CyberRisk Alliance | Business Intelligence Resources

THE PANDEMIC AS CATALYST FOR CHANGE

Seizing the Moment as Covid-19 Provokes a Reset for Cybersecurity Professionals and Decision-Makers

FULL REPORT

A Voice & Vision Research Study

CRA Business Intelligence
CyberRisk Alliance | Summer 2020

CONTENTS

INTRODUCTION

This study looks beyond the post-pandemic threat landscape, focusing instead on the pandemic's implications for cybersecurity as a profession and organizational function.

In the weeks after Covid-19 was declared a pandemic in the U.S., a consensus quickly emerged that the outbreak had significantly raised the global community's cyber risk profile — by forcing a massive shift to less-secure home-based workforces, sparking a rise in exploits that preyed on pandemic-related fears and emotions, and expanding attack surfaces in sectors like healthcare, banking and food distribution.

This study looks beyond the post-pandemic threat landscape, focusing instead on the pandemic's many significant implications for cybersecurity as a profession and organizational function.

What role did cyber-professionals play in the pandemic response? How did Covid-19 change cybersecurity's status and influence within and among businesses and organizations? How will it change their future approach to information risk management? And more.

With six pandemic months now past and more ahead, the cybersecurity industry, like many others, must assess its place in a reordered world. This study begins that process.

OVERVIEW & METHODOLOGY

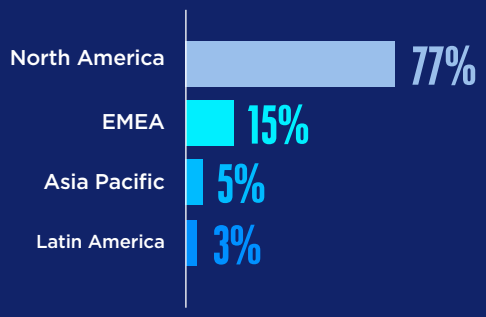
This report draws on data and insights from a proprietary survey of cybersecurity professionals conducted by CyberRisk Alliance (CRA) among 278 respondents from April 30 to June 3, 2020. Survey participants were randomly selected from CRA's active community of cybersecurity, IT and business professionals focused on cybersecurity strategy and operations at organizations across sectors. (As a result, this study does not reflect the status of cybersecurity in the general business population.)

The survey draws its power from the breadth and depth of its reach into the ranks of working cybersecurity leaders and practitioners. Moreover, the respondent base was highly engaged, providing extensive verbatim commentary to augment their questionnaire responses, and 69 respondents (one in four respondents) offered to participate in confidential follow-up interviews.

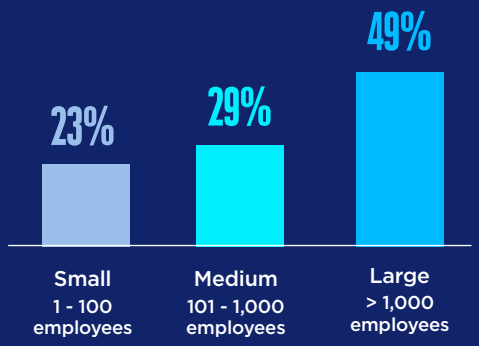
RESPONDENT PROFILE

ORGANIZATIONS

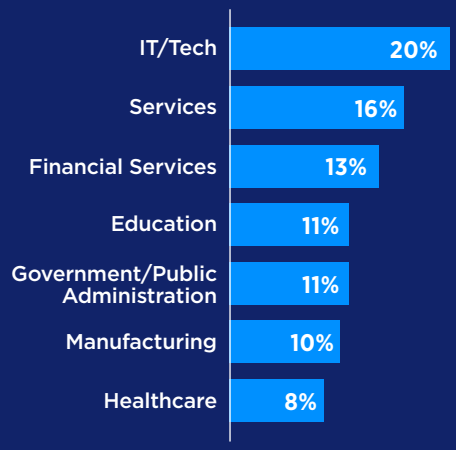
ORGANIZATION LOCATION



ORGANIZATION SIZE

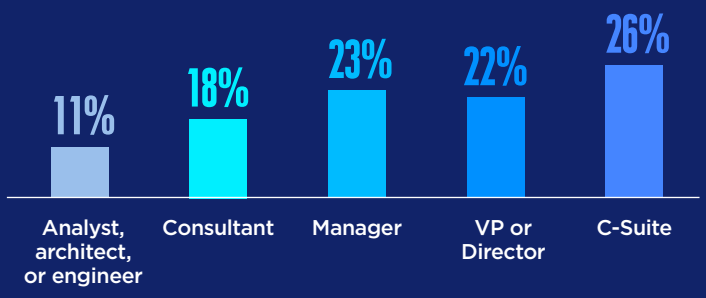


TOP INDUSTRIES

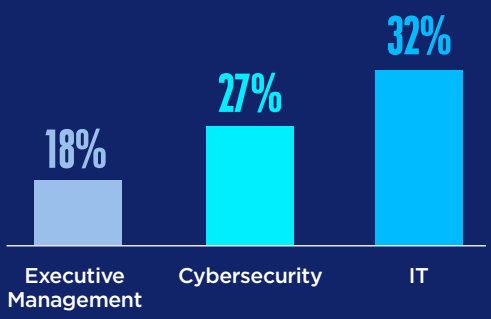


PEOPLE

TITLE/ LEVEL

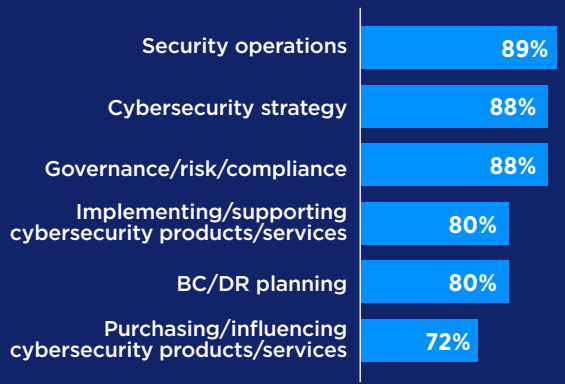


TOP PRIMARY FUNCTIONS



CYBERSECURITY FOCUS

(% of respondents with High or Moderate Focus)



NEW RESPECT FOR CYBER PROFESSIONALS?

> **The overall implication will be that cybersecurity is valued at a higher level and has a better voice within the overall organization.**
>
> **— Head of Technology & CISO**

Before the pandemic's onset on March 11, 2020, only 4% of respondents believed their organization was not at least somewhat focused on cybersecurity. Yet cyber professionals have long worried about marginalization, and even disregard, by leaders and others in their organizations. Far too often, security takes a backseat to short-term profit goals, convenience, and a host of other priorities. Senior executives often boost security in public statements but disregard their own company's email policies. Insisting on security best practices, cyber professionals are viewed as impediments to quickly implementing customer-facing IT projects.

To be sure, many organizations ascribe high value to their cybersecurity teams, but the Covid-19 pandemic is shaping up to be a turning point for the profession as a whole. Despite concerns that attention to cybersecurity would lessen owing to extenuating circumstances, 61% of respondents said their organization strengthened its focus on cybersecurity because of the pandemic compared to 7% relaxing its focus.

More compellingly, two out of three respondents believe the pandemic contributed to a shift in cybersecurity professionals' positive perception ("appreciated and valued") within their organization. The new appreciation can be attributed to security awareness that surged along with the remote workforce. An IT staff member commented that security awareness was driven by an outbreak of pandemic-specific phishing emails and web pages designed to bait and compromise users and their system.

Highly publicized Zoom-bombing incidents and other issues with the video conferencing services gave security more immediacy and relevance to more people. As another respondent put it: "Because the general population has had to function in an IT-like role, I think they will get smarter about cybersecurity in general."

A CISO at a cybersecurity vendor summed it up as follows: "There is more appreciation for the fact that we have implemented the securi-

Pain is related to how quickly pandemic-related cybersecurity security practices, policies, and tools had to be put in place. We had to rapidly change sign-on processes since we did not have people that regularly worked from home and almost 50% of our workforce used desktops.

— Chief Risk Officer

ty practices, policies, and tools from the broad leadership group in the organization.... I believe that the overall implication will be that cybersecurity is valued at a higher level and has a better voice within the overall organization."

Another driver of increased appreciation for cybersecurity teams and programs has been their perceived success in addressing the business-critical situations that emerged with the pandemic. Almost three-quarters (74%) of respondents (spanning management, IT and cybersecurity per se) said their organization's response was timely compared to its peers. Many attributed that success to advance preparation going back years — years in which they were likely subject to the resistance and skepticism typical of many organizations.

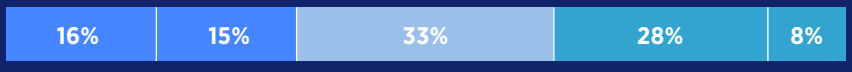
Cybersecurity's time in the pandemic's spotlight has also had adverse effects. Nearly half of all respondents said stress and burnout among cybersecurity staff has been an issue throughout the crisis, likely associated with extended hours getting VPNs and other infrastructure set up for remote workers. For smaller organizations, this becomes a longer-term problem when the same department handles identity management and other functions often handled by IT operations and help desk teams.

Despite turmoil, the pandemic leads to increased appreciation for cybersecurity professionals.

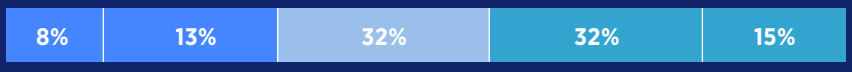
How much do you agree or disagree with each statement about the pandemic's impact on your organization?

STRONGLY DISAGREE | DISAGREE | NEUTRAL | AGREE | STRONGLY AGREE

The cybersecurity role or function is appreciated or valued at my organization



My role or responsibilities have or will materially change as a result of the pandemic



The pandemic has increased stress and burnout among the cybersecurity staff at my organization

After weathering the first wave of the pandemic, only 10% had increased cybersecurity's roles and responsibilities, and 20% said it was not in their plans through the rest of 2020. Longer-term, respondents were more likely than not to believe their roles and responsibilities would materially change because of the pandemic.

When cybersecurity roles change, there is a danger that any increase in appreciation will be rewarded with more work. Cybersecurity stepped up to the plate during the crisis. Will the rest of the company return the favor when they need additional funds to hire more staff?

Lessons and Recommendations

The pandemic has left many cybersecurity leaders and their teams with significant political capital. We recommend they spend it. Take the initiative by creating a revised plan and framework for your organization that takes into account the pandemic's learnings. Consider closely tying it to business continuity / disaster recovery. Assume the need for a permanent and ubiquitous remote workforce. Rethink your approach to security awareness training based on your organization's performance. Anticipate increased responsibilities for the cybersecurity team and seek investment to support it.

LIONS, SHEEP AND GOATS

> **We had remote access capability in place with MFA and leading email and web filtering systems. We brought forward a remote access phase that was in testing. The transition to work-at-home was not painless but it has been successful.**
>
> **— Cybersecurity professional at a governmental organization**

At a high level, appreciation for cybersecurity teams and programs parallelled appreciation for their performance and execution. Overall, 65% believe their organization demonstrated advanced or proven cybersecurity best practices during the pandemic. Furthermore, 59% reported that a general security plan had effectively improved the organization's ability to prepare for, respond to, and recover from cyberattacks during the pandemic.

Not surprisingly, in hindsight, this self-assessment often came from organizations that had already been enabling remote workers, often with services delivered via the cloud. When governments issued stay-at-home orders, these companies were able to quickly build on top of existing capabilities.

But the pandemic's broad impact across the U.S. and the world exposed sharp differences in cybersecurity preparedness and performance that map to specific organizational attributes.

Strength Bred Strength

Most organizations were already paying attention to cybersecurity, but only 30% were "extremely focused" on it before the pandemic's onset — and that extreme focus paid off for these companies *during* the pandemic. For example, 83% of organizations that were

Cybersecurity hasn't lost a step. We built a security infrastructure that functions as well remote as when we are in the office. Our only new response was working with Infrastructure to increase VPN capacity and working with our service desk team to ensure that all Zoom clients were up to date.

— Cybersecurity professional at a non-profit

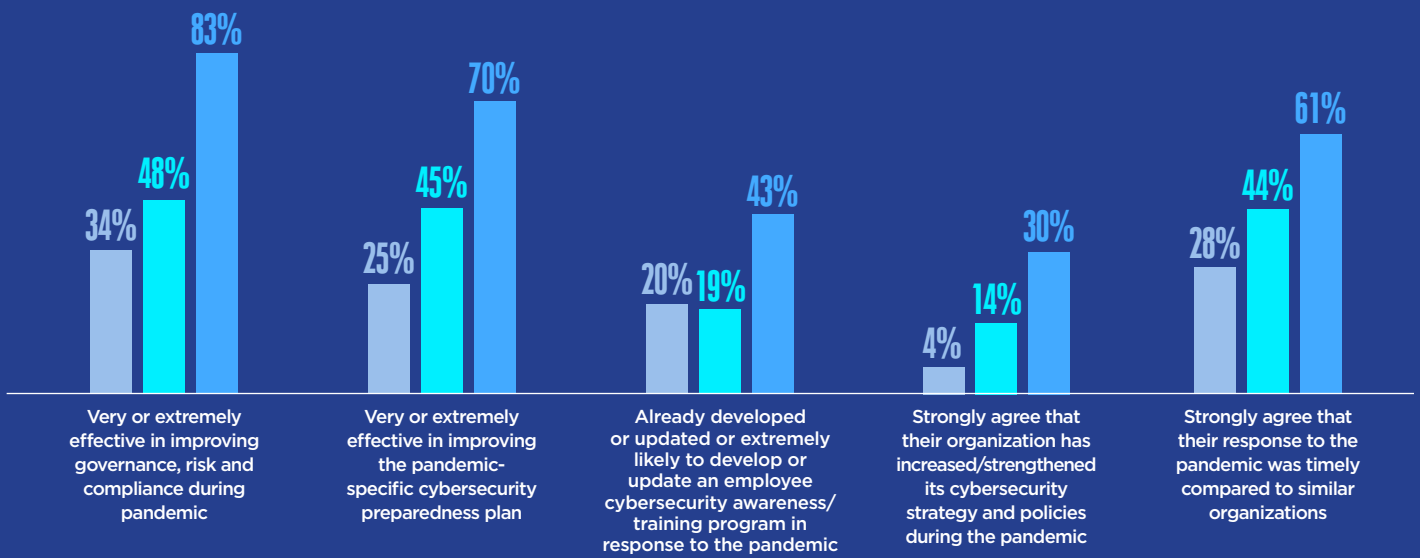
already extremely focused believe their organization effectively improved its governance, risk and compliance during the pandemic. In comparison, 34% of organizations with the lowest level of cybersecurity focus thought they were effective. The high-focus group was also more than twice as likely as the average respondent to have effectively improved its pandemic-specific cybersecurity preparedness plan.

These hyper-prepared companies have already begun updating or creating employee cybersecurity awareness/training programs in response to the pandemic. Companies that were not focused on cybersecurity have, perhaps predictably, had difficulty adjusting their cybersecurity strategy to the post-pandemic realities. In fact, respondents at high-focus organizations were more than twice as likely as those at organizations with a low focus (61% vs. 28%) to believe their response to the pandemic was timely as compared to their peers at the high-focus organization.

Organizations hyper-focused on cybersecurity before the pandemic are more effective during the crisis.

Pre-pandemic Focus on Cybersecurity Impacted the Response

Low Cybersecurity Focus Before Pandemic | Moderate Cybersecurity Focus Before Pandemic | High Cybersecurity Focus Before Pandemic



Three Distinct Groups

To better understand the impact of the pandemic on the practice of cybersecurity, CRA performed a segmentation analysis that identified three distinct classes of organization: the Lions, the Sheep and the Goats.

About half of the respondents can be considered **Cybersecurity Lions**. They were already focused on cybersecurity pre-pandemic, had a timely response to the pandemic, applied advanced or proven cybersecurity best practices during the pandemic and have a clear strategy for mitigating cyber risks related to the pandemic.

These companies' attention to security issues manifested itself in how they previously provisioned their work-from-home employees with technology. Seventy-one percent of cybersecurity champions claimed that before the pandemic's onset more than four-fifths of work-from-home employees used company-provided devices or technology such as laptops, mobile devices, and software to log in to corporate networks. In contrast, only 60% of all respondents said their organization provided equipment to more than four-fifths of work-from-home employees. One respondent said: "Quarterbacks don't get ready when the defensive line touches them."

These cybersecurity champions had success during the pandemic because of preparation that went beyond being ahead of others in terms of remote and work-from-home capabilities. The Lions were also more likely to have business continuity and disaster recovery plans. (In fact, 28% of Lions already had a pandemic-specific cybersecurity preparedness plan before March 2020.) These same companies quickly adapted their plans, so that two months later 83% had customized their cybersecurity plans to address pandemic-related issues. Cybersecurity and risk planning, along with cloud-focused infrastructure enabled a smooth transition into pandemic operations for many of these companies.

The preparation produced results. Eighty-one percent of the Lions believe the general cybersecurity preparedness plan was effective during the pandemic, and 93% demonstrated advanced or proven cybersecurity best practices. The hard work and consequent results have been noticed as the cybersecurity organization is appreciated at 93% of cyber Lion organizations. Expect these companies to be more successful than others when pursuing new investment in security resources.

Cybersecurity Sheep represent 38% of respondents. Most of this group had general cybersecurity plans in place pre-pandemic, but only 50% were very or extremely focused on cy-

bersecurity before the pandemic's onset. Organizations in this cohort are followers rather than leaders. In normal times, they find safety in meeting minimal requirements. Unfortunately, some of the Sheep are getting separated from the flock as organizations adjust to the current crisis. At the time of the study, only 36% said they have a clear strategy to mitigate cyber risks related to the pandemic — a stark drop compared to the 93% of Lions. No wonder 63% of Sheep believe that cybersecurity strategy and policies have been strengthened during the pandemic.

Beyond strategy, Sheep are having more problems with cybersecurity awareness and training. Only 41% believe their organization's employee training is effective against cyberattacks during the pandemic. There is little hope for widespread improvement; only 16% have already updated or created a new awareness program or are extremely likely to do so by the end of 2020. The impact of this inaction is noticeable as Sheep are less likely to have seen a bump in security awareness due to the pandemic.

Organizations that had put cybersecurity on the back burner are worried about keeping up with IT security demands in the coming months. Security professionals at these companies are concerned that increased remote work has increased the attack surface that has to be defended. On a positive note, 42% have already purchased or upgraded, or expect to do so in 2020, tools to support employee remote access. However, beyond this spending, the Sheep are less hopeful than the Lions that budgets and hiring will ramp up to address the new security environment.

Our study's **Cybersecurity Goats** represent the remainder of respondents (11%). These respondents may find themselves bearing responsibility for security lapses they had little ability to address beforehand. Only 27% had been very or extremely focused on cybersecurity before the pandemic's onset. Many of these organiza-

CYBERSECURITY LIONS
(50% of organizations)

- High level of pre-pandemic focus on cybersecurity
- "We were ready… Quarterbacks don't get ready when the defensive line touches them."
- More likely to describe their pandemic response as timely
- Demonstrated advanced or proven cyber best practices in the pandemic, and a clear strategy for mitigating pandemic-related cyber risk
- Had well-established remote and work-from-home capabilities
- Cybersecurity function more likely to be valued and appreciated

CYBERSECURITY SHEEP
(38% of organizations)

- Most of this group had general cybersecurity plans in place pre-pandemic, but many had relegated pandemic-specific cybersecurity to the back burner before and after onset
- Consider themselves unlikely to keep up with IT security demands in coming months
- Less likely than Lions to adopt employee cyber training or invest in WFH tools

CYBERSECURITY GOATS
(11% of organizations)

- Expressed lowest confidence about their pandemic response
- Only 27% were focused on cybersecurity pre-pandemic
- Ascribe little importance to cyber preparedness or awareness and training
- Perceive their cyber plans to have been ineffective during the pandemic
- Had the lowest pre-pandemic proportions of regular WFH employees
- Least likely to invest in WFH employee tools or infrastructure

tions did not have a cybersecurity preparedness plan. This had a negative impact on the security team's response to the pandemic, with 57% of the Goats unable to even increase their focus on security since the pandemic's onset.

These organizations were initially at risk because of a lack of focus, but it didn't help that fewer of their employees had been remote-capable before the pandemic. Already behind the curve, their response has been impeded by an inability to invest in the tools and infrastructure needed to support a remote workforce.

Lessons and Recommendations

It is a truism that preparation matters, but that makes the statement no less true. The pandemic gives cybersecurity professionals powerful opportunity to build organizational buy-in for an expanded commitment to increasing attention on cyber risk management and mitigation. For those whose organizations proved to be sufficiently prepared, the pandemic offers further leverage to drive cultural change and enforcement of policies and procedures. Perhaps the study's most powerful message is that it is insufficient to be a follower — a sheep — when it comes to cybersecurity; leadership is a necessary condition for excellence.

SELECTED SECTORS IN FOCUS

For now, consulting and services firms have made a strategic bet to focus on a people rather than a technology-oriented strategy.

Consulting and Services Firms Focused on Security Awareness Instead of Advanced Best Practices

Consulting and services firms may have done more than any other industry vertical to increase their focus on cybersecurity during the pandemic, but they started from a position of relative weakness. Twenty-five percent of this sector significantly strengthened their focus on cybersecurity because of the pandemic, which is double the rate of the average organization.

These differences are likely attributable to these firms' heavy reliance on knowledge workers, many of whom were already able to work while traveling. These companies, which provide business, scientific, consulting and for-profit educational services, had relatively little difficulty transitioning most of their employees to remote work. One way they were able to achieve this was de-emphasizing requirements for newly work-at-home employees to use company-provided hardware and other technology. Compared to highly regulated industries, the group previously had less robust remote access policies and supporting technologies. This approach creates greater risk employees who will not comply with security requirements.

For now, services firms have made a strategic bet to focus on a people rather than a technology-oriented strategy. On one hand, cybersecurity employee training and

awareness has become more important than other management priorities at two-thirds of services firms, more than any other industry. On the other hand, services firms were the least likely to demonstrate advanced or proven cybersecurity best practices during the pandemic.

Alarm Bells for Governments and Universities

The cybersecurity response to the pandemic has been sub-standard at government agencies and universities, categories that together represent some 40% of the high-risk organizations in the study. Post-onset, these organizations realized their general cybersecurity preparedness plans had fallen short. There is a big gap between the importance the public sector gives to general cybersecurity preparedness planning and how effective it has been in this area during the pandemic. Fifty-six percent believe it is more important than other management priorities, but only 43% believe their organization is more effective in this area since the pandemic's onset.

One university employee told CRA that security efforts have been reduced because keeping remote activities operational was given priority. Universities will be particularly vulnerable this fall because so many are expecting

General cybersecurity preparedness planning falls short for public sector/education.

Q: Compared to other management priorities at your organization right now, how important are each of the following types of plans or programs? (IMPORTANCE)

Q. How effective do you think each of these are/will be in improving your organization's ability to prepare for, respond to, and recover from cyber attacks during the pandemic? (EFFECTIVENESS)

(% of respondents indicating "Somewhat/Much More Important" and "Very/Extremely Effective")

> **The increase in VPN users highlights the difficulty in monitoring VPN endpoints. Are employees really using their company issued laptops, or are they using home equipment instead?**
>
> **— Systems engineer at a small business**

to continue to be solely or substantially remote. There is a real risk that security efforts will be relaxed because leadership's focus is on enabling distance learning applications and maximizing the user experience of tuition paying students.

Financial Services' Superior Response

Financial services' response to the pandemic stands out for its cybersecurity excellence and how companies are taking advantage of industry disruption. These companies were more likely to have pandemic-specific plans in place before they were needed and were highly effective in updating these plans during the pandemic. Financial companies were already well-positioned in terms of remote employees' cybersecurity compliance, which let them focus on accelerating plans to promote their digital offerings.

Financial services firms were more prepared than other organizations, but not because CEOs were able to point to a specific and highly detailed plan the CISO and a team of consultants had produced. In fact, they were just as likely as any other industry to have a cybersecurity preparedness plan. Furthermore, financial services firms were slightly less likely than the average to have increased their focus on cybersecurity because of the pandemic. This highlights the nuances between having a plan and being prepared.

But financial services firms' plans were more in-depth, at least in terms of addressing emergencies. Before the pandemic's onset, 92% of financial services had a busi-

ness continuity or disaster recovery plan (BC/DR), as compared to 81% for the average respondent's organization. The consequences were plain to see as the plans' effectiveness during the pandemic outpaced the importance the companies were putting on them.

Digging even deeper, 31% of financial services had a pandemic-specific cybersecurity preparedness plan, as compared to 21% for the average respondent's organization. Without having to worry about general security plans, these companies were able to prioritize pandemic-specific planning.

Probably because they had already been addressing the issue, financial service firms were less likely than the average organization to be prioritizing cybersecurity employee awareness and training over other management priorities. In fact, the pandemic had a positive impact on employee cybersecurity compliance at 61% of financial services firms as opposed to 50% at the average organization.

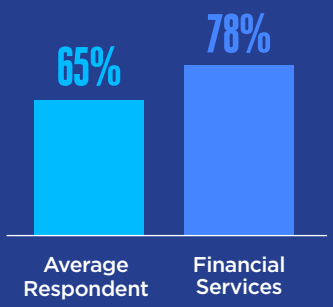
Regulatory oversight — sharpened in the wake of the financial crises of the aughts — undoubtedly had a positive impact on their cybersecurity planning. Financial services also had an edge because they had a history of investing in security more than other industries — owing to their conservative cultures and high dependency on information technologies. Cybersecurity departments at financial services firms played to type during this latest crisis: 78% demonstrated advanced or proven cybersecurity best practices during the pandemic while the average respondent did so 65% of the time.

Success on the cybersecurity front has allowed executives to focus on making the business itself successful. Almost three quarters (72%) of financial services respondents believe the pandemic had a positive impact on the overall business strategy, compared to 55% for the aver-

The pandemic response of financial companies led to overachievement on both their cybersecurity and their business objectives.

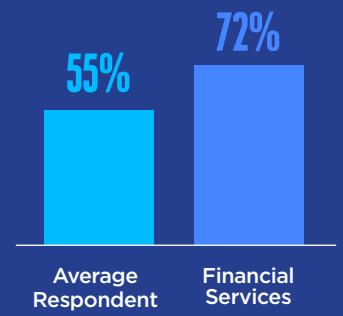
DEMONSTRATED ADVANCED OR PROVEN CYBERSECURITY BEST PRACTICES DURING THE PANDEMIC

(% of respondents who said "Somewhat Agree" or "Strongly Agree")



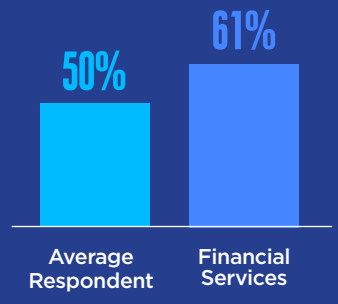
PANDEMIC'S IMPACT ON ORGANIZATION'S OVERALL BUSINESS STRATEGY

(% of respondents who said "Somewhat Positive" or "Very Positive")



PANDEMIC'S IMPACT ON EMPLOYEES' CYBERSECURITY COMPLIANCE

(% of respondents who said "Somewhat Positive" or "Very Positive")



age respondent. With bank branches and other offices closed, consumers gave a second look to many of the digital services that had been generated by the fintech boom over the last decade. These companies already had detailed digital transformation strategies. The crisis provided the push needed to accelerate adoption of internet and mobile-based offerings.

Lessons and Recommendations

Whether cybersecurity can be said to be well-embedded in an organization may depend more on external factors than it does on formally agreed principles and philosophies. In thinking about your organization's preparedness, don't fall into the trap of judging yourself solely in context of in-sector peers and practices. In assessing your posture and strategy, check yourself for "grade inflation." Consider the impact of business model, industry tradition and regulatory requirements (to which you may, or may not, be subject), and judge your organization in absolute terms.

WORDS, DEEDS & DOLLARS

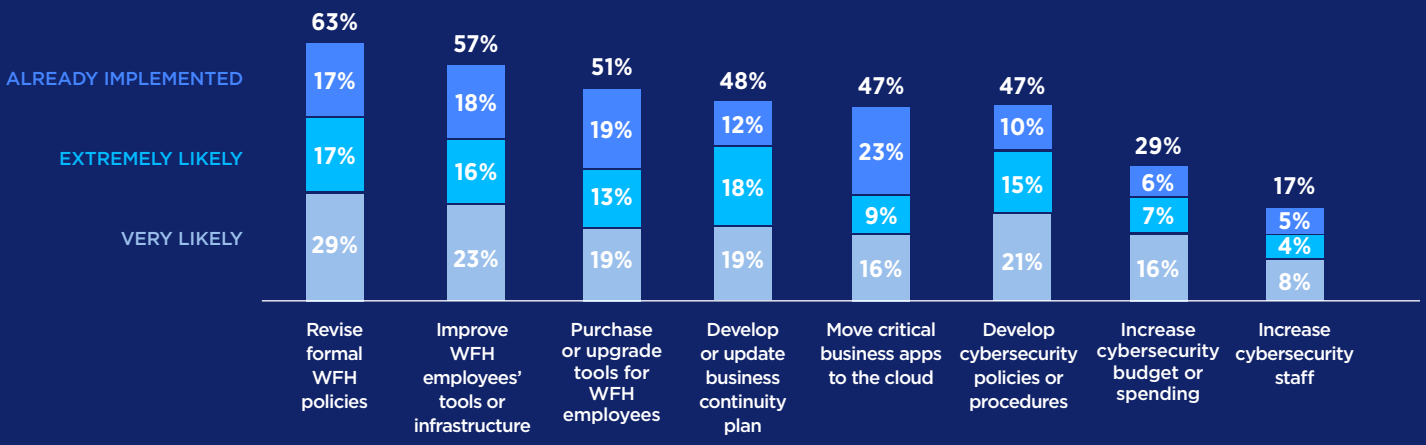
There is every reason to believe that cybersecurity spending will continue to rise year-over-year, but for now there is little evidence of massive changes in the next few months.

Post-mortems about plans' effectiveness are important but considering the necessary next steps for managing IT security post-pandemic is critical. Across a range of questions, organizations asserted a strong bias to action but paradoxically do not expect to increase spending or hiring to achieve their goals.

CRA does expect upticks in specific cybersecurity spending initiatives among many organizations in coming months, mainly to support WFH employees, but few anticipate signficant expenditures. A respondent with executive management responsibilities said: "Companies that were unprepared for work-from-home mandates will see an increase in short-term budget/spend and a hit to their P&Ls." There is every reason to believe that cybersecurity spending will continue to rise year-over-year, but

Spending and policy development to support a remote workforce is the pandemic's most immediate impact.

How likely is your organization to implement each of the following in the next 6 months as a result of the current pandemic?



> **Management was very responsive. Invested over $300,000 to upgrade VPN and bandwidth capabilities to support 500 people WFH.**
>
> **— Information security officer at a midsize manufacturer**

for now there is little evidence of massive changes in the next few months.

Compared to overall cybersecurity spending in the next six months, even fewer organizations will hire more cybersecurity staff to address needs associated with the pandemic. Half (52%) said there is no chance this will happen, while only 17% said it is at least very likely to happen or has already occurred.

By the time the survey was conducted, only 6% had already increased the cybersecurity budget or spending as result of the pandemic. Another 23% are at least very likely to increase this spending by the end of 2020.

Organizations have already experienced an initial rush to install corporate software onto personal devices and provision identities to collaboration applications like Slack. Next on their list is formalizing work-at-home policies and improving implementation of communications tools employees rely on — which sometimes means helping them download a collaboration app like Slack or Microsoft Teams. While labor intensive, this may not require additional expenditures. However, many other times, additional investment (in seat licenses and commercial-grade software, e.g.) is unavoidable. For this reason, 51% of respondents have either already allocated additional money – or are at least very likely to do so – in order to purchase or upgrade tools to support/enhance employee remote access.

Small Organizations Unable to Implement Near-term Cybersecurity Responses

Before the crisis, small organizations (100 or fewer employees)

tended to place higher value on cybersecurity than larger competitors. More than half (51%) of respondents at small organizations strongly agreed that cybersecurity is appreciated, while there was only a 33% chance of cybersecurity being similarly valued at the average organization.

Despite the positive vibes, small organizations are in trouble. Small companies are particularly sensitive to business disruptions, and their executives have been cutting unnecessary expenditures in case the world falls into an extended recession. They also have less access to the capital that would support multi-year technology projects.

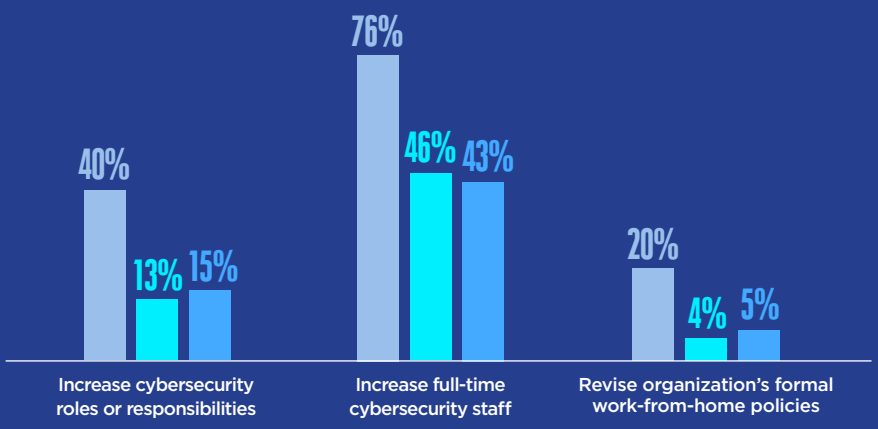
Another challenge facing smaller organizations is that cybersecurity is less likely to be separated from other IT functions. The systems administrator often does double duty managing firewalls and dealing with identity management. Just adding a few hours more work means something else must be deprioritized. On balance, however, small organizations are twice as likely to say there is no possibility the pandemic will add additional responsibilities to the cybersecurity function this year. Small organizations that have a specialized cybersecurity function will be able to focus on risk mitigation, but other companies may be less fortunate.

Budget and organizational restraints mean hiring new staff to address new security threats is not an option. According to respondents, there is no possibility that cybersecurity staff will be hired this year; the average organization is less likely to have shut the door on this option, with 52% not at all likely to hire cybersecurity staff in response to the pandemic.

For many small organizations, near-term cybersecurity changes to respond to the pandemic are not on the table.

How likely is your organization to implement each of the following in the next 6 months as a result of the current pandemic? (% of respondents that said "Not at all likely")

SMALL ORGANIZATION | MEDIUM ORGANIZATION | LARGE ORGANIZATION



Lessons and Recommendations

The gap between organizations with strong cybersecurity and those with weak is closing but remains wide. Will the pandemic be viewed as just the latest in a long line of high-profile events? Or will its impact prove more durable and farther-reaching? At a minimum, even the smallest organizations should seize this opportunity to systematically strengthen awareness and training with respect to work-from-home team members. In the meantime, the broader business community must reckon with the knowledge that the ecosystem continues to contain many weak links.

THE BUSINESS VS. TECH DISCONNECT PERSISTS

> **It should raise awareness and bring at least a short-term plus to the industry. Long-term, something else will come along and grab the attention, or budget cutbacks – maybe because of the pandemic – will take hold.**
>
> **— Cybersecurity professional at a governmental organization**

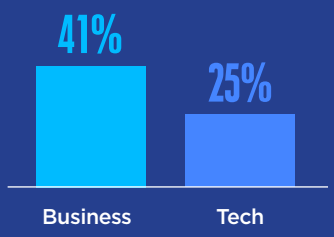
The pandemic has done little to repair the disconnect between business executives and technology professionals about how to manage cyber risk at their organizations. Before the pandemic, most business executives had only high-level understanding of cybersecurity preparedness. They had been briefed by the CISO, CIO, or risk management leader — especially if they work for a public company — but if pressed for details, they would be challenged to explain exactly what was being done.

Despite, or perhaps because of, their limited knowledge and visibility to the details, business executives consistently expressed higher confidence in the organizations than their tech colleagues. For example, 41% of business executives strongly asserted that their organization demonstrated advanced or proven cyber best practices since the pandemic's onset, while only 25% of respondents in IT and cybersecurity felt the same.

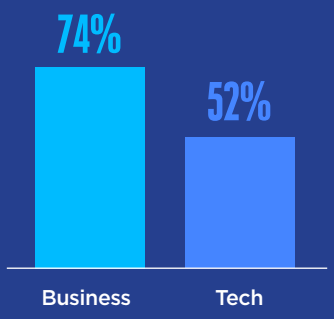
The groups also differed in their assessments of their organizations' change in cybersecurity posture after the pandemic's onset. Far more business executives (74%) were likely to say their organization had "strengthened" its cybersecurity focus than those in tech roles (52%). Furthermore, business executives

Business vs. Technology: Mind the Gap

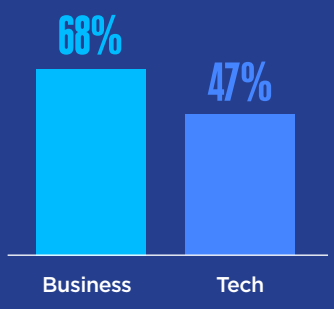
DEMONSTRATED ADVANCED OR PROVEN CYBERSECURITY BEST PRACTICES DURING THE PANDEMIC
(% of respondents who said "Strongly Agree")



CHANGE IN CYBERSECURITY FOCUS AS A RESULT OF THE PANDEMIC
(% of respondents who said "Strengthened")



PANDEMIC'S IMPACT ON ORGANIZATION'S CYBERSECURITY STRATEGY
(% of respondents who said "Somewhat positive" or "Very positive")



are significantly more likely (68%) than tech respondents (47%) to believe the pandemic had a positive impact on their organization's cybersecurity strategy.

Cybersecurity and IT are skeptical of senior executives' increased focus on security-related issues, and harbor concerns that the appreciation they've won is temporary. One respondent worried the glow "may fade more quickly than the virus." Another acknowledged that security awareness has been raised, but that "long-term, something else will come along and grab the attention or [that] budget cutbacks" would follow regardless.

Lessons and Recommendations

As most of the recommendations in this report indicate, the biggest mistake a cybersecurity leader — whether her organization is a Lion, Sheep or Goat — could make is to fail to address the cybersecurity elephant in the post-pandemic room. The misalignment between technology and business professionals is a classic case in point. The challenge for cybersecurity leaders is to directly engage any unwarranted optimism they may encounter among their colleagues — but to do so without re-erecting old barriers to communication they've long fought to bring down. Deploying data-driven insights in making your case is essential.

LOOKING AHEAD

> **This was a wake-up call to management to ensure the institution has a well-thought-out pandemic and cybersecurity plan and capabilities to support it.**
>
> **— Executive-Level Manager**

Verbatim responses include phrases like "alarm bells ringing," "eye-openers," and "wake-up calls," as respondents described their lack of cybersecurity planning for a pandemic. From the most junior employee to the C-suite, the clarion call was heard. Awareness of threats is higher than before, and senior executives appreciate what cybersecurity professionals have done.

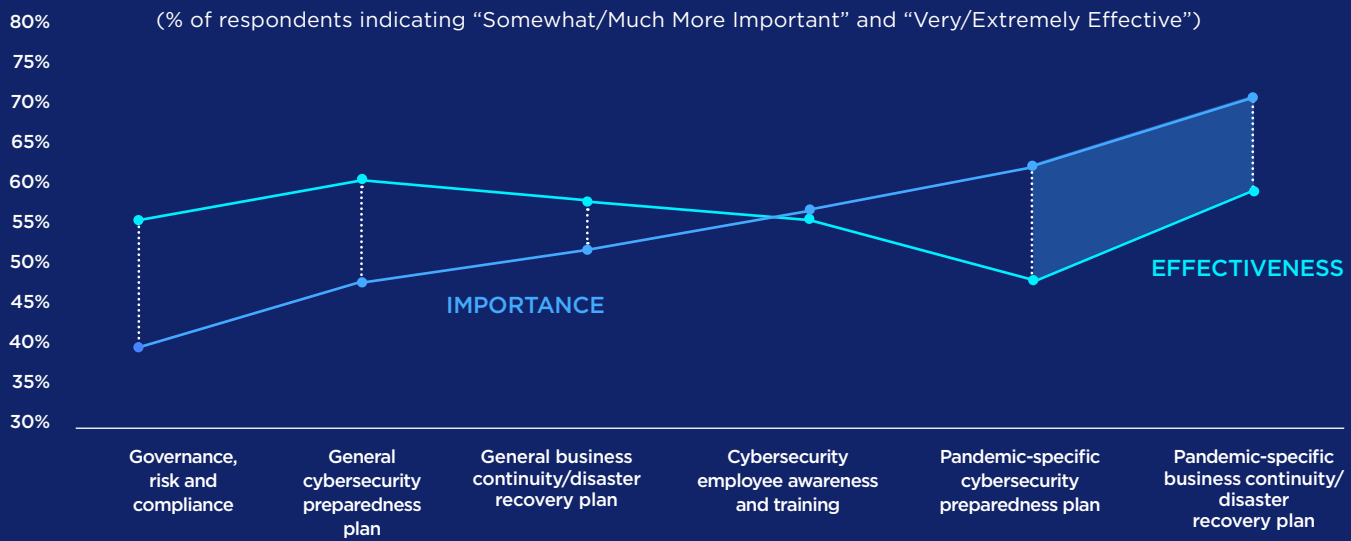
Although the increased focus may yet prove ephemeral, organizations have shifted priorities to develop new pandemic-specific cybersecurity preparedness and disaster recovery plans.

Respondents said their highest priorities had become pandemic-specific BC/DR (70%) and cybersecurity preparedness plans (62%). While many (57%) were highly confident their pandemic-specific BC/DR plans would be effective in the pandemic, only 47% were confident their new high-priority pandemic-specific cybersecurity preparedness plans would be effective. Despite the progress, the survey respondents lacked confidence that these measures will be effective.

There is a struggle to adopt effective pandemic-specific plans.

Q: Compared to other management priorities at your organization right now, how important are each of the following types of plans or programs? (IMPORTANCE)

Q. How effective do you think each of these are/will be in improving your organization's ability to prepare for, respond to, and recover from cyber attacks during the pandemic? (EFFECTIVENESS)



CONCLUSION

The Covid-19 pandemic left an indelible mark on cybersecurity, with positive and negative implications. On one hand, in important ways, it seems to have pulled some cybersecurity professionals from the margins to the center of their organizations — lifting their status and (perhaps temporarily) broadening their scope and influence. As such, the crisis can be seen as a milestone in the field's thus-far halting ascent to the corporate pantheon's uppermost reaches.

On the other hand, many of the discipline's most persistent challenges stand stubbornly in place. Notably, cyber-leaders and non-IT executives remain misaligned in key ways. And the gap between organizations with and without strong information security programs is still consequential. Finally, expectations remain low — even despite the crisis's high impact on the threat landscape — when it comes to funding new cybersecurity priorities (though the latter is likely also partly due to the sharp economic downturn that was also a pandemic byproduct).

As with other "wake-up call"-level crises (e.g., 9/11), the scope and durability of Covid-19's impact on information security will reveal itself over time — as will the degree to which its learnings influence the course and management of future crises and their cybersecurity implications. Cybersecurity leaders will be the key actors in ensuring that the pandemic's positive impacts will endure; to do so, they must seize the moment.

SUMMARY OF KEY FINDINGS

1 New Appreciation for Cybersecurity Leadership

Cyber professionals say they are newly appreciated and valued by their organizations owing to their work in the pandemic. This counters the profession's long-held sense of its marginalization, and even disregard, by leaders and others in their organizations.

2 Sharp Differences in Level of Preparedness

The pandemic's broad impact across the U.S. and the world has exposed sharp differences in cybersecurity preparedness and performance that map to specific organizational attributes. Differences were also apparent among certain industry sectors that related both to the character of their preparedness and the character of their response. Governments and universities lagged; financial services excelled.

3 Strong Commitment to Improve But Not to Spend

In considering next steps for managing IT security post-pandemic, organizations uniformly assert a strong bias to action but paradoxically do not expect to increase spending or hiring. In this regard, the challenges faced by smaller organizations in particular came into relief.

4 Disconnect between Business and Tech Professionals

The pandemic has done little to repair the disconnect between business executives and technology professionals about how to manage cyber risk at their organizations, with the former projecting more optimism than the latter perceive in the trenches.

5 Pandemic-Specific Plans Don't Inspire Confidence

Organizations have shifted priorities to develop new pandemic-specific cybersecurity preparedness and disaster recovery plans — but lack confidence these measures will be effective.

ABOUT

CyberRisk Alliance is an information services and business intelligence company serving the cybersecurity community. Our mission is to bring the community together to share knowledge and insight and find innovative solutions to the biggest challenges we face today. We build proprietary content, research and data, and leverage a deep network of industry experts, policy makers, and senior-level practitioners to provide unique insight to our rapidly expanding community of cybersecurity professionals. We deliver our content through events, research, media, and virtual learning. Our brands include SC Media, InfoSec World, CRA Business Intelligence, Cybersecurity Collaborative and Cybersecurity Collaboration Forum.

CRA Business Intelligence is a full-service market research capability focused on the cybersecurity industry. Drawing upon CRA's deep subject-matter expertise and engaged community of cybersecurity professionals — along with a world-class market research competency — CRA Business Intelligence is unique in the industry. These components together enable delivery of unparalleled data and insights anchored in our community of cybersecurity professionals and leaders eager to share their perspective on the industry's most important concerns.

CRA BUSINESS INTELLIGENCE PROVIDES:

- Unique proprietary research, including the Voice & Vision series, to educate and inform
- Custom research to support strategic product and marketing initiatives
- Innovative thought-leadership content development and promotion
- Business activity indexes, interactive tools and assessments, and more

FOR MORE INFORMATION, CONTACT:

DANA JACKSON
VP OF RESEARCH
dana.jackson@cyberriskalliance.com