Trust by Dominique Shelton Leipzig

THE SUMMARY IN BRIEF

Digital transformation is already here, and the time for CEOs and their Boards of Directors to adapt to this new reality was yesterday. From harnessing the power of data to preventing ethical lapses that damage consumer trust, success in today's business landscape requires leaders to transform their companies into responsible data stewards that benefit all stakeholders.

The book provides a comprehensive framework for leaders to align their data practices with their organization's mission, foster an ethical data culture built on trust, mitigate reputational, legal, and financial risks, and ultimately improve the bottom line through the responsible use of AI.

By sharing insights gained from advising Fortune 100 companies on digital innovation, data privacy, strategy, and artificial intelligence, author Dominique Shelton Leipzig helps leaders deeply understand their customers, monetize data opportunities, and streamline processes with responsible AI—all while increasing customer trust and maintaining legal compliance in a rapidly evolving regulatory environment landscape.

IN THIS SUMMARY, YOU WILL LEARN:

- How to find your unique personality, profile, authority, and center.
- How to align your personality with your business and your life.
- How to implement your findings in business.
- How to cultivate an aligned and fulfilling business ecosystem.

Introduction

I wrote this book for you, the business leader: whether you're a CEO, in the C-Suite, or on the board. Your company manages data, and you understand instinctively that trust in technology is vital for the future. This book aims to give you immediate expertise, offer the playbook to accelerate your company's progress, and equip you with key concepts and vocabulary so you can clearly communicate your data vision.

The pages challenge the idea that data breaches, misinformation, privacy violations, risks to our children, and bias are the only issues with technology. I look forward to sharing the essential steps leaders can take today to shift from merely using technology to leading with trust.

I hope you enjoy learning how to take control and ensure your company becomes a data leader, not a data loser. Continue reading to discover how current industry and regulatory changes present an opportunity not just to keep up but to add value to your business.

Chapter 1: Data Is Core to Your Mission

To understand what data means for your company, see digital transformation not as a vague future event, but as something that is already happening. Trust in your brand's handling of data develops through leadership and intentional effort. The first step is to learn how to understand, manage, and build with data.

Start by understanding your customers—what they want and how to reach them. The data within a company already tells a story about who the customers are. Many parts of an organization gather information about customers or products that could be used to benefit the company. These include data from digital marketing, using "social listening" vendors to monitor online discussions of your brand and competitors for advertising, internal data, and social media data more.

Implement a system to monitor customer reactions to your products and services. Have your team locate where customer comments are stored and train them to compile these data points in a centralized database so that insights can be easily gathered.

Once you have clear, real-time knowledge of who your customers are, you can develop a more efficient marketing strategy. Use this data to protect your brand and stay aligned with your mission by understanding your customers' values and perspectives.

A comprehensive data strategy is also crucial for more informed product development. Make your mergers and acquisitions strategy focused on data and needs. If you're unsure whether your current M&A process is as needs-based (and data-driven) as it could be, this is your chance to leverage data as a valuable, intangible asset. Similar to intellectual property, the value of data can be overlooked and not reflected on the balance sheet. But if data is recognized as a tangible asset, discussed quarterly as such, it shifts from being hidden to becoming a "pre-tangible" asset of the company. To do this effectively, you need to know the following:

- What data do you have or need to actualize your business strategy for a successful start?

Chapter 2: A Post-Data World in Detail

Why do I use the term "post data" to describe today's society? The digital transformation that your marketing teams keep warning you about is, in fact, already here. It is staggering to think that we are globally generating over 2.5 quintillion bytes of data each day. To put this number into perspective, one quintillion bytes has 18 zeros behind it. Additionally, developments like deep learning and generative AI make the future value of data even more significant certain.

Deep learning is a subset of machine learning, which involves neural networks with three or more layers. These networks aim to mimic the behavior of the human brain – though far from its full ability – enabling it to "learn" from large datasets. Generative artificial intelligence refers to algorithms (like ChatGPT) that can produce new content, including audio, code, images, text, simulations, and videos.

Once activated, deep learning can provide valuable insights about your business at the touch of a button dashboard.

You will likely find that your company already uses several technologies that aid in data collection, such as cloud computing, IoT (the Internet of Things), sensor data, facial recognition, biometrics, other information gathered for physical security, and data purchased from data brokers.

These are just a few ways your company is already a data-driven organization. The sooner you develop a strategy to analyze, synthesize, and understand these vast amounts of data, along with the governance practices needed to become a data leader, the better prepared you'll be to grow in the future.

Chapter 3: Geopolitical Issues Surrounding Data

Cyber-attacks are projected to cost the global economy $10 trillion by 2025. Given the geopolitical volatility worldwide, it’s logical to incorporate national security awareness into a risk management framework.

When engaging globally, it’s crucial to understand the national security risk environment along with the legal requirements your company must comply with, and then act accordingly. Consulting with the appropriate legal and national security experts is essential to protect the brand. This is the only way the CEO and the board can identify the key questions they need to ask their management team to evaluate and safeguard against these risks.

Chapter 4: C-Suite and Board Data Privacy and Security Liability

With the rising trend of officers and directors in the United States being named in lawsuits following data privacy and security incidents, it’s crucial to examine the common causes behind these lawsuits in the United States, the situation in the United Kingdom and Europe, and the steps companies can take to reduce this risk.

Outside counsel should be involved in training your C-suite and board on these regulatory risks. Some key privacy programs and cyber preparedness efforts companies can implement include:

- Prebreach or preprivacy incident, security, or privacy risk assessment.
- Privacy or security compliance audits.
- Privacy and security impacts.
- Board meetings regarding privacy or security.
- Prior privacy or security incidents.
- Training programs on privacy and cybersecurity, including training involving the board and CEO.

- Some post-privacy or security incident communications companies can include:
- All internal communications investigating a privacy or security incident.
- Mitigation, remediation, post-incidental reports, and management meetings regarding cybersecurity.
- Forensic investigations.

To permit candidate discussion of data best practices and incidents, care needs to be taken to preserve privilege so that board discussions are not weaponized against the board and the organization.

Here's an overview of lawsuits against officers and directors in the United States:

- Failure to stay informed.
- Lack of board committee with data privacy and security oversight.
- Lack of qualified officers.
- Failure to safeguard personal data.
- Failure to respond to known cyber threats.
- Failing to conduct adequate due diligence.
- False sec and other public statements.
- Lack of transparency.
- Insufficient oversight of vendors and third parties.
- Failure to provide timely and adequate notices.
- Noncompliance with laws.

Currently, the main regulatory risks for CEOs and Boards in Europe involve security breaches, direct marketing, profiling, ad tech violations, unlawful data sharing, transparency failures, and non-compliance with rights requests.

Chapter 5: Why Data Leadership Is Important Now

Nasdaq-listed companies lost over $1.4 trillion in market cap in 2022, affecting the Dow and other global markets. The headlines focus on the market losses. However, what's missing from the coverage is the stated cause of the loss in ad revenue, which initially triggered the sell-off and is based on data privacy.

Data privacy and responsible data stewardship have shifted from being just legal compliance issues to becoming a business necessity. The idea is simple. A lack of responsible data privacy leadership causes distrust among consumers and employees, which ultimately leads to a decline in market value. Your customers and partners won't keep working with your company if they can't trust your data practices. This is especially true if a competitor adopts trustworthy data practices and offers customers an alternative. If your customer base drops significantly, it becomes increasingly difficult to attract investors to invest in your company.

Although challenging, focused leadership can maintain a company's dedication to data privacy and stewardship. In this context, directors and officers need to understand the following three things:

- As with other global enterprise environmental, social, and corporate government (ESG) issues that present both risks and opportunities, data privacy and security require board-level focus.
- Global lawmakers and regulators should follow best practices to support business and consumer interests and establish consistency in law's requirements.
- Data privacy and security demand collaboration and leadership among government agencies, consumer organizations, and industry professionals to create global strategies for navigating our fourth revolution – digitalization.

Chapter 6: Board-Level Cyber, Privacy, and Data Risk Governance

As today's headlines make clear, privacy and cybersecurity have moved beyond mere IT and legal compliance issues. They are now critical ESG benchmarks that significantly influence market capitalization and shareholder value.

At a high level, data privacy relates to the personal information that companies collect, use, and share, as well as how they communicate their practices. Cybersecurity, on the other hand, involves what companies do to protect personal and critical business data and maintain resilience. Currently, over 160 countries have data protection laws. Beyond the legal framework, privacy and cybersecurity greatly impact the bottom line.

In 2021, the FTC published "Corporate Boards: Don't Underestimate Your Role in Data Security Oversight." The document urged boards to "build a team of stakeholders" who can "bring a different perspective to the issues." Along with cybersecurity, privacy has become a focus for regulators. In today's environment of increasing legal requirements, US shareholder derivative litigation risks, heightened global criminal and geopolitical cyber threats, and international regulatory guidance, boards should consider the following five steps to address privacy and cyber issues:

- Ensure there is sufficient privacy and cyber expertise in the boardroom, either through board appointments or the engagement of third-party advisors.
- Implement a risk strategy at the board level to manage data risk and enhance resilience.
- Relate cyber risk to financial exposure.

- Ensure that board members are well-informed enough to participate actively in data-driven strategy discussions.
- Look at the bigger picture. Technological innovation is bringing about a Fourth Industrial Revolution. By leveraging data effectively, companies can become disruptors rather than being disrupted.

Chapter 7: Four Ways That Strategy Can Enhance Your Revenue by Billions

You already know that Gen. Z is the first generation born into a digital-first world. This is the largest generation in the United States and is already responsible for $360 billion in consumer spending. From a company's perspective, these trends provide 360 billion reasons to adopt a targeted data strategy. The top ways that a data strategy can boost your revenue by billions are by offering the following:

- Increased awareness of demand. As discussed, implementing a data strategy will help you better understand your customers and identify their needs. This can be as straightforward as understanding a niche.
- Targeted communications with customers. A targeted message that responds to consumer demand is one of the easiest ways to make an impact. AI will enable companies to gather more feedback from customers at scale. Savvy companies will create a continuous feedback loop to improve everything from product development to recruiting the best talent to meet customer demand.
- Focused product development. Using information from both inside and outside the company, products can be created to support the company's optimal growth. Valuable sources of product improvement information include business intelligence research, social listening, consumer complaints and comments shared with the help desk, website contact portals, and customer care teams.
- Strategic hiring advantage. Every company is only as strong as its last hire. Building a workforce that is innovative, metrics-driven, and focused depends heavily on your digital strategy to attract top talent and ensure that your digital brand presence reflects the innovation within your organization.

Chapter 8: Ask These Questions to Develop a Digital Strategy and Value Your Data

By now, you've realized that your data has value, even though standard accounting practices usually do not allow such holdings to be recorded on the books. How can we address this dilemma? While the Financial Accounting Standards Board is currently exploring methods to include such nonstandard asset valuations, there are still steps you, as a company leader, can take to assess your data's worth and develop a strategy that maximizes its value. Asking these four key questions will put you on the right track:

- What data do you need, and what is the value of your data?
- What is the data?
- Who in the company is responsible for the data?
- What teams should collaborate to best leverage the data?

Arriving at a valuation of your data requires attention to and understanding of what data you have overall. Comparing the data you possess with the goals and mission of your company will quickly reveal which data is worth keeping and which should be divested. Once you determine which data is critical to the growth of your business, you should assign a value to it. Partnering with a valuation expert and the appropriate business units within your company can help you establish a line item to value your data, transforming it from a pre-tangible asset to a concrete one that can be reviewed at every board meeting. Here are the four important questions to consider when developing a digital strategy:

- Where is your data? Once you've aligned your mission with the data needed to fulfill it, you will want to determine whether you already have the data or if you need to acquire it through other means, such as mergers and acquisitions (M&A) or purchasing it from a third party. You will also want to make sure that your data teams understand where the data is resides.
- Who is responsible? As a CEO or board member, you need to know who in the company has responsibility for the company's critical data.
- Who should collaborate? Many companies have multiple individuals responsible for data within the organization. Their titles might include chief data officer, chief data strategy officer, chief innovation officer, chief privacy officer, chief information security officer, and increasingly, chief trust officer.

Chapter 9: Artificial Intelligence: The Future is Now

Artificial intelligence represents the future, and that future is happening now. In fact, if you're only now starting to address AI and its impact, you're already falling behind. The key to successful adoption and trust in AI is confidence. Business leaders need to understand how regulators, community groups, and lawmakers are thinking about trust in AI. Here's a list of priorities to address AI risks and earn, then maintain, the trust of stakeholders.

- Human oversight is crucial for the success of AI.
- Accuracy and cybersecurity are crucial for protecting the integrity of data collected for AI and its algorithmic output. Attention should be given to maintaining the integrity of the data used for training models.
- Processes should be in place for testing and monitoring algorithms before they are deployed for general use.

- Large technology companies that create generative or other AI offerings as a service must conduct a thorough antitrust analysis.
- Ensure that testing and verification are updated, and accuracy is verified even after routine changes have been made to systems, such as operating systems or software updates.
- Ensure that a diverse team works on the development of algorithms, training of data, and decisions about which data to use for model training.

The regulatory environment around data protection, privacy, and AI can be a confusing mix of laws and policies. These rules differ from country to country and even from state to state. However, no company can ignore issues of data protection and privacy when developing AI. Having policies alone is not enough. Data must be treated as a valuable asset—one whose security and integrity must be maintained paramount.

Chapter 10: Take Charge and Lead: Seven Keys to Implementing Data Strategy in Your Company

CEOs and board members should see data as a vital part of strategy. However, this doesn't mean you need to reinvent the wheel. You can still apply the principles you already have in your toolkit for every other asset of your company.

- Leverage your data assets to implement the company's long-term and short-term strategic plans.
- Build with your data. Ask how your business can grow through the strategic use of data.
- Sustain your growth with your data. Utilize AI tools, such as machine learning, to gain a deeper understanding of your business and identify what is working well and what can be improved for the future.
- "Inventory" your data. As with any other asset, you need to know what you have. This will place you in the best position for the future, as well as eliminate inefficiencies and prevent different parts of the company from duplicating data.
- Protect your data assets. You should not delegate your data asset protection solely to the CISO. Just as the C-suite gets reports about other critical assets of the company, so should those at the top be aware of your data strategy.
- Ensure your data assets. Review your insurance portfolio to ensure it covers your data, including how you collect, use, and store it.
- Avoid illegal data activity. You would never think of putting your company's most valuable product at risk by failing to pay attention to legal requirements.

Chapter 11: Leading with a Legally Compliant Data Transformation Program

Companies across the globe would do well to develop a top-line compliance strategy to ensure substantial compliance in the jurisdictions that matter most to them. Here are the six phases that will be critical to your compliance program:

Phase 1: Data Privacy/AI and Cyber Leadership

It's vital to have a task force comprising a chief data officer, a privacy and data security officer, AI engineers, and relevant stakeholders to create rules for data collection that are synergistic with legal and technical requirements in the company.

Phase 2: Conduct a Legally Compliant Inventory

This can help enhance digitization models and compliance with myriad privacy and data security laws and best practices.

Phase 3: Legal Gap Assessment

Gap assessments are critical to creating a compliant organization. They should be tied to legal assessments to compare actual practices with legal requirements and ethical best practices.

Phase 4: Impact Assessment for High-Risk Processing

Businesses should consult with experienced legal counsel to develop a template impact assessment form for high-risk processing, such as financial, location, and health data.

Phase 5: Mitigation of Risks Assessed in Phases 3-4 with Targeted Policies

The company should retain an experienced privacy council regarding tools to help mitigate risks. These will include establishing ethical data practices that meet legal requirements for AI, privacy, and cybersecurity, as well as internal governance policies, external notices for privacy and AI, litigation defense playbooks, and more.

Phase 6: Auditable Record

An auditable record can be assessed annually or periodically throughout the year, particularly when new processes or procedures are introduced. This record can be refreshed easily by using the templates established in phases one through five.

Because all companies are data companies, you are the leader of a data company. You do not need to be a technical wizard to lead change. You need to be aware of the issues, ask the right questions, and ensure you have the best leaders for this brave, new data-laden world.

The summary is not intended as a replacement for the original book, and all quotes are credited to the above-mentioned author and publisher.