keepit

The great balancing act

Cybersecurity leaders tackle rising pressures

The great balancing act

Executive summary

CISOs and CIOs are grappling with numerous challenges, including geopolitical instability, stringent regulations, and the uncertain impacts of generative AI. These issues are compounded by budget constraints and talent shortages. To understand how security leaders are managing these challenges, Keepit conducted interviews with over 30 senior IT leaders across industries in 2024. This e-book highlights their insights and strategies for addressing pressing data security and backup challenges.

The interviews revealed several key IT trends shaping enterprise technology changes. Cloud flexibility is a major trend, with 80% of organizations adopting a "cloud smart" approach that introduces new security and compliance challenges, particularly in maintaining consistent data governance across diverse environments. The rise of GenAI presents significant regulatory and expertise challenges, as many CISOs feel underprepared due to a lack of specialized knowledge in AI and cybersecurity.

Security, IT, compliance, and financial risks are more interconnected than ever, requiring CISOs to develop unified risk management strategies while aligning controls

with regional regulatory requirements. Even though security budgets are increasing to accommodate new technologies like GenAI, the ever-growing scope and number of threats to protect against means prioritization and strategic planning are more crucial than ever.

The fundamental priority of protecting and securing data is at the heart of any security leader's agenda. CISOs now have broader responsibilities, focusing on aligning cybersecurity initiatives with business objectives.

Effective communication of cyber risks to stakeholders is crucial as data volumes surge. CISOs typically have 24–36 months to demonstrate impact, emphasizing the need for quick, effective solutions and strategic vendor partnerships. Establishing effective data governance frameworks is challenging yet essential, requiring precise, practical data classification and buy-in from various functional areas.

CISOs should adopt a risk-impact framework to align cybersecurity efforts with business objectives. Engaging the board of directors in cybersecurity discussions is essential, with CISOs translating technical concepts into business terms and demonstrating the ROI of cybersecurity initiatives. Effective data classification is foundational for data governance, starting with broad categories. Customizing existing governance frameworks can help address unique organizational needs, with robust governance structures and policies critical for effective data management.

Adopting transparent cybersecurity controls with clear KPIs and strong SLAs builds trust with stakeholders.

Data security and backup and recovery are pivotal for balancing innovation and protection. CISOs and CIOs must continuously improve their strategies, collaborate effectively, and invest in robust data-centric solutions. Their ability to enable and protect data-driven innovation will define their success in the evolving digital landscape.

Introduction

In 2024, Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) face a daunting array of challenges as they strive to protect their organizations' data assets. From geopolitical instability and aggressive regulatory regimes to the powerful but uncertain impacts of generative AI (GenAI), the list of concerns keeps growing. At the same time, perennial problems like budget constraints and talent shortages are becoming even more acute.

To gain insight into how CISOs and CIOs are navigating this complex landscape, Keepit conducted in-depth interviews with over 30 security leaders and senior IT leaders across industries. This eBook distills their perspectives on the most pressing data security and backup and recovery challenges they face and the strategies they are employing to overcome them.

Market trends

01

Trends shaping enterprise IT

These interviewed CISOs, CIOs, and senior security leaders highlighted key IT trends that are driving broad organizational technology changes and challenges. Additionally, these interviewed sources reported four key trends that are driving underlying change:

1. Cloud flexibility

According to Nutanix's research, 80% of organizations are now "cloud smart" with optimized workloads across public cloud, private data centers, and edge deployments as needed. Interviewed sources highlighted this issue by reporting that the adoption of hybrid multi-cloud introduces new security and compliance challenges.

> "In our hybrid cloud deployments, our company faces the issue of maintaining consistent data governance and compliance across multiple environments while ensuring network security and identity management remain robust.
>
> Balancing the diverse security protocols of public clouds, private data centers, and edge deployments requires meticulous planning and integration efforts to mitigate risks effectively and often exceeds our internal team's experience and expertise levels."
>
> – CISO, US National Insurance Company

2. The rise of AI

Another topic that interviewees highlighted was the emergence of GenAI. GenAI has captivated business leaders, but it is not always clear what constitutes a mature, enterprise-ready AI solution. Many CISOs and CIOs interviewed reported feeling more prepared for AI from a technology and strategy perspective than from a talent and governance standpoint.

> "With the introduction of AI into enterprise platforms and applications, as well as AI used by teams and employees, we are now having to navigate the complex regulatory landscapes, such as GDPR, HIPAA, or PCI DSS, when deploying AI systems, to ensure that AI practices comply with relevant laws and regulations governing data protection, privacy, and security.
>
> But, the other issue is that AI requires specialized expertise in both AI and cybersecurity, that our teams do not have the knowledge or experience to manage."
>
> – CTO, Business Collaboration Platform

Blog:// Forrester Total Economic Impact of Keepit SaaS Data Protection

3. Interconnected risks

Security, IT, compliance, and financial risks are increasingly interlinked, but regulatory frameworks remain siloed. CISOs reported that they are tasked with developing unified risk management approaches while still mapping controls to specific regional requirements.

> "Over the past 24 months, I have found myself increasingly navigating the intricate web of interconnected risks spanning security, IT, compliance, and financial domains that previously were not as much as a concern – they were more siloed.
>
> Today, despite these risks intertwining, regulatory frameworks remain compartmentalized, leaving me with the challenge of devising unified risk management strategies while aligning controls with distinct regional requirements.
>
> I'd love some help with being able to find a framework or strategy to help with this unified risk management process."
>
> – CISO, International Financial Services Firm

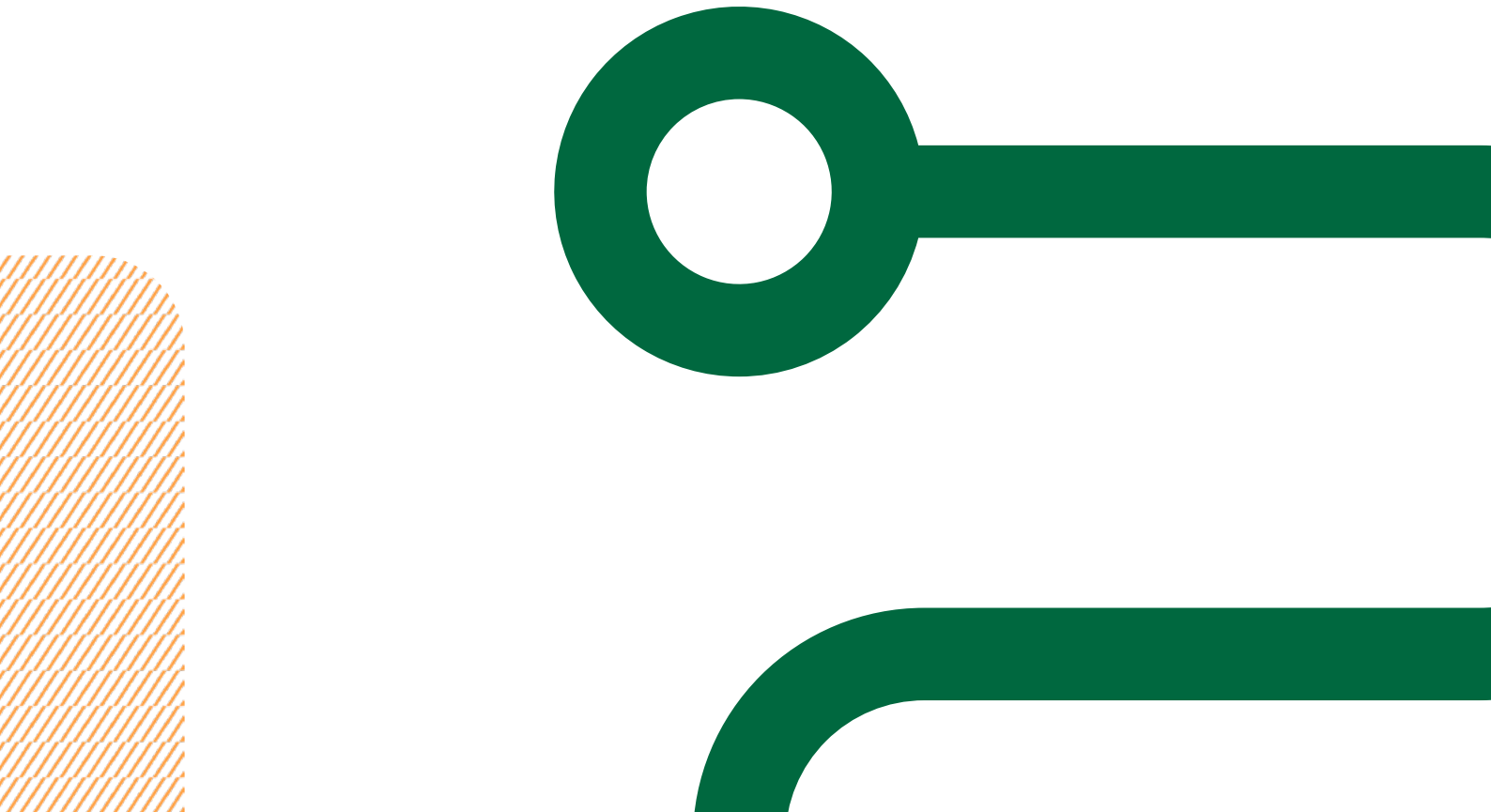
4. Budget pressures

Even as the need to invest in innovations like GenAI grows, security budgets are facing greater scrutiny. CISOs reported that they need to better articulate the business value of security investments in new ways.

> "I think one of the biggest challenges I have had as a security leader is communicating the need and value of cybersecurity, data management, and data governance in terms of value to the business using return on investment and total cost of ownership terms as well as risk to the brand."
>
> – Head of cybersecurity, Large national US retailer

The critical importance of data underpins all of these challenges. Data governance and management have become core competencies that CISOs must master, even as the cloud and AI introduce new complexities. As one CISO told us:

> "We're still adding vendors, moving to the cloud and AI. We're working hard to protect our business from everything that's happening. But it is an ongoing battle, mostly because this is a new area for us – and most people – and it is unchartered territory for our teams."
>
> – CISO, International Telecommunications Service Provider



Pain points

02

The data management and data security imperative

The fundamental priority of protecting and securing data is at the heart of any security leader's agenda. CISOs reported the following four challenges specifically related to data management that they and their organizations were experiencing:

The evolving role of CISOs and CIOs

Throughout our conversations, we consistently noticed the variability in CISOs' backgrounds and responsibilities. Our respondents had diverse paths to their roles, but the overall variability and lack of relevant expertise was discussed as a reason data-focused innovations might be slowed down or not carried out properly. Disparity in tenure was also raised as a complicating factor.

For instance, many CISOs that were interviewed came from either a security or audit background and tended to focus on outcomes — the infamous checklists. They are deft at adopting and adapting frameworks and achieving compliance, whereas CISOs with engineering backgrounds tend to be better at pushing for security maturity across operations.

While these two outcomes might feel like they are direct opposites, our own conversations and other reports show that while the two backgrounds might differ in approach, they align on mission: security by design. As both a cultural and technical strategy, whether platforms are being bought or built, CISO efforts are focused on security as they build out their infrastructure.

Interviewed CISOs also reported that their job duties are highly evolving, with CISOs increasingly focused on "ensuring cybersecurity requirements are met before technology investments are made," which again boils down to ensuring said investments are secure by design. However, when it came to the complexities and nuances of data governance, especially in the age of AI and the cloud, many felt they were lacking the expertise necessary to make it happen.

The other challenge that CISOs and ▶

"Business risk is increasingly encompassing cyber risk while business resilience encompasses cyber resilience."

CIOs reported is that their roles have broadened in focus. Where they were traditionally IT-centric, it is now essential to consider the impact on the broader organization. As one interviewed CIO from a renewable energy company stated:

> "Business risk is increasingly encompassing cyber risk while business resilience encompasses cyber resilience." In other words, "cyber risk is now business risk"
>
> – CIO from a renewable energy company

Interviewed leaders reported that as their organization's data volume surges, ensuring its security at scale becomes paramount, with confidentiality, integrity, and availability as core principles.

Interviewed CISOs and CIOs also reported that they have found themselves forced to focus on strategically integrating more robust risk management controls to safeguard against financial, reputational, and regulatory risks.

Additionally, effective communication of cyber risk to employees, partners, contractors, and board members is essential, as security teams face immense pressure to defend against sophisticated attacks, with organizational leaders bearing significant responsibility for incident response and mitigation.

> "My role, compared to it even five years ago, is going beyond hardening IT-related environments. Now, I am expected to contribute to board-level discussions on alignment of cybersecurity initiatives that contribute to broader business objectives and strategic goals, international compliance and governance standards, country-level data privacy and compliance standards, and be a thought partner to the CTO on the effectiveness and security of emerging technologies."
>
> – CISO, International Telecommunications Service Provider

Time to value

The CISOs interviewed were very conscious of the average lifecycle of a modern enterprise CISO. While there are many different data points available, most reports and research suggest that modern CISOs have between 24 to 36 months to enact their strategies and plans before a company change forces a voluntary or involuntary separation.

One CISO from a large international financial services firm told us, *"In any large enterprise, I know my typical lifespan at that organization is between 24 to 36 months because of the nature of corporate dynamics… acquisitions, leadership changes, etc. So, when I get into a new role, I have to build for the now. I need results and I need products and vendors that have a short time to value. I can't build for the future…I have to show results quickly."*

As CISOs and CIOs face the reality that they have very little time to make an impact, more pressure is placed onto their staff, contractors, and vendors. This new fact makes it so IT and cybersecurity leaders are carefully vetting vendors that can perform as strategic partners to aid in speeding that time-to-value lifecycle.

> "If I find a vendor that will truly partner with me, then I am going to bring them with me into every new role I am in. Conversely, this puts a lot of pressure on vendors. They are only as good as their last project or implementation, so it is critical to find the best and work with them."
>
> – VP of Worldwide Data Protection, Global Coffee Company UK Branch

Analysis:// The 2023 Fortune 500 CISOs

Need for data governance compliance framework

One of the top reported challenges reported by interviewed leaders was identifying and adopting an appropriate data governance framework that fits their organization. Sound data governance depends on adopting precise, yet practical, frameworks for consistent data handling across the organization. Yet, it remains elusive as security professionals, IT legal pros, and CIOs struggle with choosing and implementing the right framework. As one professional told us:

> ”The number one thing I face as a CISO challenge is to find a governance framework that works for our specific organization.’” – Head of cybersecurity, Large national US retailer.”
>
> – Head of cybersecurity, large national US retailer

CISOs and CIOs were quick to mention that establishing data governance is meaningless without first establishing and implementing a data classification foundation. Interviewed leaders said developing data classification models, compliance controls, and other elements of these frameworks is labor intensive and requires expertise and buy-in from other functional areas in order to achieve successful adoption across the organization. Further, much of data classification remains manual, and many organizations struggle to identify and ratify a data classification and corresponding governance framework that fits their business.

Another interviewed security leader put the challenge this way:

> “I have found that the current available and published regulatory and industry frameworks aren’t evolving towards consolidation. The “The number one thing I face as a CISO challenge is to find a governance framework that works for our specific organization”
>
> – Head of Cybersecurity Operations, International Commerce Retailer

Blog:// Cloud data: Shared responsibility and the importance of backup

All agree everything starts and ends with data. Beyond the macro problem of competing regulatory and compliance frameworks, successful data governance also requires rapid adoption of the chosen framework. Ideally, if they're precise and practical, they become the structures around which stakeholders will collaborate to ensure data is handled consistently across the organization.

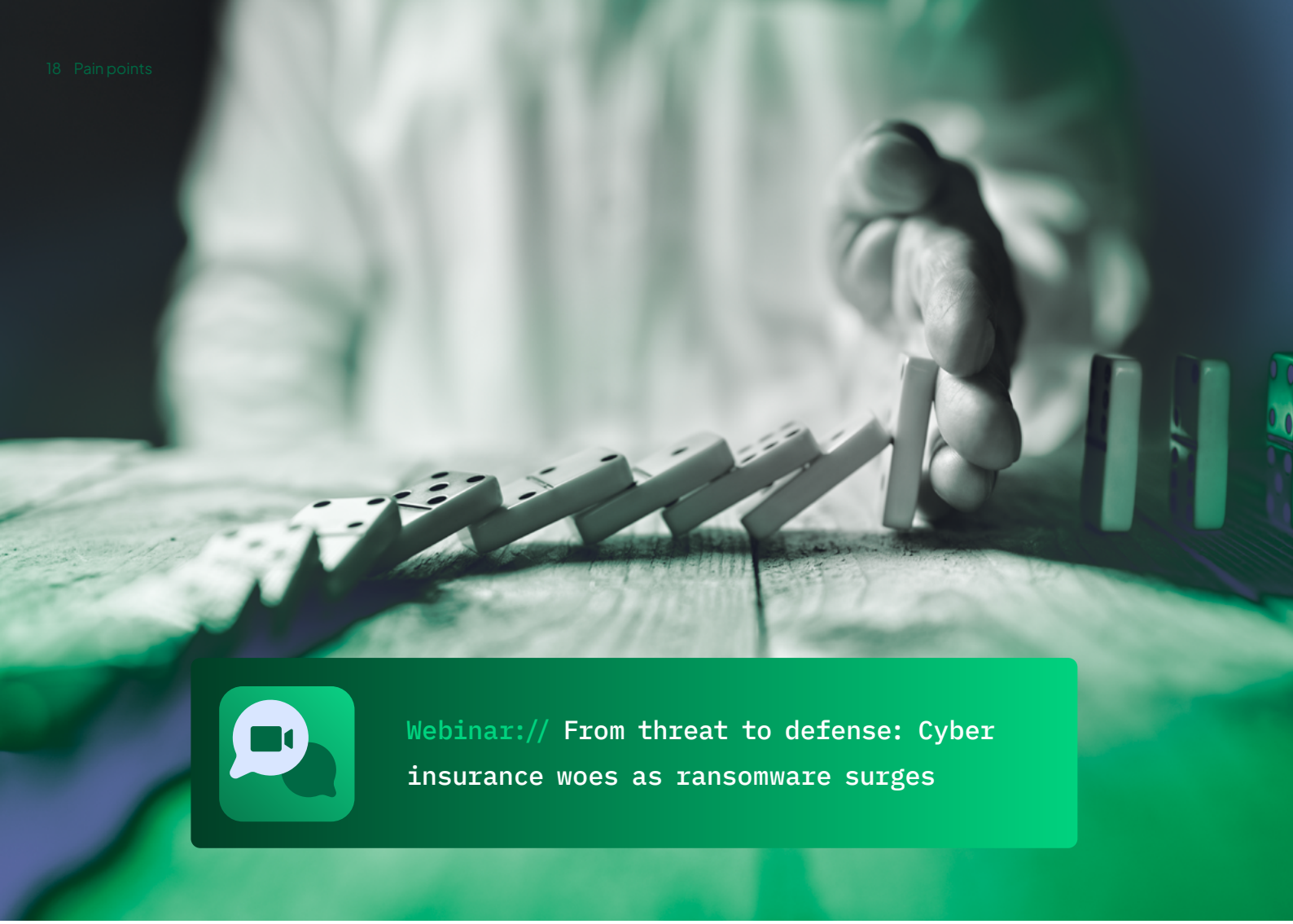
At the same time, these structures can't be so rigid they break when extended to new pipelines and processes. The best balance is a set of fundamental frameworks, with additional guidance introduced for specific applications and workflows, extending existing policies wherever possible. But it's also a lot of work, and businesses don't always have the practical or theoretical expertise to get it done.

We interviewed CISOs and CIOs who told us this complexity starts with how data is classified. What's sensitive versus public? What degree of sensitivity and why? Who manages these levels, and when and why will they change? CISOs and CIOs are tasked with synthesizing the competing demands of IT, security, operations, finance, and everybody else to produce a framework that's comprehensive but easy to use.

This classification work sets the stage for everything else, from compliance controls to AI pipeline design and deployment. We also heard that much of this work, especially classification, is still managed manually. This can make AI and other data-focused innovation precarious: How will all this administrative work scale? When can we automate our way out of this? According to multiple interviewed CISOs and CIOs, data classification is critical to establish the foundation of a general cybersecurity strategy and to enable an effective security compliance strategy. According to a CISO of a large international telecommunication service provider,

> "In my experience, governance is part of security. When I talk about data governance framework, I talk about data classification first, whether that is data loss prevention or data governance, it is all about data classification."
>
> – CISO, International, Telecommunications Service Provider

Blog:// Compliance and continuity



Webinar:// From threat to defense: Cyber insurance woes as ransomware surges

Another point the interviewed leaders highlighted is the additional risk and complexity from third parties, such as vendors, partners, and contractors.

With data- and AI-driven organizations relying on expansive data supply chains, the security practices of numerous data service and solution providers become a major risk factor. Vetting these practices is a top pain point with CISOs and CIOs reporting that they are struggling to keep up.

> "Our data supply chain – made up of internal data, data from customers, partners, and vendors – is another area that I am currently struggling with in terms of data management and hygiene.
>
> We have overlapping environments, gaps in governance frameworks, and a lack of deep expertise—which is all multiplied by the number of data service and solution providers inside our solution environment.
>
> – VP of Technologies, Online Learning Platform

Breaking down the black box

Rising regulatory scrutiny is forcing businesses to demonstrate not just security outcomes but the maturity of practices around privacy, compliance, retention, and continuity. CISOs and CIOs reported needing clear metrics to communicate data security postures to diverse stakeholders, including holders, the board of directors, and cyber insurers.

According to the head of cybersecurity operations for an international commerce retailer, "The old way CISOs have communicated to the internal leadership team, their board of directors, to their cyber insurance providers, and to investors is outdated. We need new metrics and a new codification to communicate cyber risk, data management, protection, governance, and overall proactive fortification of our IT estate. The problem is, honestly, I do not know what those metrics are or how to communicate these concepts to these four groups in a more effective way."

Speaking of insurers, CISOs and CIOs told us that cyber insurance companies are increasingly influencing cybersecurity practices by requiring stringent evidence of security controls and compliance. Cyber insurance companies are writing exclusions into their coverage based on security challenges, charging exorbitant fees, or just outright denying coverage if companies are not well prepared for multiple cybersecurity issues.

> "My board and CEO are breathing down my neck because our cyber insurance company is threatening to write in exclusions for ransomware if we do not select a more perceived 'enterprise-oriented data management vendor.'
>
> Insurers are now an influencer in who we select as a vendor. I thought the vendor we were working with was solid, but the insurer wants one that has a more robust security architecture and does not rely on the public cloud for any of its backups."
>
> - CISO, US National Insurance Company

While CIOs own cyber risk, the organization's board of directors needs to become more educated and more engaged in overseeing and governing cybersecurity strategies. CISOs and CIOs that we interviewed reported that unless there is a security breach or cyberattack, cybersecurity is not often a topic of discussion at board meetings. Interviewed CISOs and CIOs reported that more effort to educate and communicate effectively with board stakeholders is an urgent requirement. According to one senior security professional,

"Cybersecurity is full of interconnected risks, disconnected rules, and regulators.... Where security, IT, compliance, and financial risks were once managed inside autonomous silos, this is increasingly out of step with how stakeholders and regulators operate. We need the board of directors to be involved to encourage and ensure there is a top-down approach to security, governance, and compliance."

– Head of Cybersecurity Operations, international commerce retailer

"Where security, IT, compliance, and financial risks were once managed inside autonomous silos, this is increasingly out of step with how stakeholders and regulators operate."

– Head of Cybersecurity Operations, international commerce retailer

Based on the interviews of these cybersecurity and IT leaders, mastering data fundamentals, including classification and governance, is critical for compliance and a prerequisite for safely leveraging innovations like generative AI and modern cloud data platforms. As one CISO noted:

"Sensitive data will be used as input to these models and applications. The output generated might be equally sensitive for different reasons. It all has to be solved before the magic can happen."

The path forward

03

Adopting a risk-impact mindset

While the data security and backup and recovery challenges are daunting, the CISO and CIOs we spoke with remain forward-looking.

Interviewed leaders shared several strategies for solving for the highlighted challenges and advancing data management practices in response to ever-evolving roles and time-to-value challenges, such as the adoption of risk-impact thinking for prioritization and realistic solutions. By translating technical risks into business terms using common frameworks and metrics, CISOs and CIOs can improve alignment between security and business outcomes and optimize resource allocation. At the same time, leaders highlighted the need to view cybersecurity solutions through a careful balance of understanding the total cost of ownership together with the potential impact of cybersecurity threats.

Interviewed CISOs and CIOs spoke candidly about adopting a risk-impact rationalization strategy to support project prioritization, determine the realistic ability to deliver results, and better understand the value of a cybersecurity or data governance initiative to an organization.

The risk-impact analysis used by IT and CISOs and CIOs is a strategic approach to evaluating cybersecurity risks incorporating total cost of ownership with the potential impact on business value. This approach involves assessing risks based on their likelihood of occurrence and the potential consequences they pose to the organization's objectives, assets, and stakeholders. It enables IT leaders and CISOs and CIOs to make informed decisions about cybersecurity investments and resource allocations by aligning security efforts with business objectives and priorities. This approach also helps organizations prioritize risks effectively, optimize risk mitigation efforts, and maximize the value of cybersecurity investments. ▶

The risk-impact framework includes the following components:

a. **Risk identification:** Identifying and cataloging potential cybersecurity and compliance risks facing the organization, including threats, vulnerabilities, and potential impacts. This includes understanding the latest threat trends, compliance requirements, and emerging governance issues to accurately determine risks.

b. **Risk assessment:** Assessing the likelihood and potential impact of each identified risk, considering factors such as the probability of occurrence, the severity of impact, and the effectiveness of existing controls. The CISOs and CIOs we interviewed highlighted the importance of analyzing the severity of impact not just on the organization's infrastructure but also the potential impact on the organization's brand and reputation.

c. **Impact analysis:** Evaluating the business impact or significance of each risk in relation to the organization's strategic objectives, critical assets, and stakeholder interests.

d. **Prioritization:** Prioritizing risks based on their risk-impact profiles, focusing on those with the highest potential impact on business value and critical assets.

e. **Mitigation planning:** Developing risk mitigation strategies and action plans to address high-priority risks, including the implementation of appropriate controls, policies, and procedures.

f. **Monitoring and review:** Continuously monitoring and reviewing the effectiveness of risk mitigation measures, adjusting strategies as needed based on changes in the risk landscape or business priorities.

While many CISOs and CIOs we spoke to highlight the need to adopt the risk-impact framework, many were passionate about company leadership and even the board of directors helping to drive the risk-impact discussion.

According to one CISO from an international financial services firm, "the risk-impact conversation has to come from the board, not the CISO .... The board needs to acknowledge this responsibility and take on the task as well as its implications. For example, a very real scenario that we face is in Poland. We have a very small group of customers in Poland that contribute under 0.5% of our company revenue. Poland has adopted GDPR, but they have also made a modification that allows Polish citizens to request erasure of their personal data with companies needing to comply within 72 hours or face a 1,000 Euro fine for each instance. Now, as a company using the risk-impact framework, I may not want to spend 80,000 Euros per year to maintain the staff and software to support a heightened consumer data erasure process and instead just take the fines, which will likely be significantly less. I know that sounds cold, but that is a very real consideration. But we also have to analyze the potential impact to our brand ... again, the risk-impact analysis needs to come from the very top, beginning with the board of directors."

Asses your organization, department, and yourself → See appendix 1

When in search of a winning data governance framework

Involve the board of directors and investors in cybersecurity and governance strategies

Our interviews and discussions with CISOs, CIOs, and senior IT leaders showed a clear theme: They passionately argue for the need to increase involvement of organizations' boards of directors with cybersecurity and data governance strategies and process decisions. Many leaders we interviewed highlighted that it is the job of CISOs and IT leaders to rapidly earn "a seat at the (board of directors) table" to update board members, even if it is for 15 minutes of a board meeting.

According to the Director of IT Cybersecurity Consulting for a large International IT Consulting Firm, it is critical for CISOs to help board members understand more technical concepts and how they have business implications. "As a CISO, I firmly believe that the involvement of our company's board of directors in cybersecurity and data governance decisions is paramount.

Cyber threats pose significant risks to our organization's operations, reputation, and bottom line, making it essential for board members to understand and actively engage in shaping our cybersecurity strategy. Their oversight and support are instrumental in ensuring that we allocate resources effectively, prioritize key initiatives, and maintain resilience in the face of evolving threats.

By fostering a culture of cybersecurity awareness and accountability at the highest levels of leadership, we can better protect our company's assets, build trust with stakeholders, and safeguard our future success."

CISOs and CIOs that have become a trusted advisor to their board also reported other critical actions, including:

- **Align with business objectives:** Frame cybersecurity and data governance discussions in the context of the company's overall business objectives and risk tolerance. Highlight the impact of cybersecurity on key business functions, financial performance, and reputation.
- **Translate technical concepts:** Translate technical cybersecurity and data governance concepts into language that resonates with board members who may not have a technical background. Focus on business implications, risk management strategies, and the importance of cybersecurity as a business enabler rather than a purely technical issue.
- **Demonstrate ROI:** Clearly articulate the return on investment (ROI) of cybersecurity and data governance initiatives by quantifying the potential cost savings, risk reductions, and business benefits associated with effective security controls. Use metrics and case studies to illustrate the tangible impact of cybersecurity investments.
- **Seek board feedback and support:** Solicit feedback from board members on cybersecurity and data governance strategy, priorities, and challenges. Leverage board members' expertise and networks to garner support for cybersecurity initiatives and resource allocation. ■

Asses your organization, department, and yourself → See appendix 2

Enact a data classification strategy

Data classification is the process of categorizing data based on its sensitivity and importance to implement suitable effective measures based on the critical nature of the specific data category.

Data classification plays a foundational role in the protection of data from unauthorized access and ensures compliance with regulations. In our interviews, several CISOs and CIOs highlighted the importance of establishing a data classification process, which is paramount to having an effective data governance framework.

With the emergence of AI and AI-enabled software, this is where enterprises can create scalable data classification processes and systems. Data classification is the process of separating and organizing data into relevant groups ("classes") based on their shared characteristics, such as the level of sensitivity risks they present, and the compliance regulations that protect them. To protect sensitive data, it must be located, classified according to its level of sensitivity, and accurately tagged. Then, enterprises must handle each group of data in ways that ensure only authorized people can gain access, both internally and externally, and that the data is always handled in compliance with relevant regulations.

When done correctly, data classification makes using and protecting data easier and more efficient and becomes the foundation for critical data governance strategies and the driver for broad security controls. To create a data classification strategy, information is divided into predefined groups that share a common risk, and the corresponding security controls required to secure each group type are identified. Classification tools can be used to improve the treatment and handling of sensitive data and promote a culture of security that increases awareness of data sensitivity and prevents the storing of sensitive content on removable media or third-party web portals.

If a company is beginning its data classification without a platform or tool, resist the urge to get too granular, as granular classification schemes tend to cause confusion and become unmanageable. Many CISOs and CIOs we spoke to recommended three to four classification categories as being effective to start. On the following page is an example of a four-category data classification structure.

"Public"	"Internal only"	"Confidential"	"Restricted"
Data that is freely disclosed to the public	Data that is not meant to be shared outside of the company	Sensitive data that, if compromised, could negatively affect operations	Highly sensitive corporate data that, if compromised, could lead to financial or legal risk
Examples: • Marketing materials • Sales data sheets • Support documentation	Examples: • Battle cards • Sales playbooks • Organizational charts • Strategy presentations	Examples: • Contact information • Price lists • Next year go-to-market plans • Product roadmap presentations	Examples • Personal customer information (e.g., social security numbers) • Customer credit card data • Employee contact information

If a company is investing in a data management platform that will leverage AI for the analysis, classification, and labeling of data, it may be worth classifying the top and most sensitive category with sub-categories to indicate regulatory relevance or alternate access control models that may be required, such as PCI data, GDPR-relevant, and unpublished financial data. There are very effective AI-enabled data classification applications available, such as IBM Guardium, Informatica Data Catalog, or Microsoft Purview (formally Azure Purview) as a few examples. ■

Asses your organization, department, and yourself → See appendix 3

Data governance framework

Creating and leveraging a data governance framework begins with a data classification standard. Many CISOs, CIOs, and senior IT leaders we interviewed were frustrated with the lack of available governance frameworks available "out of the box." Many CISOs and CIOs held similar sentiments to what the head of IT Operations at an international satellite television provider told us:

> "Current data governance frameworks available today would require significant customization to meet our company's specific needs. We had to hire a large IT consulting firm to help design a framework for us because of some of our complexity and the lack of available governance frameworks that would fit our needs."

Many interviewed CISOs and CIOs mentioned governance frameworks that they have worked with to customize, including the Data Governance Framework:

Data Governance Framework

DGI - Data Governance Institute

Overview	Advantages	Cautions
• The framework depicts data governance as exercising decision making and authority over data-related issues. • Goals of data governance include improving decision making, reducing operational inefficiencies, protecting stakeholders, reducing costs, and training staff while building transparent processes and standards. • DGI divides each of its components into core areas — rules, people, and processes — to simplify the concepts.	DGI is a comprehensive framework covering various aspects of data governance, including drivers, components, domains, maturity model, organizational structure, and implementation roadmap, providing a holistic approach to managing data effectively.	Framework can be difficult to customize; comprehensive framework will require time, resources, and expertise to adopt
Framework provides a structured approach to data governance, emphasizing its importance in managing data as a strategic asset. Covers key components such as data governance principles, organizational roles and responsibilities, policies and standards, data quality management, and metadata management, aiming to establish effective data governance practices within the organization.	Framework offers comprehensive coverage of various aspects of data governance, including principles, roles, policies, and processes, providing organizations with a holistic approach to managing data effectively.	Framework offers principles and guidelines but may lack prescriptive guidance on implementation details, making it challenging for organizations to translate theoretical concepts into practical actions and initiatives.
Framework emphasizes a pragmatic approach to data governance, focusing on key components such as strategy, organization, processes, technology, and metrics. Emphasizes the importance of aligning data governance efforts with business objectives and ensuring that governance processes are practical, scalable, and sustainable.	Framework encourages alignment with business objectives to ensure data governance efforts are closely tied to organizational goals and priorities.	Framework may not be easily adaptable to organizations with complex or unique data governance requirements, requiring significant customization or augmentation.
Framework emphasizes strategic alignment, risk management, and operational efficiency to enable effective management and governance of data assets, with key components including governance structures, policies, data quality management, and performance metrics.	Alignment with business objectives, robust governance structures, and comprehensive approach to data governance bespoke to the needs of the organization.	The framework will require a consulting agreement with the company, which is likely beginning at six figures and going up from there for larger organizations.
Framework prioritizes strategic alignment, operational effectiveness, and risk management. Emphasizes establishing clear ownership, defining accountability, and implementing robust processes and controls to govern data effectively. The framework incorporates key components such as governance structures, policies and procedures, data quality management, and performance metrics to ensure the organization's data assets are managed efficiently and in compliance with regulatory requirements.	Extremely comprehensive and bespoke because the framework includes a consulting agreement. Deloitte's framework covers a majority of data governance aspects and is customized to the specific needs of the organization.	The framework will require a consulting agreement with the company, which is likely beginning at six figures and going up from there for larger organizations. Does not allow for customization without contracting with the company.

Unpacking the black box

In order to unpack the black box: Implement demonstrable, defensible controls. CISOs and CIOs highlighted the requirement for transparent cybersecurity controls with clear KPIs, compliance-optimized platforms, intuitive dashboards, and strong SLAs to help CISOs and CIO build trust with stakeholders and confidently tell their security story.

Most CISOs and CIOs recommended a security model based on "zero trust" that designs, builds, operates, and defends an infrastructure while continuously applying threat modeling and analysis during each of the process steps in a continuous lifecycle. CISOs and CIOs and leaders recommended a minimum of nine defensive controls to begin with, including:

- **Access controls:** Implementing role-based access controls (RBAC) and segregation of duties (SoD) to restrict access to sensitive data and systems based on users' roles and responsibilities.
- **Encryption:** Encrypting data both at rest and in transit to protect it from unauthorized access or interception, ensuring data confidentiality and integrity.
- **Data loss prevention (DLP):** Deploying DLP solutions to monitor and prevent the unauthorized transfer or leakage of sensitive data across networks, endpoints, and cloud environments.
- **Incident response plan:** Establishing an incident response plan with defined procedures and roles to detect, respond to, and recover from security incidents effectively, minimizing the impact on business operations.
- **Vendor risk management:** Implementing processes to assess and manage the cybersecurity risks posed by third-party vendors and service providers, including due diligence assessments, contract negotiations, and ongoing monitoring.
- **Security awareness training:** Providing regular security awareness training to employees to educate them about cybersecurity best practices, recognize phishing attempts, and understand their role in protecting sensitive data.
- **Patch management:** Implementing a patch management process to regularly update software and systems with security patches and updates to address known vulnerabilities and reduce the risk of exploitation.
- **Compliance controls:** Implementing controls to ensure compliance with relevant regulations and standards, such as GDPR, HIPAA, PCI DSS, and ISO 27001, including data retention policies, privacy controls, and audit trails.
- **Business continuity and disaster recovery:** Establishing business continuity and disaster recovery plans to ensure the availability and resilience of critical systems and data in the event of natural disasters, cyberattacks, or other disruptions.

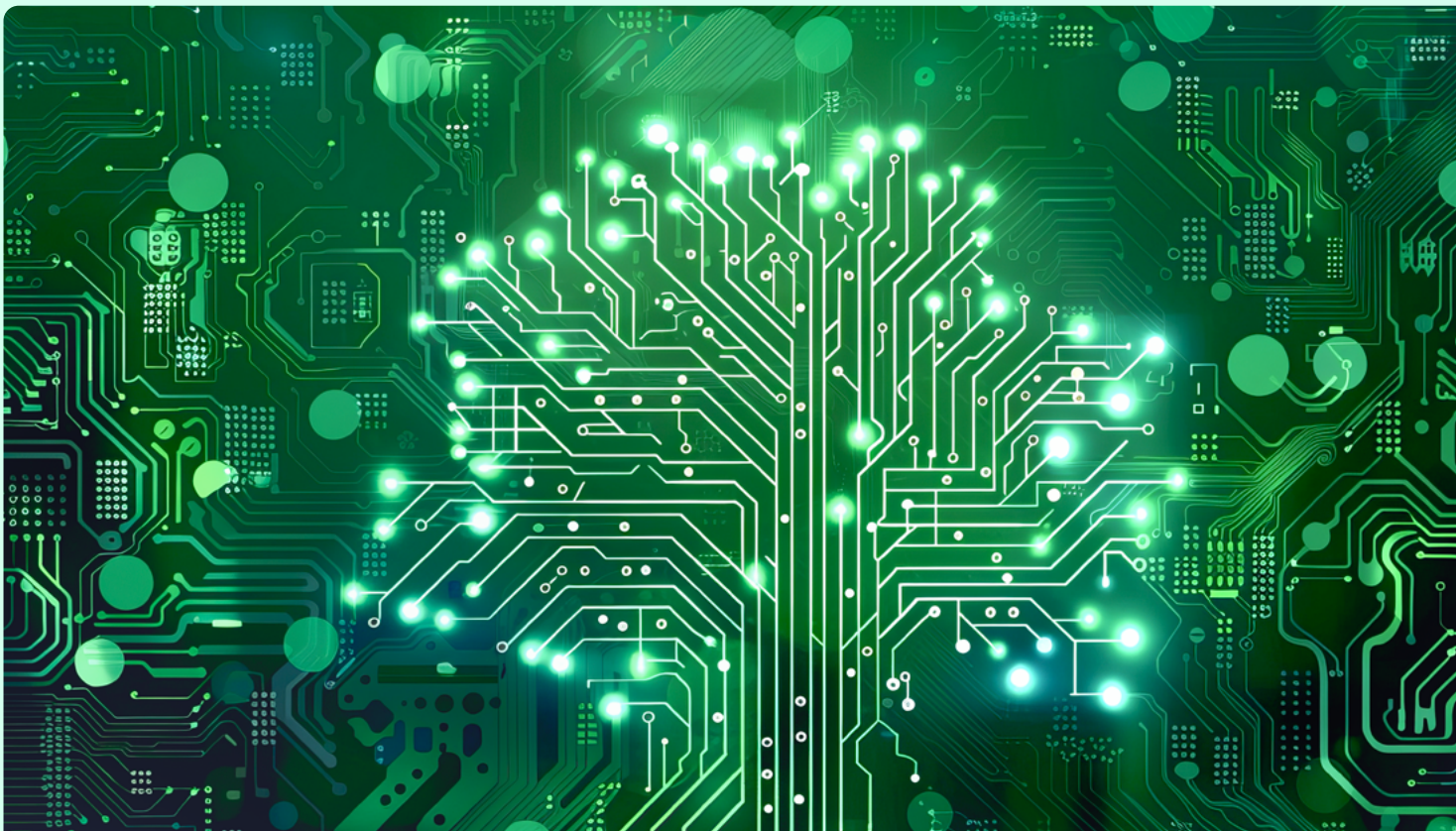
Asses your organization, department, and yourself → See appendix 5

Conclusion

Data sits at the center of both the biggest opportunities and the biggest risks facing organizations. As CISOs and CIOs strive to balance the drive to innovate with the need to protect, robust data security and backup and recovery capabilities are foundational.

The CISOs and CIOs we spoke with are rising to the challenge by adopting a mindset of continuous improvement. They are building collaborative best practices, partnering to bring in needed expertise, and investing in data-centric solutions optimized for security and simplicity.

As their role continues to evolve, the next generation of successful CISOs and CIOs will be defined by their ability to enable and protect data-driven innovation. No matter what the next wave of technology brings, data will be at the center, and CISOs and CIOs will be at the forefront of ensuring their security and resilience. ■



Next steps: Finding a trusted data protection partner

Given this challenging environment where data is central to both opportunities and risks, finding a trusted data protection partner is key — especially one that can offer robust and scalable data protection solutions tailored to your company's needs.

Look for a partner who has adopted a strategy of continuous improvement, understands the latest cybersecurity trends and threats, has a pulse on data governance requirements and effective solutions, and helps your company implement best practices.

Keepit is more than a data protection vendor. We deliver next-level SaaS data protection for your most business-critical applications and platforms. Our approach goes beyond providing tools; we collaborate with you to implement best practices, stay ahead of emerging threats, and continuously improve your data governance strategies.

By partnering with Keepit, organizations can confidently navigate the complexities of modern cybersecurity challenges with a modern solution, ensuring data is secure, compliant, and ready to support innovative business initiatives — the balance between driving innovation and maintaining robust protection.

To find out more about how Keepit can support your data protection and cybersecurity needs, join our webinar or participate in the Foundry survey. Learn how leading organizations are leveraging our solution to enhance their security posture and achieve their strategic objectives.

Reading list

Keepit resources

Security in the cloud: The SaaS backup gap challenge — and solution

– Frederik Schouboe, CVO (Chief Visionary Officer) and co-founder of Keepit

Forrester Total Economic Impact of Keepit SaaS Data Protection

– Keepit blog

SaaS data backup and disaster recovery planning

– Henrik Brusgaard, VP of Product at Keepit

Compliance and continuity

– Keepit

Webinar: From threat to defense: Cyber insurance woes as ransomware surges

– Keepit Webinar

External reports and resources:

Top Global Data Security Trends Report

– Salesforce

The changing role of the CISO

– Frank Dickson, Program Vice President of Cybersecurity producs, IDC

The 2023 Fortune 500 CISOs Analysis

– Tim Howard, founder of Fortify Experts

Appendix

Assessments 1–5

Adopting a risk-impact mindset

When in search of a winning data governance framework

Enact a data classification strategy

Data governance framework

Unpacking the black box

05

Appendix 1

Adopting a risk-impact mindset

Ask your organization	
What are the current and emerging cybersecurity threats we are facing?	☐
How do these threats impact our critical assets, brand, and reputation?	☐
What is the likelihood and potential impact of each identified risk?	☐
How does each identified risk affect our strategic objectives and stakeholder interests?	☐
What are the financial, operational, and reputational impacts of these risks?	☐
How do we quantify the business value of mitigating these risks?	☐
Which risks have the highest potential impact on our business value and critical assets?	☐
How do we prioritize these risks in alignment with our business goals?	☐
What is our threshold for acceptable risk?	☐
What are our current risk mitigation strategies and how effective are they?	☐
What additional controls, policies, or procedures do we need to implement?	☐
How do we balance the total cost of ownership with the potential impact of cybersecurity threats?	☐
How do we continuously monitor and review the effectiveness of our risk mitigation measures?	☐
What metrics and key performance indicators (KPIs) do we use to assess our cybersecurity posture?	☐
How do we adjust our strategies based on changes in the risk landscape or business priorities?	☐

Appendix 1 – continued

Adopting a risk-impact mindset

Ask your department	
Are we allocating our resources to address the most critical cybersecurity risks? If so, how? If not, why not?	☐
Are our resources aligned with our prioritized risk-impact profiles? (Do they align with the answers given by the organization when asked the questions above?)	☐
How are we ensuring that our investments in cybersecurity are yielding the desired business outcomes? Are we engaging with key stakeholders to ensure alignment on cybersecurity priorities? If not, how can we accomplish this?	☐
What mechanisms are in place for communicating risk-impact analysis results to the board and executive team?	☐
What skills and capabilities does our team need to effectively implement the risk-impact framework?	☐
Are we ensuring continuous learning and development for our cybersecurity team?	☐
What tools and technologies does our department need to support our risk-impact analysis and decision-making processes?	☐

Ask yourself	
Am I leading by example in adopting and promoting the risk-impact framework?	☐
What is my vision for integrating cybersecurity with business objectives? Am I communicating this effectively to my team and the wider organization?	☐
Do I ensure my decisions are informed by a thorough risk-impact analysis?	☐
Do I stay informed about the latest threat trends, compliance requirements, and governance issues?	☐
What steps am I taking to continuously improve our risk identification and assessment processes?	☐
How do I ensure that our risk mitigation strategies remain effective and relevant?	☐
Do I collaborate with other leaders to drive the risk-impact conversation across the organization?	☐
What influence do I have in ensuring that the board of directors acknowledges and takes responsibility for the risk-impact discussion?	☐
Do I advocate for the necessary investments in cybersecurity to support our risk-impact framework?	☐

Appendix 2

When in search of a winning data governance framework

Ask your organization	
What is the current level of understanding and engagement of our board members regarding cybersecurity and data governance?	☐
How frequently are cybersecurity updates and discussions scheduled in board meetings? What risk scenarios should we present to the board to highlight potential impacts and mitigation plans?	☐
What specific topics or areas of concern do executive leadership and board members have about cybersecurity?	☐
How can we effectively translate technical cybersecurity and data governance concepts into business language that resonates with board members?	☐
What analogies or case studies can we use to illustrate the business implications of cybersecurity threats and mitigation strategies?	☐
What educational sessions or materials can we provide to enhance board members' understanding of cybersecurity issues?	☐
What is our current level of investment in cybersecurity and data governance, and how does it compare to industry benchmarks?	☐
What are the potential cost savings, risk reductions, and business benefits associated with our cybersecurity investments?	☐

Ask your department	
How are we prioritizing cybersecurity initiatives based on business impact and risk profiles?	☐
What key cybersecurity projects require board support and approval for resource allocation?	☐
How do our cybersecurity priorities align with the strategic goals set by the board?	☐
What mechanisms can we establish for ongoing communication and collaboration between the cybersecurity team and the board?	☐
How can we leverage the expertise and networks of board members to support cybersecurity initiatives?	☐

Appendix 2 – continued

When in search of a winning data governance framework

Ask yourself	
Am I earning the perception of being a trusted advisor on cybersecurity matters?	☐
What steps am I taking to earn and maintain "a seat at the table" during board meetings?	☐
What communication strategies can I use to ensure that board members understand the urgency and importance of cybersecurity issues?	☐
How can I build a compelling narrative that links cybersecurity investments to business success and resilience?	☐
How can I ensure interest and support from the board in cybersecurity matters?	☐

Appendix 3

Enact a data classification strategy

Ask your organization	
What are the primary objectives of our data classification strategy, and how do they align with our overall data governance framework?	☐
How does data classification support our compliance with industry regulations and standards (e.g., GDPR, HIPAA, PCI-DSS)? How do we ensure ongoing compliance as relevant regulations and industry standards evolve?	☐
What are the key business functions that rely on accurate data classification, and how are they impacted by our classification strategy? What is their expected (and agreed upon) level of involvement?	☐
What types of data do we collect, store, and process, and where is this data located?	☐
How sensitive is the data we handle, and what are the potential risks associated with unauthorized access or disclosure?	☐
What predefined groups or categories will we use for data classification (e.g., Public, Internal only, Confidential, Restricted)?	☐
What tools and technologies are available to support our data classification efforts? How will we evaluate and select data classification tools?	☐
What processes and procedures will we implement to classify data according to its sensitivity and importance?	☐
How will we ensure that each data category has the appropriate security controls and access restrictions? How will we tag and label classified data to facilitate proper handling and protection?	☐

Ask your organization	
What metrics and KPIs will we use to monitor the effectiveness of our data classification strategy?	☐
How often will we review and update our classification strategy to adapt to changing risks and regulatory requirements?	☐

Ask your department	
What are the roles and responsibilities of our department in the data classification process?	☐
How will we train and educate employees about the importance of data classification and proper handling of classified data?	☐
What communication channels and reporting mechanisms will we establish to facilitate collaboration across departments?	☐
How will each department handle and protect classified data, and what access controls will be implemented? How will we manage and monitor access to classified data to prevent unauthorized use or disclosure?	☐
How will we manage data throughout its lifecycle, from creation and classification to storage, use, and disposal? How will we ensure that classified data is consistently handled according to its designated category throughout its lifecycle?	☐
What policies and procedures will we establish for data retention, archiving, and destruction?	☐

Ask yourself	
How can I champion the importance of data classification within the organization and ensure it receives the necessary attention and resources?	☐
What steps can I take to ensure that our data classification strategy is effectively communicated and understood by all stakeholders?	☐
How can I stay informed about the latest trends and best practices in data classification and governance?	☐
What steps can I take to identify and address any gaps or weaknesses in our data classification strategy or processes?	☐
How can I ensure that our data classification strategy remains aligned with evolving regulatory requirements and business needs?	☐
What strategies can I use to engage with key stakeholders, including executives and board members, to gain their support for our data classification initiatives?	☐

Appendix 4

Data governance framework

Ask your organization	
Is there an existing data governance framework that best aligns with our organization's goals and existing data management practices? If not, what specific customizations will be required to adapt the chosen framework to our organization's unique needs and complexities? Is there a way to integrate elements from multiple frameworks (e.g., DGI, DAMA DMBOK, Eckerson Group, PwC, Deloitte) to create a comprehensive and effective governance model for our organization?	☐
How does our chosen data governance framework align with our overall business objectives and strategic goals and what are the key drivers (e.g., regulatorwy compliance, operational efficiency, data quality)?	☐
How should data governance support our organization's decision-making processes and reduce operational inefficiencies?	☐
What governance structures (e.g., data governance council, data stewards) do we need to establish to oversee data governance efforts?	☐
What roles and responsibilities should be assigned to different stakeholders within the organization to ensure clear ownership and accountability across various departments?	☐
What policies and standards do we need to develop to govern data effectively (e.g., data classification, data quality, data privacy)? How can they consistently be applied and adhered to across the organization?	☐
What processes will we implement to review and update policies and standards regularly? How will we identify and address challenges?	☐
What processes, tools, and metrics will we use to monitor and manage data quality?	☐
How will our data governance framework help us comply with relevant regulations and industry standards (e.g., GDPR, HIPAA, PCI-DSS)? How will we monitor and respond to changes in the regulatory landscape?	☐
What risk management strategies will we implement to identify and mitigate data-related risks?	☐

Ask your department	
How can we ensure that these processes are practical, scalable, and sustainable?	☐
What tools and technologies will we use to support the organization's data governance efforts?	☐
How will we train and educate employees about the importance of data governance and their roles in the governance process? How will we measure the effectiveness of our training and awareness efforts?	☐

Ask yourself	
How can I champion the importance of data governance within the organization and ensure it receives the necessary attention and resources?	☐
What steps can I take to build a compelling case for data governance across departments, to executive leadership, and the board of directors? How can I foster collaboration and communication between different departments and stakeholders to support our data governance efforts?	☐
How can I stay informed about the latest trends and best practices in data governance and data management?	☐
How can I ensure that our data governance framework remains aligned with evolving business needs and regulatory requirements?	☐

Appendix 5

Unpacking the black box

Ask your organization	
How do our current cybersecurity controls align with the organization's strategic goals and risk tolerance?	☐
What are the KPIs that we need to establish to measure the effectiveness of our cybersecurity controls and communicate their effectiveness to executive leadership and board members?	☐

Ask your department	
How are we continuously applying threat modeling and analysis throughout each process step in our security lifecycle?	☐
What mechanisms are in place to verify and validate the identity of users and devices before granting access to resources?	☐
How are we implementing role-based access controls (RBAC) and segregation of duties (SoD) to restrict access to sensitive data and systems?	☐
What processes are in place to regularly review and update access permissions based on users' roles and responsibilities?	☐
What encryption methods are we using to protect data at rest and in transit?	☐
How do we ensure that our encryption practices meet industry standards and regulatory requirements?	☐
What are the defined procedures and roles in our incident response plan to detect, respond to, and recover from security incidents?	☐

Appendix 5 – continued

Unpacking the black box

Ask your department	
How do we assess and manage the cybersecurity risks posed by third-party vendors and service providers? What due diligence assessments, contract negotiations, and ongoing monitoring processes are in place for vendor risk management?	☐
How frequently are we providing security awareness training to employees? What topics are covered in our training programs to educate employees about cybersecurity best practices and recognizing phishing attempts? How do we measure the effectiveness of our security awareness training?	☐
What is our process for regularly updating software and systems with security patches and updates? How do we ensure that our patch management process addresses known vulnerabilities and reduces the risk of exploitation?	☐
What is our process for regularly updating software and systems with security patches and updates? How do we ensure that our patch management process addresses known vulnerabilities and reduces the risk of exploitation?	☐
How do we ensure that our cybersecurity strategy supports compliance with relevant regulations and standards (e.g., GDPR, HIPAA, PCI DSS, ISO 27001)? What controls are in place to ensure compliance, including data retention policies, privacy controls, and audit trails?	☐
What are our business continuity and disaster recovery plans to ensure the availability and resilience of critical systems and data? How do we regularly test and update these plans to address new and evolving threats? What measures are in place to ensure that our disaster recovery plans can be executed effectively in the event of a disruption?	☐
Do our data backups share the same risk profile as our production data? Are our backups truly immutable?	☐

Ask yourself	
How can I foster collaboration and communication between different departments and stakeholders to support our cybersecurity efforts? What strategies can I use to engage with key stakeholders and gain their support for our cybersecurity initiatives?	☐
How can I ensure that our cybersecurity strategy is aligned with the broader business objectives, risk management framework, and regulatory requirements?	☐
How can I stay informed about the latest trends and best practices in cybersecurity controls?	☐

Appendix 6

Interviewed CISO and security professionals

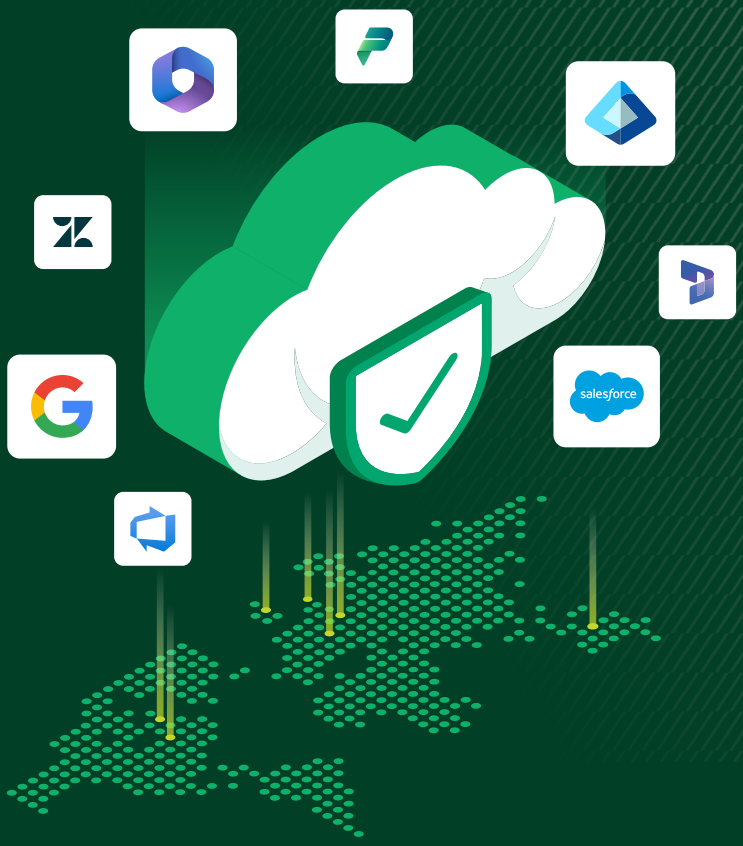
Interviews occurred from January 20, 2024, through April 10, 2024

CISO, US National Insurance Company
VP of IT, National Insurance Provider
CTO, Business Collaboration Platform
Director of Network Management, Regional Educational Office
CIO, Renewable Energy Services Company
Director of Backup, Storage, & Recovery, Cloud-Based Financial Management Software Company
Director of IT, Humanitarian Organization
Director of IT, Real Estate Investment and Management Firm
Manager of IT and Storage, Satellite Communications Provider
Head of IT Operations, Satellite Television Provider
Technical Backup Specialist, Global IT Services Company
Systems Team Supervisor, State Government Transportation Department
Tier-Two Systems Technician, IT Solutions Provider
Manager, Technical Services & Support, Multinational Manufacturing Company
VP of Technologies, Online Learning Platform
Backup & Recovery Manager, Engineering and Infrastructure Services Firm
Data Solutions Architect, Medical Data Systems Company
IT Infrastructure Manager, Insurance and Financial Services Company
Director of IT Operations and Solutions, Global Cargo Airline
Director of IT Cybersecurity Consulting, Large International IT Consulting Firm
VP of Worldwide Data Protection, Global Coffee Company UK Branch
IT Manager, Medical Devices Manufacturer
Infrastructure & Network Engineer, IT Consulting and Outsourcing Firm
Network Engineer, Online Postal and Courier Services Provider
Manager of Infrastructure, Healthcare Performance Improvement Company
Director of IT Infrastructure, Pediatric Research Hospital
CISO, International Telecommunications Service Provider
Head of Cybersecurity Operations, International Commerce Retailer
Head of Cybersecurity, Large national US retailer.
CISO, Large international financial services firm

Keepit future proof

Take the next step toward protecting your SaaS data

Request a demo



keepit®

Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection.

Headquartered in Copenhagen with offices and data centers worldwide, over ten thousand companies trust Keepit for its ease of use and effortless backup and recovery of cloud data.

HQ - Copenhagen
Denmark
Keepit A/S
Per Henrik Lings Allé 4, 7.
2100 København, Denmark
CVR: 30806883
+45 8987 7792
sales@keepit.com

Dallas, Texas
United States
Keepit USA Inc.
3232 McKinney Avenue Suite 820
Dallas TX 75204, USA
TIN: 85-358 6335
+1 469-461-4892
sales@keepit.com

London
United Kingdom
Keepit Technologies UK, LTD.
Warnford Court
29, Throgmorton Street
London EC2N 2AT, UK
Company reg. no.: 13785045
sales@keepit.com

Munich
Germany
Keepit Germany GmbH
Maximiliansplatz 22
D-80333 München
Amtsgericht München
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com

www.keepit.com