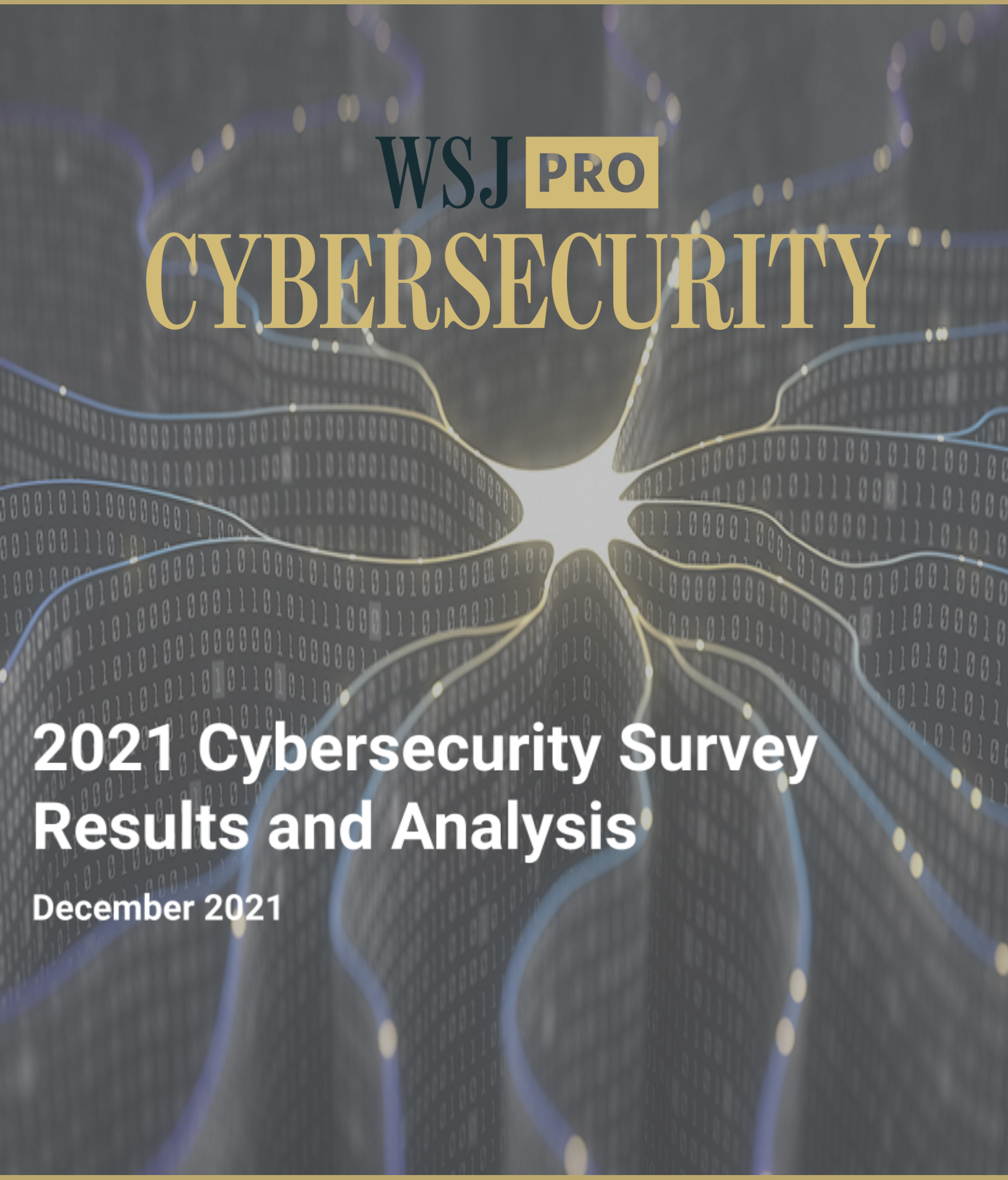


WSJ PRO

CYBERSECURITY

2021 Cybersecurity Survey Results and Analysis

December 2021

Introduction

WSJ Pro Cybersecurity conducted its 2021 survey through the lens of cybersecurity as a business risk issue. We asked respondents about a number of key cybersecurity challenges, including hiring talent, team diversity, governance and preparedness, to understand where gains have been made and where gaps remain.

Our findings show an uphill struggle: relentless threats, resource shortages and a lack of skills. Teams have been further stretched by the shift to hybrid or fully remote working and a range of new risks to manage. There are no short-term solutions and organizations will need to plan strategically to ensure they can keep data secure.

Cybersecurity leaders and their teams will need to be flexible and pre-empt or respond to changes while supporting the wider information technology effort to implement new software and digitized processes securely.

Key Findings

- **Threats** - Criminal hackers were cited as the top threat for most businesses, likely as a result of continued cybercrime. In contrast to 2020, our data shows a reduced willingness and increased uncertainty about whether to pay a ransom.

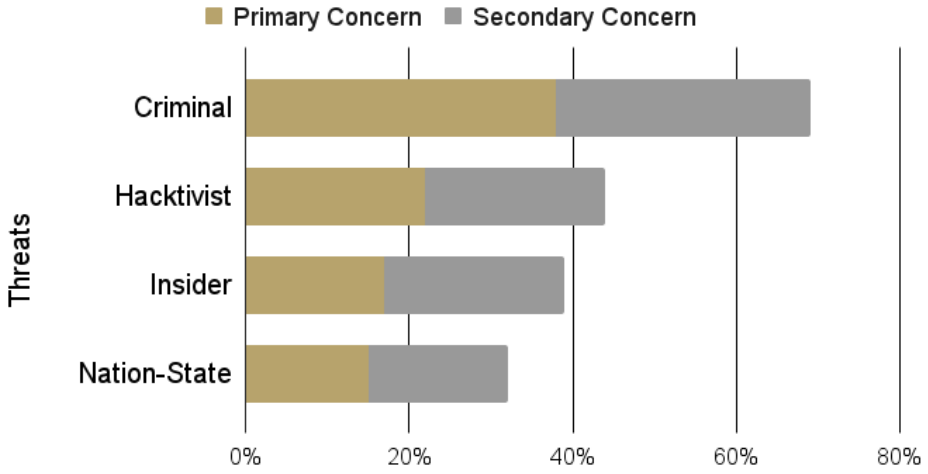
- **Talent and Diversity** - Almost half of businesses reported finding hiring cybersecurity talent more difficult. Larger firms in particular have attempted to increase diversity in cyber teams by targeting female recruits and people of color.

- **Remote work** - Securing employees while working remotely was a challenge for two-thirds of respondents, and this pressure on cybersecurity teams was compounded for around a quarter of firms that reported seeing a rise in attacks.

- **Governance** - Despite the prominence of the chief information security officer role generally, only 17% of respondents reported having a CISO in charge of cybersecurity. Many small businesses stated their chief executive or founder led cyber efforts, leading to concerns best practices may not always be followed.

- **Preparedness** - Levels of preparedness have improved over the last 12 months, but smaller businesses still lag behind larger firms. In particular, the uptake of cyber insurance coverage among respondents rose significantly since 2020.

Threat Perception



Concern for hacktivism is rising while fear of nation-state hacking remains low

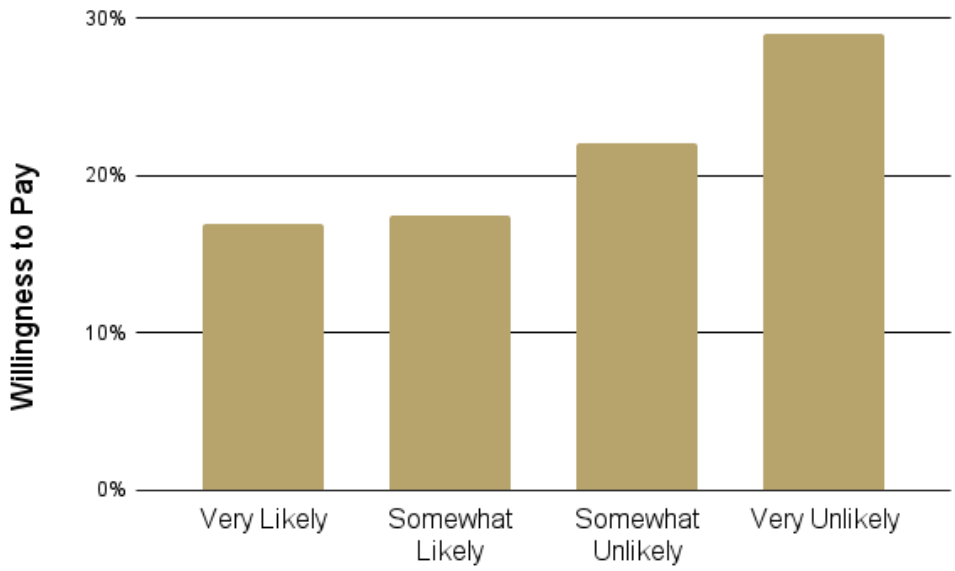
Survey respondents stated they were most concerned by the criminal cyber threat, perhaps unsurprisingly after another year of high-profile multi-faceted extortion (ransomware) attacks. 69% said the criminal threat was their top or secondary concern.

Hacktivists followed, well behind criminals, but ahead of insiders by a slight margin, in a reversal of positions from the 2020 survey. We had not expected to see a rise in fear of cause-driven attacks, though politically and environmentally motivated hacking is an ever-present threat, especially for larger companies.

The insider threat remained fairly constant across all organizations, but the perception of the threat may have decreased due to employees working from home and having less access to company resources. There have also been fewer widely reported incidents attributed to corporate insiders over the last 12 months, which may also have influenced the results.

Despite attacks that drew worldwide attention in 2020, including the compromise of hundreds of SolarWinds customers and thousands of Microsoft Exchange customers, the concern for the nation-state threat remained relatively low at 32%, with smaller companies the least concerned at 25%. While nation-state attacks are typically focused on larger companies, smaller companies holding valuable intellectual property or those supplying larger customers should carefully assess whether they may in fact be targeted.

Paying Ransoms



Less willingness to pay, less certain of strategy

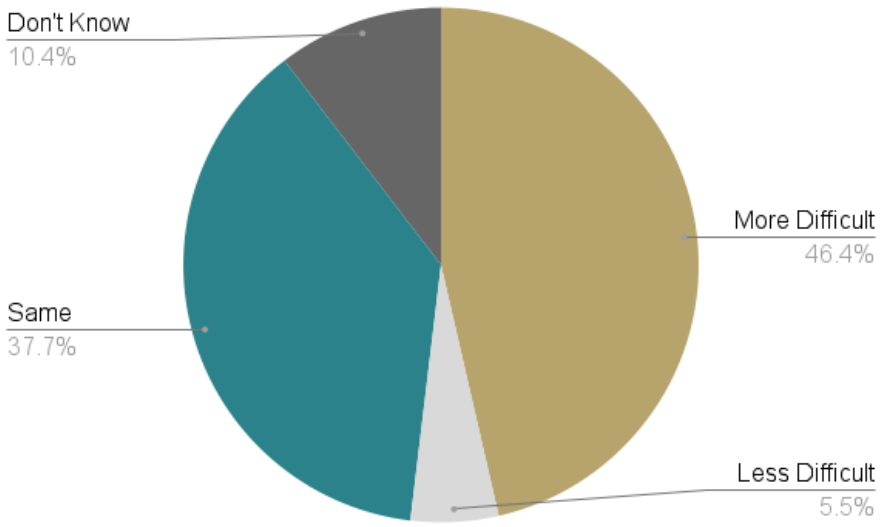
The scourge of ransomware -- or more accurately -- 'multi-faceted extortion attacks', continued throughout 2021 with attacks across industries and affecting organizations large and small.

Approximately one-third of respondents said they were 'very likely' or 'somewhat likely' to pay a ransom if they found themselves in that circumstance, while a slight majority, 51%, said they were 'very unlikely' or 'somewhat unlikely' to pay. The difference between those choices grew compared to the 2020 survey. Fewer organizations were willing to say they would likely pay a ransom than last year, perhaps as a result of either the uncertainty around regulations designed to reduce payments to certain attackers or the reputational damage suffered by those organizations that chose to pay ransoms.

The willingness to pay a ransom can be complicated by the fact that some companies pay ransoms not simply to get decryption keys that allow access to data to be restored, but to discourage attackers from publishing corporate data stolen by the attackers as extra leverage.

Across all respondents, 87% said they had taken specific steps to reduce the risk of being a victim of a ransomware attack, with minimal differences between businesses of different sizes.

Hiring Talent Remains a Challenge



The cybersecurity talent and skills shortage continues

Almost half of all organizations in our survey, and 56% of large businesses, have found it more difficult to hire skilled cybersecurity talent recently than 12 months ago. Only 5% of mainly mid-sized companies have found it easier. Perhaps because the majority of organizations have not embraced a shift to fully remote work, competing for labor in geographies adjacent to existing business locations means access to a restricted talent pool in high demand.

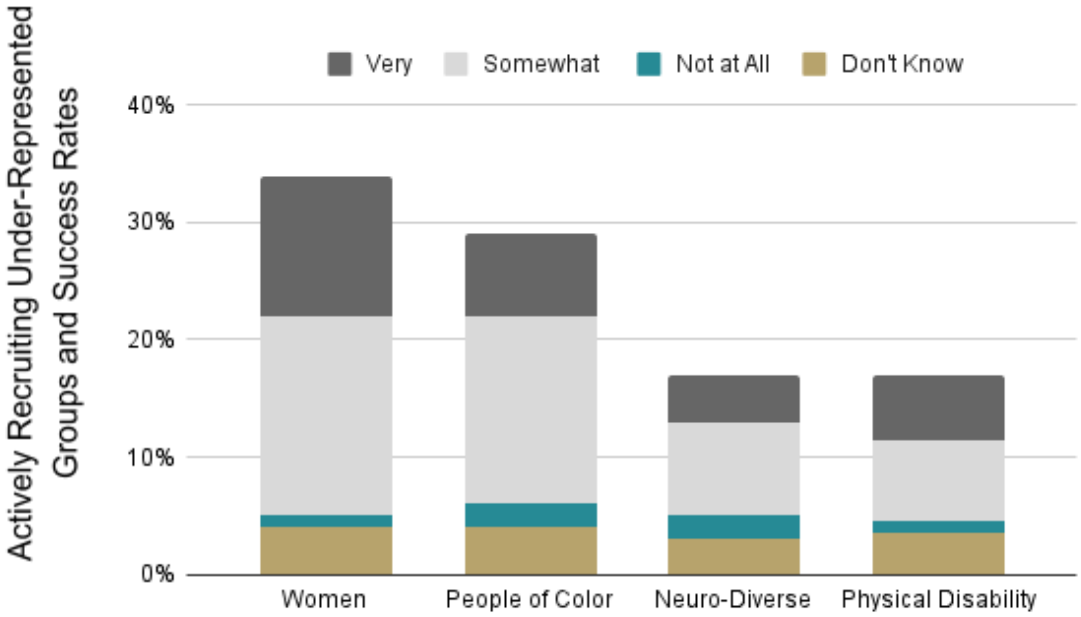
In addition to hiring struggles, 31% of our respondents said they have unfilled vacancies in their cybersecurity team, including 38% of large companies and 26% of small companies, while one third of large companies are dealing with a lack of specific skills in their team. The problem may affect smaller businesses to a lesser extent because of their greater reliance on outsourced security and managed service providers: 46% of companies with less than $50 million annual revenue rely on third parties rather than in-house personnel to protect networks and data.

31%

of companies encounter job applicants with unrealistic salary expectations

The issues companies have faced in bolstering their cybersecurity teams include: a general lack of available talent (58%); unrealistic salary expectations (31%); an unwillingness to relocate (19%); a lack of experience (44%) and a lack of specific tools/software expertise (27%).

Increased Cybersecurity Talent Diversity



Efforts to recruit from under-represented groups were largely successful

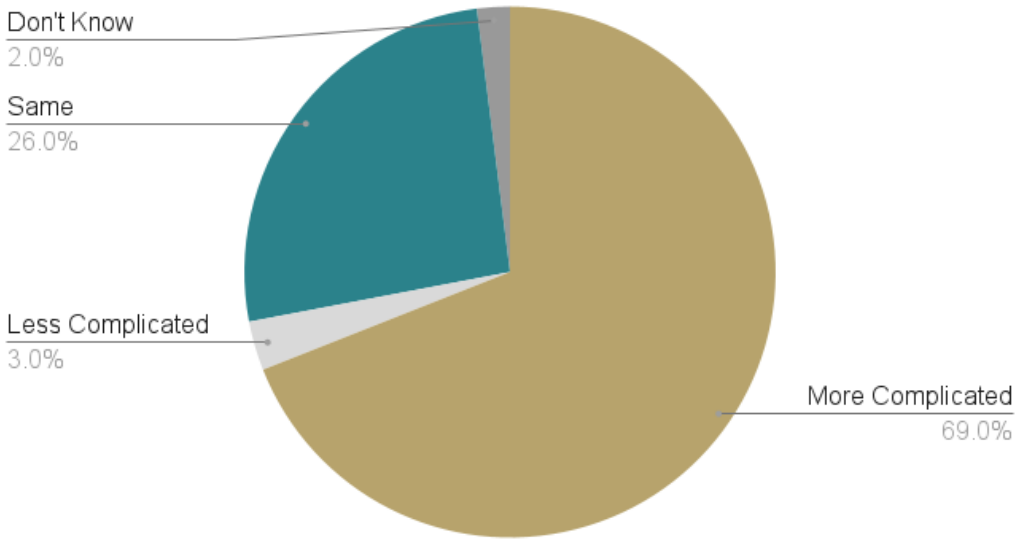
Cybersecurity is a profession historically dominated by men and few companies have traditionally cultivated diverse talent. Our survey results showed not only that companies of all sizes are trying to increase diversity in their cybersecurity teams, but that efforts to recruit from under-represented groups are proving successful.

More than a third of respondents (35%) have proactively tried to recruit female cyber professionals and around 29% have tried to actively recruit people of color. These efforts are in line with the number of companies that have actively tried to recruit veterans (31%), which has traditionally been a strong source of cyber talent. Less developed have been efforts to recruit neuro-diverse cyber professionals (17%) or professionals with a physical disability (16%).

While initiatives to increase the diversity of teams took place in companies of all sizes, large companies led the way in each of the categories, including 53% of large companies actively seeking to recruit female cyber professionals and 44% actively seeking to recruit cyber professionals of color.

The outcome of efforts to recruit from under-represented groups was positive. 84% of companies that targeted female recruits and 77% of companies that targeted people of color reported being ‘very’ or ‘somewhat successful’.

The Challenge of Securing Remote Workers



Corporate cybersecurity became much more complicated during the pandemic

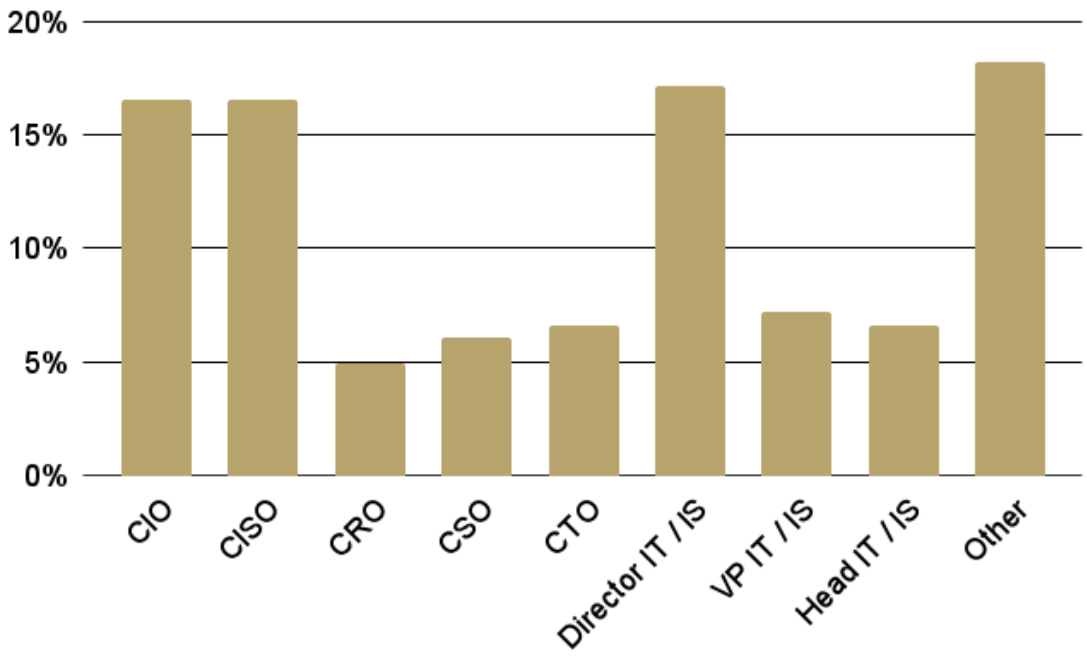
More than two thirds of survey respondents claimed the job of securing employees became more complicated during the pandemic due primarily to the complications of securing remote and hybrid staff. Twenty-six percent said the task was the same, while only 3% said the task had become easier.

Despite warnings about an increase in the number of cyber attacks, 57% of companies saw no change over previous years.

Those businesses that intend to operate on 'work from home' or 'hybrid' models for the longer-term will need to be conscious of the additional work required by their cyber teams to keep data secure, though much of the complication likely came from the initial rapid shift to remote working before normalizing over time.

A further complication for 26% of companies was an increase in the number of attacks that required a response. However, despite warnings throughout 2020 of a significant rise in the number of cyber attacks targeting home workers, 57% of our respondents stated they had noted a similar level of incidents to previous years and a small number of small and mid-sized companies even saw fewer attacks.

Executive Leadership of Cybersecurity



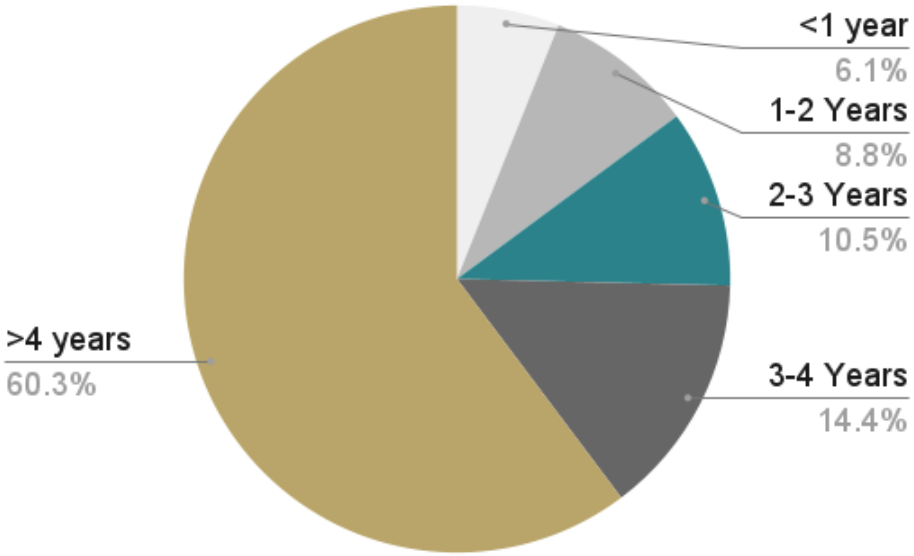
The executive in charge of cybersecurity varies widely by business size

Across all survey responses, we found an equal number of businesses with the chief information officer and CISO in charge of cybersecurity, 17% for each. Other businesses had the chief risk officer, chief security officer, chief technology officer or an executive from outside the c-suite in charge. The model varied widely and there appears to be no single approach that works for a majority of companies.

Large organizations were slightly more likely to have a CISO or CIO in charge -- 22% and 24% respectively, and 31% of public companies assigned cybersecurity responsibility to the CISO. Only 5% of small companies had a CISO in charge.

While arguments can be made for different executives owning cybersecurity, it is harder to justify the role being held by an executive from outside the information technology or information security arena. However, 44% of small businesses have the chief executive officer, chief operating officer, founder or a professional from outside the technology, security or risk function as the cybersecurity leader. This governance decision may leave them dangerously exposed to technical risks and threats that disproportionately affect small businesses.

The Cybersecurity Leader's Tenure



The CISO's tenure has extended during the pandemic

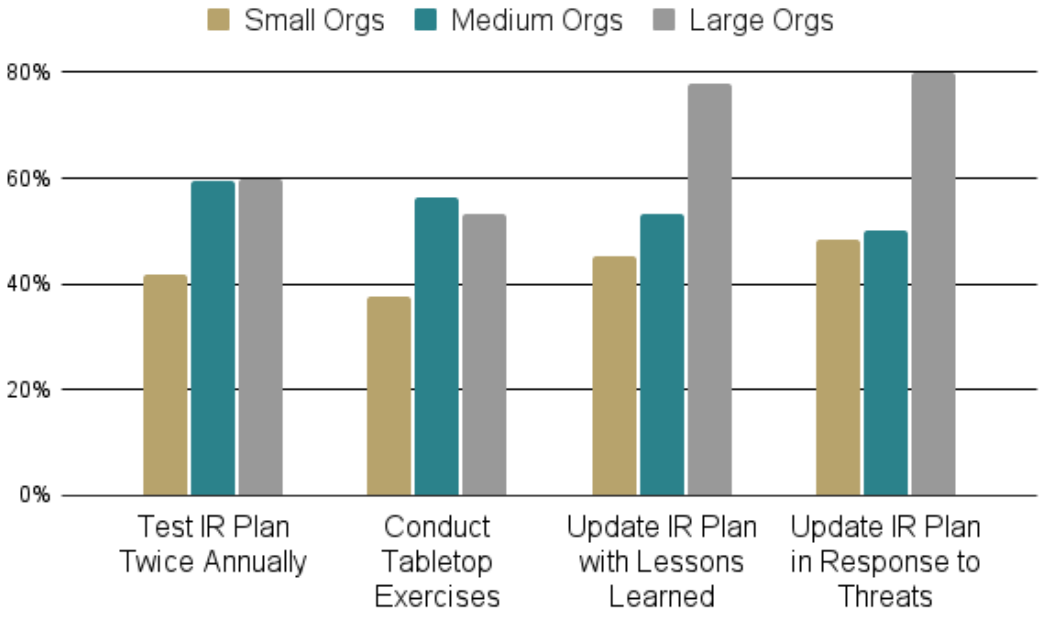
The common assumption is that cyber leaders have short tenures due to better job offers, an overload of stress or leaving in the aftermath of a breach, but the data suggests this is not the case.

Three-quarters of respondents in charge of cybersecurity at their organization reported having been in their role for at least three years and 60% reported being in their role for more than four years. Only 6% said they had been in their role for less than one year.

With regards specifically to CISOs, the data shows 53% of CISOs have held their role for at least three years and almost a quarter had been in their role for over four years. For CIOs the tenure is longer still: a resounding 80% of CIOs have been in their roles for more than three years and 70% have been in their roles for more than four years.

The pandemic may well be the reason why CISOs have stayed longer in their roles than expected. Many will have chosen stability and continuity over the uncertainty of joining a new company and potentially having to work remotely without face-to-face contact with the executive team and the cyber team. If that is the case, as companies bring employees back to offices we may soon start to see an above-average turnover of security executives who decide a move may be overdue.

Cyber Incident Response Preparedness



Small businesses lag in preparing for incidents

It has long been said that *it's not a matter of if, it's a matter of when*. If that is the case, many smaller businesses did not get the message. There is often a wide gap between preparations by small businesses and those made by larger organizations.

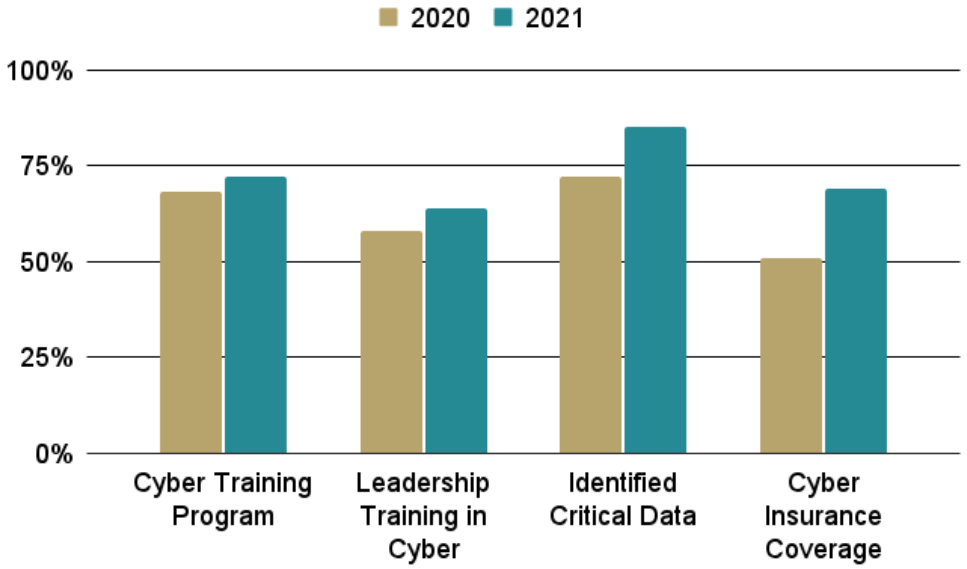
Only 22% of businesses said they were 'fully prepared' for cyber attacks, with a further 41% stating they were 'somewhat prepared'. Large businesses were more likely to update their incident response plans on an ongoing basis as a result of lessons learned or due to specific threats. Sixty percent of large businesses tested their plans at least twice annually in comparison to only 42% of small businesses. Large businesses were also more likely to conduct tabletop exercises, though mid-sized businesses led this activity with 55%.

Particularly concerning is that 18% of small businesses reported not updating or testing their incident response plan at all. While a reliance on third parties and a lack of expertise doubtless plays a role, the simple steps involved in developing and improving an incident response plan can have a significant impact in minimizing the effects of a breach.

63%

of firms consider themselves 'fully' or 'somewhat' prepared for cyber attacks

Cyber Risk Reduction Measures



Positive progress in cyber risk preparedness categories

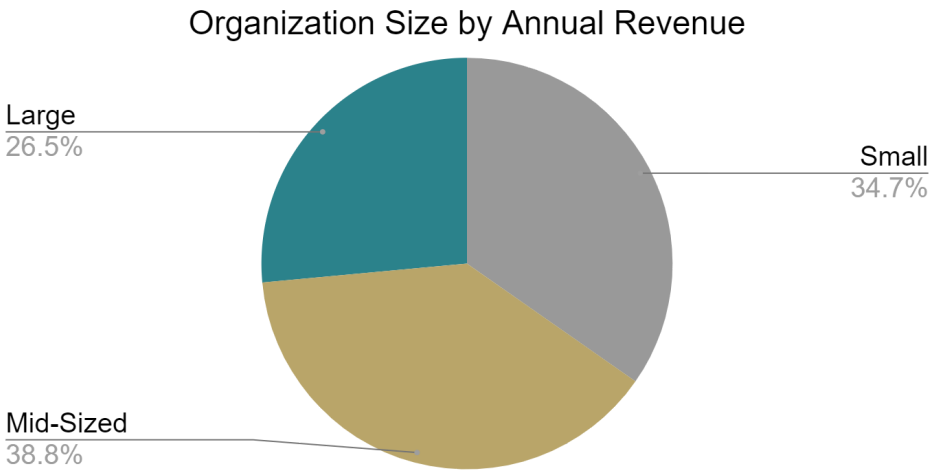
The year-over-year results show a rise in the number of companies taking steps in 2021 to reduce cyber risk in key areas in comparison to the previous year. Increases have been across the board for all company sizes.

Identifying and protecting critical data and intellectual property is the category where companies reported being most prepared, with 85% of all businesses saying they conducted this exercise. The data shows no significant difference between small, mid-sized and large companies.

Businesses also continued to exhibit a commitment to delivering cybersecurity awareness training to staff (72%, a rise of 4% over 2020) and more tailored training to executives (64%, a rise of 6% over 2020).

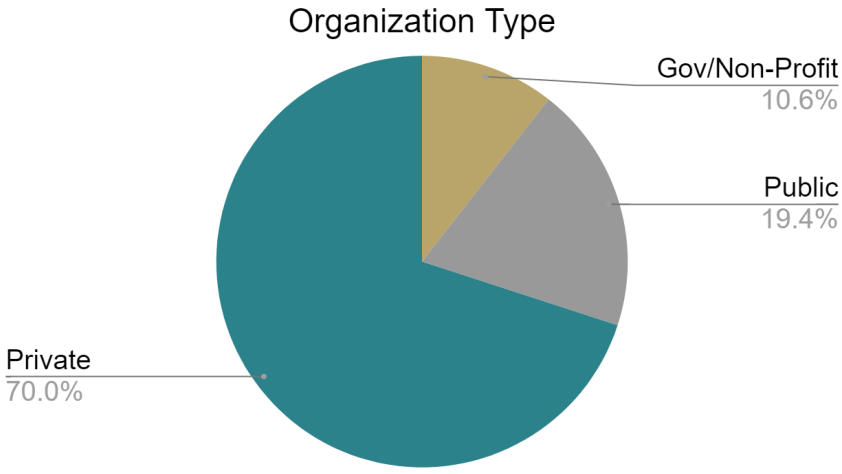
The most significant increases though came in the area of cyber insurance coverage. Sixty-nine percent of surveyed organizations, including three-quarters of mid-sized and large businesses and 52% of small businesses, have insurance coverage for cyber risks. In 2020, the survey data showed only 51% of businesses of all sizes had cyber insurance. The number of recent high-profile ransomware cases may well have been a driving factor that spurred many businesses to take this step.

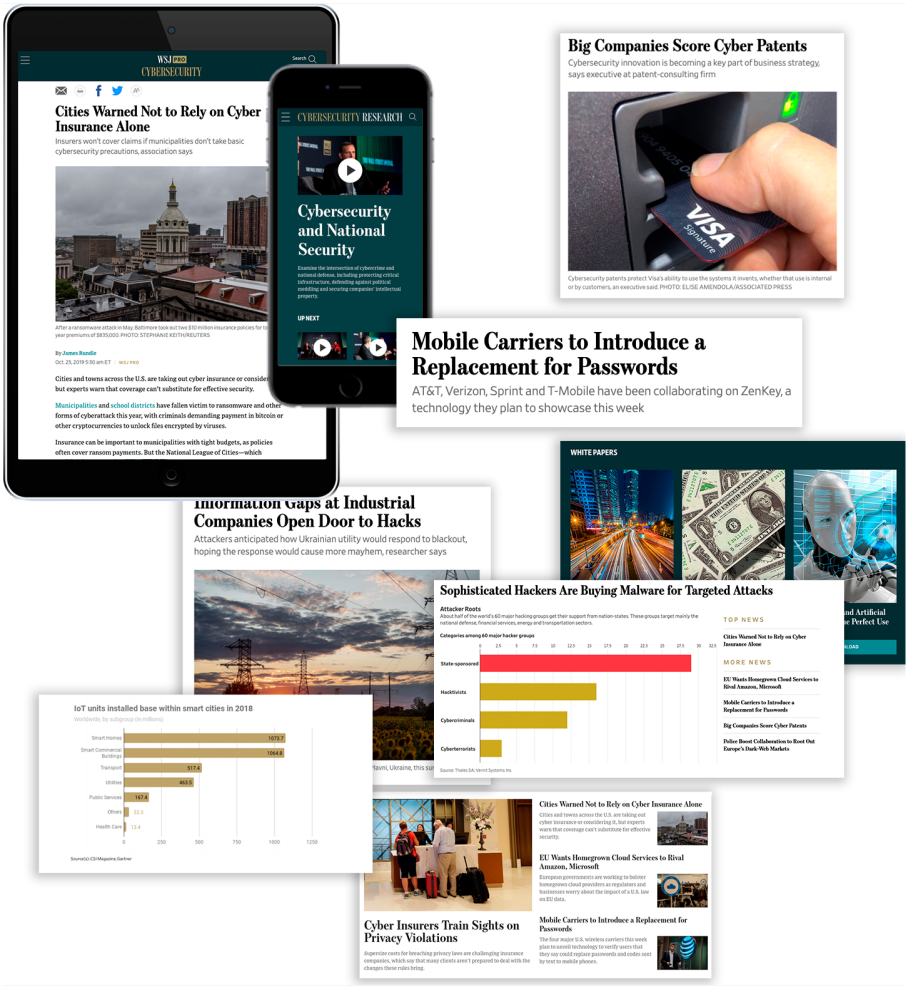
Respondent Profile and Methodology



Cybersecurity practitioners and officials familiar with their organization's cybersecurity program were surveyed to gain insights on current practices and attitudes regarding key cyber categories including threats, talent, governance, preparedness and employees returning to the workplace.

One hundred and eighty-three responses were submitted between August and October 2021. The results were analyzed according to organization size, with the small category covering businesses with less than $50 million in annual revenue, medium between $50 million and $1 billion, and large more than $1 billion in annual revenue. Seventy percent of the respondents are privately held, 19% are publicly listed and the rest comprises government entities and non-profit organizations.





For the latest cybersecurity news, research and data, please visit us at: www.wsj.com/pro/cybersecurity

Meet The Authors

Rob Sloan is research director at WSJ Pro focusing on providing thought leadership, building datasets and contributing to the WSJ Pro Cybersecurity product suite. Contact Rob at rob.sloan@wsj.com

David Breg is deputy research director at WSJ Pro, focused on providing actionable intelligence for readers interested in learning about issues involving cybersecurity through white papers and other research activities. Contact David at david.breg@wsj.com