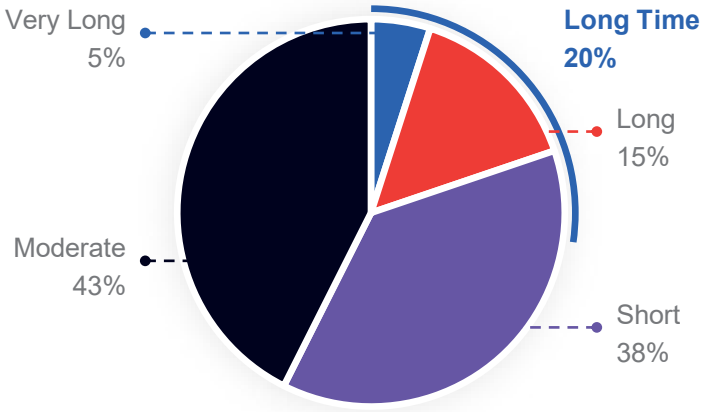


Figure 5 Longest Remediation Time from Cyberattack

Longest Disruption to Business from Cyberattacks, **by Company Size**

Beyond IT impact, we also focused on impact to the business. We broke down these numbers by large companies (2,500+ employees) and medium companies (250-2,500 employees), to see how a cyberattack impacted them differently.

The majority of large companies reported a short disruption to the business as short (57%), while only a third (33%) of the medium companies reported a short disruption.

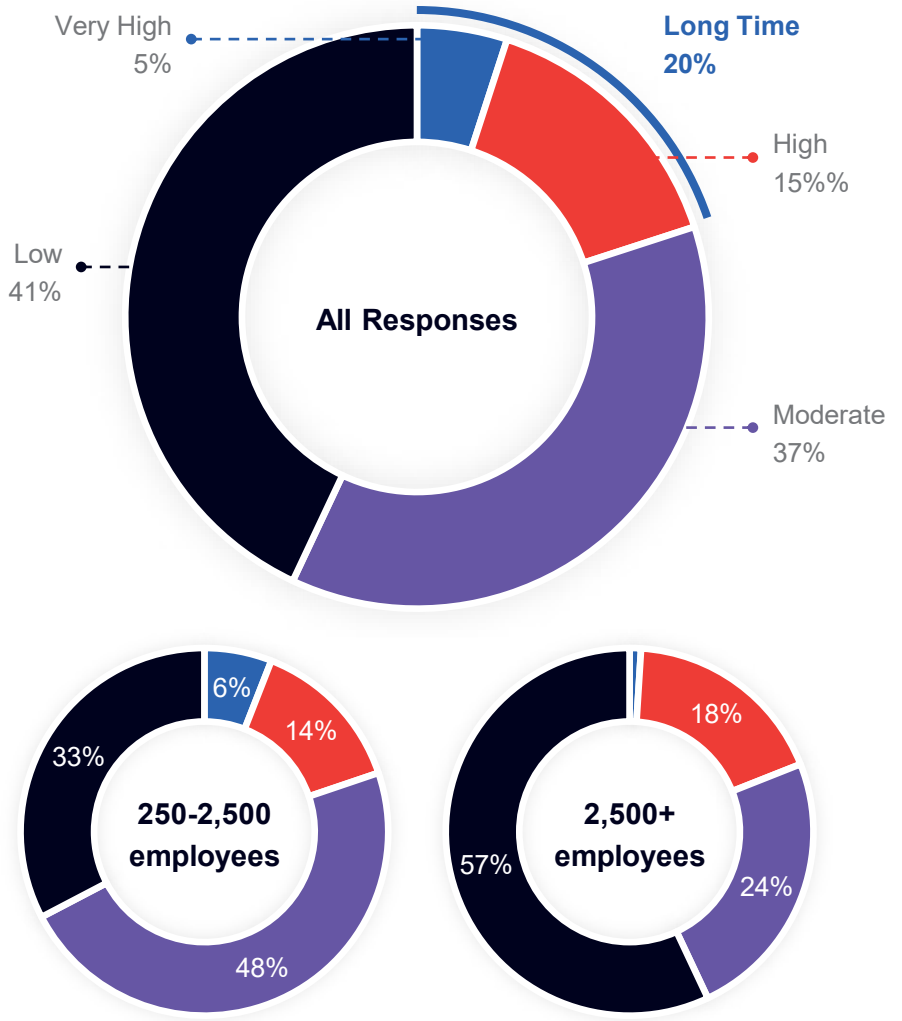


Figure 6 Longest Disruption to Business from Cyberattack

Damage to Business from Most Powerful Cyberattacks, **by Company Size**

We saw the same trend when looking at the damage to the business using the same cohort analysis – with one striking difference.

Overall, 21% of companies reported high to very high damages from the most powerful cyberattack they've experienced.

When comparing by company size however, 40% of larger companies reported low damage to the business, whereas only 27% of the medium companies reported low damage.

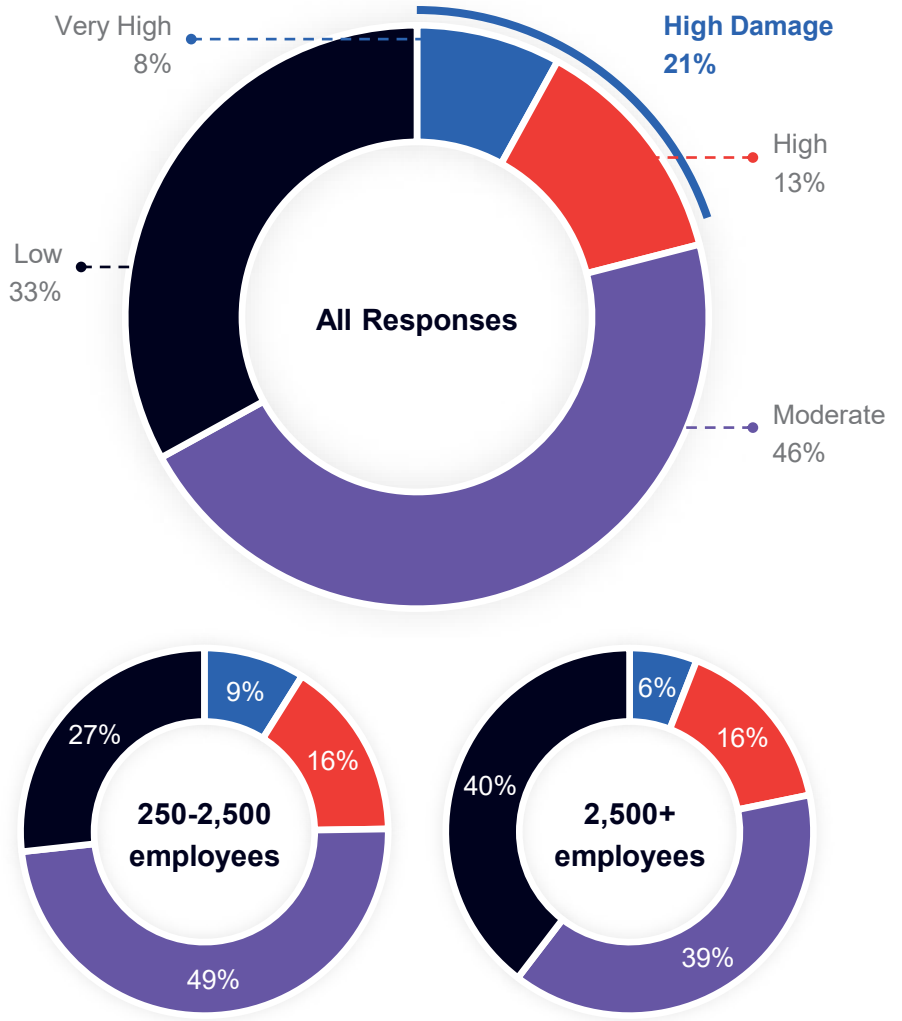


Figure 7 Damage to Business from Most Powerful Cyberattack

Team Members **Handling Breaches**

Only 9% of companies limit the handling of cybersecurity breaches to security staff alone. 91% involve two or more different team members.

A disruption in cybersecurity is a disruption to the business, so it's important to see that other stakeholders are being brought in to provide their expertise and support.

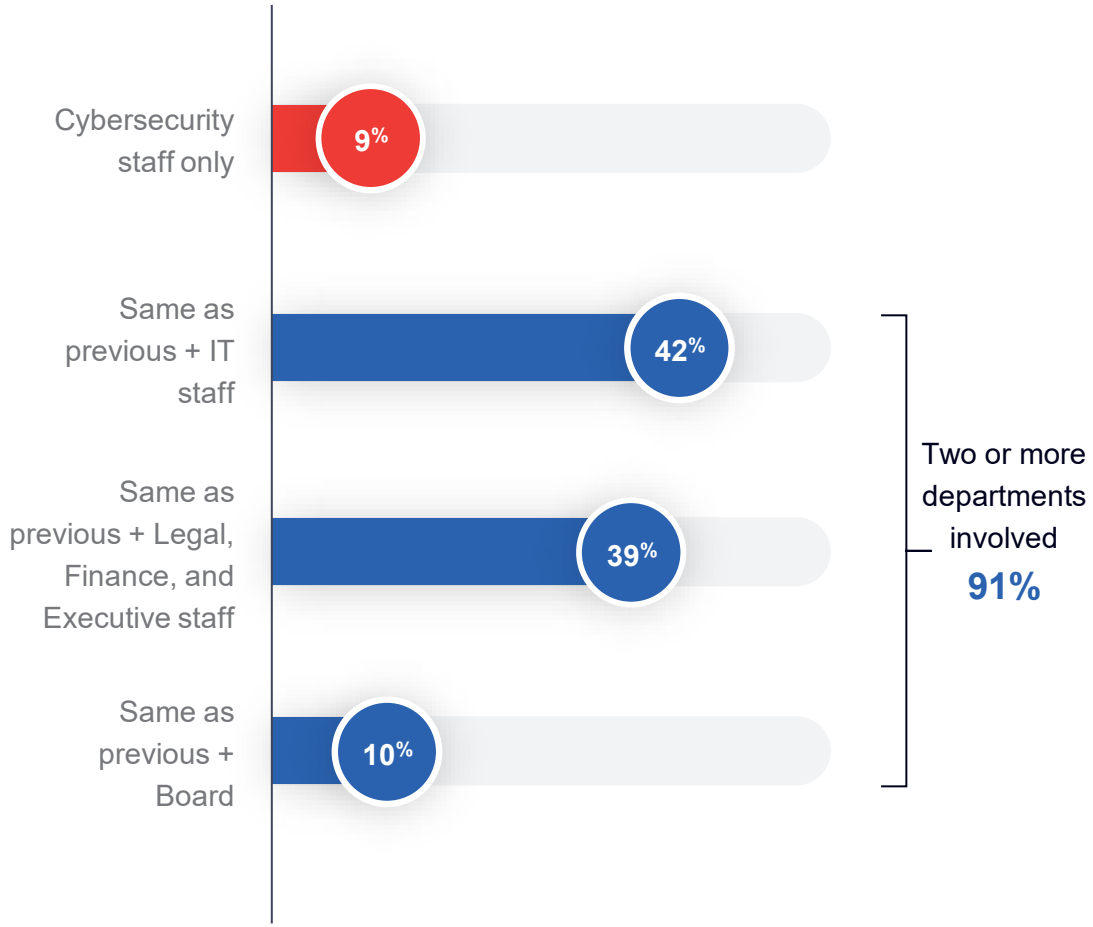


Figure 8 Team Members Handling Breaches

Business Actions Taken **Post Worst Breach**

61% of the companies took in-house business actions following the worst breach they have suffered.

The top business actions are hiring security consultants (35%), publicly disclosing the breach (22%), and hiring PR consultants or dismissing security professionals (both at 12%).

Getting support proactively from security expertise can reduce the costs of reacting to a breach after the fact.

In the worst breaches, 22% ended up making a public disclosure. It's important to think ahead about the consequences of a breach and how you would disclose it publicly, both for the media and for your impacted customers.

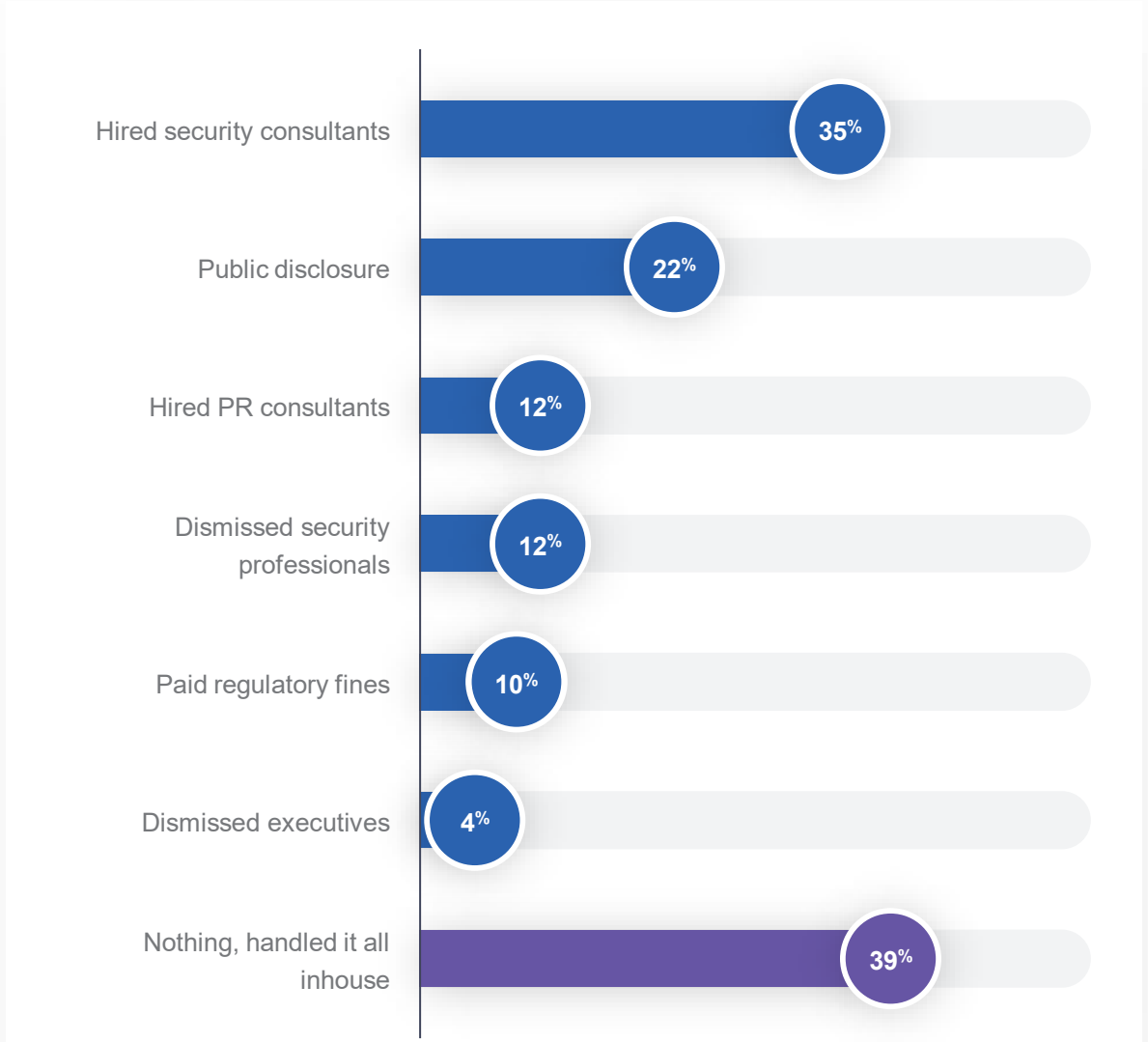


Figure 9 Business Actions Taken Post Worst Breach

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Cyberattacks Prevention, Mitigation & Remediation

The Frequency of Discussions Around Risk Reduction for **Leadership and Cybersecurity Teams**

On average, leadership and cybersecurity teams meet 13 times a year to discuss risk reduction goals.

The more they meet, the lower the chance of breaches. Those who met the most frequently (15 times a year) had no breaches at all, and those who suffered the most (6 or more breaches) met just under 9 times on average per year.

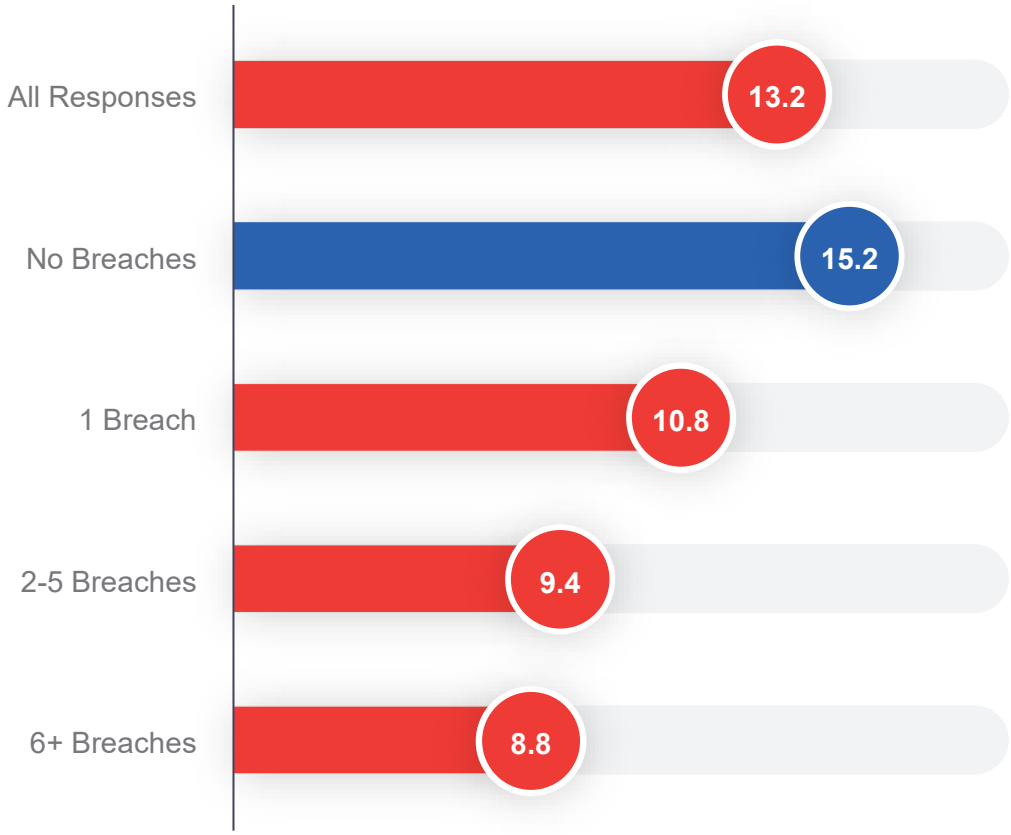


Figure 10 Average Discussions Per Year by Number of Breaches

Executives Awareness of **Cyberattacks**

Awareness is a different metric than involvement in discussions on risk reduction.

On average, executives are aware of 44% of the cyberattacks.

We compared the data on how aware executives are of cyberattacks with the number of breaches respondents experience, and we found an interesting trajectory.

In general, when executives are aware of 75% or more of attacks, the numbers drop, mirroring what we saw with involvement--more executive awareness correlates with better security posture overall.

However, it would appear that it's only as businesses experience a greater number of attacks that executives get more involved, perhaps triggering the reduction in risk as a result of their intervention.

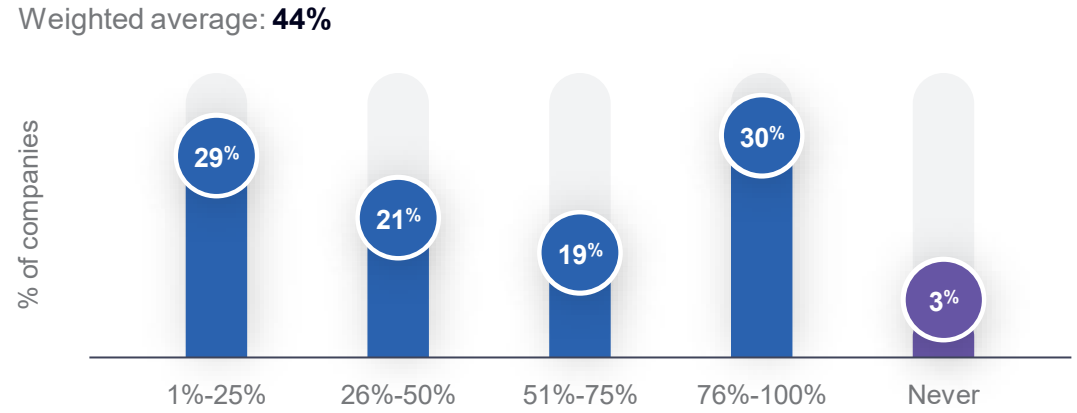


Figure 11 Executives Awareness of Cyberattacks

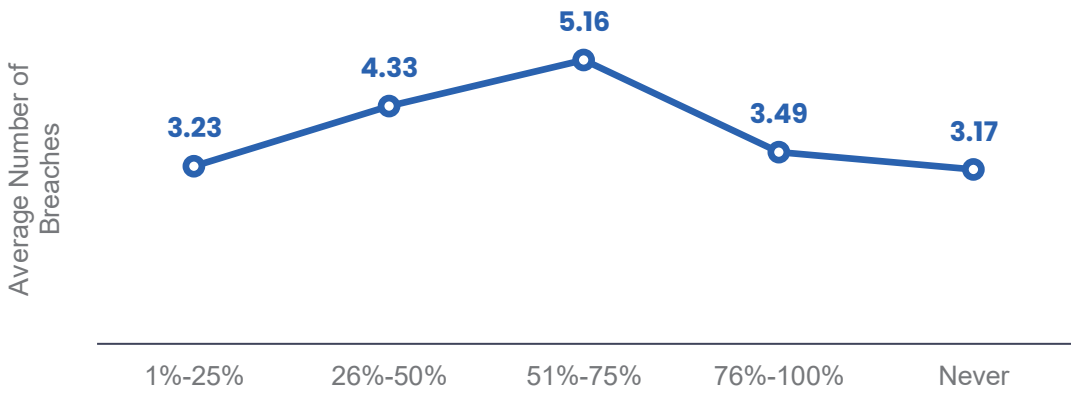


Figure 12 Average Number of Breaches by Executives Awareness

**Percentages do not add up to 100% due to rounding up of numbers*

Top Practices for Cyberattack Prevention, Mitigation & Remediation

What have businesses adopted to deal with the growing risk of cyberattacks? The top 3 practices for cyberattack prevention, mitigation and remediation are the adoption of multi-factor authentication (67%), corporate phishing and awareness campaigns (53%), and well-planned and practiced incident response plans (44%). Least privilege adoption also ranked highly, at 43%.

While traditionally we may have seen reactive measures taking the top spots, these priorities are proactive and show a shift in the mindset of today's security teams. However, it's critical to note that many respondents are still not prioritizing these techniques, with more than half not calling robust incident response a top practice in their environment.

While moving Exchange to the Cloud/Managed and offloading some activities to MSSPs are still good best practices, they seem to be less effective in preventing breaches, as companies who rely on these practices have a higher average number of breaches. In contrast to those companies who follow the top four practices.

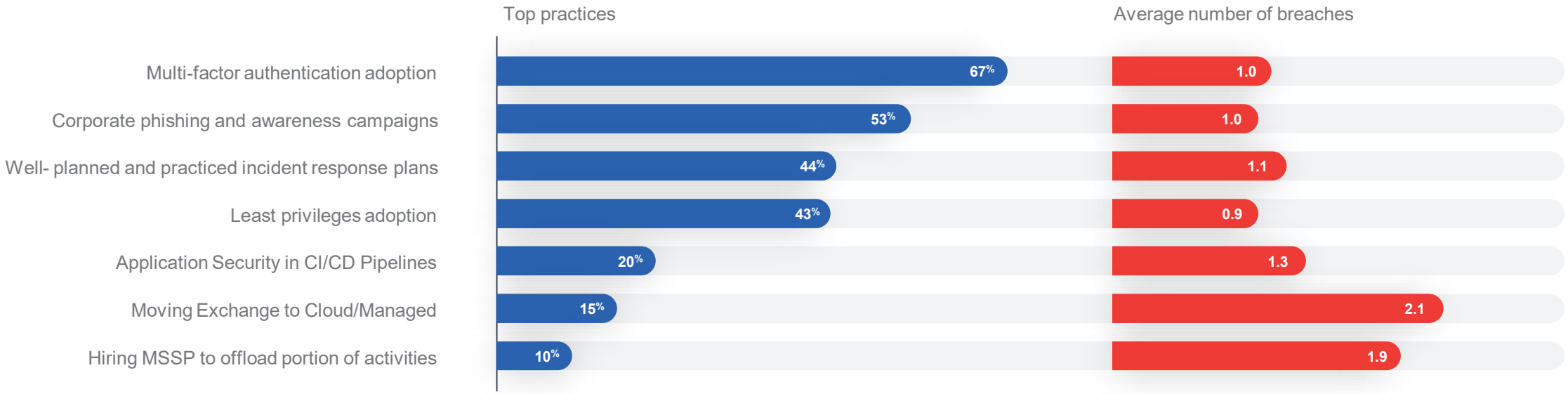


Figure 13 Top Practices for Cyberattack Prevention, Mitigation & Remediation

Top Solutions for Cyberattack Prevention, Mitigation & Remediation

Respondents reported their top solutions for cyberattack prevention, mitigation, and remediation in the following order: web application and API protection (47%), followed by the use of EDR (45%), and Identity Access Management (44%).

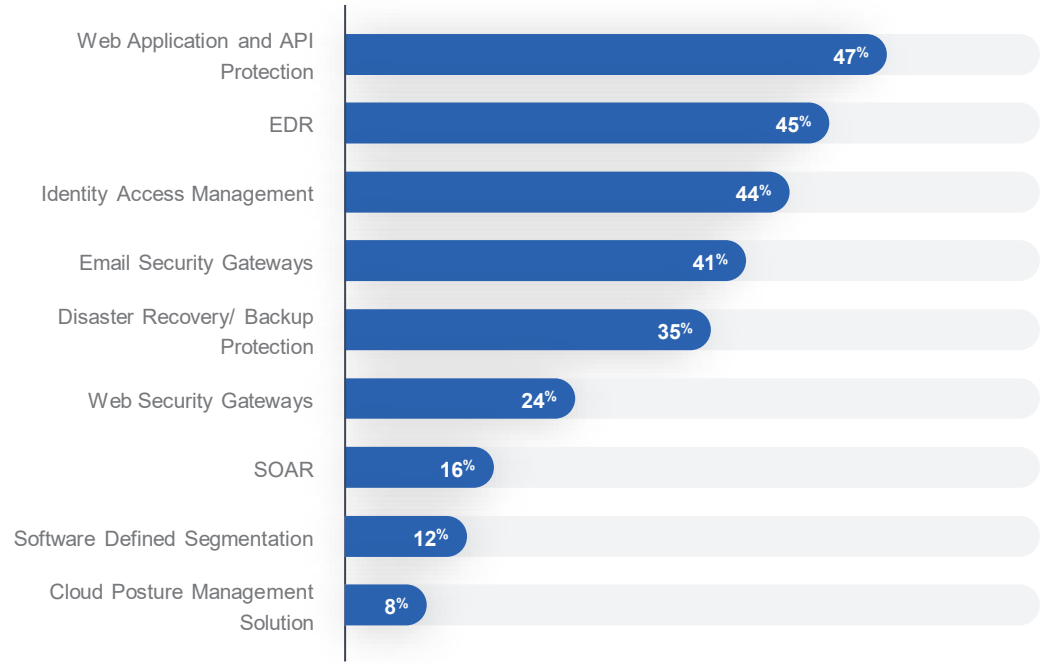


Figure 14 Solutions for Cyberattack Prevention, Mitigation & Remediation

	Average Number of breaches	
	Using	Not Using
Web Application and API Protection	3.8	4.0
EDR	3.3	4.4
Identity Access Management	4.0	3.9

Figure 15 Top 3 Solutions for Cyberattack Prevention, Mitigation & Remediation – Usage Impact on Number of Breaches

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Offensive Testing Techniques **in Use**

When it comes to offensive testing techniques in use, third party pen testing takes the top spot (62%), following by in-house pen testing / red team (59%), and attack surface management (53%). We're seeing another shift in the market, where more than half of respondents are utilizing at least one offensive testing technique, including emerging techniques like attack surface management and purple teaming.

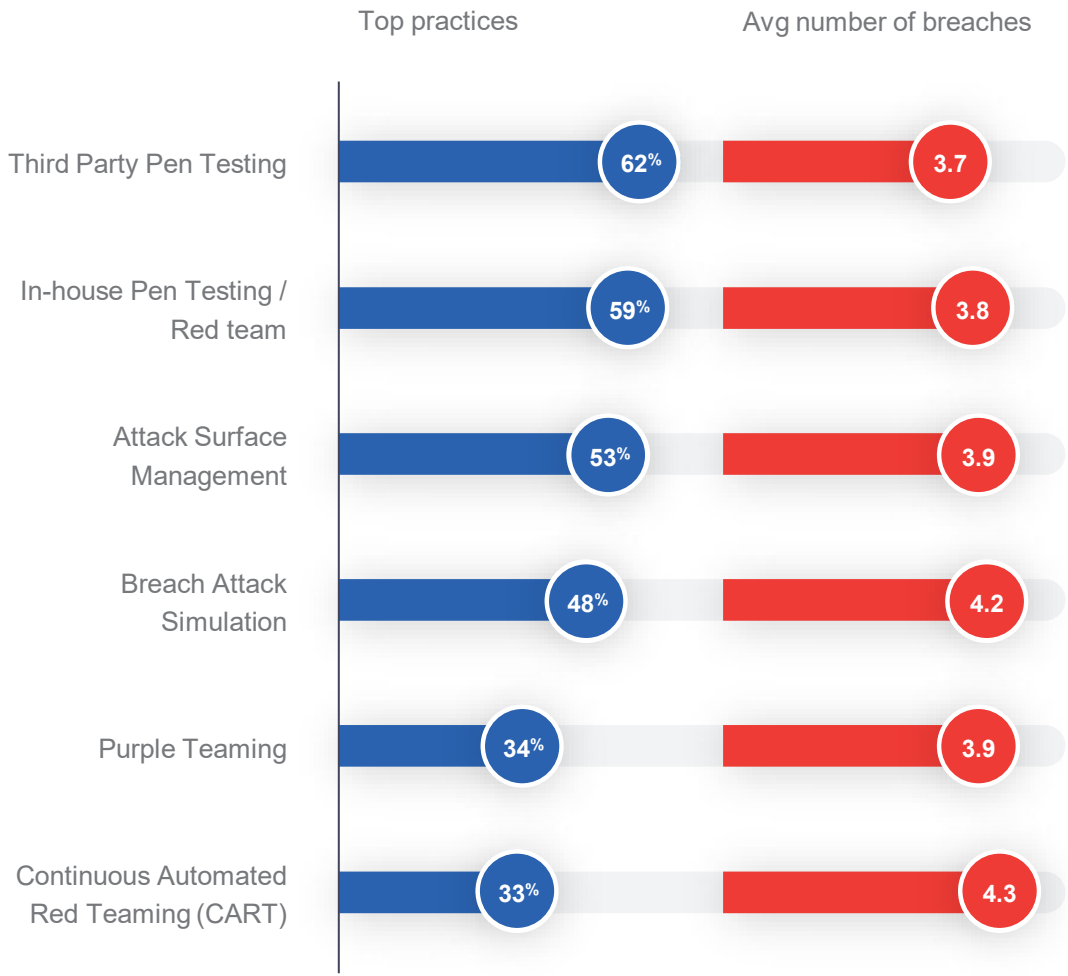


Figure 16 Offensive Testing Techniques in Use

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Demographics

Company Size, **Job Role & Seniority**

Weighted average: **13,654 employees**

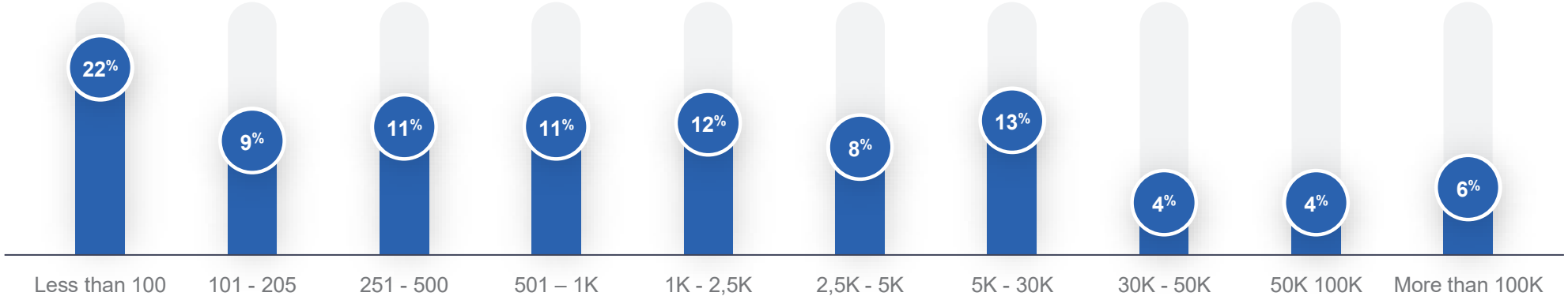


Figure 17 Company Size (Employees)

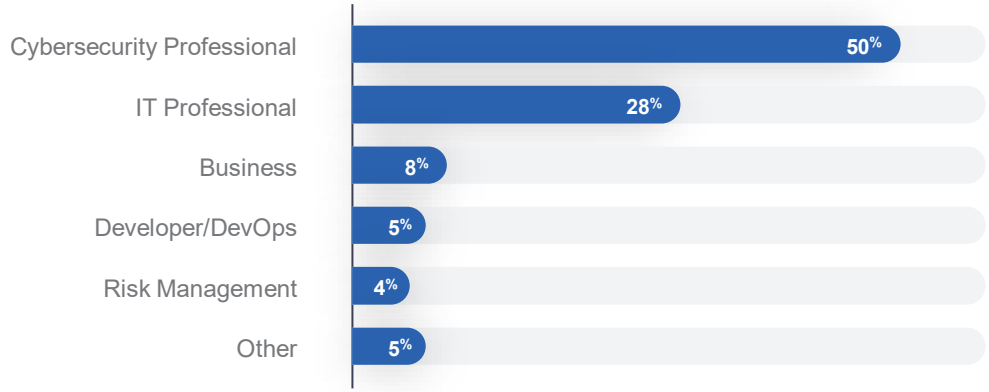


Figure 18 Role

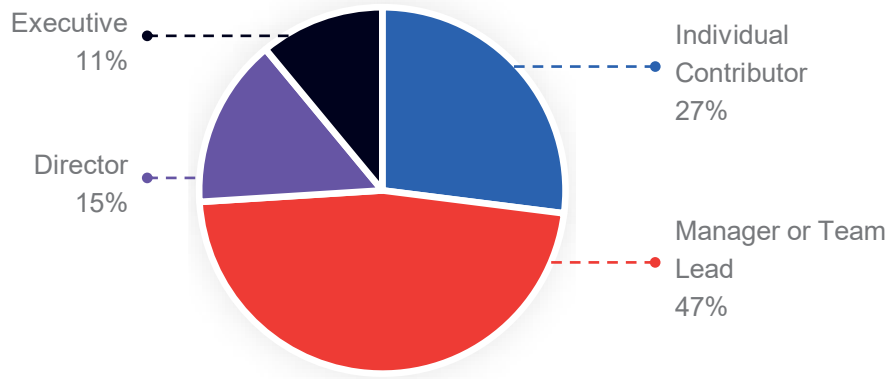


Figure 19 Seniority

Industry, Level of **Engagement & Country**

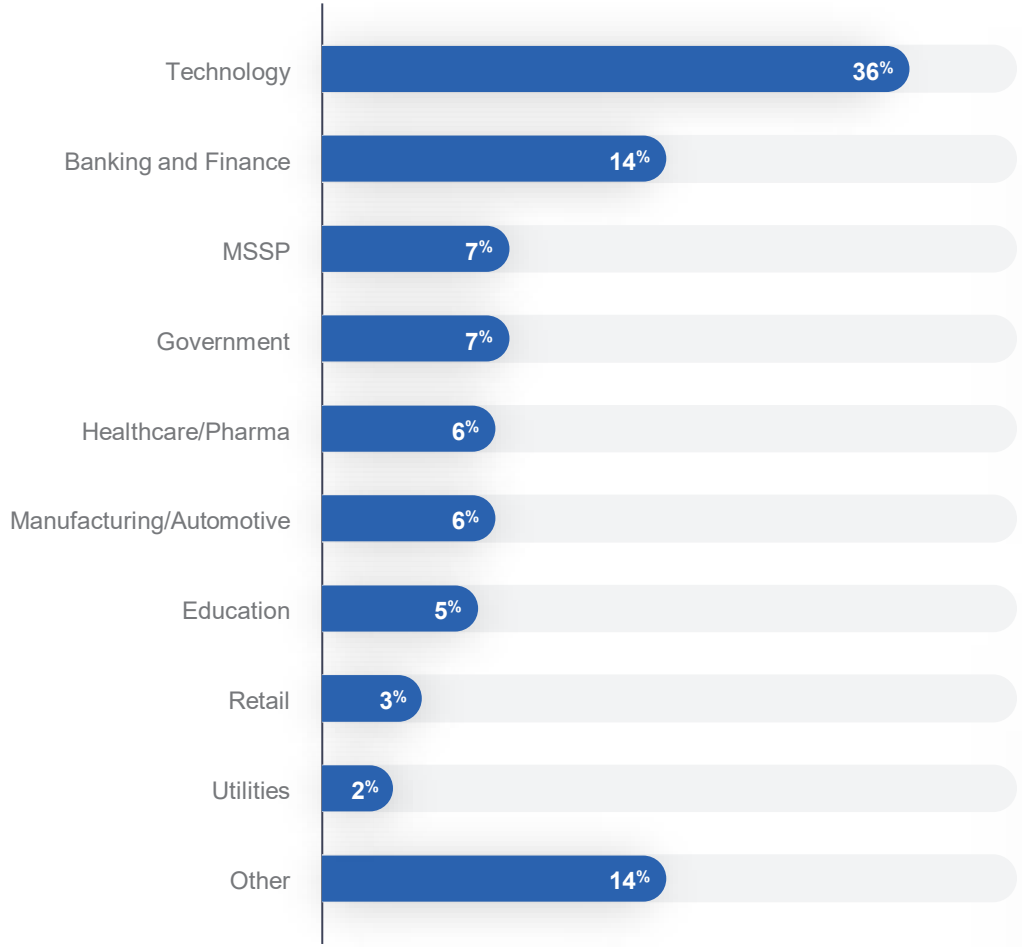


Figure 20 Industry

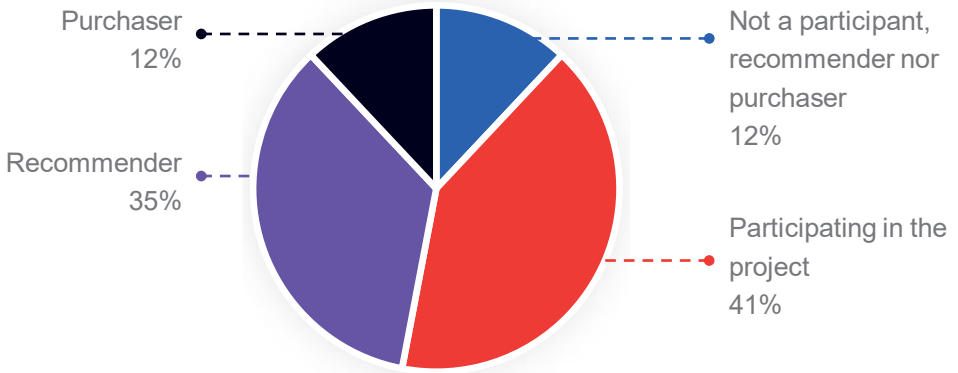


Figure 21 Level of Engagement

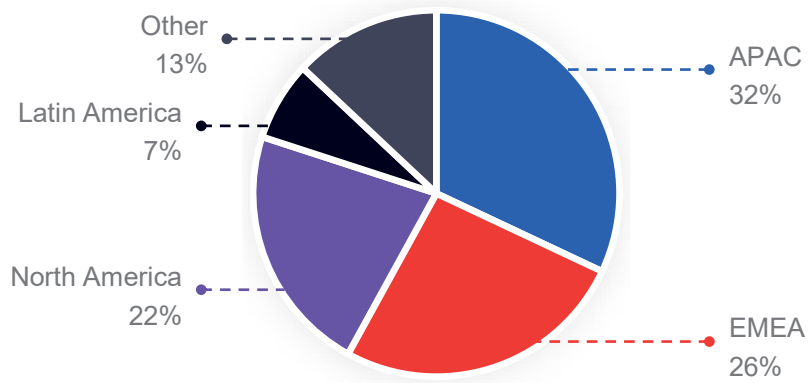


Figure 22 Country

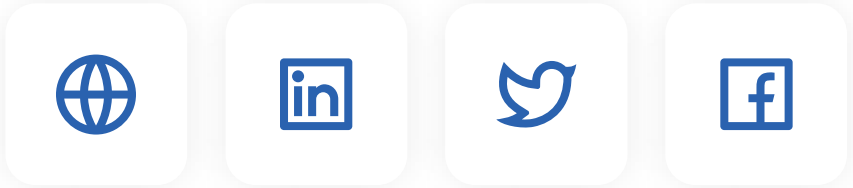
About **Cymulate**

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.

Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Uncover cybersecurity posture loopholes now

For more information, please visit us:



+44-134-4959736

info@cymulate.com