Data security as business accelerator?

The unsung hero driving competitive advantage

In collaboration with

IBM | aws

Experts on this topic

Clarke Rodgers

Director, AWS Enterprise Strategy
linkedin.com/in/clarkerodgers
rodgclar@amazon.com

With over 20 years of experience building and managing cybersecurity programs, and now, as Director, AWS Enterprise Strategy, Clarke is passionate about helping customer executives explore how strong security, risk, and compliance programs can enable their business to grow and innovate faster. Joining AWS in 2016, Clarke has advised over 700 customers across virtually every industry (from financial services to healthcare, media and entertainment, and government) on all things digital transformation (people, process, organizational change) and security, risk, compliance, and privacy topics. As a US Marine veteran, Clarke brings a unique perspective as to how business outcomes can be derived from strong security programs.

Chris McCurdy

Worldwide Vice President and General Manager, IBM Security Services
linkedin.com/in/chrismmccurdy
cmccurdy@us.ibm.com

For more than 15 years, Chris has held multiple leadership positions directing sales and strategy for IBM Security Services, consistently driving rapid growth of the security business. Before joining the company, he was a managing consultant at several consulting firms, including Andersen, International Network Services, and Lucent Technologies. He was also CIO at a large US retail automotive group. Chris holds a BBA in Information Systems from Baylor University and is a Certified Information Systems Auditor.

Gerald Parham

Global Research Leader, Security and CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham
gparham@us.ibm.com

Gerald leads the security and CIO research areas within the IBM Institute for Business Value. He advises senior executives and board members on technology and security strategy, cyber risk, and cyber-value chains. Gerald has more than 20 years of experience in executive leadership, innovation, and intellectual property development. He holds advanced degrees in science and fine arts from California State University and the University of Southern California, as well as a BA in writing from Johns Hopkins University.

Key takeaways

Secure, trusted data can supercharge innovation and deliver a competitive edge.

Strong data security establishes trust that unlocks business value.

Recent research showed that high-performing Chief Data Officers prioritize trust and security in assessing their data effectiveness.

Value is cross-functional, and this can enhance data security.

Data and security leaders must collaborate with their operations and technology peers to realize the full value of their data.

A culture of assurance helps drive better business outcomes.

The mindset around security must shift from gatekeeper to business enabler—from saying “no” to determining “how.”

Unlocking the value of trust

In the digital economy, data is like oxygen—giving life to innovation—and securing that data is critical to organizations establishing trust and delivering value. In fact, organizations with the most advanced security capabilities delivered 43% higher revenue growth than peers over a five-year period, according to research from the IBM Institute for Business Value (IBM IBV).[1]

Yet when corrupted or exposed, data can fuel disruption. Poor-quality data costs organizations an average of $12.9 million annually, while the average cost of a data breach reached almost $10 million in 2022 for US organizations.[2] When trust in data is broken, it impedes business growth and drives up spending.

The very best organizations navigate this challenge by rapidly establishing trust based on a strong foundation of secure data and then using that trusted data to unlock opportunity. In this report, we identify the paradigms, practices, and priorities that successful leaders use in managing and securing data to help deliver a competitive advantage.

Seeing around curves

The most successful Chief Data Officers (CDOs) prioritize secure, trusted data as a driver of business value. That is the clear takeaway from two recent studies of more than 3,300 CDOs, conducted independently by the IBM IBV and by Amazon Web Services (AWS). This research underscores the vital importance of trusted data as a business enabler.

The most successful Chief Data Officers prioritize secure, trusted data as a driver of business value.

CDOs in the IBM IBV study cited data security as their most critical responsibility.[3] Similarly, respondents in the AWS CDO Agenda noted data governance—an essential element of data security—as their top priority.[4] These CDOs first protect data to establish trust with employees, customers, and partners; then they use that trust to activate the data's value and generate growth more confidently and quickly.

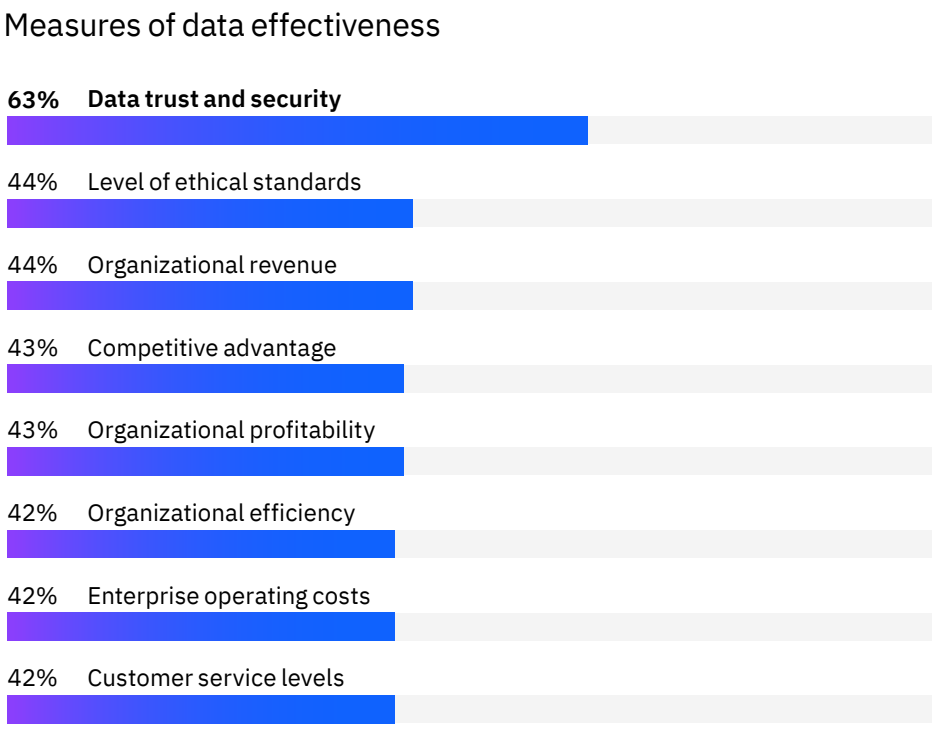
The highest-performing CDOs take these priorities a step further. The IBM IBV study identified an elite group of CDOs, dubbed "Data Value Creators," who outperform peers by 40% in innovation and 10% in revenue growth.[5] These CDOs allocate proportionally less of their revenue to data-related business processes, yet generate equal or greater value from that data. A critical differentiating trait: the way they align data with security, operations, and technology. They place a stronger emphasis than peers on cybersecurity and data ethics, on transparency in data architecture, and on trust in data effectiveness (see Figure 1).

The practices that drive results at these leading organizations can be emulated by any organization. As these leaders demonstrate, if applied in a systematic and rigorous way, basic data hygiene practices lead to greater data agility. This, in turn, can drive smarter risk-taking, more operational resiliency, and, ultimately, better business outcomes. What follows is a roadmap for gaining a competitive edge with secure and trusted data.

FIGURE 1

Prioritizing trusted data

Leading CDOs measure data effectiveness based on trust and security.



High-performing CDOs valued "data trust and security" far more than other measures of data effectiveness.

Source: "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023.

Supercharging data innovation

Former racing driver Mario Andretti once said, "It's amazing how many drivers, even at the Formula 1 level, think that brakes are for slowing the car down." Rather, as Andretti demonstrated, brakes allow experienced drivers to go faster.[6]

Similarly, strong data security helps organizations move confidently and realize value more efficiently. Businesses can dare to go faster and take risks knowing they have implemented effective controls.

Leading CDOs illustrate the point. Their organizations use modern tech tools to help protect data from unauthorized access, help enforce data privacy, and manage compliance and governance. They establish a security foundation that positions them to more quickly achieve operational goals—from increasing revenue and profits, to improving customer relationships and marketing, to enabling new products and services, processes, business models, and strategies.[7]

Aligning their data, operations, technology, and security strategies to the organization's primary business objective, or "North Star," ultimately helps strengthen data security and establish the trust required to fuel better decisions and better performance (see Figure 2). In acknowledging the relationships between functional areas, leaders create an environment where collaboration is the norm and where functional strategies are connected to power innovation at scale and speed.

Leading data organizations also recognize that culture drives outcomes. They do the following things differently:

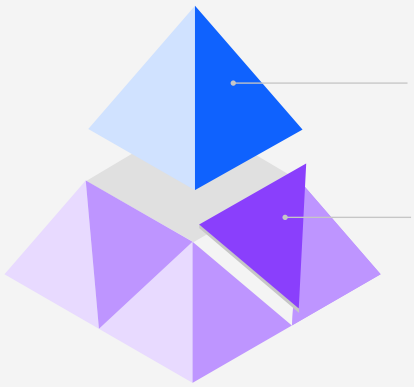
- Remove obstacles that erode trust
- Build a culture of assurance
- Plan for resilience.

Like brakes on a race car, strong data security helps organizations move faster with greater confidence.

FIGURE 2

The secret to high performance

Data and security are two components of a larger value engine.

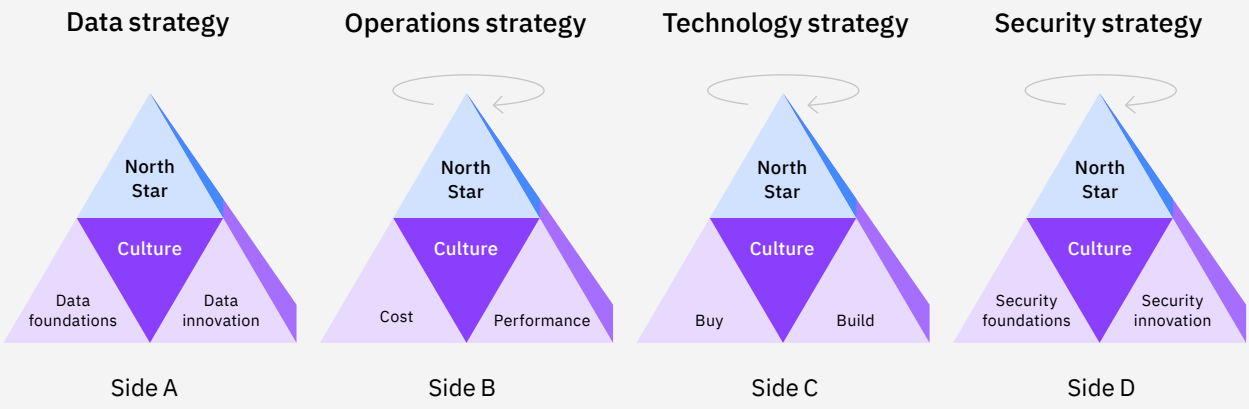


Value engine

North star
Business strategy ties value (growth) to values (mission)

Culture is what connects domain strategies to each other

- Core values: Act with integrity and transparency
- Communicate: Raise awareness and foster trust
- Collaborate: Accelerate insights and innovation
- Coordinate: Enhance resilience and extend reach



Source: IBM IBV

Leading practice one

Removing obstacles that erode trust

Improving an organization's data security posture typically requires change, and change inevitably encounters obstacles. But by consciously addressing these challenges—from siloed, domain-specific solutions to gaps in transparency and accountability—data security can be turbocharged to accelerate new business opportunities.

Bridging siloed agendas

It's simple enough to say: instill a secure, data-driven, agile culture that remakes legacy businesses using digital environments and services. But for most organizations, acting on this goal presents daunting challenges. For instance, data, operations, technology, and security functions often operate independently, with domain-specific strategies that do not reinforce each other. To unlock value through operational efficiency or performance outcomes, these disparate capabilities must build upon each other and be aligned with the organization's North Star, a point of reference that embodies the common business strategy and core mission.

Nearly one-third of respondents in the AWS CDO Agenda said they share responsibility for data management with other C-suite leaders.[8] While this could be seen as a barrier, leaders recognize they need each other to succeed and must nurture relationships to build stronger, more mature capabilities. Without a culture of collaboration where domain-specific strategies support each other, an organization is limited in its ability to identify trade-offs or agree on its most pressing business objectives.

Leaders recognize that collaboration and strategy alignment across the organization can build trust.

Reducing operational friction

A digital economy derives value based on the free flow of data. As centralized, static data has given way to data in the cloud, on-premises, at the edge, and from business partners, traditional security policies and controls must evolve to address increasing complexity and risks. Leaders know their organizations must focus beyond their network boundaries and their hosting infrastructure to the data itself, whether it's at rest, in motion, or in use.

They also must cast an eye to the future as new technologies further complicate status quo approaches. For example, emerging quantum computing capabilities will require updating many current approaches to data encryption.[9] Looking ahead, homomorphic encryption, blockchains, AI-generated content, and automated decision-making will challenge long-standing practices and assumptions around data security.[10]

Eliminating ambiguity

Transparency into how data is accessed, stored, processed, and shared is essential for both internal business users and external customers, especially in highly regulated industries (see Perspective, "Earning trust"). Yet historical data management practices and data architectures often can't provide visibility into the volumes and types of data that organizations use. Both the IBM IBV study and prior research from AWS revealed a greater need for transparency between the teams that understand source data and front-line users who make decisions using that data.[11]

CDOs realize this transparency divide must be narrowed or trust in the data deteriorates—especially at the most senior levels. While 68% of CDOs in the IBM IBV study indicated employees largely trust the organization's data, nearly 40% reported their executive leadership does not.[12] This may reflect underlying concerns around data taxonomies, data security, and data governance. CDOs must address this skepticism, or it will undercut investment, momentum, and business potential.

Perspective

Earning trust in highly regulated industries: Opportunity awaits

Every organization must meet a minimum data security baseline to conduct business with confidence. For highly regulated industries dealing with sensitive data, that baseline is higher. In industries such as healthcare, banking and financial services, energy, and pharmaceuticals, one-quarter of the cost of a data breach accrues more than two years *after* the breach occurs.[13] This is due to lingering regulatory, legal, and brand reputation costs stemming from individuals' sensitive and personally identifiable information (PII) being exposed.[14]

The biggest gap for CDOs in highly regulated industries—and the biggest opportunity—is prioritizing secure data outcomes. Only 30% of banking and financial market CDOs were likely to view data regulatory compliance as a critical responsibility, according to IBM IBV research. Remarkably, only about half of banking and financial market CDOs said it is important to adhere to industry privacy and ethics policies and regulations.[15]

We found the same pattern in other highly regulated industries. Only 63% of healthcare and life sciences CDOs and 63% of government CDOs prioritized industry privacy and ethics policies and regulations.[16] If trust is a precious resource that is hard won yet easily lost, addressing these data privacy and ethics considerations is critical to more consistent engagement, stronger relationships, and ultimately, a competitive advantage.

Leading practice two

Building a culture of assurance to drive outcomes

Like the confidence gained in handling a race car, a culture of assurance—where leaders, employees, partners, and customers trust the data they are using—leads to a more predictable, higher-integrity, high-performance environment. But everyone from the mailroom to the boardroom must accept their responsibility for data security.

Leading with "how"

Top organizations encourage a new way of thinking about security. Starting at the top, executives raise the bar for cyber-risk awareness across the enterprise—a necessity, considering one study found that 95% of cybersecurity issues can be traced to human error.[17] Leading organizations give team members incentives and permission to prioritize security, even to the point of delaying product delivery if security capabilities aren't operating as intended.

This mindset is easier to adopt when security is positioned to support business outcomes rather than simply as policy enforcement. As leaders succeed in shifting the role of security from gatekeeper to business enabler, security decisions become more about "how" instead of an automatic "no"—a decisive shift in outlook.

Everyone from the mailroom to the boardroom must take responsibility for data security.

Taking a fresh approach to talent

Rethinking the makeup of security teams—including partnering with non-technical personnel—can result in a stronger, more multifaceted defense. Because data and security are inherently cross-functional, leading organizations recognize they must tap into new ways of seeing familiar challenges.

For example, a human resources professional may better understand the perspective of a threat actor employed by the hour or by the deliverable. A marketing and communications professional can provide guidance on how best to share news of a data exposure. Someone without a college degree may demonstrate a proficiency with emerging technologies in ways no formal education could replicate.[18] Such openness introduces fresh perspectives, plus expands a talent pool where skills and expertise come at a premium.

Rethinking the makeup of security teams —including partnering with non-technical personnel— can result in a stronger, more multifaceted defense.

Making compliance, privacy, and ethics ways of doing business

While compliance is often seen as an impediment by some business users, it is essential to achieving data privacy and data ethics. CDOs realizing the most value from their data said they outperform peers in data ethics, transparency, and cybersecurity (see Figure 3). They demonstrate how these capabilities can deliver a competitive edge.

For example, a proactive approach to compliance can remove friction. In a recent podcast, Samara Moore, AWS Senior Manager of Security Assurance, encourages security teams to develop strong relationships with business and technology counterparts to mediate between operational and regulatory concerns. She advises leaders to view compliance as an element of design, with functionality embedded into solutions.[19]

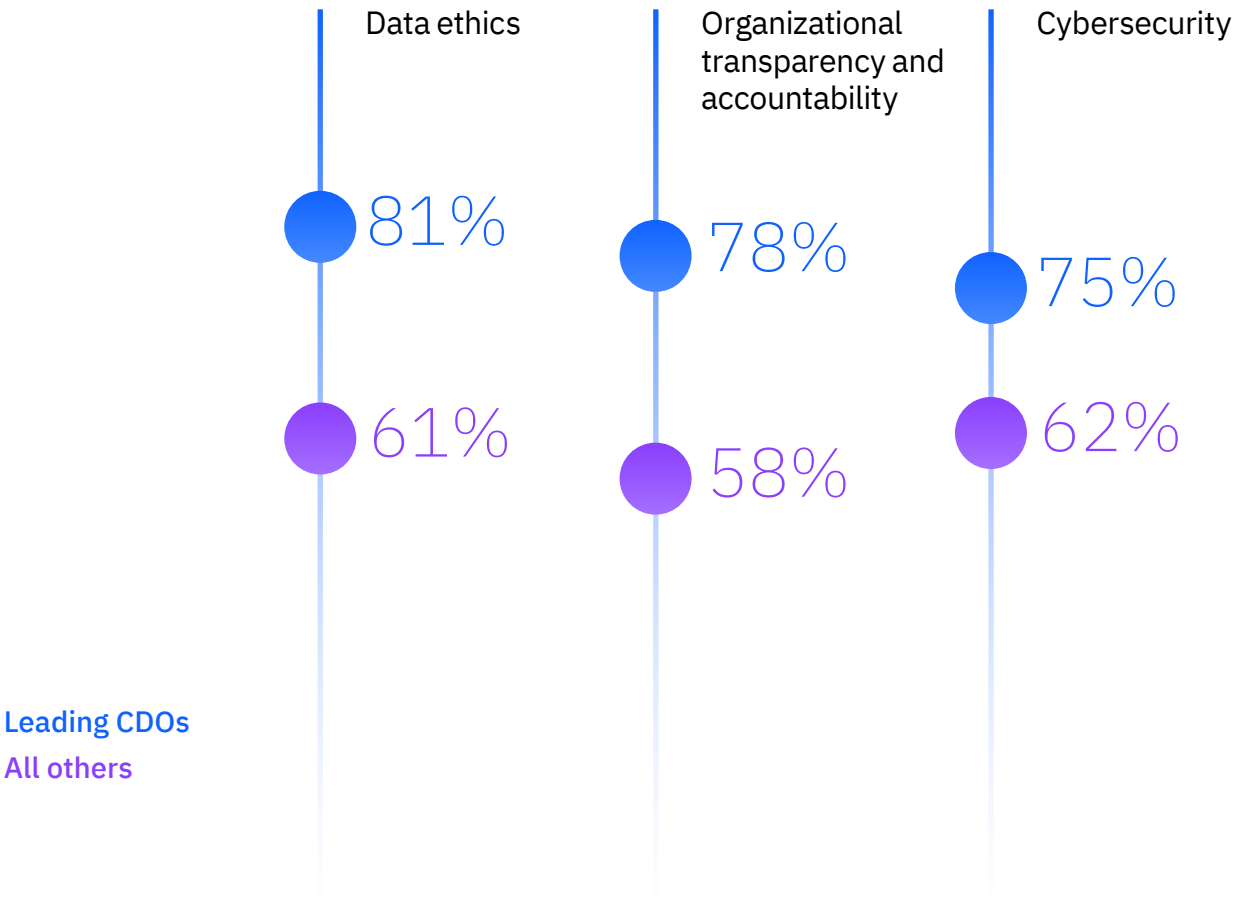
Similarly, compliance management software can make administration of policies and controls less visible and more automatic. Research shows that automated compliance tools can cut audit prep time by up to 75% —a notable improvement in operational efficiency.[20]

A proactive approach to compliance can be a competitive differentiator.

FIGURE 3

Protecting data value

Top-performing CDOs outperform peers in trust-related data practices.



Source: "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023.

Leading practice three

Planning for resilience

As unexpected events fall on the heels of each other—the global pandemic, supply-chain disruptions, climate-related disasters, the war in Ukraine, economic uncertainty—organizations are contending with a series of shocks that upend planning assumptions and conventional risk mitigation techniques.[21]

Operations environments become rife with uncertainty and, at times, even chaos. Meanwhile, threat actors are eager to capitalize on new vulnerabilities. In response, leading CDOs team with their security leaders to double down on basic security hygiene—improving data governance while boosting operational resilience (see Perspective, “Back to basics”).

Becoming comfortable with the uncomfortable

With ambiguity and bad actors disrupting business as usual, leaders can prepare for the unexpected and protect the value engine driving the business. Readiness begins with a rigorous, honest evaluation of capabilities and vulnerabilities. Embracing the principles of “chaos engineering” helps organizations assess risks and understand dependencies. By intentionally impairing systems or removing critical components, they can identify where and how data, operations, technology, and security capabilities break down.

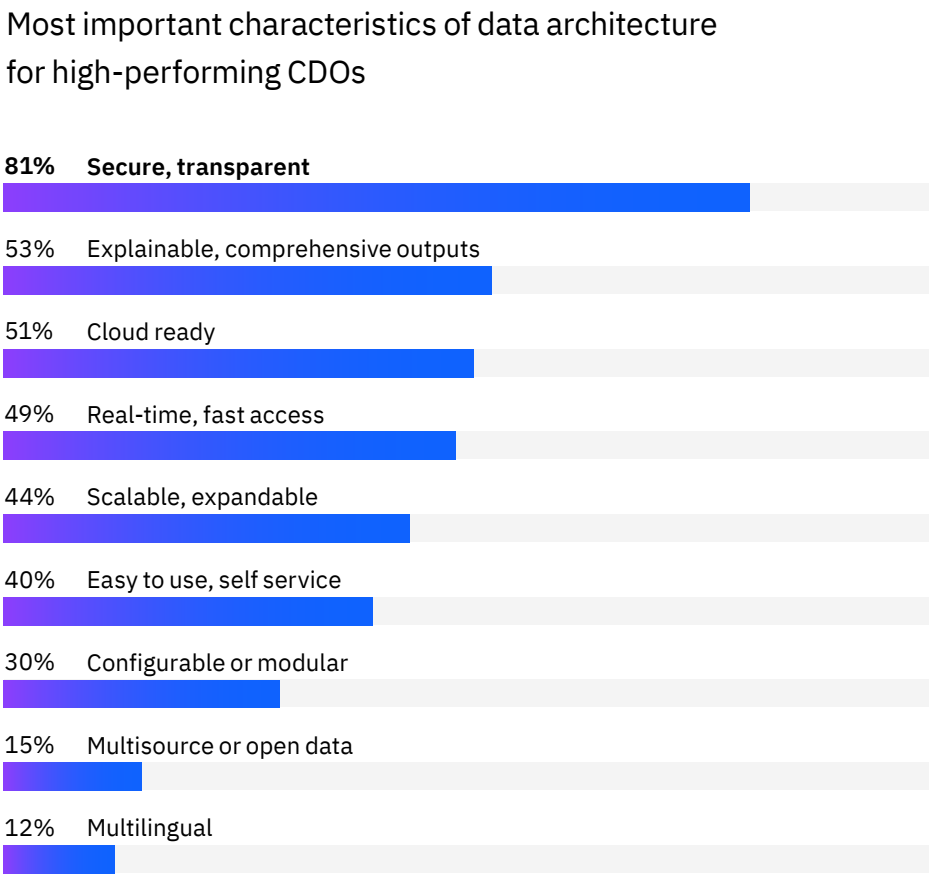
Leaders double down on basic security hygiene to be ready for the unexpected.

With this knowledge—and by working across domains to address the weaknesses—leaders are better positioned to build a resilient technology and operations environment that can respond more effectively to disruption and protect trusted data. In support of this goal, effective leaders prioritize a secure, transparent data architecture, cited by more than 80% of top CDOs in the IBM IBV study (see Figure 4).[22]

FIGURE 4

Optimizing for opportunities

A secure data architecture positions organizations to take risks on new business possibilities.



"Secure, transparent" far outranks other data architecture characteristics.

Source: "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023.

Perspective

Back to basics: Better data hygiene sets the stage for higher performance

Understand the data to identify challenges and opportunities

Organizations must first assess their operations environment by inventorying, categorizing, and classifying data according to sensitivity and criticality. This includes knowing how efficiently the organization can generate evidence of regulatory compliance.

A data classification and administration strategy enables leaders to make risk-based decisions based on the sensitivity and criticality of data assets and services. When uncertainty arises, leaders can rely on a playbook to streamline decisions and prioritize remediation based on risk factors such as likelihood or severity.[23]

Secure the data environment to establish and extend trust

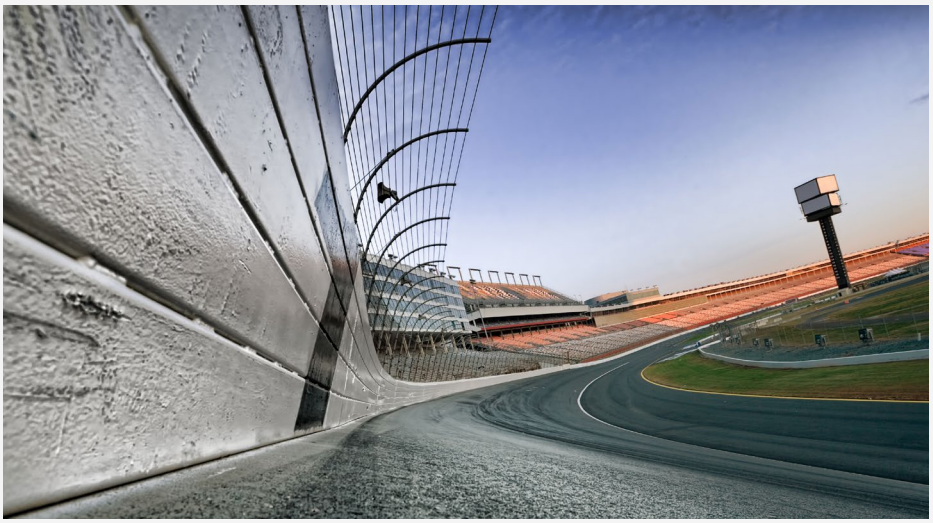
Each organization has a unique appetite for risk. Understanding risk exposure through risk qualification and quantification capabilities can help communicate the importance of secure and trusted data—something many stakeholders may take for granted. Assessing the existing control plane—especially through stakeholder feedback—can help focus attention on areas where controls may be too strict or too lax. Security telemetry and event logging are critical capabilities.

Because many security services are becoming context-dependent and event-driven, organizations need to be proficient in identifying users, devices, and increasingly, automated service entities. They need to incorporate dynamic risk scoring into their operations and make services available or unavailable based on whether the request is familiar versus unfamiliar, known versus unknown, or typical versus anomalous. Security solutions that incorporate User and Entity Behavior Analytics (UEBA) or XDR (Extended Detection and Response) capabilities are designed for this.[24]

Monitor data environments to improve data security and agility

Taken together, all of these should influence the data governance environment and the security controls used to enable greater data security and agility. Standardizing and streamlining data taxonomies can lead to greater efficiency. Reducing operational complexity adds benefits in terms of using, securing, and sharing data. Many of these capabilities can be augmented with the help of service partners.

For enablement, many organizations are using service tiers to denote higher and lower levels of data sensitivity and criticality, as well as for categorizing suppliers that may require more stringent security controls. Finally, every organization needs a well-rehearsed Incident Response (IR) regimen and Business Continuity Planning (BCP) capabilities. These must incorporate stakeholders from across the organization, as well as critical partners outside the organization—for example, marketing and communications partners to communicate the potential downstream impacts of data breaches.



Leveraging AI and automation

As CDOs lean into advanced analytics and AI to harness value from their data, security teams must also leverage these tools to help maintain and enhance the organization's security posture. AI and automation can accelerate the ability to respond to security events automatically, identify typical versus atypical behavioral patterns, and intelligently manage exceptions and escalations.

In recent IBM IBV research, leading adopters of AI security tools detect, respond, and recover from incidents in nearly half the time as organizations with the least mature security AI capabilities.[25] And fully deployed security AI and automation is the single greatest factor in reducing overall costs associated with data breaches.[26]

But AI must be trusted to deliver on its full potential. The next generation of AI—the large language models such as OpenAI's ChatGPT tool—offers great potential but also raises critical questions around data privacy, data security, and data ethics (see Perspective, "Generative AI"). For example, some researchers have identified issues with "AI hallucinations," where models make spurious inferences or assume causal relationships that don't exist.

Leaning on partners

As organizations increasingly rely on external business partners to supplement capabilities, security leaders view these relationships as potential threat vectors. But with proper governance and accountability, external parties can become essential sources of resilience. When partners share core values and a mutual commitment to shared responsibility and accountability, organizations can re-envision the network as a joint investment in operational awareness, risk mitigation, and redundancy that protects all parties.

A smart strategy recognizes that partners can help each other speed insights, reduce risks, and capture new sources of value. In fact, leading CDO organizations with a mature partner strategy saw 63% more revenue growth.[27]

Integrating data, operations, technology, and security strategies across the organization and the partner network helps build trust. And with trust in place, organizations are positioned to unlock more value.

With proper governance and accountability, external partners can become essential sources of resilience.

Perspective

The risks and opportunities of generative AI

The risks

A recent Salesforce survey reveals that most senior IT leaders expect generative AI to help their organizations take better advantage of data to serve customers and operate more efficiently. But 71% expect it to introduce new security risks to their data.[28]

While tools such as ChatGPT have captured the public's imagination, they also introduce data privacy issues. For example, a curious user could expose business-sensitive information to the public through the prompts submitted to the system.[29]

Generative AI tools also give threat actors a quick way to generate new, more complex types of malware and phishing schemes.[30] The ability to generate and execute code should be of concern to everyone—and is why many leaders advocate caution.[31] Both the inputs and the outputs of generative AI tools are subject to manipulation. This becomes even more dangerous when autonomous AI agents are used to generate fake content, to take actions, or trigger attacks at scale and speed.[32]

The opportunities

Generative AI offers defensive advantages as well. It can simulate attacks that strengthen an organization's training and readiness.[33] Organizations can tailor large language and foundation models to improve training and knowledge management—for example, by curating content to help bridge skills gaps. Additionally, customized models can respond to audit questions as well as create intelligence and risk reports that give organizations greater context for security incidents.[34]

When engaging in generative AI projects, business leaders must ensure they establish strong AI ethics and governance mechanisms to mitigate the risks involved. And to facilitate the responsible use of generative AI in cybersecurity, leaders need to implement security policies and controls that recognize both offensive and defensive use cases. For all the efficiency generative AI promises, the technology requires leaders to develop new practices around monitoring inputs and outputs for manipulation. Finally, to foster trust, every organization should articulate a set of guidelines for how to use—and not use—generative AI solutions.

Action guide

Data security as business accelerator?

The unsung hero driving competitive advantage

For the C-suite

Calibrate

Build a common foundation by aligning with your organization's North Star.

Start now

- Align data, operations, technology, and security strategies to your organization's core business strategy, your North Star.
- Identify areas of friction for partners and customers, focusing on procedural and governance factors that impede decision-making, value realization, or trust.

Next steps

- Identify high-impact risks and develop cross-functional mitigation plans to minimize business disruption.
- Focus on higher value propositions that require coordinated decisions across data-operations-technology-security capabilities.

Cultivate

Foster a culture that prioritizes secure and trusted data as the fastest path to value.

Start now

- Incentivize data security practices and data literacy from boardroom to mailroom.
- Re-envision data security as the foundation for higher performance (higher trust, smarter risks, faster decision-making, greater resilience).
- Proactively liaison between regulators and your organization to position compliance as a competitive differentiator.

Next steps

- Evaluate the makeup of your security teams. Don't focus only on degrees and certifications. Invite those with non-security backgrounds, diverse perspectives, and different ethnic backgrounds to join the conversation and build a more complete security perspective.
- Add security and data privacy responsibilities to every employee's job description.
- Become an advocate for the business value of better data privacy and ethics capabilities.

Action guide

For functional and line-of-business leaders

Anticipate

Become comfortable with the uncomfortable by enhancing your cyber risk capabilities.

Start now

- Embrace risk quantification and qualification to continuously evaluate your potential attack surface; never settle.
- Adopt a “how” approach to data security instead of a “no” approach that limits new features and functionality.
- Double down on data security basics and everyday security hygiene practices to help ensure your security team can respond effectively to unplanned disruptions.

Next steps

- Use the principles of chaos engineering to anticipate potential future shocks.
- Use incident response simulations to practice how your data, operations, technology, and security teams work together and perform.

Orchestrate

Use integrated data, operations, technology, and security capabilities to enhance cyber resilience across your partner network.

Start now

- Identify partners that share your core values and your approach to risk. Select partners that help you deliver on North Star business objectives, particularly those that encompass data, operations, technology, and security functions.
- Deploy AI and automation solutions to improve productivity across data, operations, technology, and security functions. Use AI to complement human expertise and to accelerate detection, response, and recovery from cyber incidents.

Next steps

- Deploy partner-level dashboards to increase visibility and transparency around common data, operations, technology, and security practices.
- Align partner network decisions to your North Star, using accepted governance standards to reduce complexity, streamline decision-making, and enhance overall cyber resilience.

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based on conversations with leading subject-matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at https://ibm.co/ibv-linkedin.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

About AWS

For over 15 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud offering. Today, we serve millions of customers, from the fastest growing startups to the largest enterprises, across a myriad of industries in practically every corner of the globe. We've had the opportunity to help these customers grow their businesses through digital transformation efforts enabled by the cloud. In doing so, we have worked closely with the C-suite, providing a unique vantage point to see the diverse ways executives approach digital transformation—the distinct thought processes across C-suite roles, their attitudes and priorities, obstacles to progress, and best practices that have resulted in the most success.

About the AWS-IBM Security partnership

IBM is an AWS Premier Tier Consulting Partner, including three security competencies and a total of 16 AWS competencies across IBM Technology and IBM Consulting. Together, IBM and AWS bring fast, security-rich, open software capabilities to the cloud platform of choice for more than 1 million customers every day. The power of cloud-native AWS capabilities, combined with 50+ IBM solutions available on AWS Marketplace, enables clients to access AI-powered IBM Software with turnkey delivery and integration. For more information, visit https://www.ibm.com/aws/security

Related reports

Prosper in the cyber economy

McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik, Ph.D. "Prosper in the cyber economy: Rethinking cyber risk for business transformation." IBM Institute for Business Value. November 2022. https://ibm.co/security-cyber-economy

Turning data into value

"IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

Chief Data Officer (CDO) Agenda 2023

Davenport, Thomas H. "Chief Data Officer (CDO) Agenda 2023: Prioritizing business value creation." AWS. 2022. https://aws.amazon.com/data/cdo-report/

Acknowledgements

This paper is the result of collaboration across several teams at Amazon Web Services (AWS) and the IBM Institute for Business Value (IBM IBV). We'd like to highlight the essential contributions and guidance of Heather Deguzman, Sandra Woods, Teresa Rollins, Dinesh Nagarajan, Bhuvana Chandar, Bob Breitel, Mahmoud Elmashni, and Liam Cleaver. This paper would not have been possible without the exceptional talents and creativity of Joanna Wilkins, Editorial Lead, and Nancy Pendleton, Design Lead.

Notes and sources

1 McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Dr. Jacob Dencik. "Prosper in the cyber economy: Rethinking cyber risk for business transformation." IBM Institute for Business Value. November 2022. https://ibm.co/security-cyber-economy

2 Sakpal, Manasi. "How to Improve Your Data Quality." Gartner. July 14, 2021. https://www.gartner.com/smarterwithgartner/how-to-improve-your-data-quality; "Cost of a Data Breach Report 2022." IBM Security and the Ponemon Institute. July 2022. https://www.ibm.com/reports/data-breach

3 "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

4 Davenport, Thomas H. "Chief Data Officer (CDO) Agenda 2023: Prioritizing business value creation." AWS. 2022. https://aws.amazon.com/data/cdo-report/

5 "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo and unpublished data

6 Milne, Duncan. "The Brakes Aren't There to Slow Us Down. What Can Legal and Compliance Programs Learn from the Fastest Sports Teams on the Planet?" The Compliance and Ethics Blog. January 31, 2022. https://www.complianceandethics.org/the-brakes-arent-there-to-slow-us-down/

7 Davenport, Thomas H. "Chief Data Officer (CDO) Agenda 2023: Prioritizing business value creation." AWS. 2022. https://aws.amazon.com/data/cdo-report/

8 Ibid.

9 Harishankar, Ray, Dr. Sridhar Muppidi, Michael Osborne, Dr. Walid Rjaibi, and Dr. Joachim Schaefer. "Security in the quantum computing era." IBM Institute for Business Value. December 2022. https://ibm.co/quantum-safe-encryption

10 Wayner, Peter. "Hot areas for encryption innovation." CSO. September 28, 2020. https://www.csoonline.com/article/3575830/4-hot-areas-for-encryption-innovation.html

11 "In unpredictable times, a data strategy is key." MIT Technology Review Insights in collaboration with AWS. https://pages.awscloud.com/GLOBAL-ln-GC-600-SOL-Unpredictable-Times-Data-Is-Key-learn.html?trk=d267b9ce-17c0-4ebc-9f42-24f6e3e4ab26; "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

12 "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. Unpublished data.

13 "Cost of a Data Breach Report 2022." IBM Security and the Ponemon Institute. July 2022. https://www.ibm.com/reports/data-breach

14 Ibid.

15 "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. Unpublished data.

16 Ibid.

17 Zhadan, Anna. "World Economic Forum finds that 95% of cybersecurity incidents occur due to human error." January 18, 2022. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

18 Subramoni, Santha. "Cybersecurity: Why we need to shift the narrative to build a cyber-ready workforce." World Economic Forum. February 8, 2023. https://www.weforum.org/agenda/2023/02/cybersecurity-cyber-ready-workforce-training-reskilling/

19 "#125: Think Like an Auditor: How to Measure Security Compliance." AWS podcast. https://aws.amazon.com/podcasts/125-think-like-an-auditor-how-to-measure-security-compliance/

20 "The Total Economic Impact™ Of IBM Security Guardium: Cost Savings And Business Benefits Enabled by Guardium." Forrester Research, commissioned by IBM. October 2020. https://www.ibm.com/resources/security/forrester-tei-guardium

21 Paydos, Timothy and Mike Stone. "Preparing governments for future shocks." IBM Institute for Business Value Blog. July 13, 2022. https://www.ibm.com/thought-leadership/institute-business-value/blog/government-prepare-future-shocks; Scott, Tony, "Preparing governments for future shocks: An action plan to build cyber resilience in a world of uncertainty." https://ibm.co/governments-future-shocks

22 "IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less." IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

23 "How to Use (And Understand) a 5x5 Risk Matrix." HASpod. September 20, 2020. https://www.haspod.com/blog/paperwork/5x5-risk-matrix

24 "IBM Security QRadar Suite." IBM webpage. Accessed May 9, 2023. https://www.ibm.com/qradar; "What is User and Entity Behavior Analytics (UEBA)?" Palo Alto Networks website. Accessed May 9, 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-ueba

25 Muppidi, Sridhar, Lisa Fisher, and Gerald Parham. "AI and automation for cybersecurity: How leaders succeed by uniting technology and talent." IBM Institute for Business Value. June 2022. https://ibm.co/ai-cybersecurity

26 "Cost of a Data Breach Report 2022." IBM Security and the Ponemon Institute. July 2022. https://www.ibm.com/reports/data-breach

27 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

28 “IT Leaders Call Generative AI a ‘Game Changer’ but Seek Progress on Ethics and Trust.” Salesforce News & Insights. March 6, 2023. https://www.salesforce.com/news/stories/generative-ai-research/

29 Gal, Uri. “ChatGPT is a data privacy nightmare. If you’ve ever posted online, you ought to be concerned.” The Conversation. February 7, 2023. https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283

30 Jackson, Terrance. “Exploring The Security Risks Of Generative AI.” *Forbes*. April 19, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/04/19/exploring-the-security-risks-of-generative-ai/?sh=10d46e993594

31 Metz, Cade. “The Godfather of A.I. Leaves Google and Warns of Danger Ahead.” *The New York Times*. May 1, 2023. https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html

32 Keary, Tim. “How prompt injection can hijack autonomous AI agents like Auto-GPT.” VentureBeat. https://venturebeat.com/security/how-prompt-injection-can-hijack-autonomous-ai-agents-like-auto-gpt/

33 Linthicum, David. “Generative AI and Cybersecurity: Advantages and Challenges.” eWeek. April 10, 2023. https://www.eweek.com/artificial-intelligence/generative-ai-and-cybersecurity/

34 Jackson, Terrance. “Exploring The Opportunities of Generative AI For Improving Security Operations.” *Forbes*. March 22, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/03/22/exploring-the-opportunities-of-generative-ai-for-improving-security-operations/?sh=769ec03f1d04

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | June 2023

WYZMYZAQUSEN-00