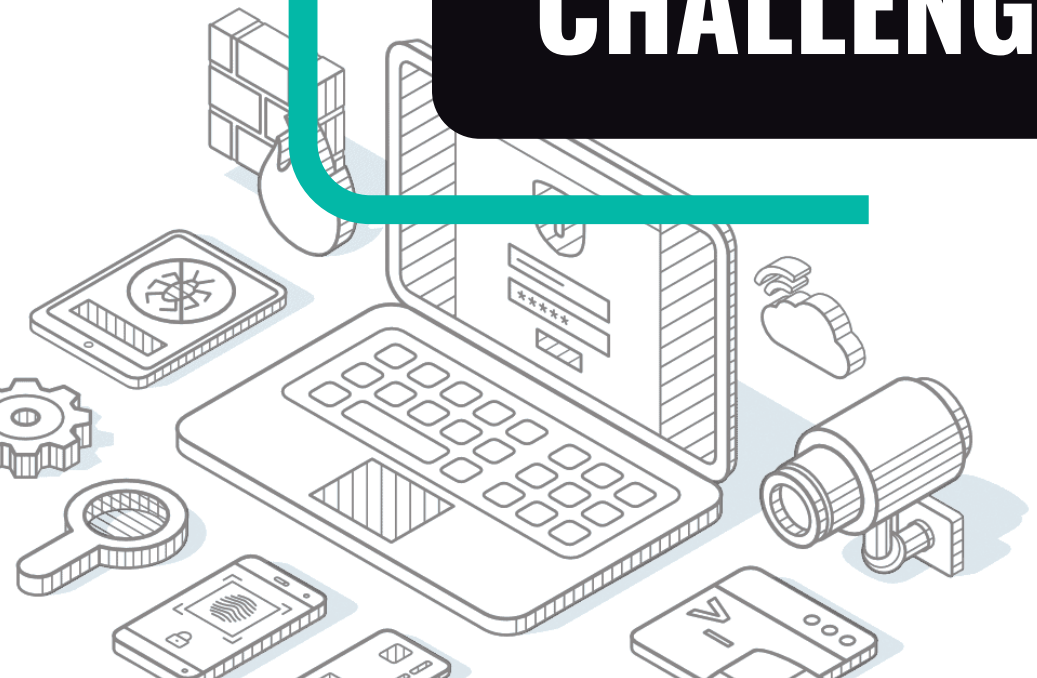
The CISO Society

Q2 2024

THE CISO SOCIETY **2024 STATE OF DATA SECURITY REPORT**

AI, BUDGETING, PRIVACY AND MORE IN AN INCREASINGLY CHALLENGING LANDSCAPE



SUPPORTED BY: BigID

CONTENTS

TASK FORCE

Steve Hindle
CISO-in-residence
The CISO Society

Tyler Young
CISO
BigID

Peter Holcomb
Head of Information Security
Datavolo Inc.

Rupa Parameswaran
VP of Security & IT
Handshake

Vlad Brodsky
CISO
OTC Markets

Robyn Wright
CISO
Wiley

Adam Holland
CISO
The Wendy's Company

Louis Bedigian
Analyst & Author

OPENING REMARKS

Data Security is often presumed; commonly misunderstood; and often neglected. Organizations focus on cybersecurity without directly addressing data security. Foundational security tooling and strategies focus on everything except the data. Regulations insist that data is secured but aside from encryption at rest and in transit, the rest is left open. Ownership of securing data is frequently deflected from the actual data owner to the data custodian - which inevitably becomes the CISO. It is imperative for CISOs to share and benchmark against one another to understand how they, and their respective organizations, are tackling these challenges, highlighting the important role communities like The CISO Society play in helping security leaders collaborate and improve.

Steve Hindle
CISO-in-residence, The CISO Society

Here's the reality: data security is no longer a reactive game. As data breaches continue to impact organizations, security leaders must prioritize data security initiatives that aim to provide visibility and capabilities to protect sensitive data. Modern CISOs need a proactive solution that centralizes how to discover, classify, remediate, and secure their entire data environment. Data Security Posture Management (DSPM) is the bridge to empower organizations to move beyond basic scanning and achieve true proactive data security. At BigID, we confront these challenges head-on, every single day. We are committed to helping organizations know and act on their most critical risks, vulnerabilities, and confidently secure their most valuable asset - their data.

Dimitri Sirota
CEO, BigID

INTRODUCTION

THE IMPORTANCE OF DATA SECURITY CANNOT BE UNDERSTATED.

Malicious actors are eagerly targeting company, employee and customer data as they search for ways to steal, sell and otherwise exploit any information they obtain.

IBM's most recent annual report found that the average cost of a data breach reached $4.45 million in 2023[1] – a 2.3% increase over 2022. In 2023, more than 80% of the breaches involved data stored in the cloud.

Apple sponsored a study on data breaches as well and revealed that 2.6 billion personal records were compromised in 2021 and 2022[2]. That same report, conducted by MIT professor Dr. Stuart E. Madnick, showed that the number of data breaches nearly tripled between 2013 and 2022.

Ransomware is also on the rise, and there is no shortage[3] of reports[4] detailing the risks and problems associated with every successful attack.

With this in mind, The CISO Society wanted to take a closer look at how our members are tackling their many challenges. 168 members participated in a survey to determine how much of their budget, past and projected, is being allocated to data security tools. We asked about any gaps that may exist in their data security strategy. We also wanted to know about their organization's response plan for data security incidents.

These are just a few of the topics we explore in our community Data Security report. Read on as we dive into the plans, processes and strategies employed by our members.

1. https://www.ibm.com/downloads/cas/E3G5JMBP

2. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

3. https://www.thalesgroup.com/en/worldwide/security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware-attacks

4. https://www.guidepointsecurity.com/newsroom/guidepoint-security-finds-increased-ransomware-activity-new-group-behavior-patterns-in-q1-2024-ransomware-report/

PAST AND FUTURE INVESTMENTS: BUDGETS REMAIN FAIRLY STEADY WITH FEW OUTLIERS

Organizations of all types and sizes have been very careful about how they apply their security budget. The majority (57.4%) spent 1-5% of their budget on data security tools in 2023 and half (50.3%) expect to invest the same amount in 2024. Nearly a quarter (23.7%) spent 5-10% of their security budget on data security tools in 2023. Only 8.3% spent more than 20% of their budget on data security tools.

Just under 31% of businesses with 5,000-10,000 employees spent more than 20% of their budget on data security tools, compared to just 3.1% of enterprises with more than 10,000 employees. Interestingly, 18.9% of organizations with 1,000-5,000 employees spent more than 20% as well.

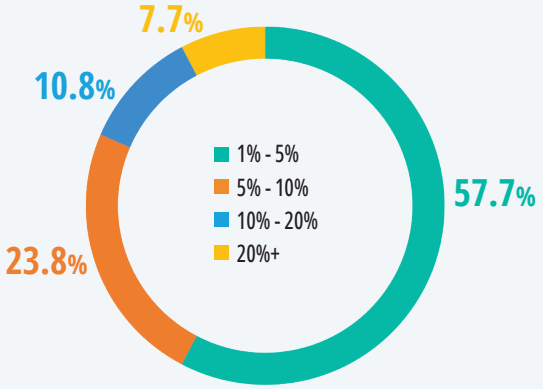
Most organizations don't expect to massively change their expenditures in 2024. However, 6.3% of businesses with 10,000+ employees anticipate that they will spend 20%+ of their budget on data security tools this year – a 2X increase over 2023. More than 30% of organizations with 5,000-10,000 employees believe they will also allocate 20%+ of their 2024 budget to data security tools.

Nearly three quarters (71.6%) of all CISOs surveyed said their business will not increase their security team headcount to manage data security in 2024, but larger organizations are more likely to do so. More than 37% of businesses with 10,000+ employees and 35% with $500M-$1B in revenue plan to acquire more talent. Smaller firms are less likely to increase their headcount, but there is one outlier: 84.6% of enterprises with 5,000-10,000 employees said they don't plan to make new hires.

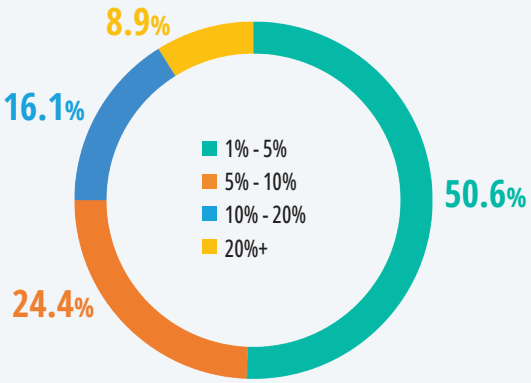
In order for CISOs and their respective organizations to effectively maintain and evolve their security programs, it's vital they are given the ability to benchmark their activities and strategies against their peers across all industries and company sizes, in a safe and trusting environment.

Jason Cenamor
Founder, The CISO Society

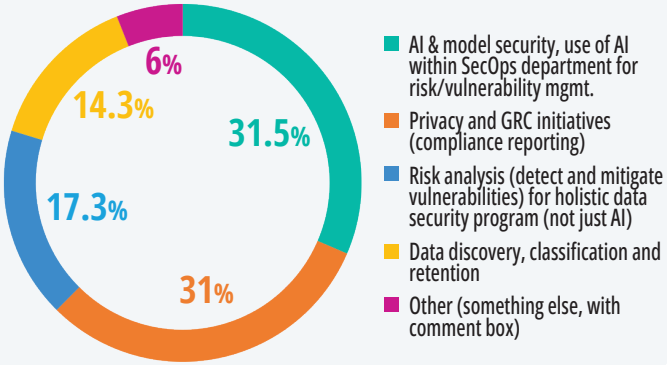
What percentage of your security budget was invested in data protection tools in 2023?



What is the projected percentage of your security budget being allocated to investing in data security tools in 2024?



What are your priorities for strengthening your data security program?



GAPS AND PRIORITIES IN AN INCREASINGLY CHALLENGING

When devising a plan to strengthen their data security program, nearly one-third (32%) of CISOs said their organization will focus on data discovery, classification and retention. Nearly as many (30.8%) plan to use risk analysis to detect and mitigate vulnerabilities for a holistic data security program. Just over 17% are looking at privacy and GRC initiatives and only 14.2% are considering how AI and model security can help.

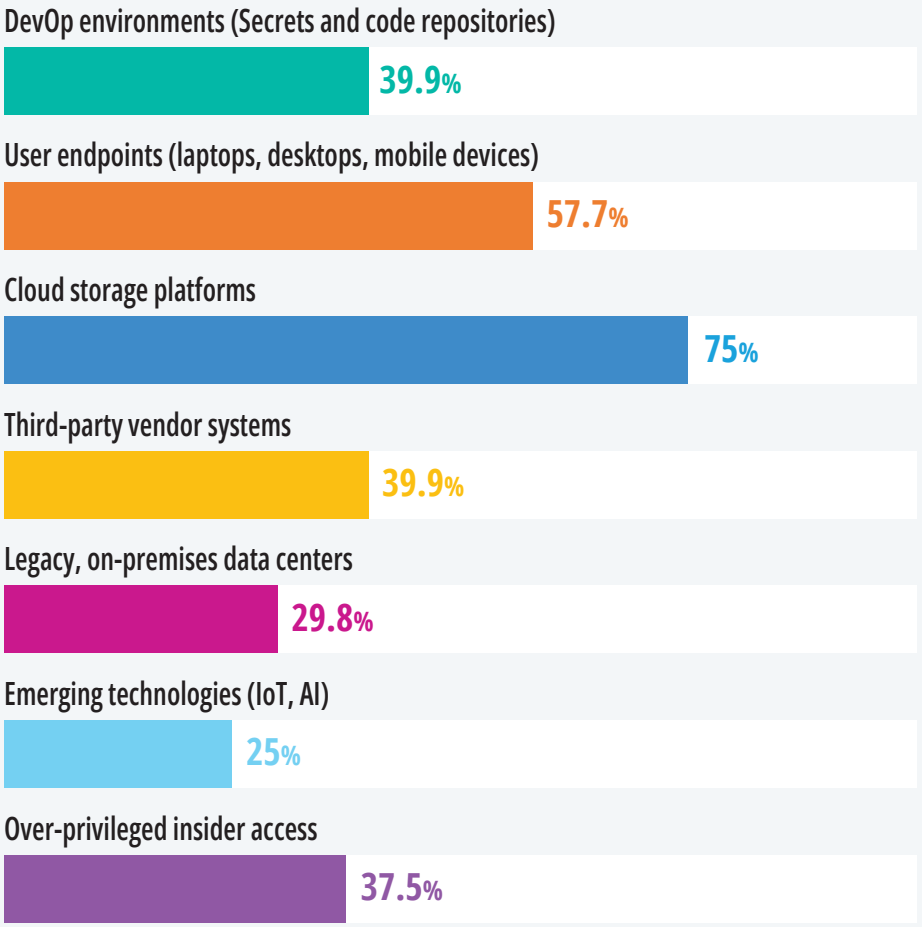
Larger, higher-earning organizations are more interested in AI than their smaller and lower-revenue competitors. Roughly 22% of businesses with 10,000+ employees plan to use AI to strengthen their data security program compared to just 10.4% of organizations with 200-1,000 employees. Similarly, 35% of enterprises with $500M-$1B in revenue are interested in AI versus 9.1% of organizations earning less than $100M.

These businesses are surely evaluating how much of an impact the aforementioned solutions will have on any gaps they may have within their data security strategy. More than 27% attribute their gaps to a lack of funding to support a data security program while 26.6% blame the lack of necessary resources and ownership. Just over 14% of CISOs said their gaps are caused by a lack of understanding of the various elements that make up their data security program while 10.7% attribute it to the lack of executive/leadership buy-in.

Not surprisingly, larger organizations (in terms of both employee size and revenue generation) more frequently highlight the lack of funding over the lack of executive buy-in. This suggests that execs at bigger firms are more likely to recognize the need to address gaps even if they aren't willing to provide financial support.

When asked about the biggest challenges their organization faces in classifying and discovering data, most CISOs (73.8%) pointed to data sprawl across multiple data sources. More than half (57.7%) are challenged by their limited resources or budget while 56% find it difficult to identify sensitive data in unstructured formats, such as emails and documents.

Which areas are you prioritizing the protection of data most at risk?



DATA SENSITIVITY, PROTECTION AND MORE

Most CISOs surveyed (54.4%) base their data sensitivity levels on both regulatory compliance requirements and the potential impact to their business. But some (13.6%) don't formally assess data sensitivity at all. The percentage of businesses that don't is higher for smaller (20.5% of firms with 1-200 employees and 18.2% of firms with less than $100M in revenue) organizations. Larger firms (75% of enterprises with 10,000+ employees) are more focused on regulatory compliance and business impact. Nearly 19% of these businesses based their data sensitivity levels on regulatory compliance requirements alone.

When asked which areas they are prioritizing for the protection of data most at risk, three quarters of CISOs (75%) said cloud storage platforms. More than half said user endpoints and nearly two-fifths (39.9%) said both DevOps environments and third-party vendor systems. More than one-third (37.5%) said over-privileged insider access and one quarter (25%) mentioned emerging technologies like IoT and AI.

Regardless, most organizations do not have clear visibility into who has access to their data on-premises and in the cloud. Just 18.9% said they do by maintaining detailed access logs and by regularly reviewing them. Most (68%) admitted that while they have some visibility there is room for improvement. Thirteen percent said their visibility is limited, especially in the cloud.

Smaller enterprises (29.5% of firms earning less than $100M in revenue and 33.3% of firms with 1-200 employees) more frequently stated that they have clear visibility than larger, more profitable organizations. Only 7.7% of businesses with 5,000-10,000 employees, 8.1% with 1,000-5,000 employees and 10% earning $500M-$1B in revenue said the same. This could be attributed to the complexity of operating a bigger company with more employees. That said, the absolute largest firms surveyed (18.1% with 10,000+ employees and 19.6% with $1B+ in revenue) seem to be more capable of handling this challenge and said they also had clear visibility. ■

The speed of business growth now moves at the speed it can identify and leverage key data points about its operations and customers. While this path helps with creating growth and strategy, regulatory and security requirements mean in addition to the speed of analytics there is a need to be able to discover and classify data. This is a key component of data security to protect a valuable commodity and as we expand AI and other tools it is also critical we understand what we use to teach and train both programs and our teams.

Adam Holland
CISO, The Wendy's Company

MOST ORGANIZATIONS DO NOT HAVE CLEAR VISIBILITY INTO WHO HAS ACCESS TO THEIR DATA ON-PREMISES AND IN THE CLOUD

USER PERMISSIONS ARE CRITICAL, BUT NOT EVERYONE IS IN AGREEMENT WITH HOW THEY SHOULD BE MANAGED

No cybersecurity initiative would be complete without a strategy for managing user permissions, but most businesses are not very confident they have built a zero trust model with least privileged permissions. Almost one-third (30.8%) of all CISOs surveyed said they are not confident at all and lack the necessary tools and processes for a zero trust environment. More than two-fifths (43.2%) are somewhat confident and nearly one quarter (23.7%) are mostly confident. Only 2.4% said they are very confident.

This is in spite of the fact that nearly three-fifths of CISOs (59.8%) said they regularly (quarterly or semi-annually) conduct reviews of user access permissions. Almost one-third (32%) do so occasionally while 8.3% said they rarely or never conduct reviews.

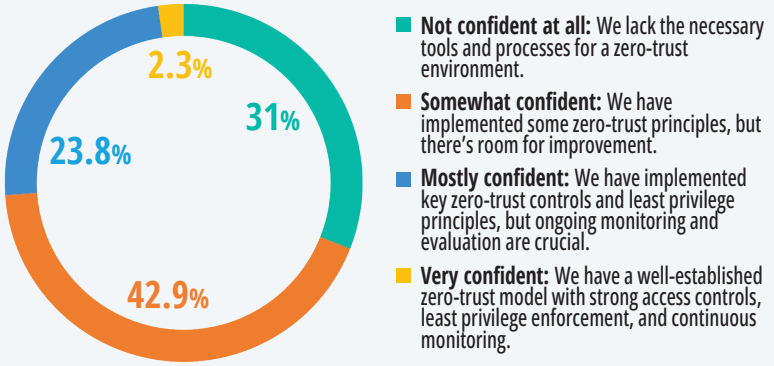
When asked how CISOs manage user permissions for accessing data on-premises and in the cloud, 76.2% said they use role-based access control (RBAC). More than half (57.7%) use an identity and access management (IAM) platform and just over two-fifths (44%) employ manual permission assignments. Less than one-fifth (17.3%) use Just-in-Time (JIT) access management while 11.9% manage their user permissions with attribute-based access control (ABAC).

To manage and monitor overexposed data or over-permissioned users, just under half (47.6%) do so by conducting data classification and access reviews to revoke unnecessary permissions and lock down exposed data. Nearly as many (45.8%) rely on data loss prevention (DLP) tools and/or continuously monitor user activities and behaviors for anomalies.

Almost one quarter (23.8%) said they don't have visibility into data exposure or user permissions, which is nearly triple the number of respondents who said they rarely or never conduct reviews of user access permissions. The lack of reviews surely contributes to this problem, but for some firms it is clear that visibility remains an obstacle and that their reviews aren't enough. ■

...NEARLY THREE-FIFTHS OF CISOS (59.8%) SAID THEY REGULARLY (QUARTERLY OR SEMI-ANNUALLY) CONDUCT REVIEWS OF USER ACCESS PERMISSIONS

How confident are you that you have built a zero trust model with least privileged permissions?



It's imperative to not only understand the sensitive data in your organization but also to have full visibility into who has access to it. Being able to correlate access and activity on your data is crucial. Once you have this visibility and a true understanding of the risks, controlling access and permissions becomes much easier.

Tyler Young
CISO, BigID

AI'S ROLE IN DATA SECURITY

AI USAGE AND THE MANY RISKS THAT FOLLOW

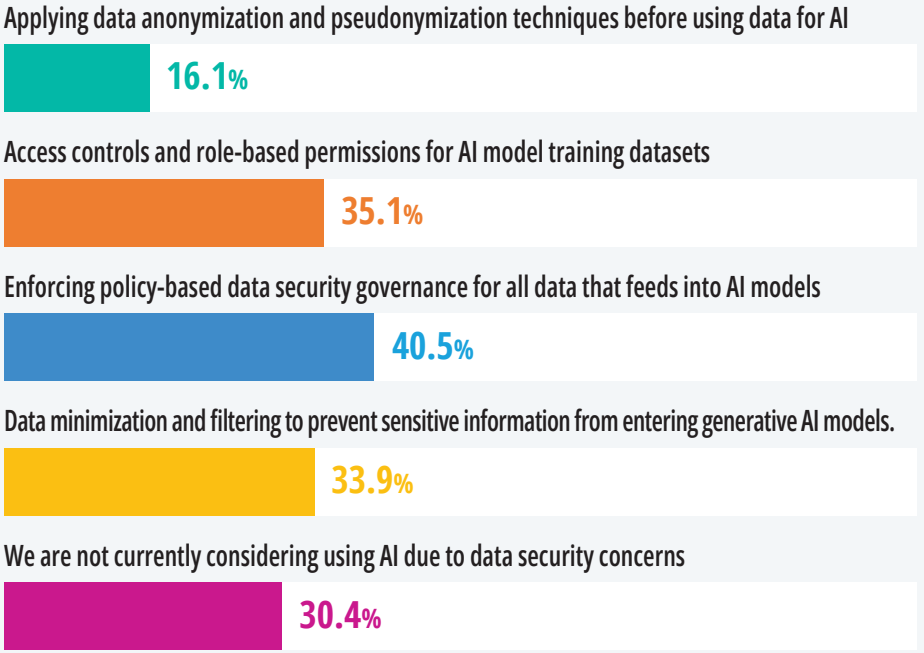
Visibility is also a problem for organizations using artificial intelligence (AI). More than one-fifth (21.9%) of CISOs surveyed said they have no visibility into the data flowing into their AI models. Roughly one-third (33.1%) have limited visibility and nearly as many (30.8%) said they have partial visibility. Less than one-tenth (5.9%) have full visibility while 8.3% said they are unsure.

To mitigate the data security concerns associated with using AI, and perhaps to compensate for this lack of visibility, 30.4% of CISOs said their firm is not currently using AI. Among those that do, 40.5% enforce policy-based data security governance for all data that feeds into AI models to ensure that sensitive and confidential information is protected.

Less than two-fifths (35.1%) have implemented access controls and role-based permissions for AI model training datasets. Roughly one-third (33.9%) use data minimization and filtering to prevent sensitive information from entering generative AI models. Just over 16% said they apply data anonymization and pseudonymization techniques before using data for AI.

Despite their efforts to protect their data, CISOs continue to be concerned about how data is used in AI programs. More than four-fifths (82.1%) are worried about the inadvertent leakage of

What measures does your organization implement to ensure that sensitive and confidential information is protected from AI models?



AI's role in data security encompasses malware analysis, vulnerability detection and remediation, and incident response. Ensuring data security for AI systems requires robust observability governance. Data observability for AI relies on four pillars: metrics, metadata, lineage, and logs, which visually represent the data's journey from source to consumption. This helps security professionals recognize complex data patterns, provide actionable recommendations, and enable autonomous mitigation through automation tools. By implementing these best practices, we enhance data quality, supporting informed decision-making—a win-win for both the security team and the company.

Peter Holcomb
Head of Information Security, Datavolo, Inc.

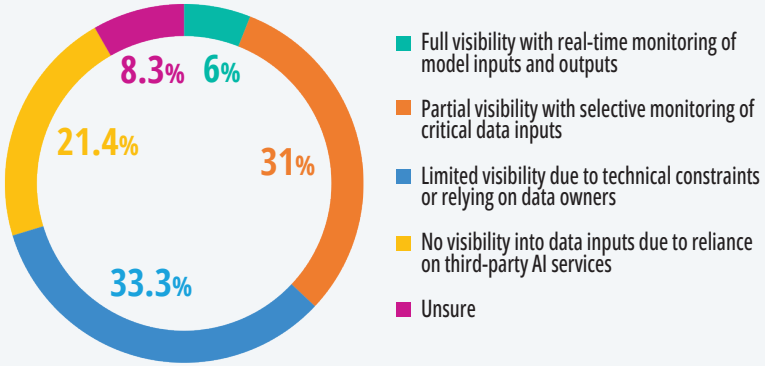
personal or confidential information by the AI program/platform to unintended audiences. Well over half (60.1%) are concerned that AI models could be manipulated or attacked. More than 50% think about the lack of transparency into how AI models arrive at their decisions, which makes it difficult to trust their outputs. Nearly as many (47.6%) are concerned about any biases that may be present in the training data and how that could lead to unfair or discriminatory outcomes from AI models.

Most businesses (52.7%) do not currently have processes in place to ensure their AI systems comply with privacy regulations and ethical standards. The rest are fairly divided, with 18.9% incorporating privacy-by-design principles in the AI development processes. Nearly 15% integrate privacy impact assessments into AI project lifecycles while 7.7% conduct regular audits and assessments of AI algorithms for privacy compliance. Just under 6% implement transparency measures for the AI decision-making processes.

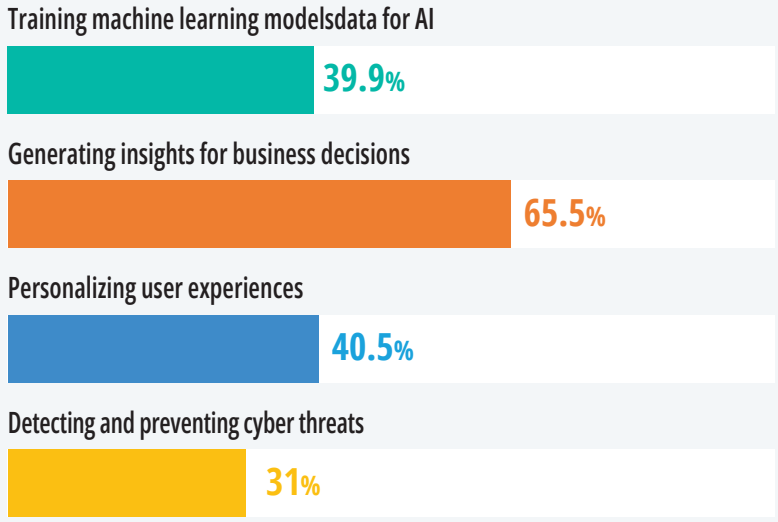
When all is said and done, enterprises overwhelmingly turn to AI to generate insights for business decisions (65.5%). Just over 40% use AI to personalize user experiences and 39.9% deploy the technology to train machine learning models. Less than one-third (31%) use AI to detect and prevent cyberthreats. ■

CISOS CONTINUE TO BE CONCERNED ABOUT HOW DATA IS USED IN AI PROGRAMS

To what extent does your organization have visibility into the data flowing into AI models?



How is the data being used for AI?



AI has a significant role to play in data security. For instance, AI tools can be used to enhance processes such as data classification and categorization via various forms of advanced supervised machine learning. AI can also be used to monitor sensitive data, once it has been classified, and take actions to alert on or block dangerous user or system behavior. AI's ability to process vast amounts of data, automate actions, and identity patterns, make it an ideal technology in a company's data security toolbox.

Vlad Brodksy
CISO, OTC Markets Group

INCIDENT RESPONSE AND THE QUEST TO ADDRESS CYBER ATTACKS

Most organizations understand the increasing risks of malicious actors with more than half (55.6%) stating that they have a defined response plan for data security incidents but noted that it needs improvement. Nearly one-third (31.4%) said they have and regularly test a highly detailed plan. Roughly 10% have a basic outline but nothing formalized. Only 2.4% said that they have no formal IR plan in place.

Larger firms (43.8% with 10,000+ employees and 45.7% with $1B+ in revenue) more commonly said they have a highly detailed plan. That's more than double the number of smaller enterprises (15.4% with 1-200 employees and 20.5% with less than $100M) that said they have a highly detailed plan in place. Smaller firms (7.7% with 1-200 employees and 4.5% with less than $100M) more frequently stated that they don't have a formal IR plan, while none of the largest firms said the same.

With or without a plan, it seems that most companies are not very confident in their ability to trace who had access to compromised data during a security incident. Only 29% said they do compared to 58.6% who said they are somewhat confident. Just under 12% are not confident and 0.6% said they were unsure.

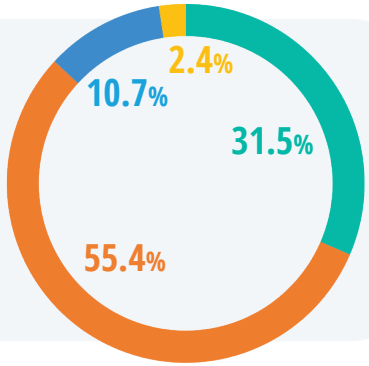
Confidence level is associated with company size, with larger firms (37.5% with 10,000+ employees and 30.4% with $1B+ in revenue) reporting that they are very confident. Only about one-fifth (20.5% of both firms with 1-200 employees and firms with less than $100M in revenue) said the same.

In the event of a data incident, 10.7% of all CISOs surveyed said their organization can, using real-time data access monitoring, immediately identify which data unauthorized parties may have accessed. Nearly half (45%) can do so within hours because they have an efficient data inventory and classification system. More than one-third (34.9%) can pinpoint unauthorized data access within days, but only if a manual investigation is carried out. More than 9% said they weren't sure because their data exposure identification process needs improvement.

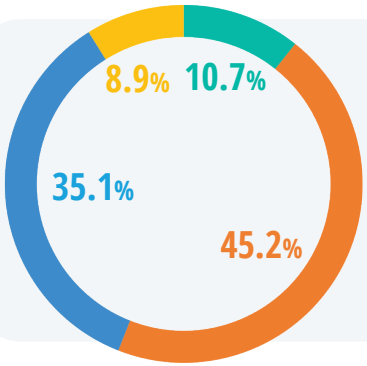
As expected, larger entities (21.9% with 10,000+ employees and 19.6% with $1B+ in revenue) were more commonly able to immediately identify unauthorized data access. Only 7.7% of organizations with 1-200 employees and 9.1% with less than $100M in revenue said the same.

When assessing the impact of a data incident, 39.6% of all CISOs surveyed said that their company has predefined criteria and metrics to evaluate incident severity. More than one-third (37.3%) base their severity assessment on the potential impact on data subjects and regulatory requirements. Roughly one-fifth said they assess incidents on a case-by-case basis without a standardized criteria while 3.6% said they are unsure because their incident severity assessment process needs refinement.

How well-defined is your organization's response plan for Data Security incidents?



In the event of a data incident, how quickly can your organization identify what data any unauthorized parties had access to?



Incident response remains a formidable challenge, regardless of an organization's experience with past incidents. The stress on the incident commander is considerable due to the need to quickly yet precisely pinpoint and mitigate the cause and restore business continuity. This pressure is compounded by the rapidly evolving threat landscape, the growing number of data and privacy regulations, and the mandates to report breaches within strict timelines. These factors demand accurate assessment of incident severity, strategic stakeholder engagement, and meticulous execution of response and remediation protocols.

Artificial Intelligence (AI) holds significant promise in streamlining this process. It can provide reliable assessments of risk by analyzing trends and sensitive company data, offer informed guidance on regulatory reporting obligations tailored to the incident's scope and severity, suggest relevant stakeholders for engagement, and propose actionable remediation strategies. While AI is not a substitute for human judgment, it can serve as a powerful tool to alleviate the stress inherent in incident response by enhancing decision-making with data-driven support.

Rupa Parameswaran
VP of Security & IT, Handshake

DATA PRIVACY AND THE NEED TO SAFEGUARD ALL INFORMATION

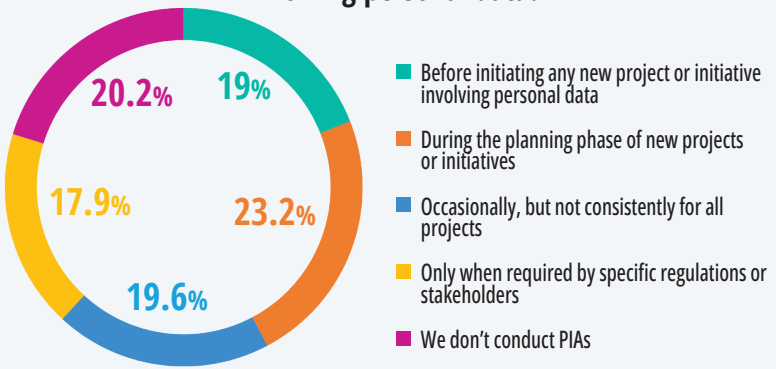
Privacy is paramount to any organization. CISOs want and need to be able to safeguard company, client, employee and consumer information at every turn. To that end, 33.1% of all CISOs surveyed said their company has dedicated processes and teams in place to handle Data Subject Access Requests (DSARs) efficiently. Roughly the same amount (33.7%) manage DSARs on an ad-hoc basis. Only 4.7% said they rely on third-party service providers for DSAR management but a fairly sizable 28.4% said they are unsure because they haven't formalized their DSAR management process.

The majority of organizations (84.5%) said they ensure data privacy and security in cloud environments by encrypting data at rest and in transit in cloud storage. Nearly as many (82.7%) said they have implemented access controls and identity management in cloud platforms. Well over half (66.7%) said they employ continuous monitoring and alerting on cloud activities, and roughly the same number of CISOs (65.5%) said their firm conducts regular security assessments and audits of cloud service providers. More than two-fifths (44.6%) use data minimization and governance. Only 10.7% rely solely on a cloud provider's security controls.

When asked how frequently they conduct Privacy Impact Assessments (PIAs) for new projects or initiatives involving personal data, 23.1% said they do so during the planning phase. Just over 20% said they conduct PIAs occasionally but not consistently for all projects. An equal number said they don't conduct PIAs at all. Roughly 19% do so before initiating any new project or initiative involving personal data and 17.8% said they only do so when required by specific regulations or stakeholders.

Among those who do conduct PIAs, 70.2% primarily consider the type of personal data collected and processed when assessing privacy risks. More than three-fifths (63.1%) consider the security measures in place to protect personal data. Nearly as many (61.9%) look at the purpose and duration of data processing while 58.3% evaluate the lawfulness and transparency of data processing activities. More than half (53.6%) also consider the potential for data breaches and unauthorized access. Just under half (49.4%) consider data subject rights and access.

How frequently does your organization conduct Privacy Impact Assessments (PIAs) for new projects or initiatives involving personal data?



Data privacy regulation(s) continue to emerge globally which makes protecting data even more important and subject to regulatory scrutiny. Well established Governance, Risk Management, and Compliance (GRC) provide the appropriate reporting to ensure we're continuing to improve our cyber programs. Effective data privacy protocols and measures help organizations comply with the regulatory requirements, build trust with customers and stakeholders and can be a differentiator for an organization. By prioritizing data privacy, organizations can safeguard their reputation and avoid significant financial and legal ramifications.

Robyn Wright
CISO, Wiley

CONCLUSION

THE BATTLE FOR DATA SECURITY CONTINUES

The CISO Society 2024 State of Data Security Report provides an inside look at how CISOs are tackling some of their biggest challenges. They shared their priorities for strengthening their data security program with 32% focusing on data discovery and nearly as many using risk analysis. They primarily attribute their data security gaps to a lack of funding (27%) and lack of resources (26.6%). Most CISOs don't plan to dramatically alter their budget or increase their headcount to manage data security in 2024.

More than 50% of CISOs base their data sensitivity levels on both regulatory compliance requirements and the potential impact to their business. Just 18.9% said they have clear visibility into who has access to their data, 21.9% have no visibility into the data flowing into their AI models, and only 2.4% said they are very confident that they have built a zero trust model with least privileged permissions.

Despite their shortcomings, 55.6% of CISOs have a defined response plan for data security incidents, and more than 30% have and regularly test a highly detailed plan. Many (39.6%) have predefined criteria and metrics to evaluate incident severity.

Regarding cloud environments, more than 84% ensure data privacy and security by encrypting data at rest and in transit in cloud storage, and nearly as many have implemented access controls and identity management.

These findings highlight that CISOs are aware of their challenges and shortcomings but aren't in a hurry to increase their budget to solve them. Many have plans in place to deal with the increasing risks associated with cyberattacks and data breaches but most admitted that their strategy could be improved. This could open the door to future threats, especially as malicious actors become more advanced and rely more heavily on AI. While it is not yet clear how successfully businesses can use AI to stop cyberthreats, cybercriminals will undoubtedly use the technology in any way they can to get an advantage. Attackers don't need to be perfect – they just have to be lucky.

Until all gaps and vulnerabilities are resolved, they will continue to find ways to infiltrate the enterprises they target. And if and when those vulnerabilities are eliminated, new threats that no one thought of will inevitably materialize, ensuring the battle for data security will continue on. ■