An Enterprise Data Governance Whitepaper from Infotel

Managing Governance, Risk, & Compliance in the Wild West of Converging Data Security & Consumer Privacy Policy

>>> With 7 Steps to Achieve Compliance

In today's rapidly evolving digital landscape, large enterprise CxOs in regulated industries find themselves at the frontier of new data territory. This landscape — where data security and privacy policies are converging at breakneck speed and artificial intelligence is rapidly reshaping the terrain — presents both unprecedented challenges and opportunities.

Like pioneers charting unexplored territory, we're tasked with managing GRC in a business world where the "map" is constantly being redrawn. This whitepaper aims to be your guide through this complex territory, offering insights and strategies to help you navigate the converging worlds of data security and privacy policy effectively and within the scope of ever-changing compliance mandates.

The stakes in this new frontier are staggeringly high. IBM's Cost of a Data Breach Report 2024 places the global average cost of a data breach at $4.88 million.[1] Even more alarming is the finding from the 2024 Verizon Data Breach Investigations Report that 68% of breaches involve the human element.[2] These statistics underscore the urgent need for a unified strategy that addresses both technical vulnerabilities and human factors in data protection.

CONTENTS

What's more, the 2024 IBM report sheds light on emerging threats caused by technological shifts, particularly the rise of shadow data.[1] This term refers to data residing in unmanaged sources — think of an employee maintaining a

personal spreadsheet with sensitive customer information outside the company's secure systems. Alarmingly, the report reveals that 35% of breaches in 2024 involved shadow data.[1] This significant figure underscores a growing challenge for organizations, as shadow data often eludes traditional security measures and complicates compliance efforts.

For those at the helm of data governance strategy in large enterprises and government institutions, the challenge is multifaceted. It involves not only implementing robust technical solutions but also crafting policies that align with constantly evolving regulations, managing the human aspect of data security, and ensuring that data governance measures support rather than hinder business objectives. The convergence of these responsibilities — once distributed among separate roles like CIOs, CTOs, DBAs, and CISOs — now falls on the shoulders of a new breed of business and technology leaders.

This whitepaper explores the rapidly evolving landscape of data security, privacy policy, and now AI governance, offering insights and strategies specifically tailored for enterprise data strategists and technology leaders. Our goal is to provide:

1. A clear understanding of the historical context and current challenges in data protection
2. Insights into the convergence of data security, privacy, and emerging AI governance requirements
3. Practical strategies for implementing a unified approach to data protection
4. Actionable recommendations to enhance your organization's data governance practices

By understanding these critical issues and implementing the strategies outlined in this paper, enterprise data strategists and technology leaders can position themselves as key drivers of their organizations' data protection strategies. This approach not only mitigates risks but also turns potential vulnerabilities into opportunities for innovation and competitive advantage.

As we delve into the complexities of modern data governance, we'll explore how the roles of technology leaders have evolved, the challenges of balancing security with accessibility, and the strategies for creating a cohesive data protection framework that spans from mainframe systems to cloud environments. We'll examine case studies that illustrate both the pitfalls of fragmented approaches and the benefits of integrated strategies, providing you with insights that can be applied to your own organizational context.

In the following sections, we'll trace the evolution of data protection regulations, examine the current landscape of InfoSec and privacy governance, and look ahead to emerging trends, particularly in AI and machine learning. Throughout, we'll focus on practical, actionable insights that can help you navigate this complex terrain and lead your organization toward a more secure, compliant, and data-driven future.

THE ROAD TO HERE: A Brief History of Data Protection

To understand where we are and where we're heading, let's take a quick look back. The story of data protection is filled with long stretches of calm punctuated by wake-up calls that changed the game overnight.

The 1995 EU Directive: Setting the Stage

It all started back in 1995 when the EU rolled out its Data Protection Directive. This was the first real attempt to get serious about protecting personal data on a large scale. For those of us in the tech world, it meant we had to start thinking about privacy as more than just an afterthought.

The directive introduced some key ideas that are still with us today:

- Don’t keep data longer than you need it
- Give people rights over their own data

At the time, these concepts were considered revolutionary. But for many organizations, especially outside the EU, they remained more theoretical than practical for years to come.

The Early Internet Boom (1995 - Early 2000s)

In the years immediately following the EU directive, we witnessed the beginning of an unprecedented explosion in data creation and collection. The internet revolution took hold, and e-commerce began to emerge as a viable business model. For many organizations, this meant venturing into uncharted digital territories.

During this period, the focus was primarily on establishing an online presence and figuring out how to leverage this new digital frontier. While the EU directive provided some guidance, many businesses, especially those outside the EU, were still grappling with how to apply these principles in practice.

The Social Media Revolution and Big Data Emergence (Early 2000s - Early 2010s)

As we moved into the new millennium, the pace of digital innovation accelerated dramatically. Social media platforms emerged as major players in the digital landscape, and the concept of ‘Big Data’ began to take shape. Suddenly, organizations found themselves collecting and managing more data than ever before.

For many of us in tech leadership roles, these were exciting times. We were discovering new ways to leverage data to drive business growth and innovation. However, let’s be candid, in the rush to capitalize on these new opportunities, privacy and security often took a back seat to speed and functionality. We were building complex digital ecosystems at a breakneck pace, sometimes leaving critical safety features as afterthoughts.

This era was characterized by rapid innovation, but also by a lack of comprehensive data protection frameworks. Many organizations operated in a regulatory gray area, pushing the boundaries of data collection and usage without fully grasping the potential risks and ethical implications.

As we’ll see, this period of unchecked digital expansion set the stage for the significant challenges and wake-up calls that were to come.

The Target® Breach of 2013: A Rude Awakening

Then came 2013, and with it, the Target data breach, which resulted in the exposure of as many as 110 million customer records.[3] This wasn’t just another security incident — it was a seismic event that shook the entire industry and exposed the vulnerabilities inherent in complex, interconnected systems.

The breach included personal information such as names, addresses, phone numbers, and email addresses for up to 70 million customers, as well as credit and debit card information for 40 million customers. Suddenly, data security was front-page news.

What made this breach particularly alarming was its origin. Despite Target’s substantial investment in security measures, the attackers found an unexpected entry point: a third-party vendor. This vendor, a refrigeration contractor with access to Target’s point-of-sale (POS) system for billing purposes, became the unwitting conduit for the breach. The hackers first compromised the vendor’s system and then used their legitimate access credentials to infiltrate Target’s network.

This incident highlighted a critical blind spot in many organizations’ security strategies: the security protocols of their partners and vendors. Target had robust internal security measures, but they weren’t adequately monitoring or enforcing security standards for entities with access to their systems.

Even more concerning, there were missed opportunities to prevent or mitigate the breach. Reports suggest that Target’s own security systems detected suspicious activity, but these warnings went unheeded. The breach continued for weeks before it was finally addressed. For those of us managing data and technology, it was a massive wake-up call. We realized that data breaches weren’t just an IT problem anymore — they could shake a company to

its core. Overnight, terms like "data security," "breach prevention," and "third-party risk management" went from tech jargon to boardroom priorities.

The Target breach served as a stark reminder that in our interconnected digital ecosystem, a company's security is only as strong as its weakest link — which may well lie outside its own walls. It underscored the need for a more comprehensive, ecosystem-wide approach to data security and privacy.

The Great Tightening (2013-2018)

In the years following the Target breach, we saw a major shift in how organizations approached data security. Companies started pouring money into cybersecurity. The role of Chief Information Security Officer (CISO) became crucial. For many of us, it meant relearning how to balance security with usability and efficiency.

We started encrypting more data, tightening access controls, and practicing what we'd do in case of a breach. It was a lot of work, but it also brought security and IT teams closer to the heart of business strategy.

GDPR: The New Sheriff in Town (2018)

Just when we thought we were getting a handle on things, along came the General Data Protection Regulation (GDPR) in 2018. This wasn't just an update to the old EU directive, it was a complete overhaul that brought some serious muscle to data protection:

- Huge fines for non-compliance (up to 4% of global revenue!)
- Stricter rules on consent for data collection
- New rights for individuals, like the "right to be forgotten"
- Requirements for breach notifications within 72 hours

For those of us leading data strategy and technology, GDPR was both a challenge and an opportunity. It forced us to take a hard look at our data practices, but it also gave us a chance to build trust with our customers and stand out from the competition.

Post-GDPR and Where We Stand Today

And that brings us to today. We're operating in a world where data is more valuable than ever, but also more regulated and, in some cases, more vulnerable. The old divisions between data security, consumer privacy, and business strategy don't work anymore.

As enterprise data strategists and technology leaders, we're now juggling a complex set of responsibilities:

- Keeping data secure from increasingly sophisticated threats
- Ensuring compliance with a patchwork of global regulations
- Leveraging data for business insights and innovation
- Managing the ethical implications of new technologies like AI

It's a tall order, but it's also an exciting time to be in this field. In the next sections, we'll dive into the current landscape and explore strategies for navigating these choppy waters.

THE MODERN DATA GOVERNANCE LANDSCAPE: Navigating a Complex Terrain

Now that we've taken a trip down memory lane, let's talk about where we are today. If you're an enterprise tech leader, you're probably feeling like you're trying to solve a Rubik's Cube blindfolded — and the cube keeps changing colors on you.

The Silo Situation: Signs You Might Be Stuck

Remember when we could just focus on keeping the lights on and the servers running? Those days are long gone, but you might

not have noticed how much the landscape has changed. Here are some signs that your organization could be operating in silos without realizing it:

- **The Security Team:** These folks are laser-focused on keeping the bad guys out. They're all about firewalls, intrusion detection, and incident response. But do they regularly interact with other departments beyond enforcing policies?

- **The Consumer Privacy Squad:** Often led by legal, they're knee-deep in compliance requirements, consent management, and data subject rights. How often do they collaborate with the IT security teams on proactive measures?

- **The Data Team:** These are your data scientists and analysts, always looking for new ways to squeeze insights out of your data. But are they fully aware of the latest privacy regulations or security protocols?

- **The Ops Crew:** They're making sure your systems are up, efficient, and ready for whatever the business throws at them. Do they have a seat at the table when discussing data governance strategies?

- **The Business Units:** This includes teams like Marketing, Sales, Finance, and HR. They're the primary consumers of data, using it to drive decisions, strategies, and day-to-day operations to generate revenue for the business. While they need extensive data access, they may not always be fully versed in the complexities of data security and compliance guidelines. How much do they interact with the security or privacy teams beyond mandatory training? During onboarding, what was the educational process for data security and privacy?

It's possible that each of these groups operates with its own tools, priorities, dialect of "data-speak," and respective data silos. If this sounds familiar, you might be inadvertently building different parts of a car without ensuring they'll fit together seamlessly.

Consider this: With various business units requiring more data access than ever, could the potential for security and compliance missteps be growing without you realizing it? It's worth taking a closer look at how your teams interact when it comes to data management, security, and privacy.

The Silo Effect: A Recipe for Compliance Disaster

Picture this: You're in a restaurant kitchen. The chef is creating a masterpiece, but the sous chef doesn't know what spices are being used, the line cook isn't aware of food allergies, and the server has no idea about the cooking time. Sounds like a recipe for disaster, right? Well, that's exactly what's happening in many organizations when it comes to data management and compliance.

The Hidden Costs of Data Silos: Increasing Risk in Your Organization

- **Inconsistent Data Handling:** When teams don't communicate, you end up with inconsistent data practices. Marketing might be using applications and collecting customer data that IT doesn't know about, or Finance might be using outdated security protocols for storing sensitive information.
- **Blind Spots in Data Flow:** Without a holistic view, it's easy to lose track of where data is going. Did that sensitive customer information end up in a test environment? Is personal data being shared with third-party vendors without proper safeguards?
- **Fragmented Response to Regulatory Changes:** When new regulations like GDPR or CCPA come into play, siloed organizations struggle to implement cohesive responses. You might end up with conflicting policies or, worse, gaps in compliance. This fragmentation also impacts breach response times. According to the 2024 IBM Cost of a Data Breach Report, organizations take an average of 194 days to identify a breach and 258 days to contain it.[1] While these figures represent an improvement from previous years, they underscore the critical need for unified, efficient response strategies in the face of evolving regulatory landscapes.
- **Increased Risk of Human Error:** When teams don't have a shared understanding of compliance requirements, the risk of mistakes skyrockets. It's like playing a game of telephone with your data practices — the message gets distorted with each handoff.

The Cost of Fragmentation

This fragmented approach isn't just inefficient, it's downright dangerous. Here's what we're up against:

- **Increased Risk:** When teams don't communicate, vulnerabilities slip through the cracks. It's like having a state-of-the-art alarm system, but leaving the back door unlocked.
- **Compliance Nightmares:** With regulations like GDPR, CCPA, and an alphabet soup of other state laws and regulations, a disjointed approach can lead to costly violations for both company and individual alike.
- **Missed Opportunities:** When data is locked in silos, we miss out on valuable insights that could drive innovation and growth.
- **Inefficiency:** Duplicate efforts, conflicting priorities, and lack of shared knowledge all add up to wasted time and resources.

The AI Wild Card

As if things weren't complicated enough, along comes artificial intelligence and machine learning. These technologies are reshaping how we use and protect data. They offer amazing possibilities, but also bring new challenges:

- **Data Hunger:** AI models need lots of data to be effective. But how do we balance this need with privacy requirements?
- **Black Box Problem:** Many AI systems are "black boxes" — it's hard to explain how they make decisions. This can be a big issue for both privacy and security.
- **Algorithmic Bias:** AI systems can perpetuate or even amplify biases present in their training data. This raises serious ethical and legal concerns.

The Great Data Shift: When Business Takes the Wheel

The landscape of data ownership and consumption has undergone a significant transformation over the past two decades. While it's true that IT has long been the custodian of data infrastructure, the accessibility and utilization of data across business units have evolved dramatically.

The early 2000s marked a turning point in how organizations handled data. The emergence and rapid adoption of Customer Relationship Management (CRM) systems like Salesforce, Microsoft's Great Plains (now Dynamics), and ACT! fundamentally changed the game. These systems, which gained traction between 2003 and 2005, began to democratize data access, putting customer information directly into the hands of sales and marketing teams.

This shift, while empowering business units with valuable insights, also marked the beginning of a new era of distributed data risk. As CRM and other business intelligence tools proliferated, data that was once centralized began to spread across various departments and systems. Each new access point and each new user became a potential vector for data breaches or misuse.

Today, we're seeing the full impact of this transformation. Business units are not just consuming data; they're often driving data strategy, collection, and analysis. Marketing teams run sophisticated data-driven campaigns, sales departments rely on real-time customer data, and operations teams leverage data for everything from supply chain management to workforce optimization.

This democratization of data has undoubtedly driven innovation and efficiency. However, it has also exponentially increased the complexity of data governance and security. The challenge now lies in balancing the benefits of widespread data access with the imperative of protecting sensitive information and maintaining regulatory compliance.

As we navigate this new reality, it's crucial to understand that data risk is no longer confined to the IT department. It's a shared responsibility that touches every corner of the organization. The question we now face is: How do we empower our business units with the data they need while also ensuring robust security and compliance across this vastly expanded data ecosystem?

The Elephant in the Room

While our business colleagues are data-savvy in their domains, they often aren't as attuned to the nitty-gritty of data privacy and security as our IT teams. It's not their fault — it's just not been their primary focus.

Think about it:

- Do they know the ins and outs of GDPR or consumer privacy compliance?
- Are they aware of the latest encryption standards and is encryption built into their systems per these compliance requirements? Do you know what systems they are using (corporate-assigned or personal devices) to access your organization's systems and IP?
- Can they reduce the time it takes to respond to anomalous behavior that might indicate a data breach, moving from months to weeks or even days? Some organizations are no doubt doing this.

A Ray of Hope: Emerging Unified Approaches

It's not all doom and gloom, though. Forward-thinking organizations are starting to break down these silos, and the results are promising:

- **Unified Data Governance:** Forward-thinking organizations are creating cross-functional teams that bridge the gap between business and IT. These teams bring together experts from sales, marketing, and operations alongside security, privacy, and data professionals.
- **Privacy-Enhancing Technologies (PETs):** New tools are emerging that allow for data analysis while preserving privacy, bridging the gap between data utility and protection.
- **Automated Compliance:** AI is being used not just for data analysis, but also for monitoring and ensuring compliance across complex systems.
- **Security and Privacy by Design:** Leading organizations are baking security and privacy considerations into their systems and processes from the ground up, rather than treating them as afterthoughts.

This shift isn't a problem to be solved — it's an opportunity to be seized. But it requires a new approach:

Cultivating a Security-First Culture: It's not just about bringing our business partners up to speed – it's about instilling a security mindset from day one. A robust onboarding program is key here. By baking data security and privacy best practices into every new hire's introduction to the company, we can significantly reduce the risk of breaches. This isn't a one-and-done deal; it's about creating an ongoing culture where security is everyone's responsibility, not just IT's.

1. **Forging a Compliance Alliance:** We need IT and business units working hand in hand, not in silos. Think of it as creating a "compliance alliance" across the organization. This means regular check ins, shared goals, and a common language around data governance. It's about improving communication and aligning on safe, low-risk data consumption across the entire organization. When Marketing wants to launch a new campaign or Finance intends to run a new analysis, they should see IT as partners in making it happen securely, not as roadblocks.
2. **Empowering with Smart Tools:** We need to provide user-friendly tools that inherently implement security and privacy features, ensuring that best practices are followed automatically in day-to-day operations.
3. **Adaptive Governance:** We need clear policies and procedures that work for both IT and business needs. But let's face it — in today's fast-paced environment, governance can't be static. We need frameworks that can evolve as quickly as the threats do, and as quickly as our business needs change.
4. **Continuous Education and Awareness:** While a strong onboarding sets the foundation, the learning can't stop there. Regular training sessions, simulated phishing exercises, and even "security champions" programs can help keep security and privacy top of mind across all departments.

By embracing these strategies, we're not just protecting our data — we're unleashing its full potential across the entire organization. We're creating an environment where innovation and security go hand in hand, where compliance is a shared goal rather than a hurdle to overcome. As enterprise tech leaders, we must recognize that the most critical step in addressing our data security and privacy challenges is fostering alignment at the executive level. The costliest

silo isn't between departments — it's the potential disconnect between business and IT leadership.

The path forward requires a top-down driven approach to Governance, Risk, and Compliance (GRC). Here's what this might look like:

- **Executive Alignment:** Business and IT leaders must work in lockstep to drive change and structure throughout the organization. This means regular, meaningful communication about data governance strategies, risk assessments, and compliance requirements.
- **Cascading Communication:** Once aligned, leadership needs to ensure that GRC priorities and strategies cascade effectively down to middle management and frontline workers. This isn't a one-time effort, but an ongoing process of reinforcement and refinement.
- **Holistic Onboarding:** GRC education should start from day one. HR teams should collaborate with business and IT leaders to integrate comprehensive GRC training into the onboarding process. This could include having executives speak directly to new hires about the importance of data responsibility.
- **Breaking Vertical Silos:** While horizontal silos between departments are often discussed, we must also address vertical silos that can exist between upper management, middle management, and frontline workers. Regular cross-level communication and feedback loops are essential.
- **Technology as an Enabler:** While many organizations have invested heavily in InfoSec software and procedures, technology alone isn't the solution. It's a tool that, when coupled with clear communication and a culture of responsibility, can significantly enhance our GRC efforts.
- **Human Factor Focus:** Recognizing that human error remains a primary risk factor, our strategies must prioritize ongoing education, clear communication of procedures, and fostering a culture where every employee feels responsible for data security and privacy.

In the following sections, we'll explore practical strategies for implementing this top-down approach. We'll look at how to build cross-functional teams that span hierarchical levels, implement technologies that facilitate communication and accountability, and create a pervasive culture of data responsibility — from the C-suite to the newest hire.

Remember, effective GRC isn't about restricting access or stifling innovation. It's about creating an environment where data-driven innovation can thrive securely and compliantly. By aligning our leadership, breaking down silos both horizontal and vertical, and engaging every level of our organization, we can turn our GRC efforts into a competitive advantage.

Breaking Down the Silos

Enhancing our approach to data governance and security is an ongoing process, one that can benefit every organization regardless of their current practices. A key strategy in this evolving landscape is the creation of a "compliance alliance." This collaborative approach can help organizations stay ahead of potential challenges and optimize their data management practices. Let's explore how we can build this alliance:

1. **Establish Cross-Functional Data Governance Teams:** Get IT, Legal, and key business units in the same room (virtual or physical) regularly. Make data governance everyone's business.
2. **Create a Common Data Language:** Develop a shared vocabulary around data practices that everyone in the organization understands. No more tech jargon or legal speak — let's make it accessible.
3. **Implement Holistic Data Mapping:** Understand how data flows through your entire organization. This isn't just an IT exercise — every department needs to be involved in tracking where their data comes from and where it goes.
4. **Develop Unified Compliance Training:** Don't just train IT on security or Legal on regulations. Create comprehensive training that gives everyone a basic understanding of data security, privacy, and compliance.
5. **Use Technology to Bridge Gaps:** Implement tools that provide visibility

across silos. Think centralized data catalogs, automated policy enforcement, and real-time compliance monitoring.

THE TRUE COST OF POOR DATA COMPLIANCE: Direct and Indirect Hits to Your Bottom Line, and the Things You Don't See

We've talked about the risks, the challenges, and the strategies. But let's get down to brass tacks: what does poor data security actually cost? Spoiler alert: it's probably more than you think, and it goes way beyond just writing a check.

The Immediate Hit: Direct Costs

Let's start with the numbers that keep CxOs up at night. According to the latest IBM Cost of a Data Breach Report:

- **Data Breach Costs:** The global average cost of a data breach has hit a record high of $4.88 million. But for US companies? Brace yourself — it's a staggering $9.48 million on average.[1]
- **Regulatory Fines:** With stricter data privacy regulations like GDPR and CCPA, fines can reach up to 4% of global annual revenue.
- **Time is Money:** On average, it takes organizations 258 days to identify and contain a breach — that's 258 days of potential data exposure and business disruption. In the case of the Target breach, someone in the Target organization notified a supervisor something was amiss and, of course, the work silos took over, and months later…
- **Industry Vulnerabilities:** Healthcare and financial services face the highest average breach costs, with ransomware attacks continuing to be a major cost driver.

While these costs are substantial, they can be mitigated through proactive measures. Implementing a multi-layered security strategy that goes beyond basic compliance, adopting advanced technologies like tokenization, and maintaining vigilant monitoring of network activities can significantly reduce the risk and impact of breaches. As the Target case demonstrated, compliance alone is not enough; organizations must stay ahead of evolving threats through continuous improvement of their security posture.[10]

The bad news: These are just the costs you can easily put a number on. The real financial impact often lies in the less tangible, long-term consequences.

The good news: Organizations with strong security programs, well-prepared incident response teams, and regular employee training face significantly lower breach costs. In the world of data security, an ounce of prevention is worth millions in cure.

The Lingering Pain: Indirect Costs

- **Reputational Damage:** This is the gift that keeps on giving — to your competitors. Studies have shown that a significant number of data breach victims lose trust in an organization following a breach. This loss of trust can translate to customer churn, potentially impacting your bottom line for years to come.
- **Loss of Intellectual Property:** If your secret sauce gets out, it's not just about the immediate loss. It's about the long-term impact on your competitive advantage. How do you put a price tag on that?
- **Operational Disruption:** In the aftermath of a breach, productivity often takes a nosedive. Systems might be offline, employees might be distracted, and normal business operations may be disrupted. This downtime and loss of productivity can significantly add to the overall cost of a breach. In a recent healthcare industry ransomware attack, employees were unable to do any work for several months when the breached organization refused to pay the hackers.

- **Increased Insurance Premiums:** After a breach, expect your cybersecurity insurance premiums to skyrocket — if you can get coverage at all.

- **Loss of Future Business Opportunities:** In regulated industries, a major breach might mean you're no longer considered a trustworthy partner. Those lucrative government contracts? They might suddenly be out of reach.

However, the 2024 IBM Report also highlights how certain practices can significantly mitigate these costs:

- Organizations with fully deployed security automation saved an average of $3.05 million per breach compared to those without automation.[1]
- Companies with an incident response team and regularly tested IR plans saved an average of $2.66 million per breach and identified breaches 54 days faster compared to those who neglect this essential practice.[1]

These statistics underscore the value of continued investment in and refinement of security practices.

The Hidden Costs: What You're Not Seeing

- **Employee Morale and Turnover:** A data breach can shake employee confidence. Low morale leads to reduced productivity, and in some cases, you might lose key talent who no longer trust the company's leadership.
- **Innovation Slowdown:** When you're in crisis mode, innovation often takes a back seat. The opportunity cost of not moving forward on key initiatives while you're putting out fires is hard to quantify, but it's real.
- **Increased Cost of Capital:** If your company's perceived risk increases, so might your cost of borrowing. Over time, this can add up to significant amounts.

The Bottom Line

In today's complex digital landscape, data security is a continuous challenge that impacts every aspect of an organization. Despite sophisticated security systems and well-architected protocols, the human element remains a critical factor in maintaining robust data protection.

The costs associated with data breaches are significant and can have long-lasting impacts on an organization. However, it's important to recognize that these challenges persist not due to a lack of technical expertise or investment, but often because of the inherent complexities of managing human interactions with data systems. By acknowledging the ongoing nature of these challenges and the critical role of human factors, organizations can focus on strategies that complement their existing technical safeguards.

In our next section, we'll explore emerging trends in InfoSec, Privacy, and AI governance. In these rapidly evolving fields, staying ahead of the curve is key to building upon the strong foundations already in place. Remember, effective data security isn't just about protecting data — it's about safeguarding your entire business ecosystem. It's an ongoing investment in both technology and people, one that supports innovation while managing risk in our interconnected world.

THE ROAD AHEAD: Emerging Governance Initiatives for InfoSec, Consumer Privacy and AI LLMs

As enterprise data strategists and technology leaders, staying ahead of the curve is crucial in navigating the complex landscape of data governance. Let's break down what these emerging changes mean for you and how you can proactively prepare your organization.

United We Stand: Building a Stronger Cybersecurity Ecosystem

The Biden Administration's Cybersecurity Strategy, released in March 2023, marked a pivotal shift towards a more collaborative approach. This strategy emphasizes the critical need for "close collaboration across the

private sector, civil society, state, local, tribal and territorial governments, and international partners."[4]

It's important to note this push for collaboration isn't just bureaucratic jargon — it's a recognition that our current siloed approach to cybersecurity is leaving us vulnerable. Much like the early days of the Combined DNA Index System (CODIS), where DNA databases weren't shared across state lines, we're facing a similar challenge in cybersecurity. Each entity — be it a corporation, a government agency, or a non-profit — has its own tools and strategies, but they're often operating in isolation.

The implications of this isolationist approach are significant:

- **Fragmented Cyber Defense:** When organizations don't share information, cybercriminals can exploit the same vulnerabilities across multiple targets.
- **Duplicated Cyber Efforts:** Without collaboration, different entities might be working on solving the same problems, wasting resources that could be better allocated.
- **Incomplete Cyber Threat Intelligence:** No single organization has a complete view of the threat landscape. Only by pooling information can we get a comprehensive picture.
- **Slower Cyber Response Times:** In the event of a large-scale cyberattack, a lack of established collaboration channels can significantly slow down response times.

The new strategy calls for breaking down silos that exist between industries, companies, and government entities, encouraging a more unified and robust cybersecurity ecosystem. This doesn't mean compromising individual security or sharing sensitive data indiscriminately. Instead, it's about creating secure channels for sharing threat intelligence, best practices, and coordinating responses to cyber threats.

For enterprise data strategists and technology leaders, this shift presents both a challenge and an opportunity. It requires rethinking security strategies to incorporate external collaboration, but it also opens up new avenues for strengthening defenses and staying ahead of emerging threats.

As we move forward, those who can effectively bridge these silos — both within their organizations and with external partners — will be best positioned to navigate the complex cybersecurity landscape of the future.

The Evolving Landscape of Consumer Privacy

As we navigate the complex terrain of data governance, one area demands particular attention: consumer privacy. The landscape is shifting rapidly, with new regulations emerging and existing ones evolving. Understanding this changing environment is crucial for any organization handling personal data.
While the EU's General Data Protection Regulation (GDPR)[5] set a high bar for privacy protection globally, we're now seeing a proliferation of privacy laws across different jurisdictions, each with its own nuances:

United States: In the absence of comprehensive federal legislation, states are taking the lead:

- California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Utah Consumer Privacy Act (UCPA)
- Connecticut Data Privacy Act (CTDPA)
- Others by state emerging

Brazil: Lei Geral de Proteção de Dados (LGPD)

China: Personal Information Protection Law (PIPL)

India: Personal Data Protection Bill (PDPB)
While these laws share common themes — such as data subject rights, consent requirements, and data breach notifications — they also have significant differences in scope, enforcement, and specific obligations.

Key Trends in Consumer Privacy Regulation

Expansion of Data Subject Rights: Beyond the "right to be forgotten," we're seeing an expansion of individual rights, including data portability and the right to opt out of data sales or sharing.

Heightened Consent Requirements: There's a trend towards more explicit, granular consent for data collection and processing.

Increased Focus on Children's Privacy: Many new laws are incorporating specific protections for minors' data.

Algorithmic Transparency: As AI and machine learning become more prevalent, there's growing emphasis on explaining automated decision-making processes.
Data Localization: Some jurisdictions require certain types of data to be stored within their borders.

Implications for Organizations

This evolving landscape presents several significant challenges for organizations. The proliferation of privacy regulations, often with conflicting requirements across different jurisdictions, has dramatically increased the complexity of ensuring compliance. This regulatory patchwork is forcing companies to navigate a complex maze of obligations, impacting operations across the board — from product design and marketing practices to IT infrastructure. Moreover, effective data governance has transitioned from a "nice-to-have" to an absolute necessity for managing privacy risks and meeting regulatory obligations.

Beyond mere compliance, organizations are realizing that robust privacy practices are becoming a key differentiator in the marketplace. In an era of increasing data breaches and privacy concerns, companies that can demonstrate strong privacy protections are better positioned to build and maintain consumer trust, potentially gaining a significant competitive advantage.

As we move forward, organizations need to adopt a proactive, flexible approach to privacy. This means not just complying with current regulations but anticipating future developments and building privacy considerations into the core of business operations and strategy.

Remember, privacy is not just about avoiding fines — it's about respecting your customers, building trust in marketplaces, and creating a sustainable foundation for data-driven innovation in an increasingly privacy-conscious world.

EVOLVING AI GOVERNANCE: Global Initiatives and Frameworks

As artificial intelligence continues to reshape industries and societies, a complex ecosystem of governance frameworks, regulatory initiatives, and implementation approaches has emerged. Understanding these various approaches is crucial for enterprise leaders navigating the AI landscape.

Established Regulatory Frameworks

The EU AI Act: Setting the Global Benchmark

The European Union, known for its pioneering approach to digital regulation, is once again at the forefront with its Artificial Intelligence Act (AI Act), enacted in July of 2024.[6] The EU's Artificial Intelligence Act aims to establish a global benchmark for AI governance, much like GDPR did for data protection.[7] The Act takes a risk-based approach, categorizing AI applications into four levels:

- **Unacceptable Risk:** The Act prohibits AI systems deemed to pose an unacceptable risk to society. This includes systems that manipulate human behavior to circumvent free will, social scoring systems used by governments, and real-time remote biometric identification systems in public spaces for law enforcement purposes (with some exceptions).
- **High Risk:** AI systems classified as high risk will face stringent requirements. These include systems used in critical

infrastructure, education, employment, essential private and public services, law enforcement, migration and border control, and administration of justice. High-risk systems must undergo conformity assessments, implement risk management systems, ensure high-quality datasets, enable human oversight, and maintain detailed documentation.

- **Limited Risk:** This category includes AI systems with specific transparency obligations. For instance, chatbots must disclose that they are AI, deepfakes must be labeled as artificially generated or manipulated, and emotion recognition systems must inform users that they are being subjected to such technology.
- **Minimal Risk:** The vast majority of AI systems fall into this category and can be developed and used without additional legal obligations.

The Act emphasizes transparency and proposes significant penalties for non-compliance, up to €30 million ($32 million, November 2024) or 6% of global annual revenue. While still in the proposal stage, it's expected to have far-reaching implications globally.

The NIST Framework: A Technical Foundation

The National Institute of Standards and Technology (NIST) released its AI Risk Management Framework (AI RMF 1.0) in January 2023.[8] This adaptable framework is structured around four key functions:

- **Govern:** This function emphasizes the importance of cultivating a culture of risk management. It encourages organizations to integrate AI risk management into broader enterprise risk management strategies. This includes defining clear roles and responsibilities, ensuring diverse perspectives in AI development and deployment, and fostering open communication about AI risks.

- **Map:** This stage involves contextualizing the AI system within its larger socio-technical environment. Organizations are urged to identify and document the potential impacts of their AI systems, both positive and negative. This includes considering how the AI system might affect various stakeholders, from direct users to broader society.

- **Measure:** The framework emphasizes the importance of quantifying AI-related risks. This involves developing metrics to assess the performance, safety, security, and fairness of AI systems. NIST recommends regular testing and evaluation throughout the AI system's lifecycle, not just during development.

- **Manage:** This function focuses on allocating resources and implementing strategies to address identified AI risks. It includes developing mitigation strategies, establishing ongoing monitoring processes, and creating mechanisms for continuous improvement.

A key strength of the NIST framework is its adaptability. Recognizing the rapid pace of AI advancement, the framework is designed to evolve over time. NIST plans to update the framework regularly based on technological developments, implementation feedback, and emerging best practices.

The NIST framework takes a holistic view, considering the technical, operational, and societal implications of AI. It serves as a common language for discussing AI risks across departments and with external stakeholders.

ISO 42001: Setting Global Standards for AI Management Systems

The International Organization for Standardization (ISO) has taken the initial step in the U.S. for AI governance with the release of ISO 42001. As the first international standard providing requirements for AI management systems, it represents a crucial development in establishing consistent global practices for AI governance. A key strength of ISO 42001 is its compatibility with other ISO management system standards, making it easier for organizations to integrate AI governance into their existing management frameworks.

The standard takes a systematic approach, focusing on:

- **Risk-Based Management:** Organizations must identify and assess AI-specific risks

throughout the system lifecycle, from development through deployment and maintenance.

- **Process Integration:** Rather than treating AI governance as a separate function, the standard emphasizes integrating AI management into existing organizational processes and management systems.

- **Continuous Improvement:** The framework establishes requirements for ongoing monitoring, measurement, analysis, and evaluation of AI systems' performance and impacts.

- **Stakeholder Engagement:** Organizations must identify and engage with relevant stakeholders, ensuring their needs and expectations are considered in AI system development and deployment.

The harmonization with established standards helps organizations build upon their current governance structures rather than creating entirely new ones.

The standard's release marks a significant milestone in AI governance, providing organizations worldwide with a concrete framework for implementing and maintaining responsible AI practices. While compliance is voluntary, ISO 42001 is likely to become an important benchmark for demonstrating commitment to responsible AI development and deployment.

Leading US Technology Companies: AI Governance in Practice

Major US technology companies are developing governance approaches that build upon these foundational frameworks while addressing specific challenges in AI development and deployment. Companies like IBM, Microsoft, and Google are focusing on key areas:

Transparency and Explainability: Developing methods to make AI decision-making processes understandable

- **Bias Detection and Mitigation:** Creating tools to identify and address potential biases
- **Data Governance Integration:** Ensuring data quality and privacy throughout the AI lifecycle
- **Ethical AI Design:** Incorporating ethical considerations from development through deployment
- **Continuous Monitoring:** Implementing ongoing assessment and refinement processes

European Innovation in AI Governance

Europe's contribution to AI governance extends beyond regulatory frameworks to include both public and private sector initiatives.

Public Sector Implementation

The French government's Albert AI represents a novel approach to implementing AI within public service constraints. While operating within existing regulatory frameworks like GDPR and national AI guidelines, Albert AI demonstrates how government entities can deploy AI solutions that prioritize transparency, accountability, and public service. This implementation helps inform future governance frameworks for public-sector AI applications.

Private Sector Innovation

Companies like Mistral AI, emerging from Europe's growing AI ecosystem, represent a new generation of AI developers working within evolving regulatory frameworks. While not creating governance frameworks themselves, these companies are actively shaping how AI governance principles are implemented in practice, particularly in addressing European-specific requirements and values.

Looking Ahead: Innovation and Responsibility

As AI becomes increasingly central to business operations, these frameworks and approaches will become essential tools for technology leaders. They provide structured approaches to navigating the complex landscape of AI risks and opportunities, helping organizations harness the power of AI while mitigating potential downsides.

The diverse landscape of governance approaches highlights several key trends:

1. The move toward risk-based classification of AI systems
2. Growing emphasis on transparency and explainability

3. Integration of ethical considerations throughout the AI lifecycle
4. Recognition that governance must evolve with technology
5. The importance of balancing innovation with responsible development

For enterprise leaders, understanding and implementing these various approaches is crucial for developing AI strategies that are both innovative and responsible. As frameworks continue to evolve, organizations must maintain robust testing and evaluation processes, recognizing that AI governance is an ongoing journey rather than a destination.

Convergent Themes in Global AI Governance

Despite the diversity of approaches — from regulatory frameworks to corporate implementations, from public sector initiatives to private innovation — several fundamental themes emerge across the global AI governance landscape:

Transparency is King: The era of "black box" AI is ending. Whether driven by EU regulations, NIST guidelines, or corporate governance frameworks, organizations must be able to explain how their AI systems work and why they make specific decisions. This transparency requirement spans both technical documentation and clear communication with stakeholders.

Bias Detection and Mitigation is Non-Negotiable: What began as an ethical consideration has evolved into a regulatory requirement. US tech giants are developing sophisticated detection tools, while European initiatives like Albert AI demonstrate how public sector implementations can prioritize fairness. The focus has shifted from merely acknowledging bias to actively preventing and mitigating it.

Continuous Evaluation is the New Normal: AI governance isn't a one-time compliance check. From NIST's emphasis on ongoing measurement to corporate continuous monitoring practices, the industry recognizes that AI systems require constant assessment and refinement. This includes regular testing, performance monitoring, and impact assessment throughout the AI lifecycle.

Privacy and AI are Inseparable: As AI systems process increasingly large volumes of personal data, privacy considerations have become central to governance frameworks. This convergence is evident in everything from the EU's dual focus on AI and data protection to the privacy-preserving features being built into new AI implementations.

Cross-Border Collaboration is Essential: The global nature of AI development and deployment demands coordination across geographical and organizational boundaries. This is exemplified by the influence of EU regulations on global standards and the adoption of frameworks like NIST's beyond US borders.

These common themes underscore a crucial point: while approaches to AI governance may vary, the fundamental goals of ensuring responsible, ethical, and effective AI implementation remain consistent across the globe. Organizations that align their AI strategies with these core principles will be better positioned to navigate the evolving regulatory landscape while maintaining innovation and competitive advantage.

Preparing for the Future: Your AI Governance Action Plan

As we stand on the brink of this new era in AI governance, you might be wondering how to prepare your organization for the changes ahead. Think of it as embarking on a journey. One that requires careful planning, teamwork, and adaptability. Your first step on this journey is to map out your AI landscape. Like explorers of old, you need to know your territory. Take stock of all the AI systems in your organization, including those still in development or provided by external vendors. This AI inventory will be your map, guiding your future decisions and helping you identify areas of potential risk or opportunity.

As you venture further, you'll need to shed light on the inner workings of your AI systems. Start developing practices that make your AI's decision-making processes more transparent and explainable. It's like training your AI to be a good communicator, able to articulate its reasoning in a way that builds trust and understanding. Along the way, you'll encounter the challenge of bias — a treacherous terrain that requires vigilant navigation. Invest in

tools and processes that can help you identify and mitigate bias in both your AI systems and the data used to train them. Think of this as establishing a system of checks and balances, ensuring your AI remains fair and impartial.

Remember, this journey isn't a solo expedition. You'll need a diverse team to navigate the complex landscape of AI governance. Create cross-functional teams that bring together not just IT experts, but also legal minds, ethicists, and business strategists. This collaborative approach ensures you're considering AI governance from all angles, much like a ship's crew where each member brings a unique and vital skill to the voyage.

As you press on, don't forget about the importance of solid ground beneath your feet. Robust data governance is the foundation upon which responsible AI is built. Shore up your data practices, ensuring they're strong enough to support your AI ambitions. The landscape of AI governance is constantly shifting, like dunes in a desert. Stay alert to these changes by assigning someone to keep watch on the horizon, tracking new developments, and helping you adjust your course accordingly.

Finally, keep a detailed log of your journey. Document your AI development and deployment processes as you go. When new regulations appear on the horizon, you'll be glad to have this record of your travels, helping you navigate any regulatory challenges with confidence. By approaching AI governance as a journey rather than a destination, you'll be well-prepared to adapt to whatever changes come your way. With careful planning, teamwork, and a spirit of continuous learning, you can turn the challenges of AI governance into opportunities for growth and innovation.

Most Importantly: Embrace the Change

These emerging governance initiatives aren't just hurdles to overcome — they're opportunities to build trust, enhance your brand, and create more robust, reliable AI systems. By proactively addressing these trends, you're positioning your organization as a leader in responsible AI use.

In the world of AI and data governance, early adoption of best practices isn't just about compliance — it's a competitive advantage. Embrace these changes to drive innovation, build trust, and create AI systems that are not only powerful but also responsible and ethical.

YOUR DATA GOVERNANCE ACTION PLAN: Sleeping Soundly in the Digital Age

We've navigated the complex terrain of data ownership, explored the financial repercussions of security breaches, and ventured into the frontier of AI governance. Now, it's time to translate this knowledge into action. Let's wrap up with a concrete, seven-point checklist for robust data governance — your roadmap to peace of mind in the digital age.

Your organization will need three things most critically:

1. People who understand the criticality of the convergence of data security, consumer privacy, and AI/LLM governance. A good first step to this understanding is for you to share this whitepaper
2. Technology solutions that give you and your team visibility and transparency, along with an audit trail
3. A GRC management process that's flexible enough to facilitate these initiatives today and the additions/changes that are to follow tomorrow.

Remember, the stakes are high. The 2024 IBM Cost of a Data Breach Report puts the global average cost of a breach at $4.88 million[1], while the 2024 Verizon Data Breach Investigations Report reveals that 68% of breaches involve the human element.[2] These sobering statistics underscore the critical importance of each step in this action plan.

Bridge the Silos

- Schedule regular cross-functional meetings with IT, Legal, Marketing, and other key departments

- Implement a common data language across your organization
- Create a "data governance council" with representatives from each department

Why it matters: The IBM report shows that organizations with cross-functional incident response teams saved an average of $2.66 million per breach.[1] Breaking down silos isn't just about efficiency — it's a crucial defense against costly incidents.

Cultivate a Security-First Culture

- Develop a comprehensive onboarding program that emphasizes data security and privacy
- Implement ongoing training programs to keep everyone up to date on best practices
- Recognize and reward employees who demonstrate strong data governance practices

Why it matters: With human error implicated in 68% of breaches,[2] creating a security-aware culture is your first line of defense. The IBM report found that organizations with strong security cultures detected and contained breaches 30% faster.[1]

Embrace the Compliance Alliance

- Forge partnerships between IT and business units to align on safe data consumption practices
- Develop shared KPIs that balance data utilization with security and privacy concerns
- Create a system for rapid communication of new compliance requirements across the organization

Why it matters: The IBM report indicates that regulatory compliance failures were the costliest root cause of data breaches, increasing breach costs by an average of $0.54 million.[1]

Implement Smart, Integrated Technologies

- Invest in tools that provide visibility across data silos
- Look for solutions that bake in security and privacy features
- Consider AI-powered tools for continuous monitoring and anomaly detection

Why it matters: According to IBM, organizations with fully deployed security AI and automation experienced breach costs that were $3.05 million lower than those without these tools.[1]

Prepare for AI Governance

- Conduct an inventory of all AI systems in use or development
- Develop protocols for explaining AI decision-making processes
- Implement bias detection and mitigation strategies for AI systems

Why it matters: While specific data on AI governance is still emerging, proactive preparation can help you avoid potential regulatory penalties and reputational damage as AI regulations evolve.

Stay Ahead of the Curve

- Assign a team to monitor emerging regulations and industry best practices
- Regularly reassess and update your data governance strategies
- Engage with industry peers and regulatory bodies to help shape future governance frameworks

Quantify and Communicate Value

- Develop metrics to track the ROI of your data governance initiatives
- Regularly report on prevented incidents, efficiency gains, and other benefits
- Use concrete examples and data to make a case for continued investment in data governance

Why it matters: Effective cross-organizational compliance and security collaboration is crucial, as the IBM report shows that breaches involving multiple factors — like system complexity, skills gaps, and regulatory issues — can each add hundreds of thousands of dollars to breach costs.

By implementing these seven steps, you're not just ticking boxes — you're building a resilient, forward-thinking organization capable of turning data governance challenges into competitive advantages. In a world where data is both a valuable asset and a potential liability, this comprehensive approach is your key to not just surviving but thriving in the digital age.

TURNING INSIGHT INTO ACTION:
Infotel's Unified Information Governance Suite

As we've explored the complexities of data governance, risk, and compliance, it's clear that organizations need robust, comprehensive solutions to address these challenges. This is where Infotel's Unified Information Governance (UIG) Suite comes into play.

The UIG Suite includes two powerful tools designed to address the key challenges we've discussed:

- **Arvitam:** A digital archiving solution that securely preserves your digital assets for the long term, ensuring full compliance with records management policies across various industries.

- **deepeo:** A user-friendly, configurable agentic system to visually manage your business data and maintain comprehensive data privacy compliance across multiple regulatory frameworks.

These tools, working in tandem as part of the UIG Suite, provide a comprehensive approach to the data governance challenges we've explored in this whitepaper. They offer practical solutions to bridge silos, enhance security, ensure compliance, and prepare for the future of AI governance.

Bridging Enterprise Data Systems

In today's enterprise environment, effective data governance must span all organizational data sources. Infotel's **InfoUnload** plays a crucial role in this ecosystem by providing high-performance data extraction capabilities across multiple platforms — whether from Db2 for z/OS, data lakes, or distributed systems databases. This high-speed utility maximizes performance through parallel processing capabilities and flexible output options, ensuring that critical enterprise data can be efficiently integrated into modern governance frameworks.

By enabling organizations to efficiently move and transform their mainframe data, InfoUnload helps ensure that governance strategies can be consistently applied across all enterprise data, regardless of its origin or location.

The Path Forward: From Compliance to Competitive Advantage

Robust data governance isn't just about avoiding fines or preventing breaches. It's about building trust with your customers, empowering your employees, and unlocking the full potential of your data. When we break down silos and get everyone in the organization on the same page about data practices, we create opportunities that go far beyond risk mitigation:

- **Innovation Flourishes:** With teams collaborating more effectively across departmental boundaries, new ideas and insights can emerge from unexpected places. Data-driven innovation becomes a company-wide endeavor rather than the domain of a single department.

- **Customer Trust Grows:** As your data practices become more consistent and transparent, customers feel more secure in their interactions with your company. This trust can translate into stronger customer relationships and increased loyalty.

- **Adaptability Increases:** A unified approach to data governance allows your organization to adapt more quickly to new regulations and market changes. You're no longer playing catch-up; you're prepared to pivot as needed.

In a world where data is the new oil, good governance is the refinery that turns that raw resource into real value. It's what allows you to innovate with confidence, to move fast without breaking things (or laws), and to turn potential risks into clear competitive advantages.

Yes, the landscape is complex and ever-changing. But armed with the insights from this whitepaper and the action plan we've outlined, you're not just prepared for the challenges ahead — you're poised to lead the way.

Remember, data governance isn't just an IT issue or a legal issue. It's a business issue. It's a leadership issue. And for those who get it right, it's an opportunity to not just survive, but thrive in the digital age.

Your Next Steps

Armed with the insights from this whitepaper and the action plan above, you're well-positioned to tackle the data governance challenges ahead. But you don't have to do it alone. Here's what you can do next:

1. Assess your current data governance practices using the action plan we've provided.
2. Explore how Infotel's UIG Suite, including Arvitam and deepeo, can address your specific data governance needs.
3. Reach out to the Infotel team for a personalized consultation. Their experts can help you navigate the complexities of data governance and tailor solutions to your organization's unique requirements.

Remember, in the digital age, effective data governance isn't just about avoiding risks — it's about seizing opportunities. With the right tools and expertise, you can turn data governance from a challenge into a competitive advantage. Ready to take the next step in your data governance journey? Contact Infotel today and discover how the UIG Suite can help you sleep soundly in the digital age while driving your business forward.

You can reach us at **software@infotel.com** or **infotel-software.com**

Here's to a future of secure, compliant, and value-driving data governance. The path ahead is clear, and with Infotel, you're well-equipped to lead the way.

About Infotel

With U.S. headquarters in Tampa, Florida, Infotel serves large enterprises in the digital transformation of business. The Infotel group has been a primary solution and services provider for enterprise IT departments and key accounts for over 40 years and develops its expertise across two complementary divisions: IT services and software publishing.

Industries served by Infotel include banking, insurance, automotive, retail, aerospace, and other regulated sectors. Infotel has large enterprise deployments throughout Europe, the Americas, and in the Far East. With a global workforce numbering nearly 3,200 people, the Group, listed on Euronext Paris (ISIN: FR0000071797), generated revenue in 2023 exceeding $335 million and has been growing steadily year over year.

---

[1] IBM Security. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

[2] Verizon. (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir

[3] Target, Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores (Dec. 19, 2013) https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

[4] https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[5] https://gdpr.eu/

[6] https://artificialintelligenceact.eu/implementation-timeline/

[7] https://artificialintelligenceact.eu

[8] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://www.nist.gov/itl/ai-risk-management-framework

[9] IBM. (2023). AI Ethics. https://www.ibm.com/artificial-intelligence/ethics

[10] Case Study, Target Breach. https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/