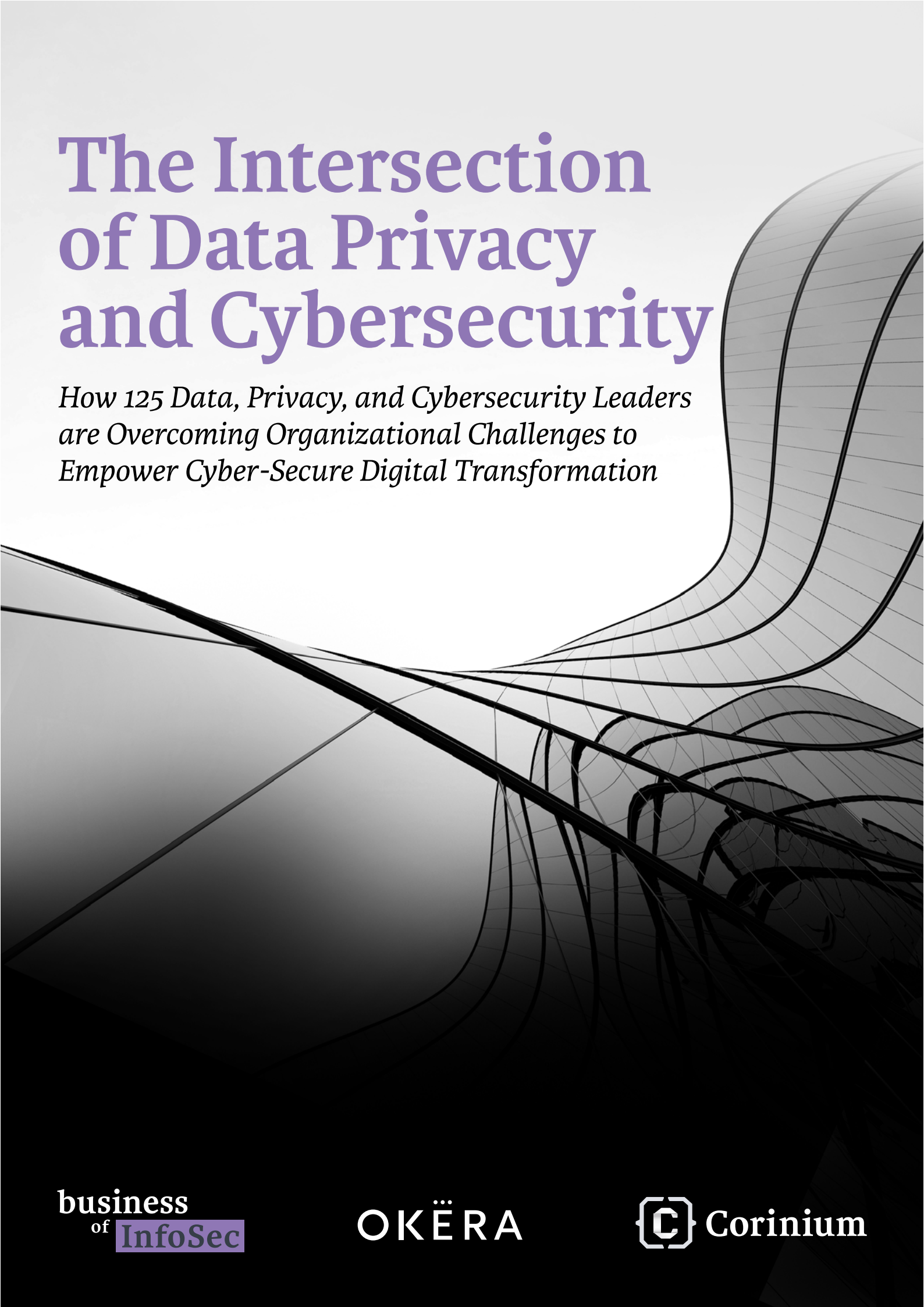
The Intersection of Data Privacy and Cybersecurity

How 125 Data, Privacy, and Cybersecurity Leaders are Overcoming Organizational Challenges to Empower Cyber-Secure Digital Transformation



business of InfoSec

OKERA

Corinium

Contents

Click below to navigate

Executive Summary

Data privacy and cybersecurity have risen to the top of corporate agendas since the onset of the global pandemic, fueled by the rapid shift to remote work and accelerating digital transformation roadmaps.

In addition, public interest in data privacy is stronger than ever with tech giants like Apple and Facebook engaged in a PR war over their use of customer data.

This report, conducted with our partners at Okera, summarizes our research into how businesses are responding to these challenges.

Our findings show that digital transformation initiatives are continuing apace and that providing secure access to sensitive data is a key concern for leaders in data governance, security, and privacy teams.

In addition, with increasing volumes of data being stored and shared in the cloud, many security leaders are seeing the benefits of centralized data access and control.

Compliance with fast-evolving data privacy regulations is also a top priority for data governance, security, and privacy leaders, in order to avoid both financial and reputational penalties.

Alongside the survey results, we present highlights from several top executives who shared their views on the intersection of data privacy and cybersecurity, as well as what they believe lies ahead. ■

Key Findings

72%
have moved at least half of their organization's data to the cloud

The #1
benefit of centralizing data authorization and control is ensuring data security at a fine-grained level

70%
are either 'very confident' or 'extremely confident' that they know where all their data is located

94%
see compliance with data privacy as a top priority

45%
are not concerned about penalties and fines due to non-compliance

Better regulatory compliance
is the leading driver of data privacy investments

Source: Corinium Intelligence, 2021

Methodology

This representative survey of 125 data privacy, cybersecurity and data leaders was conducted in April and May 2021.

Respondents included Chief Data and Analytics Officers, Chief Data Officers, Chief Information Officers, Chief Privacy Officers, Chief Information Security Officers, and Business Information Security Officers, as well as other individuals of similar standing.

The research focused on large companies in North America with 93% of respondents having more than 1000 employees, and 61% having more than 10,000 employees. Participating companies included: Home Depot, Travelers Insurance, Procter & Gamble, Pfizer, and JPMorgan Chase & Co.

We asked the respondents 15 questions about how they are overcoming challenges to enable cyber-secure digital transformation, keeping up with data privacy regulations, and ensuring secure data access and control.

The survey findings were then combined with commentary from ten industry experts to put these unique findings into context. ■

Contributors

Raj Badhwar
SVP & CISO,
Voya Financial

Michael Owens
BISO,
Equifax

Sharon Bauer
Founder & Privacy Consultant,
Bamboo Data Consulting

Lydia Payne-Johnson
Director, Information Security, Identity and Risk Management,
The George Washington University

Rick Doten
VP, Information Security & CISO,
Carolina Complete Health

Dan Power
Managing Director,
Data Governance,
State Street Global Markets

David Levine
VP, Corporate & Information Security, CSO,
Ricoh USA, Inc

Marian Reed
President and Cybersecurity Consultant,
SecurRisks Consulting

Nong Li
Founder & CTO,
Okera

Miguel Sanchez Urresty
Chief Data and Analytics Officer LATAM, Principal

Foreword

Ensuring data security and privacy is hard, and there seems to be no end to the string of major hacks and breaches making headlines. As I write this foreword, ransomware attacks on companies like JBS and Colonial Pipeline are front page news in the United States. Only a few weeks prior, a ransomware group followed through on its threat to release personnel files of the Metropolitan Police Department of the District of Columbia. The examples are endless and unrelenting. Simply put, digital data is stolen because it's valuable, and the global supply of data is increasing every day.

We all know and appreciate that governments at all levels have issued guidance, orders, and regulations to reduce the frequency and mitigate the severity of cyber attacks.

When the European Union issued the General Data Protection Regulation (GDPR) in 2018, it demonstrated the seriousness of data protection by imposing fines up to 4% of revenue for companies that failed to comply. Four percent is a huge number when you consider the investments companies make to reduce their tax burden. But we have all heard about companies that are not worried about fines, so we asked about it in this survey. The answers surprised us. The data indicates that many companies (45%) are indeed not worried about fines, but that doesn't mean they're not worried about compliance. On the contrary, respondents overwhelmingly report (94%) that compliance is an organizational priority, but their motivations appear to be focused on building trust with their customers and partners. In other words, they're looking at compliance strategically.

Additional survey results indicate a maturing and readiness for enterprise-scale data security. For example, all respondents have made investments to comply with data protection laws. A mere 6% report that they focused only on a single privacy regulation such as GDPR. The remainder are addressing multiple regulations, with an impressive 49% reporting a higher level strategic approach, in which they automate and standardize enforcement with multiple laws.

Similarly, 70% report that they're very or extremely confident that they know where all their data is. This is highly encouraging, because once companies know where their data is, they can manage it. Like everyone concerned with data security, we at Okera encourage a zero-trust approach to data access and authorization. It may be counterintuitive at first, but by locking down data by default, it becomes easier for companies to feel confident using an automated data authorization platform like Okera to provision access to those who need it for legitimate business purposes.

We at Okera thank Corinium Intelligence for conducting this survey and for the fascinating follow-up interviews with front-line industry experts. I hope you learn and enjoy the ah-ha! moments as much as we did.

No matter what software or processes you employ, I wish that you, your employees, customers and partners can always use data responsibly to achieve your goals and accelerate innovation. ■

Nong Li
Founder & CTO,
Okera

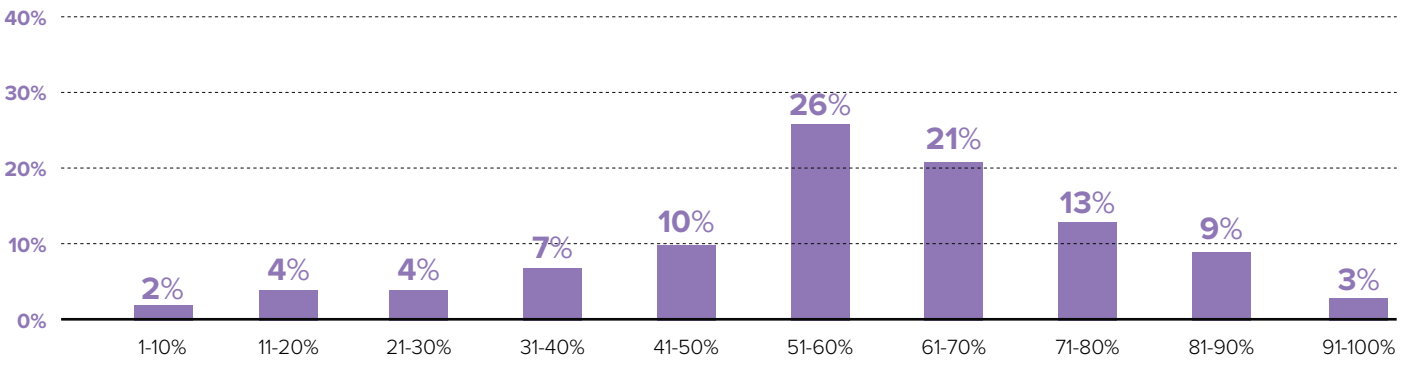
Data Security and the Journey to the Cloud

KEY FINDING

Data, security, and governance teams are facing fresh challenges as businesses walk the path of digital transformation

What percentage of your organization's data has been migrated to the cloud?

Select one



A disgruntled employee uploads customer data to a third-party platform, triggering the public naming and shaming of your company. A cache of regulated data is left unencrypted on an open server, creating a prime target for a cyberattack.

While nightmare scenarios like these are enough to keep data privacy and cybersecurity executives up at night, unfortunately, such events are **increasingly common.** Considering high levels of public interest in data privacy and the rapid acceleration of digital transformation roadmaps for enterprises, strong data governance frameworks and effective cybersecurity are essential.

Our survey of 125 data privacy, security, and governance executives on behalf of data access and governance technology company Okera, shows that companies are putting more of their data into the cloud as they walk the path to digital transformation.

In fact, 72% already have moved at least half of their organization's data to the cloud. This has many benefits, such as the ability to conduct analytics at speed, rapidly scaling artificial intelligence and machine learning initiatives, and reducing capital expenditure on hardware.

However, it also creates new challenges, like how to ensure data security at a fine-grained level and how best to manage the thorny question of data access and control – especially by third parties. ▶

"New innovations have completely changed our organizational structure and what we thought IT security would be. It's a new world – everything's moving to the cloud"

Rick Doten
VP, Information Security at Centene Corporation and CISO at Carolina Complete Health

Accelerating Cloud Transformation Roadmaps

Before the global pandemic, digital transformation was already underway for many enterprise companies. However, the disruption it caused changed mindsets and accelerated roadmaps.

As the pandemic required organizations to rapidly pivot to remote work and expand their digital infrastructure, the conventional 'walled garden' approach to network security was replaced by borderless networks.

"The explosion of remote working has created borderless networking in a way that we have never seen," says Equifax BISO Michael Owens. "Services that were done in-house are now being moved to the cloud. That's redefining what traditional network boundaries look like."

At the same time, our research shows that companies are moving more data to the cloud and buying more cloud-based services. This means businesses are more reliant on third parties to assure both their data security and the data privacy of their customers.

"The move to the cloud means companies are relying more and more on third parties, which extends and increases the number of external entities that are involved in every supply chain," says Owens.

"The move to the cloud means companies are relying more and more on third parties, which extends and increases the number of external entities that are involved in every supply chain"

Michael Owens
BISO, Equifax

Meeting Data Residency Requirements

This increased reliance on third parties complicates requirements when it comes to where data is stored, where it is backed up, and who has access to it. Depending on how regulated the industry, this could have significant ramifications on compliance.

"If you're using a cloud-based provider or solution, you have to look at a variety of key aspects including what data will be involved and its classification," says David Levine, VP of Corporate and Information Security and CSO at information management and digital services company Ricoh USA, Inc.

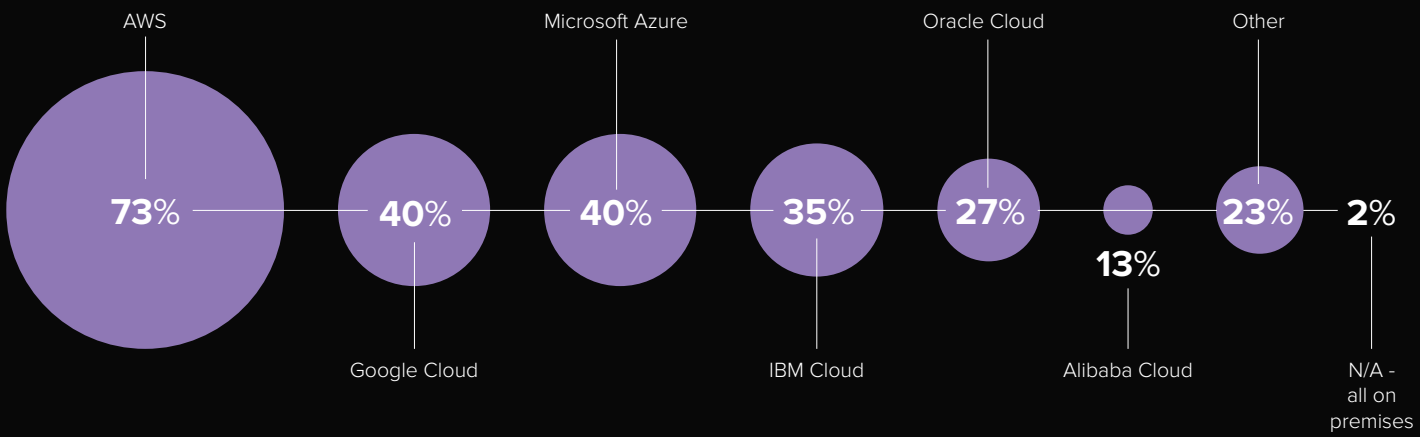
Asking these questions helps security and privacy-focused executives to determine how much risk is involved and informs the appropriate decisions about where data should reside.

Levine continues: "If the data and backup are in the US, that's one thing, but if the data, backups, or users are in Europe, that will likely have significant implications."

The accelerated transition to the cloud has presented security and privacy-focused executives with new challenges. Business leaders must consider where data is, how well it's protected and how it is accessed to keep up with fast-evolving data privacy regulations.

As digital transformation initiatives progress and more sensitive data is uploaded to the cloud, secure access and control of all data will become an ever more pressing priority. ■

What cloud services providers do you use?
[select all that apply]



Enabling Cyber-Secure Digital Transformation

KEY FINDING

As businesses continue to transform digitally, privacy, security, and data teams are balancing priorities on multiple fronts

From a data privacy perspective, the results of our survey of 125 security, privacy, and data executives are encouraging. They show that keeping up with data privacy regulations was a key priority for executives as they facilitate cyber-secure digital transformation.

However, keeping up with data privacy regulations is not their only concern. Our research shows that respondents are balancing other challenges too, like the potential for role bloat and policy complexity as they scale (50%), data breaches, internal or third-party misuse of data (50%) and rogue datasets (43%).

To face these challenges, privacy and security leaders need to develop a strong working relationship and come together early to develop a strategic roadmap to enable cyber-secure digital transformation.

"It goes back to the age-old saying that you can't do privacy without security, and you can't do security without privacy," says SecurRisks Consulting President and Cybersecurity Consultant Marian Reed. "Most organizations and most security programs are really focused on deploying tools to make sure that the whole network is protected without really understanding the business or the data that's involved."

She continues: "You have to look at the overall business risk and figure out what are the security components that really make sense, and what do we need to deploy in this organization to protect it? And you can't do that if you don't have your privacy team at the table."

One method of doing this effectively is to bring key stakeholders together regularly to discuss the transformation roadmap and ensure that data privacy and security concerns are being considered.

"I created an IT security committee, which had stakeholders from Legal, HR, and Privacy," says Reed. "They felt that they had a stake in the game and that their voices were being heard."

Collaborating in this way was an essential part of building a digital transformation roadmap that prioritizes data privacy and security by design.

"Don't design it, bring it to them and then hope for the best," concludes Reed. "Instead, make them part of the design phase so that they are actually helping you develop the program to meet the needs of both privacy and security." ▶

"It goes back to the age-old saying that you can't do privacy without security, and you can't do security without privacy"

Marian Reed
President & Cybersecurity Consultant, SecurRisks Consulting

When Spinning up New Services is a Problem

The potential for role bloat and policy complexity as they scale is a leading concern for 50% of senior executives, according to our research.

"Things like role bloat and rogue datasets we have versions of in our on-premises environment, too. So, most of those concerns are not brand new," says Dan Power, Managing Director of Data Governance Global Markets at financial services firm State Street. "But they are bigger, and the velocity and the scale have changed."

The potential for bloat in the technology stack has been fueled by the explosion of software as a service (SaaS). For enterprises with multiple business functions operating across the US and internationally, this surge in the use of SaaS could cause security and integration issues as well as inefficient spending.

"What happens is that one person doesn't realize there's another person on the other side of the company doing much the same thing, but with a different vendor. And they don't have a way to communicate," says Power. "The initial expense of buying the license or the subscription isn't the problem. It's seven or eight years later when you find out that you've essentially paid for the same solution repeatedly."

"When it comes to rogue datasets our biggest challenge from a security perspective is not some hacker, it's the disgruntled employee who sits down the hall"

Dan Power
Managing Director, Data Governance,
State Street Global Markets

Dealing with Internal Misuse of Data

Our research also revealed that the potential for misuse of data, either by employees or by third parties, is a top concern for half of data, privacy, and security leaders.

"When it comes to rogue datasets our biggest challenge from a security perspective is not some hacker, it's the disgruntled employee who sits down the hall," says Power.

He continues: "It's a constant moving target. Some new file sharing platform comes up that an employee knows about and suddenly they're uploading data to it and you don't even know until it's too late."

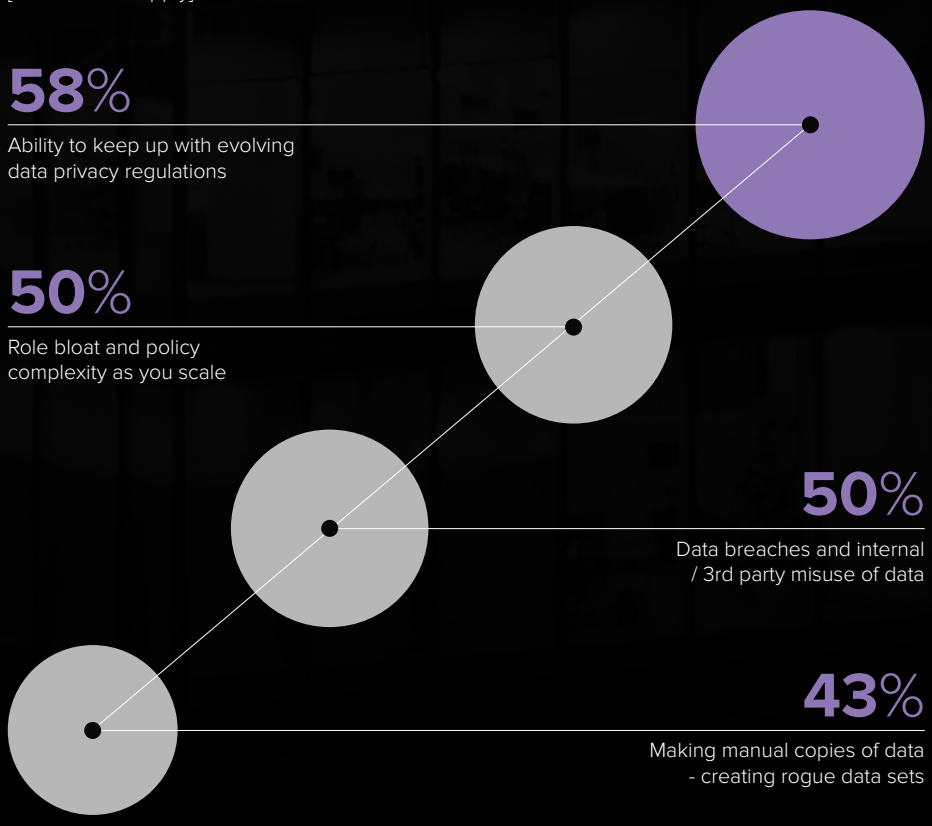
Of course, internal, or third-party misuse of data need not necessarily be tied to malicious intentions. Negligence can also lead to private or regulated data being exposed online.

In April 2021, Experian, one of the largest credit bureaus in the US, unintentionally **exposed the credit scores** of tens of millions of Americans to anyone online who could supply a name and mailing address.

In this case, poor API security meant that the database could be queried directly, without requiring any kind of authentication. With more data sharing between businesses and third parties taking place, it's increasingly important for businesses to share properly encrypted data through secure APIs.

"Digital transformation has led to a lot of APIs. So, API security is a concern," says Voya Financial SVP and CISO Raj Badhwar. "We put a lot of focus on API security to make sure that any API that is exposed externally or internally or otherwise in the cloud environment is fully authenticated." ■

What are your biggest concerns about enabling cyber-secure digital transformation?
[select all that apply]



Centralizing Data Access and Control

KEY FINDING

With more confidential, personally identifiable, and regulated data stored in the cloud, businesses are increasingly focused on improving their data governance practices and ensuring secure access

Understanding where sensitive data is located is the first step on the path to securing it. This aspect of data governance has been a persistent challenge for data-focused executives for many years.

"It's all about data governance. It's something the industry has been ignoring for decades," says Rick Doten, VP of Information Security at Centene Corporation and CISO at Carolina Complete Health.

As companies continue to transform digitally, developing proper data governance practices is essential, especially when data is increasingly being stored and shared in the cloud.

On that front, our research is very encouraging. An impressive 70% of data privacy, security, and governance executives are either 'very confident' or 'extremely confident' that they know where all their data is, and only 4% are 'not at all confident'.

This suggests that businesses are rapidly maturing in their approach to data governance, and that they feel they have the tools they need to do it.

Of course, there are several priorities relating to the location of data in the cloud, or elsewhere. Data-focused executives should know not only where the data is, but also its classification, how it is being controlled, who has access to it, and how that access is monitored.

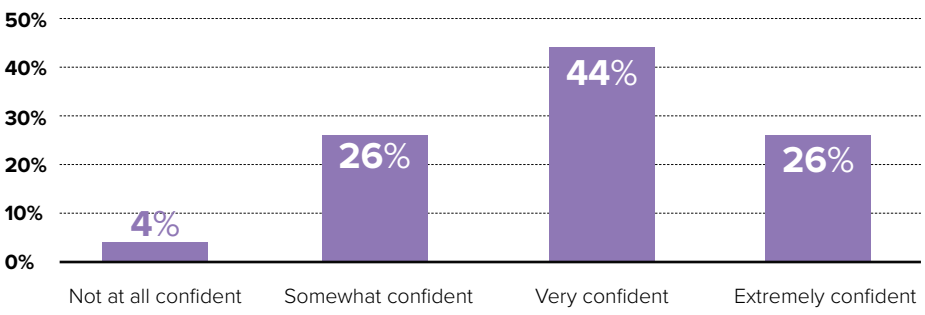
"We need to know where our data is, what it is, which applications access it, and who uses those applications," concludes Doten. "Then, we need to be able to tag it and control it. Data governance is the answer."

The Benefits of Centralizing Data Authorization and Control

Managing multiple databases and IT systems can complicate the task of effectively controlling data security and access. Technical difficulties in granting secure fine-grained access to data where it lives can lead to problems like the creation of rogue datasets.

According to our research, the biggest benefit of switching to a centralized platform for data authorization and control is to ensure

How confident are you that you know where all of your data is?
[select one]



data security at a fine-grained level. This would allow all sensitive data to be managed by a tightly controlled, centralized process, mitigating the dangers associated with rogue datasets.

"Having a single pane of glass view into the overall health, compliance, and auditing of your entire company as well as its the applications and data – that that would be fantastic," adds Equifax BISO Michael Owens.

Other benefits that companies attribute to centralized data authorization and auditing include adoption of a zero-trust policy for data access, improved customer experiences, the ability to drive innovation, and create new revenue opportunities.

Getting data into the hands of the right people is critical to data-driven businesses. Our research suggests that the benefits of centralized data access and control on business drivers like improving customer experiences and enabling innovation are even more desirable than conventional concerns like improving operational efficiency and cost savings.

"I think that it certainly will help with business value, automation and also more optimization of processes which leads to greater efficiency and speedier delivery," says Voya Financial SVP and CISO Raj Badhwar.

Adding value in this way helps security, privacy and governance leaders to position investments into data governance and security as value-generating in themselves.

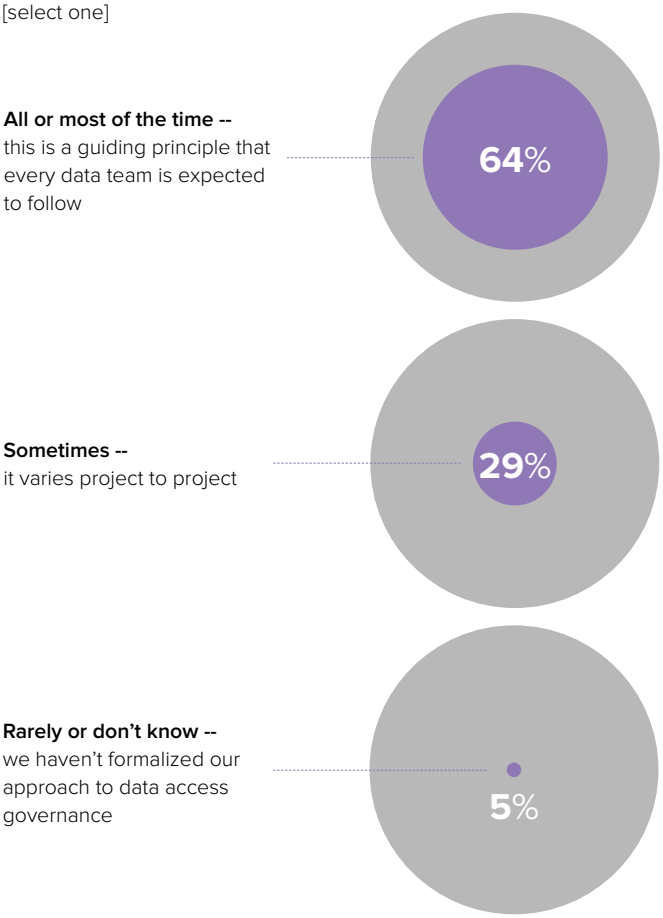
"The security function generally is not a moneymaker. It is commonly a cost center," continues Badhwar. "So, any added benefit that you can give to the business through any kind of centralization optimization certainly is welcome."

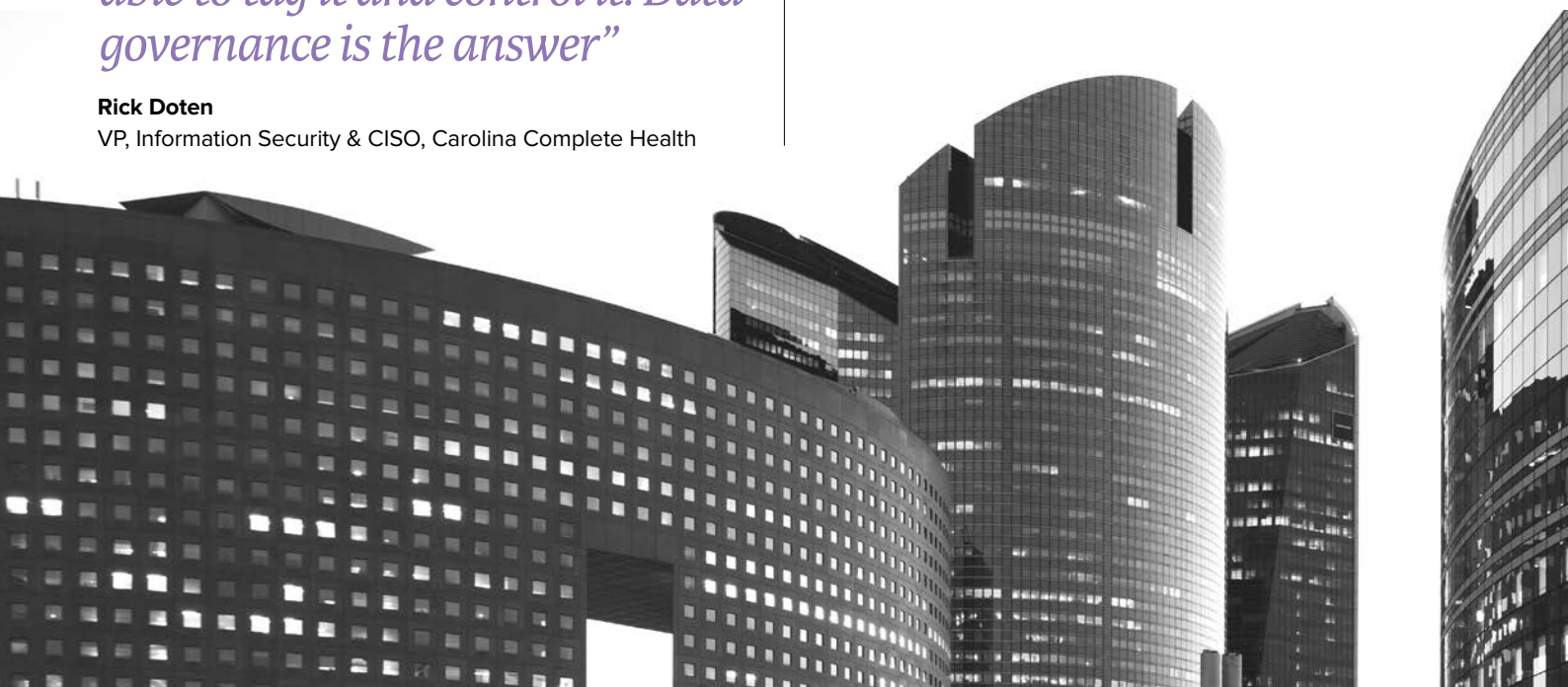
"We need to know where our data is, what it is, which applications access it, and who uses those applications. Then, we need to be able to tag it and control it. Data governance is the answer"

Rick Doten
VP, Information Security & CISO, Carolina Complete Health

Does your company take a zero-trust, least-privilege approach to secure data access?

[select one]





Adopting a Zero-Trust Approach to Data Access

Zero trust has become an increasingly important priority for security teams since the pandemic began. This is largely due to the rapid transition to working from home, as the resulting pivot away from a 'walled garden' approach to data security.

Our research shows that another key benefit of centralizing data authorization is the ability to adopt a zero-trust approach. However, while 64% of respondents reported that zero trust was already adopted as a guiding principle all or most of the time, 29% have not yet implemented it uniformly.

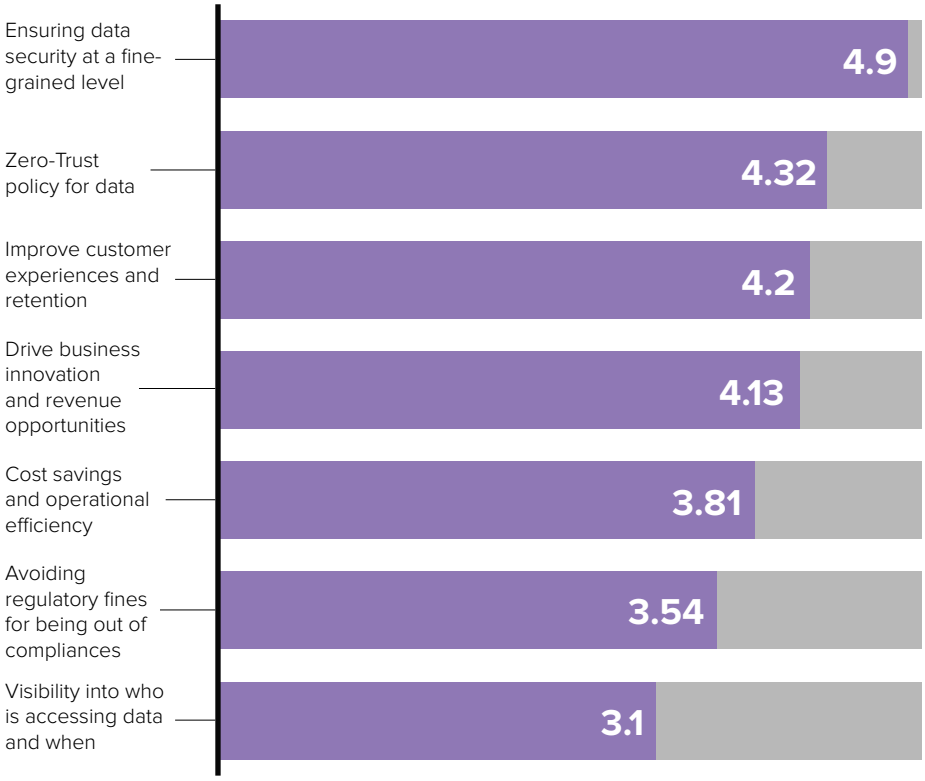
Part of the problem is that overlaying a concept like zero trust on an existing security stack is no simple task. Instead, many security leaders are focusing on aspects of zero trust to complement their existing framework.

"You can't just go buy zero trust. It would be great if you could as it's such a broad, sweeping endeavor with many nuances. The important thing, however, is just to get started," says David Levine, VP of Corporate and Information Security and CSO at information management and digital services company Ricoh USA, Inc. "There are a lot of different aspects to that, like multi-factor authentication and micro-segmentation, which is even more important now with the proliferation of ransomware."

While a zero-trust approach is very different from traditional methods of looking at perimeter defense, it all comes down to making sure that only the people who need access to particular applications or environments have it. This is particularly important for companies in heavily regulated industries that hold large amounts of sensitive data.

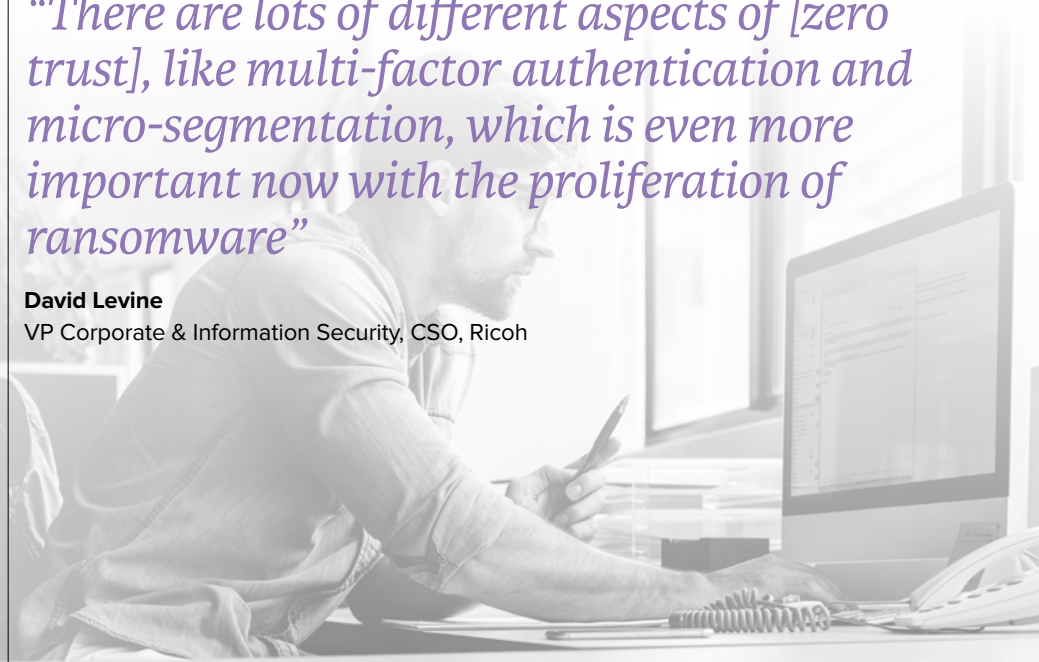
"We have databases that grow by half a billion records a day so it can be hard to keep your arms around all that data and to give access thoughtfully," says Power. So, we're prioritizing investments based on simplifying our infrastructure and making it more resilient." ■

If you could centralize data authorization and auditing across your entire data ecosystem, how would your company benefit most?
[rank in order of biggest benefit]



"There are lots of different aspects of [zero trust], like multi-factor authentication and micro-segmentation, which is even more important now with the proliferation of ransomware"

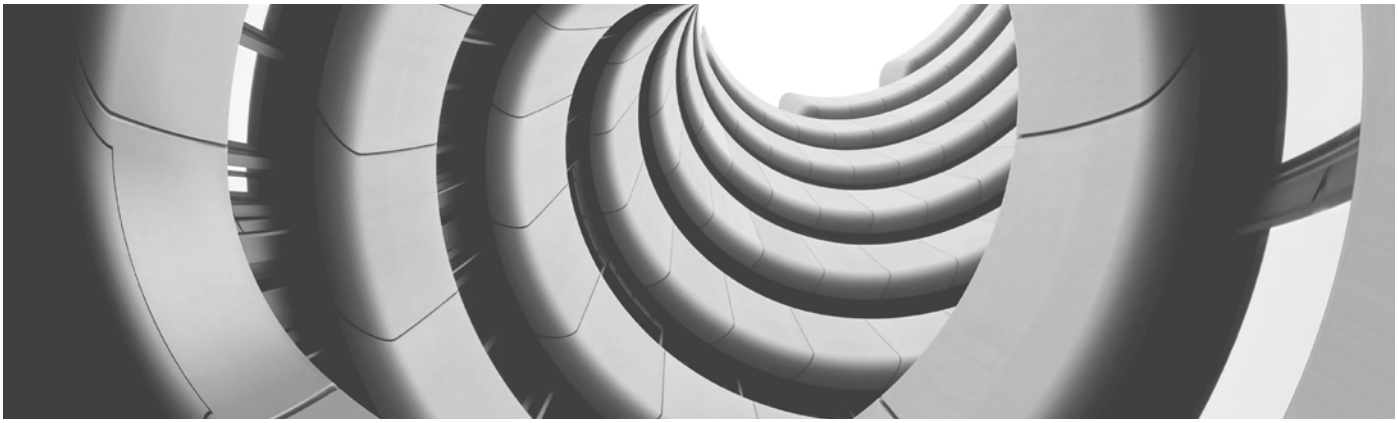
David Levine
VP Corporate & Information Security, CSO, Ricoh



Keeping up With Evolving Data Privacy Regulations

KEY FINDING

Compliance with data privacy regulations is a top priority for security, privacy, and governance teams



In January of 2018, California became the first state to pass comprehensive consumer data protection legislation in the US. Since then, **several states** have followed suit, with several more bills currently moving through their respective state legislatures.

However, the lack of centralized, federal regulations on data privacy in the US has created a regulatory landscape that is not only fast-moving but also fragmented.

These factors, as well as the introduction of sweeping data privacy regulations internationally, like GDPR in Europe and POPIA in South Africa, are likely driving data privacy up the list of priorities for businesses in the US. Our research shows that 94% of data, security, and governance executives now consider meeting compliance requirements 'very much a priority', or 'an extremely important priority'.

Interestingly, 45% of respondents reported they are not worried about penalties or fines due to data privacy regulations.

This is surprising as penalties, at least theoretically, can be **extraordinarily large.** However, these concerns may be mitigated by the belief that smaller, less prominent companies may not become the target of regulators. Or, if they are targeted, that the fines will not be as significant.

The survey results strongly suggest that companies take privacy regulations seriously. However, interpreting this survey result is somewhat difficult, as 31% of respondents report not being worried about fines specifically because they are already in compliance.

Our findings hint that there may be reasons to seek compliance for reasons other than fear of being fined, which is discussed next.

"It's a business decision. If the fines are manageable, some companies just budget that in," says Rick Doten, VP, Information Security at Centene Corporation and CISO at Carolina Complete Health. "If it is more expensive to do all this stuff to be compliant, then they'll just pay the fine." ▶

"You take a reputational risk when you fall out of regulatory compliance. If you lose customer trust, you can't simply pay a fine to fix it"

Raj Badhwar
SVP and Global CISO, Voya Financial.

A New Focus on Reputational Risk

Customer trust, once lost, can be difficult to regain. Reputational damage due to being non-compliant is another reason for businesses to take compliance seriously.

"You take a reputational risk when you fall out of regulatory compliance," says Raj Badhwar, SVP and CISO at Voya Financial. If you lose customer trust, you can't simply pay a fine to fix it. So senior leaders are very worried about the reputational risk."

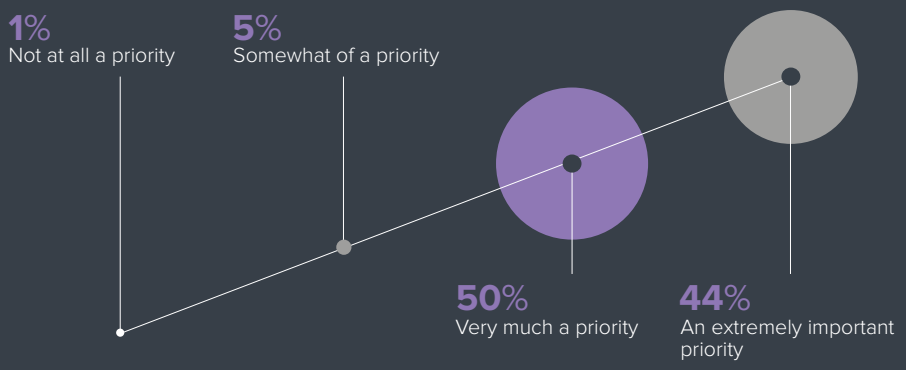
"There is naming and shaming happening all the time by regulators and the media," adds Sharon Bauer, Founder and Privacy Consultant at Bamboo Data Consulting. "And more recently by nonprofit organizations who are putting companies in the spotlight if they abuse people's privacy."

In contrast, some privacy and security leaders are proactively using customer-facing data privacy policies for positive public relations. This approach is particularly timely as the very public conflict between two of the largest technology companies in the world, Apple and Facebook, **plays out** in the media over their use of customer data.

"We asked ourselves, how can we create a strategic advantage out of this regulation?" says Miguel Sanchez Urresty, Chief Data and Analytics Officer LATAM at financial firm Principal. "If we are compliant and we can make that public, we can increase customer confidence in our company. For me, that's going to be an advantage point for businesses in the future."

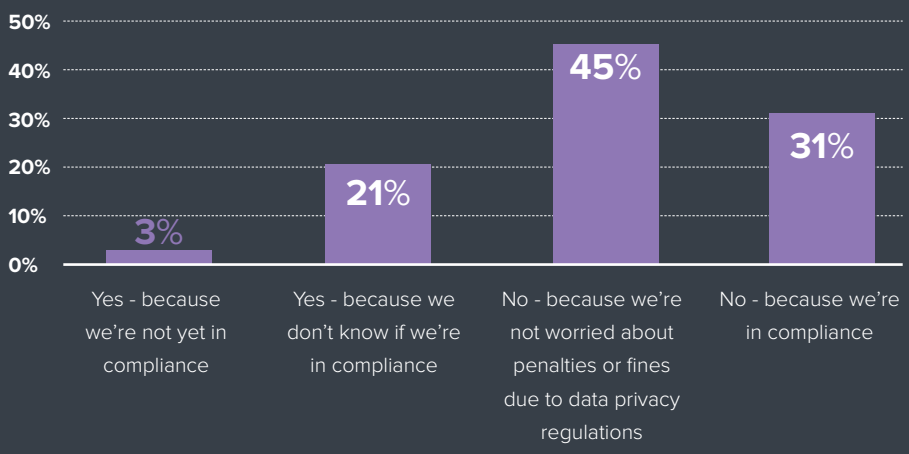
How much of a priority is compliance with data privacy for your organization?

[select one]



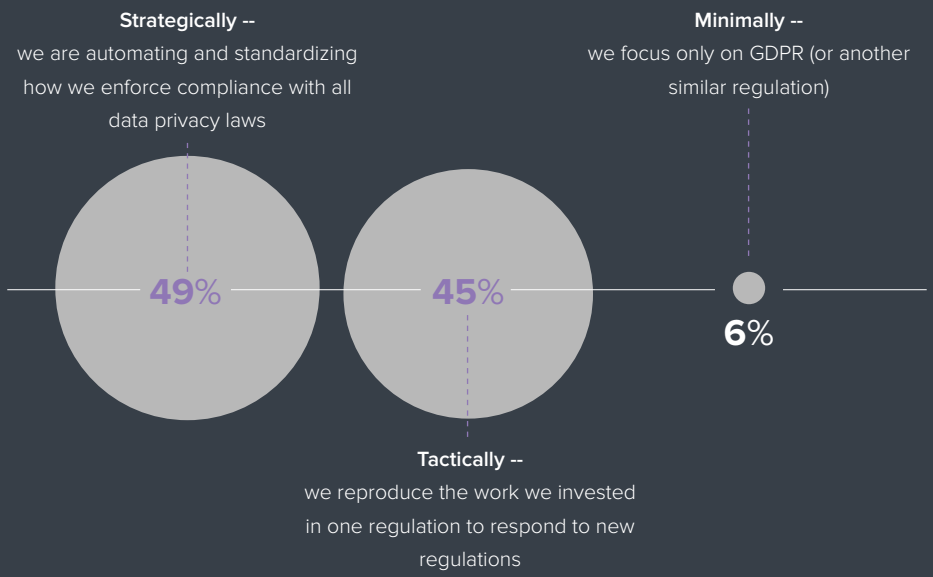
Are you worried about penalties or fines due to data privacy regulations?

[select one]



How is your company responding to the rapid expansion and evolution of data privacy laws?

[select one]



Two Approaches for Data Privacy Compliance

All the participants in our research have implemented protections for personally identifiable information (PII) stored in their systems. The responses suggest that the vast majority are operating in multiple states or regions. Only 6% are responding to rapidly expanding and evolving data privacy regulations minimally, by focusing on one specific regulation.

Of course, different businesses operating in different industries and regions will base their approach to data privacy compliance on their circumstances. However, our research hints at a rapidly maturing response to regulations as companies progress beyond tactical projects to strategic automation and standardization.

45% of respondents are taking a tactical approach by reproducing the work invested into one regulation to respond to new regulations. One effective means of doing this is by taking the requirements of the most stringent regulation and applying them uniformly across the business' data privacy landscape.

"If you benchmark the organization against the gold standard in privacy, then the organization will likely be compliant with all other regulations," says Sharon Bauer, Founder and Privacy Consultant, at Bamboo Data Consulting. "For example, if GDPR is the gold standard and the most prescriptive privacy legislation out of all of them, then it may make sense to benchmark yourself against the GDPR."

Meanwhile, our research also shows that an impressive 49% of respondents are taking a strategic approach by automating and standardizing flexible systems to to dynamically enforce compliance with a wide variety of evolving regulations.

"Standardization and centralization are good things in this area, as long as the laws are uniformly applied," says Voya Financial SVP and CISO Raj Badhwar.

Ultimately, businesses will decide how to approach the rapid evolution of data privacy laws based on their unique circumstances. However, all businesses will need to keep their eye on the horizon as new laws are introduced at the state level, federally, or internationally. ■

"We asked ourselves, how can we create a strategic advantage out of this regulation? If we are compliant and we can make that public, we can increase customer confidence in our company"

Miguel Sanchez Urresty
Chief Data and Analytics Officer LATAM, Principal

Making the Case for Data Privacy and Cybersecurity Investments

KEY FINDING

To secure budgets for data privacy and security initiatives, governance, security, and privacy leaders must be able to prove the software's utility to the business as well as ROI

In the past, some organizations treated privacy and cybersecurity as siloed risk areas. Other organizations experienced a 'turf war' between CISOs and CPOs over who should own the responsibility for data privacy.

However, the rapid escalation and increasing sophistication of cyberthreats, the evolving regulatory landscape, and the acceleration of digital transformation are highlighting the need for CISOs and CPOs to focus on common objectives.

"CISOs and CPOs need to align their information risk and privacy risk programs to create an integrated approach that supports business risk management, establishes realistic controls that support business processes, and enables better investment decisions," says Lydia Payne-Johnson, Director, Information Security, Identity and Risk Management at The George Washington University.

"Thinking of privacy as a component of your overall security stack is what sometimes gets missed," Payne-Johnson concludes. ▶

"CISOs and CPOs need to align their information risk and privacy risk programs to create an integrated approach that supports business risk management, establishes realistic controls that support business processes, and enables better investment decisions"

Lydia Payne-Johnson
Director, Information Security, Identity and Risk Management, The George Washington University

Framing Risk in Business Language

CISOs and CPOs need to work together when justifying investments into the access and security of confidential, personally identifiable, or regulated data to senior leadership or the board.

Our research points to a significant variation between businesses in terms of who is responsible for authorizing the budget to ensure that sensitive data is properly accessed and secured.

When it's time to justify that spend, however, the responsible person should communicate the risk of inaction in a context the board can understand – the language of business risk.

"One of the key things is that you've got to be able to explain to your executive team what the risks are," says SecurRisks Consulting President and Cybersecurity Consultant Marian Reed. "For too many years, we've [taken the approach of] scaring our executives by warning that we could get fined. But no one has really talked to them about the impact at the business operational level."

Our research shows that the top three drivers of investments into the secure access of confidential, personally identifiable, and regulated data are better regulatory compliance (54%), improved business efficiency (50%), and managing costs (44%).

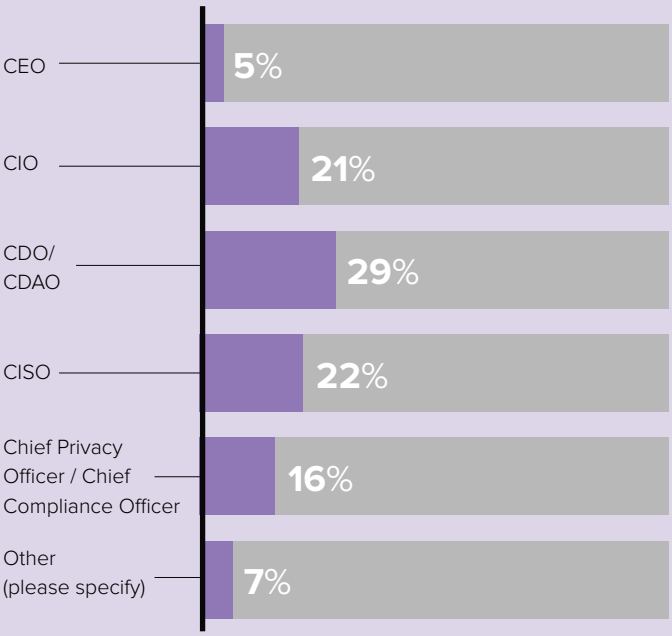
"I think the CPO and CISO need to be in almost constant communication about how they are determining and measuring how adequately risk is being assessed within the organization," adds Equifax BISO Michael Owens. "It should be a very collaborative relationship and when possible, a combined risk assessment should be seamlessly presented to

"For too many years, we've [taken the approach of] scaring our executives by warning that we could get fined. But no one has really talked to them about the impact at the business operational level"

Marian Reed
President and Cybersecurity Consultant, SecurRisks Consulting

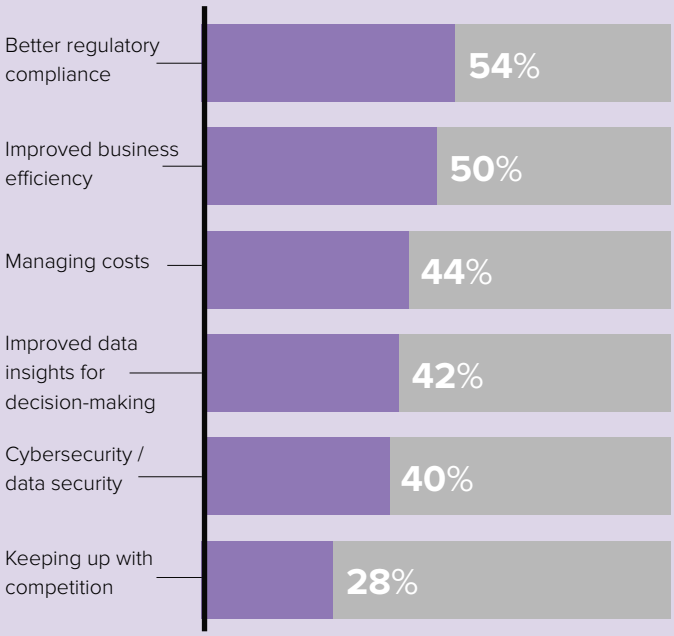
Who in your organization authorizes the budget to assure that confidential, personally identifiable, and regulated data is properly accessed and secured?

[select one]



Which of the following drivers have the biggest impact on investment decisions relating to the access and security for confidential, personally identifiable, and regulated data?

[select up to three]



the board."

Measuring the Success of Tech Investments

Another key component of justifying investments into data privacy and security technology is how the success of those investments is measured.

Our research highlights the leading metrics that organizations are using, including utilization, like the number of permitted users and consumption patterns (62%), ROI (53%), and time to market or delivery on business objectives (40%).

While ROI is often promoted as the most important measurement of success, the leading metric selected by our respondents was a much more basic metric: utilization. Users can and do reject technology that does not provide business benefits. The survey results suggest that simple usage and consumption metrics can proxy achievement for goals that are much harder to measure, such as building a data culture or technical maturity.

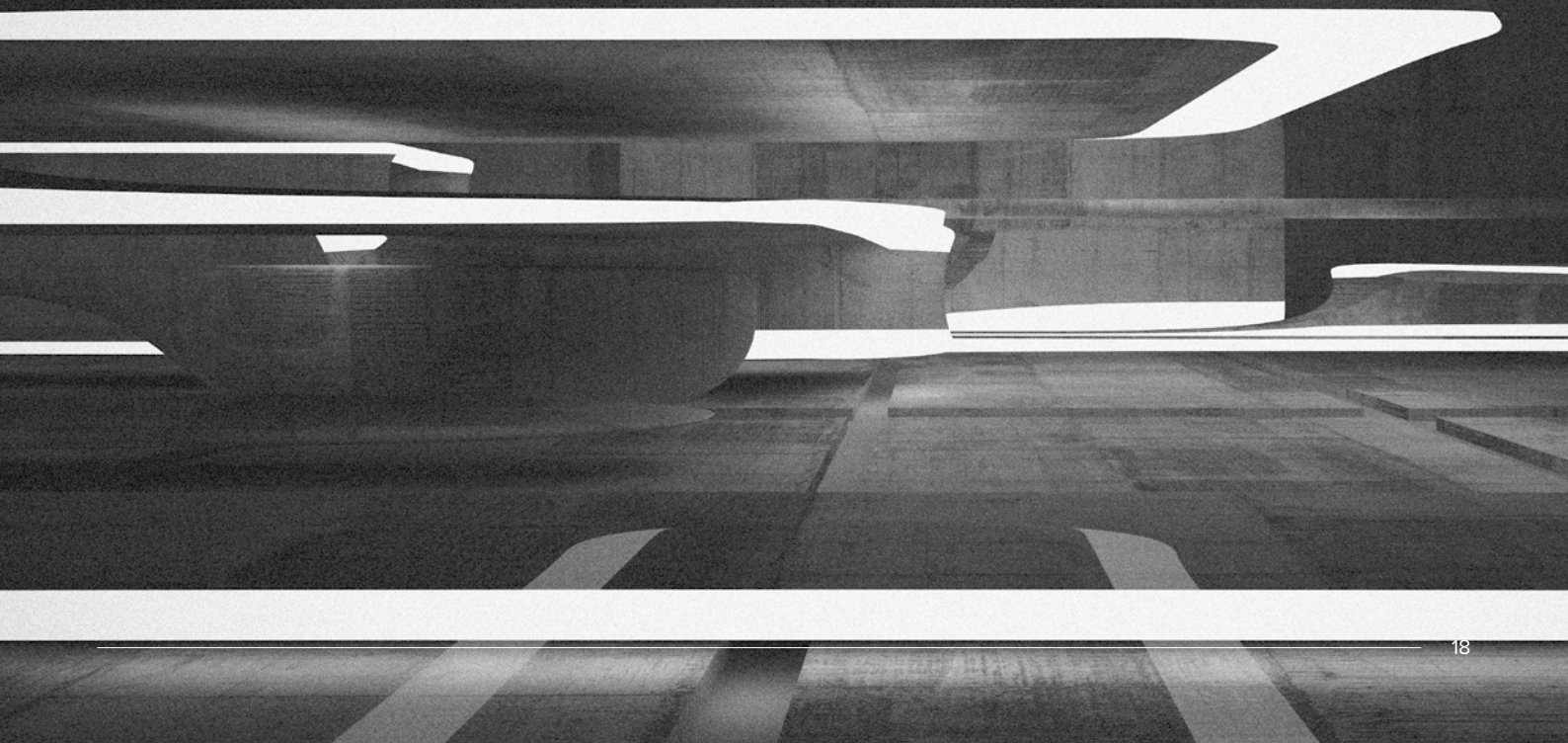
Secondly, data, privacy, and security leaders are measuring the ability of technologies to drive ROI and their impact on overall business goals. And while ROI may be challenging to prove, particularly about security and privacy risk avoidance, many organizations do have means to quantify indirect ROI.

"We are held accountable [for our investment decisions] and we have to show the return on investment, either direct or indirect. And most of us have a calculator for that," says Voya Financial SVP and CISO Raj Badhwar. "You're going to have some returns from the betterment of data security by the reduced number of exfiltrations or unauthorized access. You must also quantify the reduced reputational risks."

CISOs and CPOs must foster a strong working relationship to champion the cause of privacy and security risk throughout businesses. In addition, by presenting a clear and unified message to the board they can more effectively justify investments designed to ensure secure access to confidential, personally identifiable, and regulated data. ■

What metrics do you use to measure the performance of your tech investments?

[select all that apply]



Discover More Essential Information Security Insights

As anyone who has attended our global conferences or events will know, our 40,000-strong network of information security leaders boasts many of the most forward-thinking minds in the industry.

Our new content hub, **Business of InfoSec,** brings those same essential insights direct to you and is packed with exclusive research, video podcasts, in-depth articles, interviews, and reports. Discover how other information security leaders are tackling the challenges they face today while maintaining the confidentiality, integrity, and availability of their organization's data.

For a limited time, subscribing to the **Business of InfoSec** is free. So, make sure to subscribe today for complimentary access to exclusive insights you just can't find anywhere else.

SUBSCRIBE NOW

business of InfoSec

Follow us on LinkedIn

Follow us on YouTube

About Okera

OKERA

Use Data Responsibly with Universal Data Authorization

Okera, the universal data authorization company, helps modern, data-driven enterprises accelerate innovation, minimize data security risks, and demonstrate regulatory compliance. The Okera Dynamic Access Platform automatically enforces universal fine-grained access control policies. This allows employees, customers, and partners to use data responsibly, while protecting them from inappropriately accessing data that is confidential, personally identifiable, or regulated. Okera's robust audit capabilities and data usage intelligence deliver the real-time and historical information that data security, compliance, and data delivery teams need to respond quickly to incidents, optimize processes, and analyze the performance of enterprise data initiatives.

Okera began development in 2016 and now dynamically authorizes access to hundreds of petabytes of sensitive data for the world's most demanding F100 companies and regulatory agencies. The company is headquartered in San Francisco and is backed by Bessemer Venture Partners, ClearSky Security, and Felicis Ventures

.For more information, please visit: **www.okera.com**

About the Editor

Gareth Becker is an experienced editor and content marketer and produces B2B stories that focus on emergent trends in data and analytics, cloud computing, information security and more.

He works with world-leading brands to shine a light on fresh ideas and innovative products using a range of multimedia content.

To share your story or enquire about appearing in a Corinium report, blog post or digital event, contact him directly at **gareth.becker@coriniumgroup.com**

Gareth Becker
Content Strategist,
Corinium Global Intelligence

Corinium

Partner with Business of InfoSec by Corinium

We'll develop in-depth benchmarking research, special reports and editorial content to establish your brand as an industry thought leader.

Find out more:
www.corinium-digital.com

Discover Corinium Intelligence

Corinium is the world's largest business community of more than 300,000 data, analytics, customer experience and digital transformation leaders.

We're excited by the incredible pace of innovation and disruption in today's digital landscape. That's why we produce quality content, webinars and events to connect our audience with what's next and help them lead their organisations into this new paradigm.

Find out more: **www.coriniumintelligence.com**

Connect with Corinium

- **Join us at our events**
- **Visit our blog**
- **Read our white papers**
- **Follow us on LinkedIn**
- **Follow us on Twitter**
- **Like us on Facebook**