SURVEY RESULTS

# CISO Perspectives:

# Data Security Survey 2022

How Has COVID-19 Permanently Changed How CISOs Approach Data Security?

FORTRA

iSMG
INFORMATION SECURITY
MEDIA GROUP

# Table of Contents

*This survey was conducted in the winter of 2021-2022. Focused across sectors and regions, the study attracted more than 180 responses. Of the respondents, 42% come from EMEA, 27% from North America and 36% represent enterprises with over 10,000 employees.*

# Letter From the Editor

**TOM FIELD**
*SVP, Editorial, ISMG*
*tfield@ismg.io*

Field is responsible for all of ISMG's 28 global media properties and its team of journalists. He also helped to develop and lead ISMG's award-winning summit series that has brought together security practitioners and industry influencers from around the world, as well as ISMG's series of exclusive executive roundtables.

## Welcome to the report summarizing the CISO Perspectives: Data Security Survey 2022.

The backdrop of this study is: Cloud migration. Remote work. Security at the edge. These are some of the many ways that the COVID-19 pandemic has permanently changed cybersecurity.

At the same time, data security threats continue to rise. Whether it's new social engineering attacks or the risk of sensitive data falling into the wrong hands, security leaders have never faced such pressure to protect both their organization's data and reputation from the dangers that surround them.

What has been COVID-19's impact on pure data security? How do global security leaders feel about their relative success at protecting critical data in 2022? Are they winning? Losing? Holding ground?

The key question for survey respondents: How have their data security perspectives and practices evolved because of the pandemic response? Areas of focus include:

- The state of data security early in 2022;
- Key concerns for digital transformation initiatives;
- Top cybersecurity priorities for the next 12 months.

More than just survey results, this report offers expert analysis of why and how enterprises are evolving their data security strategies. This report intends to go beyond the survey statistics to tell you not just what respondents said, but how to put these results to work to enhance your own journey.

Best,

**Tom Field**
*SVP, Editorial, Information Security Media Group*

# Executive Summary

## Data: We have never had more of it, and it has never been so challenging to protect.

Since 2020 and the start of the COVID-19 pandemic, global organizations have created more data than ever, and they have spread it across a larger potential attack surface than at any point in history – corporate devices, personal devices, IoT, public cloud, private cloud ...

Over that same period, adversaries – ranging from cybercriminals who increasingly leverage tools previously ascribed to nation-state actors, as well as nation-state actors who increasingly engage in cybercrime – have taken advantage of the broader potential attack surface. SolarWinds, Colonial Pipeline, Kaseya and Log4j are but the most publicized examples of attacks that have targeted software zero-days, supply chains and managed services providers.

The names of the attacks have not changed appreciably. We are still talking about ransomware, business email compromise and traditional phishing. But the scale of these attacks has increased enormously and the target – data – is only more precious to defend.

This study set out to gauge how enterprises have been affected by COVID-19 regarding cybersecurity, how they have focused their digital transformation initiatives and what they intend to do in the year ahead to improve data security.

An interesting quandary discovered at the outset of this survey: Eighty-nine percent of survey respondents say their enterprises are more – or at least as – cyber-secure as they were one year ago. And yet, 52% say

**89%**

of survey respondents say their enterprises are more – or at least as – cyber-secure as they were one year ago.

**52%**

say cyberthreats have become fiercer in that time period.

**19%**

say COVID-19 has disrupted their data security initiatives.

cyberthreats have become fiercer in that time period. Among the points the survey statistics reinforce:

## The More Things Change ...

Who even knew what a hybrid workforce was two years ago? Now,  people work in and out of the office on corporate and personal devices, connecting via secured internal networks and unsecured external connections. The perimeterless enterprise has created a broadened attack surface that's attractive to cyber adversaries.

## The More Threats Stay the Same.

Ransomware. Business email compromise. Phishing. The threats are the same as pre-COVID-19 – but at a scale we have never before seen. Survey respondents are concerned about cybercriminal groups, which have ramped up attacks on critical infrastructure organizations and supply chains. If your detection and response capabilities were inadequate pre-COVID-19, your exposure now is greater than ever.

## It's About the Data

Respondents make it clear that data visibility is the biggest challenge facing their organizations today (63%) and that they most fear sensitive customer data exposure/breach (64%).

## Securing the Future Is Now

Nearly 100% of respondents (97%) expect level or increased funding for 2023, and their priorities are aligned with the cybersecurity concerns they express. Asked where they will invest resources, they cite enterprise data loss prevention (56%), data classification (40%) and encryption (35%).

Cary Hudgins, vice president of product at Fortra's PhishLabs, which sponsored this research, says he finds these responses and priorities encouraging.

"If this survey was taken a year ago, it would have had a very different feel to it," Hudgins says. "It looks like a lot of companies are returning to a state of normalcy. They've definitely shown resiliency, getting through that rocky 12 to 18 months of COVID. Companies are returning back to more strategic planning, although there are absolutely, definitely some gaps. And companies are playing catch-up and trying to implement controls to support their hybrid workforce."

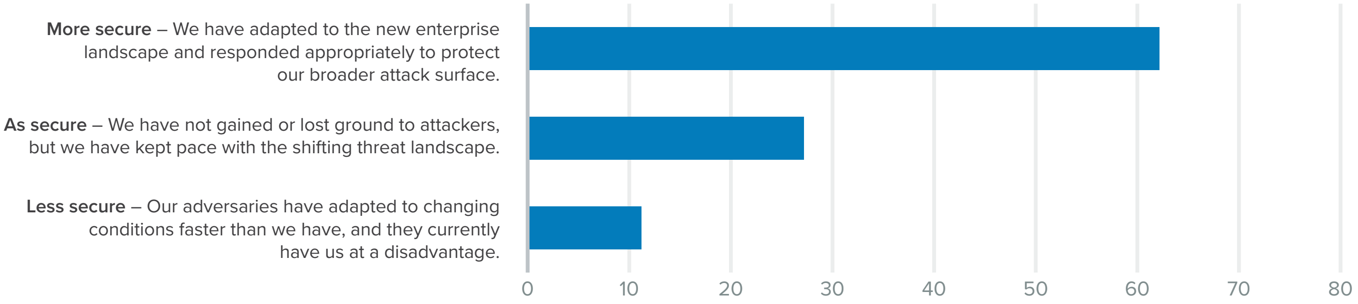
# Part 1: Baseline Questions

This opening section of the report takes the pulse of the attendees, getting their initial take on their enterprise's cybersecurity posture, as well as the threats that matter most.

No surprise: 43% cite ransomware as the threat of greatest concern.

Other responses:

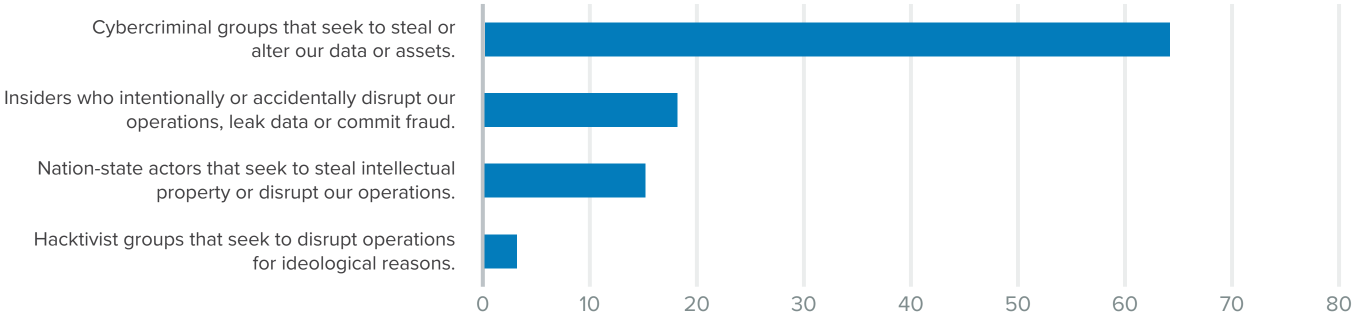
## Do you believe your enterprise is more or less cyber-secure today than it was a year ago?



Sixty-two percent of respondents say their organizations are more secure today than a year ago – that they have adapted to the new enterprise landscape and responded appropriately to protect their broader attack surface.

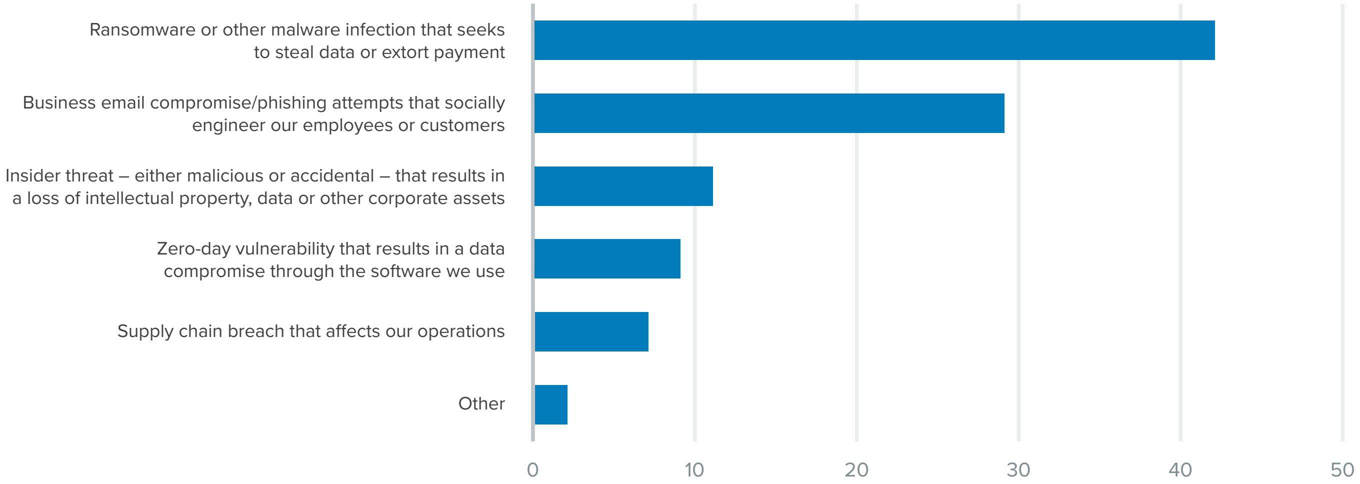
In balance, 27% say they are just as secure as a year ago – that they have not gained or lost ground to attackers – while 11% believe they are less secure and that adversaries are adapting better and faster to changing conditions.

## Which threat actor(s) concerns you the most today?



While nation-state actors grab the big headlines, cybercriminal groups are the top concern for 64% of respondents. Insiders, malicious or accidental,  place second at 18%, with nation-state actors following at 15%.

## Which cyberthreat poses the greatest danger to your enterprise and data today?



Asked which cyberthreat poses the greatest danger to their enterprise and data, 43% of respondents pick ransomware/malware infection, and BEC and phishing are a distant second at 29%.

The next section reviews statistics on the 2022 Data Security Landscape.

While nation-state actors grab the big headlines, cybercriminal groups are the top concern for **64%** of respondents.

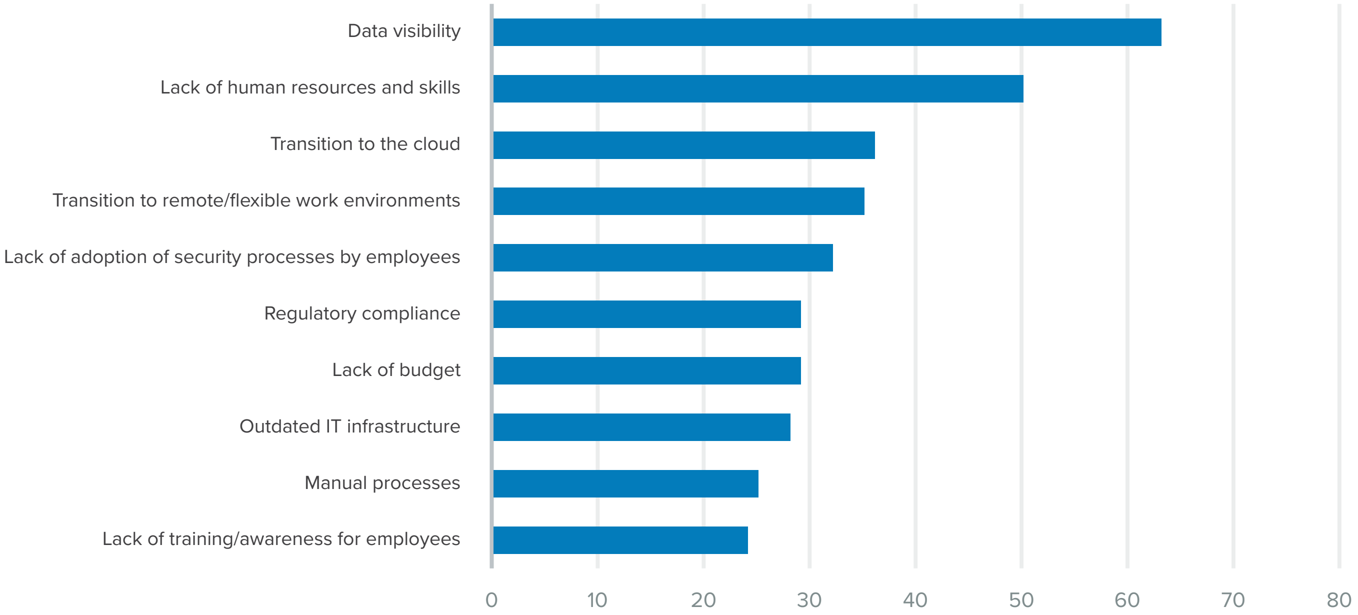
# Part 2: 2022 Data Security Landscape

The focus here is on how organizations approach data security today and where they feel most challenged. Among the findings:

- 80% say data security has increased as a priority over the past 12 months.
- 63% say their biggest data security challenge is visibility into what they have, where it lives and who has access to it.

See full results in the following charts.

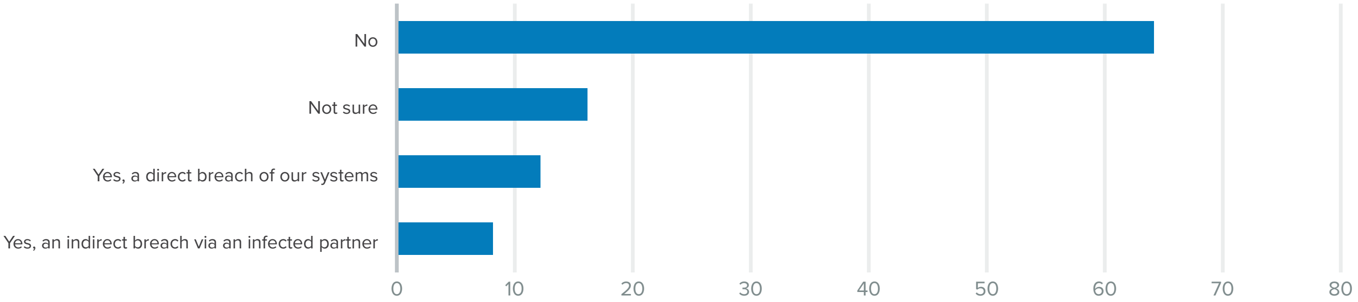
## What are the biggest challenges facing your organization today when you consider your data security?



The challenges to data security are numerous. But to narrow it down to a top three, survey respondents call out:

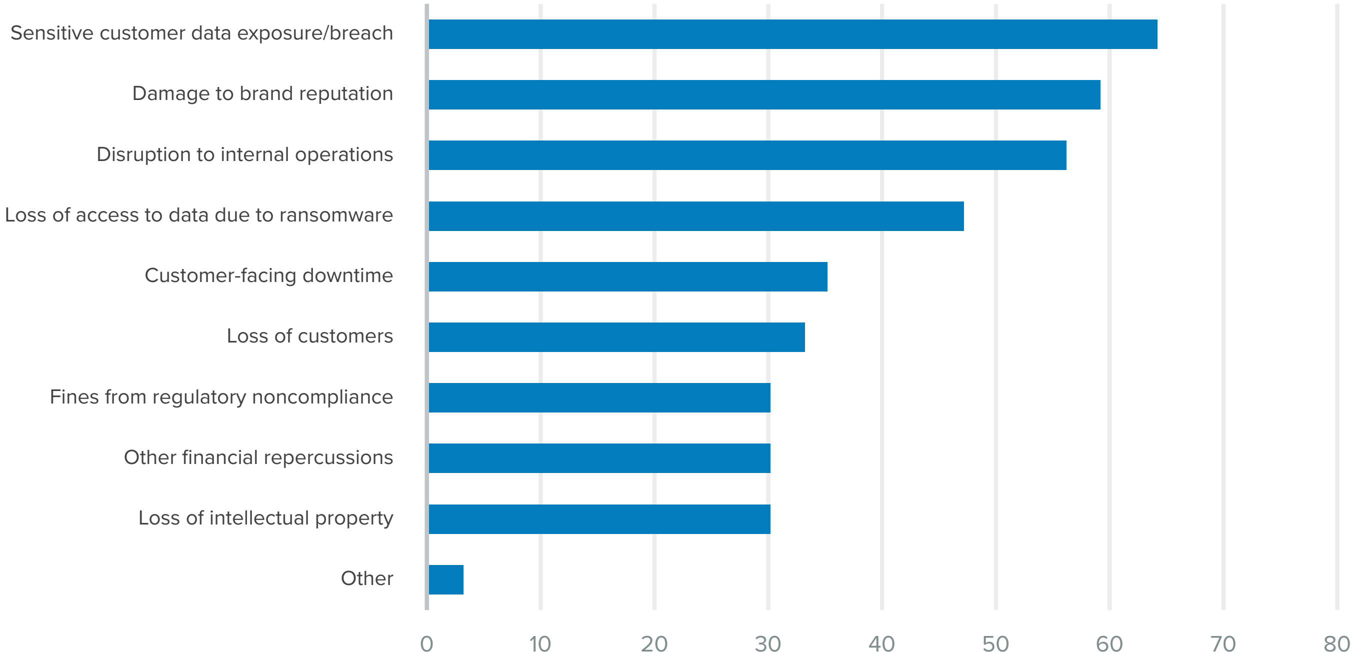
- Data visibility - 63%
- Lack of human resources and skills - 50%
- Transition to cloud - 36%

## Has your organization suffered a data breach – direct or indirect – in the past 12 months?



While two-thirds of respondents say their enterprises have not suffered a direct or indirect (supply chain) data breach over the past year, 20% say they have – and a troubling 16% are not sure.

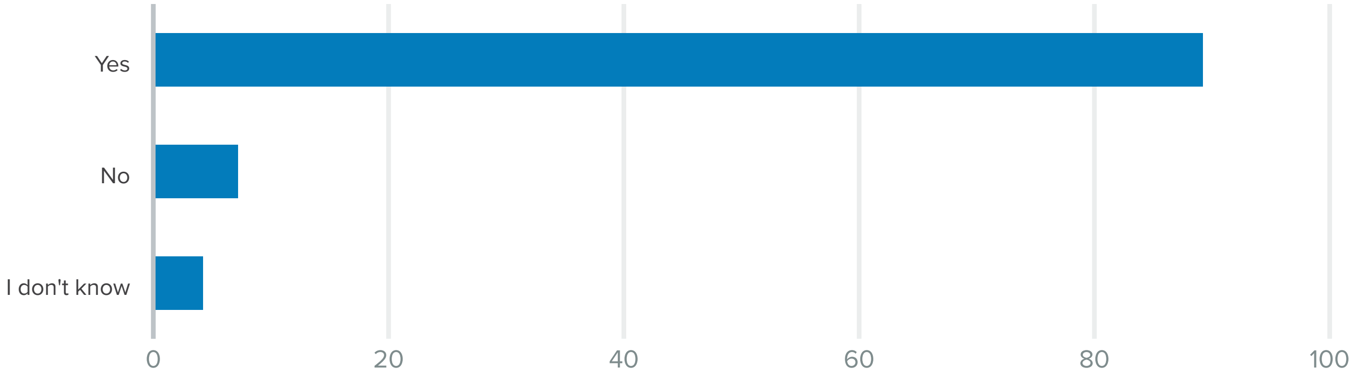
## Which of the following implications of a data breach does your organization fear the most? (Select all that apply)



Asked about breach impact and which implications they fear most, respondents cite:

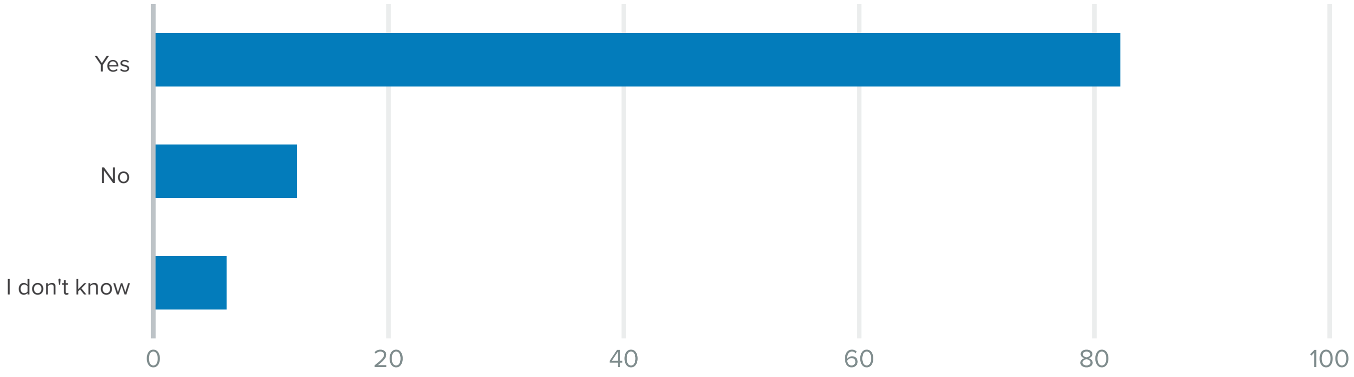
- Sensitive customer data exposure/breach - 64%
- Damage to brand reputation - 59%
- Disruption to internal operations - 56%

## Does your organization have a defined data security policy?



Encouraging news: 89% of organizations have a defined data security policy.

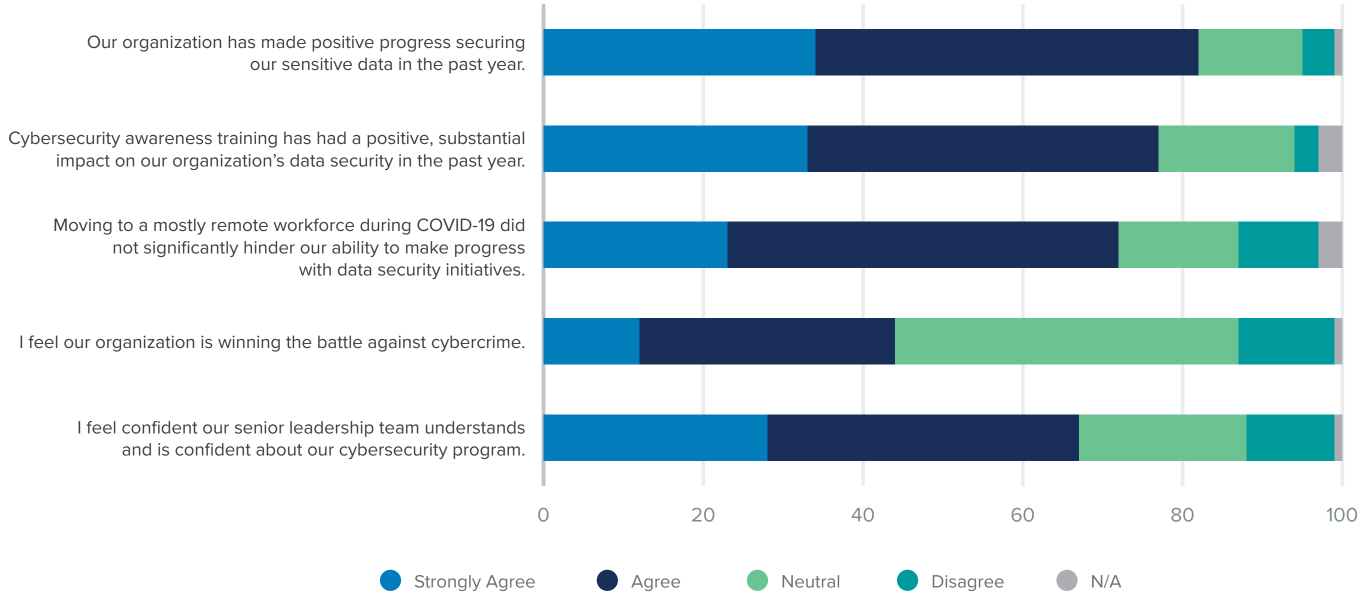
## Has your organization updated this data security policy in the past two years?



And more than 80% have updated this policy over the past two years of COVID-accelerated digital transformation.

89% of organizations have a defined data security policy.

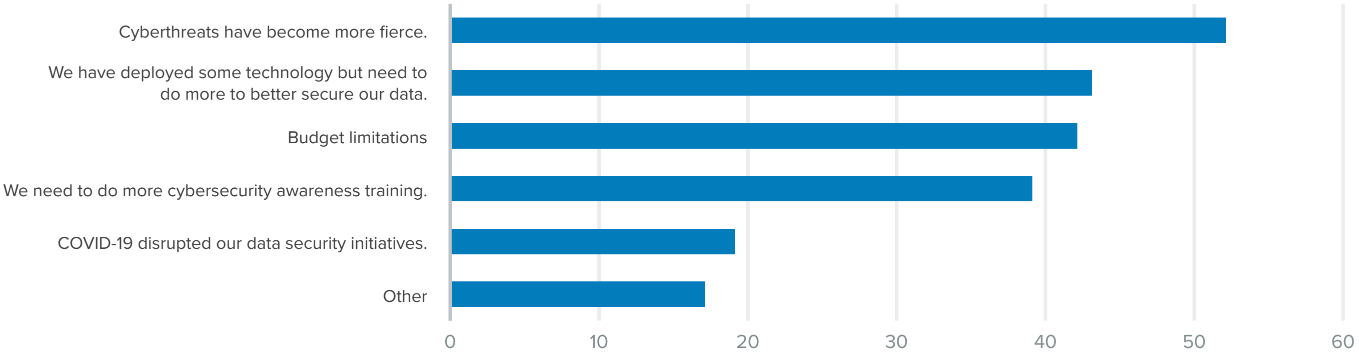
## Please indicate your response to the statements below.



Here, respondents were given the opportunity to agree/disagree with a series of statements about data security. Among the responses:

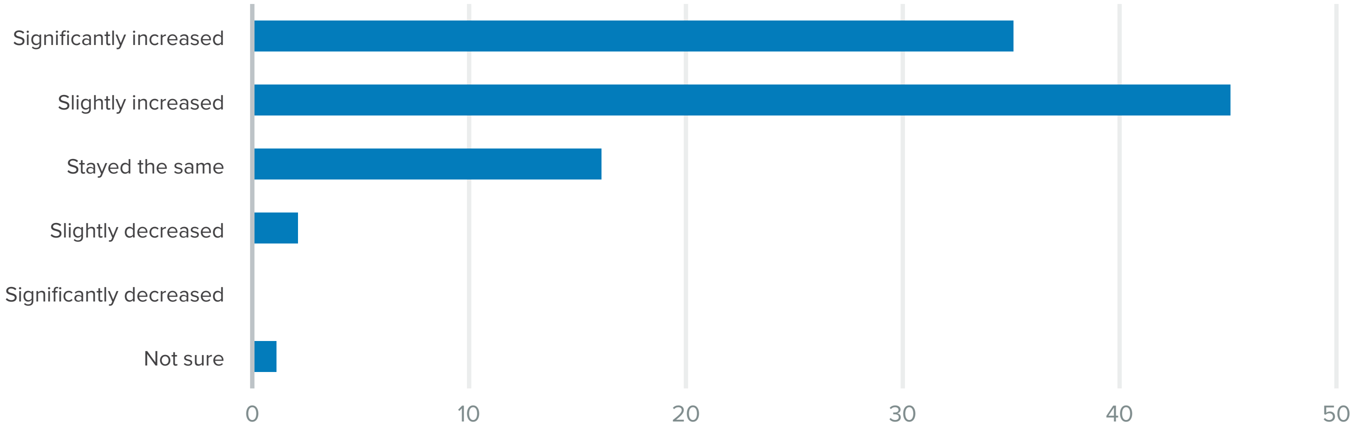
- Our organization has made positive progress securing our sensitive data in the past year - 82% agree/strongly agree.
- Cybersecurity awareness training has had a positive, substantial impact on our organization's data security in the past year - 77% agree/strongly agree.
- Moving to a mostly remote workforce during COVID-19 did not significantly hinder our ability to make progress with data security initiatives - 72% agree/strongly agree.
- I feel our organization is winning the battle against cybercrime - only 44% agree/strongly agree; 43% are neutral.
- I feel confident our senior leadership team understands and is confident about our cybersecurity program - 67% agree/strongly agree; 33% are neutral or disagree.

## If you answered mostly “Disagree” or “Strongly Disagree” to the statements above, what are the main reasons why?



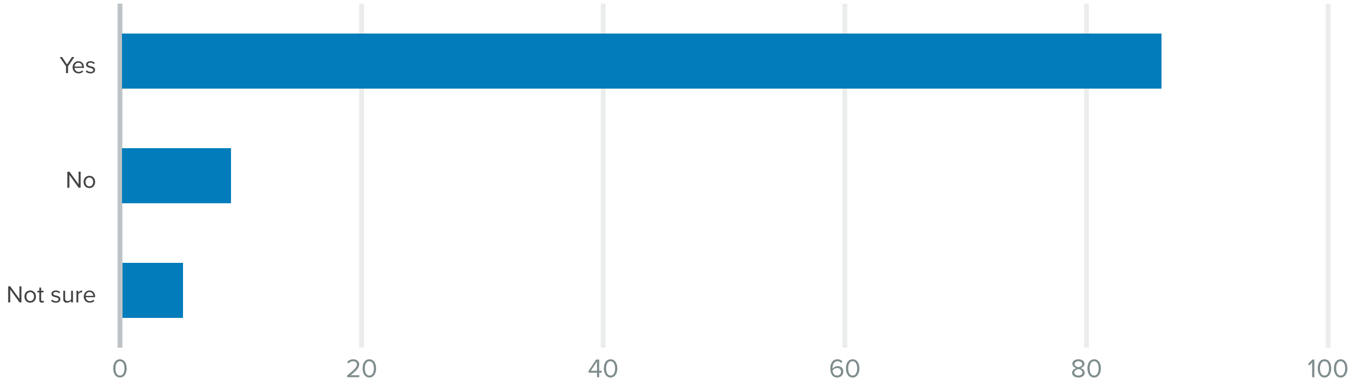
Digging further into respondents who answered disagree/strongly disagree, the survey asked why. Top response: Cyberthreats have become fiercer (52%).

## How has the priority of data security within your organization changed over the past 12 months?



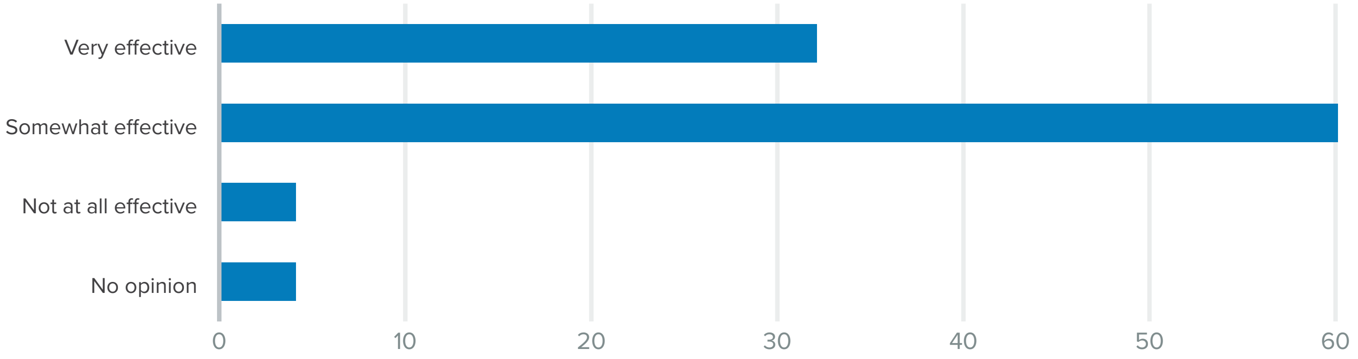
A strong majority – 80% – say data security as a priority has risen over the past 12 months. Only 2% say it has decreased.

## Have your employees gone through security awareness training in the last 12 months?



Further, 86% say employees have undergone security awareness training over the past year.

## How would you rate the effectiveness of this training?



Alas, only 32% of respondents say that training has been “very effective.” Sixty percent call it “somewhat effective,” while 4% say “not at all effective.”

Next, the report reviews budgeting and investment plans for 2023.

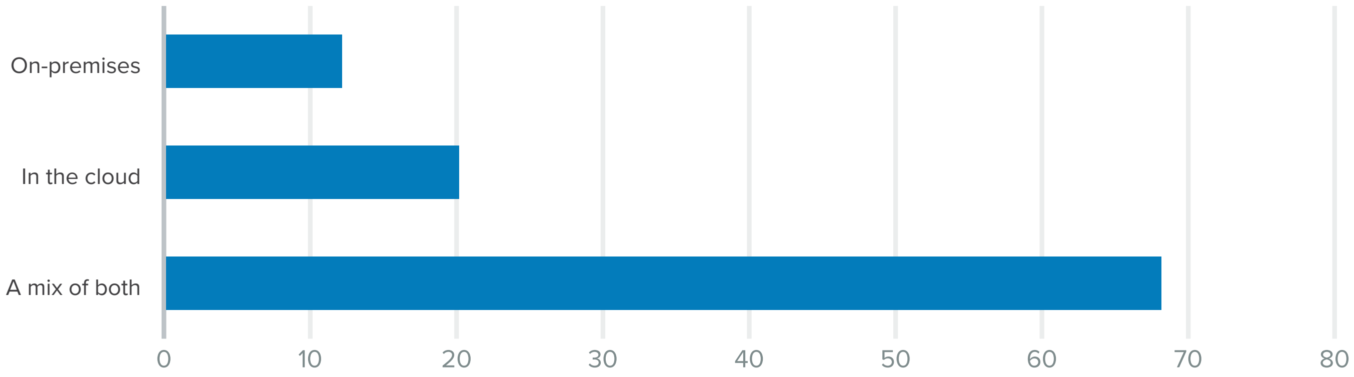
# Part 3: Planning for the Year Ahead

Most encouraging for any cybersecurity leader: 97% of surveyed organizations expect level or increased budgets for 2023. Among their investment goals:

- Enterprise DLP - 56%
- Data classification - 40%

See the full 2023 investment plans in the charts below.

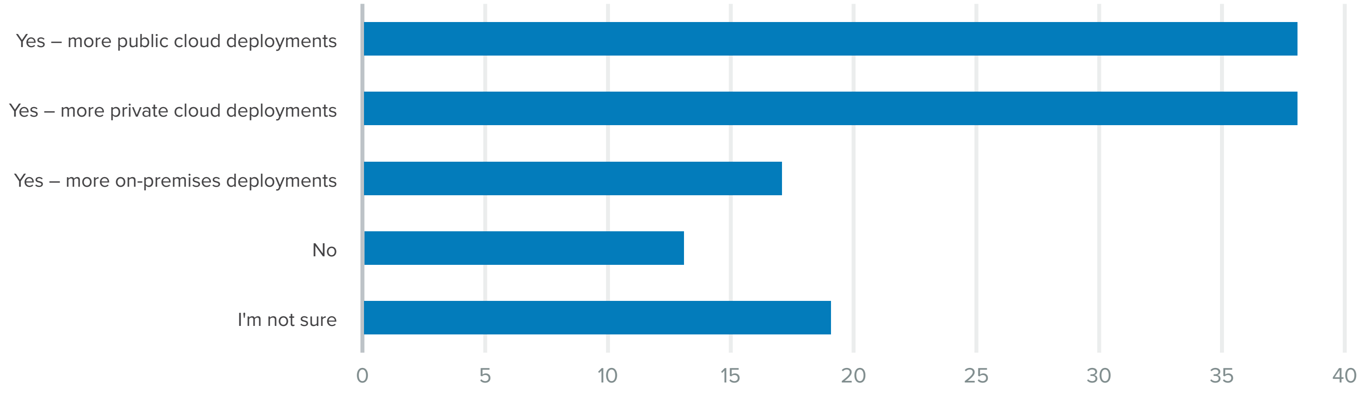
## Going forward, how will your organization choose to deploy new data security software today?



No surprise. After two years of digital transformation and cloud migration, when respondents are asked how they will deploy new data security software, 20% say in the cloud, and 68% say both in the cloud and on-premises.

97% of surveyed organizations expect level or increased budgets for 2023.

## In the next 1-2 years, do you expect your organization’s deployment of new data security software to change?

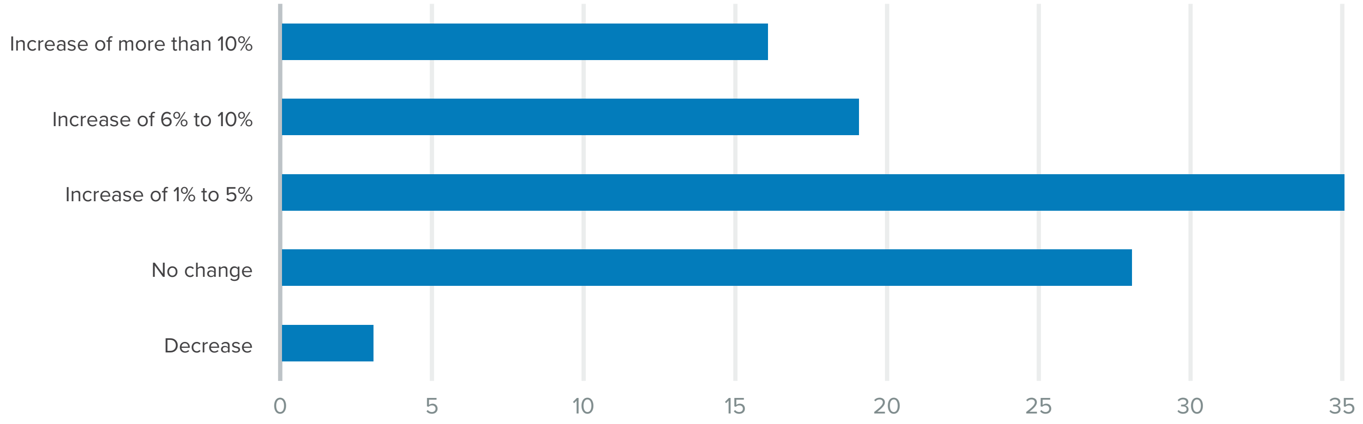


When asked how they expect their enterprise deployment of new data security software to change, respondents say:

- More public cloud deployments - 38%
- More private cloud deployments - 38%

Only 17% expect more on-premises deployments.

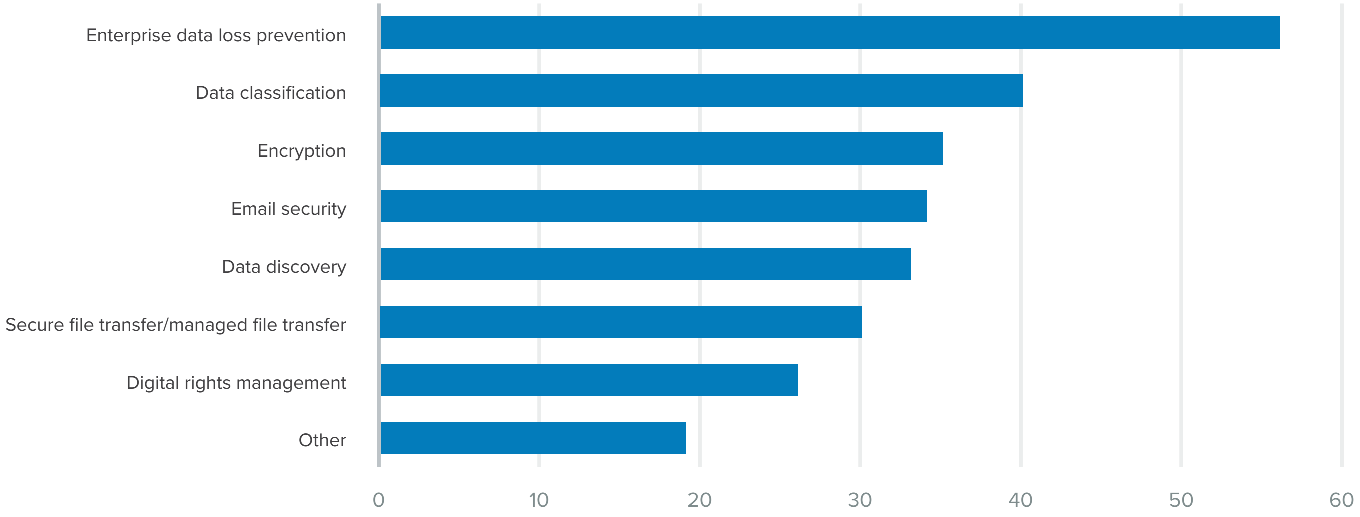
## How will your budget for cybersecurity change in 2022?



Looking toward 2023 investments, 35% of respondents expect increases of 1% to 5%, while 19% plan for increases of 6% to 10%.

Where will these funds be invested?

## In the next 12 months, which technologies do you plan to invest in?



The big three winners for 2023 data security planning:

- Enterprise data loss prevention - 56%
- Data classification - 40%
- Encryption - 35%

What does all of this mean? This report winds down with a set of conclusions next, followed by expert analysis of the results and how best to put them to work in your own organization.

The big three winners for 2023 data security planning: enterprise data loss prevention, data classification and encryption.

# Conclusions

In summing up the survey results, it is helpful to look back at some of the key findings articulated at the very beginning:

- 89% of survey respondents say their enterprises are more – or at least as – cyber-secure as they were one year ago.
- 52% say cyberthreats have become fiercer in that time period.
- 63% say data visibility is the biggest challenge facing their organizations today when they consider data security.

With these points in mind, and reviewing other insights unveiled in the survey responses, this report closes with the following conclusions:

## What Got You Here Won't Secure You Tomorrow

Yes, your enterprise might feel more stable than it did amid COVID-19, when it was a victory to achieve remote connectivity and avoid business disruption. But amid mass cloud migration, new software vulnerabilities and an adversarial focus on supply chain disruption, the security strategies and tactics that protect the enterprise today are not the ones you will rely on tomorrow. Cloud migration calls for cloud security strategies. It is, as the cloud service providers say, "a shared responsibility," and it is imperative to define what your share is.

## It All Starts With Data Security

A majority of respondents (63%) do not have adequate visibility into where data resides within their enterprise, and just as many (64%) are fearful of sensitive customer data being exposed in a breach. These concerns are the foundation for three 2023 spending priorities expressed clearly in this survey:

- **Data Classification**: Understand what data you have and where it resides.
- **Encryption**: Protect that data at its core so that in the event of a breach, there is no exposure.
- **Data Loss Prevention**: Adopt new processes and tools to protect the data wherever it resides, regulating who has access and permissions.

## New Ventures Require New Partners

This report lands amid the time that is referred to as “The Great Resignation.” After two years of COVID-19 quarantine, employees everywhere are awakening to new ambitions and opportunities. What was already a cybersecurity skills/staffing crisis has exploded into a greater global challenge. This reality puts a premium on partnerships – vendors that can offer the technology and skills necessary to address the heightened data security concerns showcased in this study.

“Finding talent to support cybersecurity goals and objectives is extremely challenging today,” says Cary Hudgins, vice president of product at Fortra's PhishLabs, which sponsored this research. “One of the things that Fortra can do is: We’ve got services; we’ve got solutions. We can partner with organizations to help you meet your objectives and close those security gaps that you might have that you can’t fill with personnel.”

For more of Hudgins’ analysis and commentary, see the last section of this report.

> “We can partner with organizations to help you meet your objectives and close those security gaps that you might have that you can’t fill with personnel.”
>
> – Cary Hudgins

SURVEY ANALYSIS

# CISO Perspectives: 2022 Data Security Survey

## Executive Insights on What Survey Results Mean – and How to Put Them to Work

NOTE: ISMG's Tom Field discussed the survey results with Cary Hudgins, vice president of product at Fortra's PhishLabs. This is an excerpt of that conversation.

Cary Hudgins

### The Results: Gut Reaction

**TOM FIELD:** What are your gut reactions to the findings?

**CARY HUDGINS:** In general, I have a very positive reaction. If this survey was taken a year ago, it would have had a very different feel to it. Based on the results, it looks like a lot of companies are returning to a state of normalcy. They've definitely shown resiliency, getting through that rocky 12 to 18 months of COVID. Based on some of the investments that were in the survey results, we see that companies are returning to more strategic planning, although there are absolutely, definitely some gaps. And companies are playing catch-up and trying to implement controls to support their hybrid workforce. We're still seeing the work from home/work in the office, and controls are being implemented to support that.

**FIELD:** What most surprised you?

**HUDGINS:** The fact that companies felt very in control of security was a little bit of a surprise to me. COVID security bounce-back is a real thing, a very material thing. So we were caught off guard a year ago, and now companies have truly bounced back and they're feeling like they've got their confidence back and they've got their swagger back. We're seeing budgets start to free up to do more strategic planning and less reactive planning around it, or less reacting to current events. In general, companies are starting to return to normal and accept the fact that where we are today is likely where we're going to be on an ongoing basis.

### Threats and Actors

**FIELD:** We asked the respondents about the threats and threat actors of greatest concern to them. Were their responses in line with what you see and hear from your own customers?

**HUDGINS:** Absolutely. The email-based threats continue to be among the top concerns for our clients and prospects that we talk to. That could be a run-of-the-mill credential theft-based email threat or a BEC attack. It could be ransomware or any malware that's delivered via an email. It's right to be concerned around those.

> "If this survey was taken a year ago, it would have had a very different feel to it."

We've seen about a 30% increase year over year of those email-based threats, and cybercriminal groups are primarily responsible for them.

**FIELD:** When our respondents tell us that they believe that cyberthreats have become fiercer, what do you believe that they're describing?

**HUDGINS:** "Fierce" likely means the severity of the impact. When we look at what's happening today in the threat landscape, threat volume is up, variety of threats are up and impact of those threats is also up. You have a trifecta of impact across the board. And at the same time, threat actors are becoming more creative and opportunistic. They're trying to take advantage of employees and companies that are in a state of change. They're trying to take advantage of a new and different digital footprint that companies have. As a result, attacks are up, and cybersecurity professionals should be concerned around the severity of the impact – whether it's financial, reputational or operational disruption.

## Cloud Security

**FIELD:** The one thing that was clear in the responses is that cloud is a big part of these organizations' futures. What risks and gaps should they prioritize as they forge ahead with this migration?

**HUDGINS:** Cloud migration is a positive thing. There is a lot of benefit with migrating to the cloud. But companies shouldn't get complacent and think that a cloud migration is going to, overnight, solve security concerns. A lot of traditional threats that target data centers cross right over to the cloud. So just because you've moved to the cloud doesn't mean you've suddenly secured your organization.

Also, a migration to the cloud is going to pose new challenges and new considerations to think about. Do you understand what data has been migrated to the cloud? How are you going to handle access controls? That is a big one. What are you doing from a role-based access perspective? What are you doing from a geographic perspective? And you still have GDPR considerations to keep in mind when you've migrated to the cloud. Do you have resources? The expertise to be able to manage a data center versus a cloud infrastructure can be very different.

## Priorities for 2023

**FIELD:** I'm not sure I've ever seen a figure quite this high: 97% of our respondents expect to see leveled or increased budgets in the year ahead for the issues we've talked about here. How do you respond to the priorities that they selected?

**HUDGINS:** It makes a lot of sense. It ties back to companies not only migrating to the cloud but also having a diverse and dispersed workforce. Workforces are likely to stay dispersed. And because of that, we're interacting with our co-workers in a very different manner. And cybersecurity organizations and leaders are being asked by their leadership team: How are you going to secure our

> "A lot of traditional threats that target data centers cross right over to the cloud. So just because you've moved to the cloud doesn't mean you've suddenly secured your organization."

“Mature security teams are investing heavily in a couple key categories. So as an organization, I would ask, ‘Where am I not investing, and why?’”

data and applications with a remote workforce? That’s a broad question, but if you look at where they’re investing, we can break it down further.

The first thing is: Do we even have an idea of where our sensitive data lies? If the answer is “no,” then it probably makes sense for a company to look into investing in a data classification solution so it can at least get a handle on what its sensitive data is. If data classification is under control, then the next question is: “How are you going to secure that data so that it doesn’t leave your organization unintentionally?” – so it doesn’t get leaked. If that’s a risk for your organization, you likely want to invest in a data loss prevention solution. And, as part of business as usual, companies and employees need to communicate sensitive data and files and transfer that information between themselves and other organizations. So what are your encryption plans? What is your secure file transfer solution? Those are three very fundamental, smart places to start thinking about investments.

## The Fortra Approach

**FIELD:** How is Fortra working with its customers to respond to the challenges that were discussed in the survey?

**HUDGINS:** There are two key areas where we can partner with our clients. One has to do with finding talent to support cybersecurity goals and objectives, which is extremely challenging today. There are about 3 million cybersecurity jobs open today. It’s very hard to get and retain talent. One of the things that Fortra can do is: We’ve got services; we’ve got solutions. We can partner with organizations to help you meet your objectives and close those security gaps that you might have that you can’t fill with personnel.

The second piece is something that’s been growing over the past decade and probably peaked during COVID: vendor fatigue or vendor sprawl. We have clients who work with 20 to 50 security vendors. That in itself is extremely challenging, and it takes security professionals away from executing on their key objectives. Fortra has established best of breed security solutions that cover a lot of different use cases – data loss prevention, digital risk protection, email security, data classification, secure file transfer, to name a few – [for which] a company may have previously had to retain 10 or 15 vendors. A client can come to this suite of solutions, and we can manage and solve a lot of their needs and help them meet their objectives without having to go out and find 10 unique vendors to do the job. Then the security professionals can focus on other areas of key need within their organization.

## Put Survey Results to Work

**FIELD:** What are your recommendations to our audience for how they can take these survey results and put them to work in their organizations?

**HUDGINS:** Take from the survey the insights that a majority of the respondents are all facing the same flavor of threats and challenges you are. And mature security teams are investing heavily in a couple key categories. So as an organization, I would ask, “Where am I not investing, and why?” Understand your points of weakness and your risk in those areas, and get a strategic plan around trying to solve those gaps. You may tackle it internally or partner with a vendor like Fortra. Changes aren’t going to happen overnight, but you can prioritize and execute and learn from what the mature organizations are doing. ■

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANKINFOSECURITY® CUINFOSECURITY® Just for Credit Unions GOVINFOSECURITY® HEALTHCAREINFOSECURITY®

infoRisk® TODAY CAREERSINFOSECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io