

**George Westerman
Richard Hunter**

IT Risk

**Turning Business Threats
into Competitive Advantage**

Harvard Business School Press
Boston, Massachusetts

Introduction

IT Risk and Consequences

A HALF CENTURY of adopting information technology at an astonishingly rapid rate has created a world in which IT is not just widely present but pervasively, complexly interconnected inside and outside the enterprise. As enterprises' dependence and interdependence on IT have increased, the consequences of IT risk have increased as well. What is IT risk? It's the potential for an unplanned event involving a failure or misuse of IT to threaten an enterprise objective—and it is no longer confined to a company's IT department or data center. An IT risk incident has the potential to produce substantial business consequences that touch a wide range of stakeholders. In short, IT risk matters—now more than ever.

This change in the meaning and importance of IT risk has caught some executives unaware. Every executive at some time has experienced problems with his IT organization and systems, including delays and unexpected costs in development projects, temporary or extended

loss of service, data loss or theft, processes made unnecessarily complex by systems interfaces and limitations, inaccurate information from redundant or “buggy” systems, and a myriad of other ills. Executives have generally learned to perceive—and even tolerate—such episodes as regrettably common but relatively limited in their impact on key business metrics. Case studies of companies like Tektronix and Comair, however, demonstrate how such perceptions no longer apply.

Comair, a \$780 million subsidiary of Delta Air Lines, experienced a runaway IT risk incident on December 24, 2004, when the company’s crew-scheduling system failed.¹ An airline’s crew-scheduling system is mission critical. Federal Aviation Administration safety regulations limit the number of hours any aircrew member can work in a twenty-four-hour period. The scheduling system is what ensures compliance with that strictly enforced regulation. Without its scheduling system, an airline does not fly.

Because of the holidays, December is always the busiest month for U.S. airlines. December 2004 was busier than normal because unusually bad weather forced airlines to cancel or reschedule many flights, including 91 percent of all flights between December 22 and December 24. No one at Comair knew that the crew-scheduling system (which had been purchased from an external vendor) was capable of handling a maximum of only thirty-two thousand changes a month.² At about 10 p.m. on Christmas Eve, when Comair entered one more flight change, exceeding the monthly capacity, the system abruptly stopped functioning.

Comair technicians realized soon after, to their dismay, that the system could not simply be restarted. The only solution was to reload the entire system from scratch as quickly as possible. The tech team accomplished that task and relaunched the system late on December 25, but by then Comair had problems assembling its widely dispersed crews and aircraft where they were needed. The airline didn’t resume normal operations until December 29.

As the company struggled to recover from the disaster, nearly two hundred thousand stranded Comair passengers helplessly roamed

airport terminals throughout the United States. Airlines were fully booked for the holiday travel season, and there were few alternative flights. Throughout the Christmas holiday, camera crews from local and national television news outlets followed passengers through those terminals, broadcasting travelers' and Comair's distress to the American public.

Two weeks after the system failure, the U.S. Secretary of Transportation announced an investigation into the incident. A week later, the company's president, Randy Rademacher, resigned. In addition to the damage to the company's reputation, its management, and its customers, Comair's revenue losses as a direct result of this incident are estimated at about \$20 million.³ In other words, the loss from this single incident was nearly as high as the firm's entire \$25.7 million operating profit for the previous quarter.

The company had planned, and delayed, replacement of the scheduling system several times before it failed.⁴ Despite the outcome, these decisions could be defended as rational business decisions. The system had been running for years, and the likelihood of a complete system failure—especially one that resulted from an entirely unsuspected source—was apparently low. That the system failed at a point in time when its failure was maximally damaging to the company and its customers was extremely bad luck but hardly predictable.

But something more was involved than an unfortunate decision to defer an upgrade. Comair lacked a viable plan for the immediate recovery of this mission-critical business process. Its executives failed to plan for such a high-impact failure, however unlikely it seemed. When the software went down, there was no backup system that could be pressed into immediate service, no outsourcer on call and ready to step in, no plan that could keep the company running manually while the system was fixed.

In other words, it wasn't just the computer system that failed—it was Comair's process for understanding and managing the business consequences of IT risk. And making sure that an organization's

major corporate risks—IT or otherwise—are managed to an acceptable level is the responsibility of the organization's senior executives. Perhaps that's why it was the company's president, not the CIO, who departed in the wake of the incident.

The Comair case is about the risk of *availability*. The Tektronix case is about *agility*—the ability to change rapidly with controlled cost and risk. In the mid-1990s, executives at the \$1.8 billion electronics manufacturer learned that their plans to divest a major business unit had hit an unexpected snag.⁵ Key financial and manufacturing processes for three Tektronix business units were riddled with undocumented interdependencies between critical systems. Extracting one business's systems from that tangled mass was like removing a load-bearing wall from a building—it couldn't be done without major restructuring. The separated unit would require duplicating nearly every one of Tektronix's major systems (including the sensitive corporate data they contained), as well as finding technicians to maintain the systems. The difficulty of spinning out a division, with or without its IT systems, brought a focus to those IT agility risks that had been present for years.

Tektronix arrived at this strategic dilemma gradually. For decades the company's IT department had extended existing systems, built new stand-alone systems, and written software to link systems as needed. Every new "solution" was an unconscious trade-off of long-term agility in favor of short-term benefits. The problems inherent in this approach weren't immediately apparent to executives, but they compounded over time, just as it takes time for unplanned, uncontrolled growth in a city to visibly overload roads, schools, sewers, and support services.

By the early 1990s, Tektronix executives knew their IT systems had problems. Changes took much longer to implement than they should have and than executives would have liked. It was frustratingly difficult to get an integrated view of the company's customers, products, and orders. Business managers complained that IT support

was getting worse and worse, and IT managers knew that the systems were becoming more and more difficult to maintain. Extensive coordination by smart support staff covering for system inadequacies was so frequent that it produced a motto: “Five calls does it all.”

But these ongoing signs of agility risks seemed relatively low impact. They were annoying, of course, but they were a more or less normal part of the way business was done at Tektronix and at many other companies. It was only when Tektronix executives tried to break from the past that they saw the real threat those familiar annoyances posed.

The Tektronix and Comair cases are extreme in their consequences, but they are not unique. Other events in multiple industry sectors show that executives must learn to think of IT risk in terms of serious business consequences:

- In mid-2005, CardSystems Solutions, Inc. reported that unknown persons had gained unauthorized access to computerized credit transactions for 40 million credit card holders. A few weeks after the breach, CardSystems’ two largest customers, Visa and MasterCard, terminated their business with the company, which was soon after sold.⁶
- In 1996, a failed implementation of SAP’s enterprise resource planning software at FoxMeyer, a \$4 billion pharmaceutical distributor, allegedly led to the company’s bankruptcy. The company’s trustees filed suit against SAP (the software vendor) and Accenture (the systems integrator for the project), asking for \$500 million in damages from each. The case was settled out of court in 2005.⁷
- In December 2003, the United Kingdom’s Inland Revenue put a new system for managing tax credits into production. Preproduction testing had been limited to four weeks rather than the planned twenty weeks because the project was

behind schedule. It is estimated that over £2 billion in erroneous tax credits were paid out by the system before errors were recognized and corrective measures taken.⁸

We could easily continue—there is no shortage of recent incidents of this sort, and more are reported every week. IT has become more and more central to business over the past twenty years, but many enterprises have not adjusted their processes for making key decisions about IT and IT risks. The result is risk incidents that have three factors in common:

1. They involve significant harm to constituencies inside and outside the enterprise that results from failure of IT systems or controls on IT processes.
2. Increasingly, they involve public disclosure, resulting in reputation damage and regulatory scrutiny.⁹ Such public disclosure amplifies the consequences of IT risk, with subsequent consequences sometimes far exceeding the initial economic losses.
3. They expose failure to account for potential business consequences in managing IT risks—in other words, they expose a failure of general management, not just IT management.

Executives who invested—wisely—in IT as a strategic weapon simultaneously increased the IT risk to their enterprises. By depending more on IT for key processes, competitive efficiencies, and links to customers and suppliers, they increased their firms' dependence on smoothly functioning IT systems, as well as their vulnerability to external threats.

Many managers do not yet understand the full implications of this shift. To put it bluntly, management of IT risk has not kept pace with the reality of IT risk. IT risk in many enterprises is still handled as a technical issue and is largely ignored by business executives. Even when business executives understand the strategic importance

of IT to their enterprises, they often have not been able or willing to make the hard trade-offs necessary to manage IT systems effectively.

The Causes of IT Risk

To understand what causes IT risk in organizations and how to manage it effectively, we undertook a set of research studies that combine academic rigor with the practical insights we have each gathered in over twenty years of working in and with IT organizations. More than 50 firms participated in case studies, and more than 130 firms participated in a survey associated with this endeavor. Executive presentations with more than two thousand IT and non-IT executives have helped us refine our research findings and relate them to real-world situations.

Our research shows that most IT risks arise not from technical or low-level people issues but from the failure of the enterprise's oversight and governance processes for IT. Such failures produce a series of poor decisions and badly structured IT assets that are manifested as ineffective IT governance, uncontrolled complexity, and inattention to risk.¹⁰ In other words, most IT risk results not from technology itself but from decision-making processes that consciously or unconsciously ignore the full range of potential business consequences of IT risk. Over time, as risk-blind actions accumulate and compound, the conditions for disastrous, runaway risk incidents increase.

Ineffective IT Governance

Many of the risk factors we discuss throughout the book are symptoms of a common condition: a history of ineffective IT governance (see “What Is IT Governance?”).

Inadequate IT governance—the absence of appropriate structures and processes for business involvement in IT investments and decisions—paves the path to risk in two important ways:

1. *Locally optimized decisions create enterprise risks.* IT organizations in many enterprises are organized and motivated (for example, through reporting lines and responsibilities) to be closer to the business organizations they serve and to respond to requests from the business as quickly as possible, rather than to take an enterprise view of IT decisions. Although each locally optimized decision may seem entirely justifiable and safe, the agility risks implicit in such decisions compound over time to dangerously high levels, as they did for Tektronix.
2. *Without business involvement, IT managers can make incorrect assumptions about which risks matter most to the business.* When markets, competitors, or corporate strategy change, the IT organization may learn slowly, if at all, that basic

What Is IT Governance?

IT governance is defined as “specifying the decision rights and accountability framework to encourage desirable behavior in using IT.”^a Just as in financial or corporate governance, IT governance is embedded in formal structures that allocate rights and responsibilities for decisions in certain IT domains (such as applications, architecture, and security) to appropriate business and IT executives. Governance decisions are supported by processes for surfacing information and driving resulting actions. In short, an IT governance arrangement describes how an enterprise’s decisions related to IT are made and enforced.

a. Peter Weill and Jeanne Ross, *IT Governance: How Top Performers Manage IT Decisions Rights for Superior Results* (Boston: Harvard Business School Press, 2004), 2.

business assumptions and standard operating procedures must also change. The result is a gap between real and perceived risks and controls, leading to overinvestment in managing minor risks and underinvestment in more critical ones.

Effective IT governance is especially important in times of rapid strategic change, when previously valid assumptions about what matters most (and why) are questionable—and rapid strategic change is a fact of life in most industries today.

Uncontrolled Complexity

Complexity per se is not necessarily more risky than simplicity. Modern automobiles are much more complex than automobiles from the 1960s, but they are also generally safer, more reliable and efficient, and of far better quality overall. But complexity without solid engineering increases risk in many ways. Most important, complex environments that are not carefully engineered tend to be fragile. They have many moving parts, and the parts are prone to break or function unpredictably, with equally unpredictable effects on other business and technical systems. Such haphazardly complex environments demand a great deal of knowledge and attention to manage effectively, and those resources are scarce. The result is increased risk.

Inattention to Risk

Inattention to risk encourages operational risks. Symptoms of inattention include:

- *Missing or inadequate knowledge.* Layoffs, retiring personnel, promotions, and reliance on external consultants reduce an enterprise's core knowledge and open the door to risk.

- *Poor infrastructure management.* Inadequate device management and refusal to retire old, unreliable technologies lead to high costs and failure rates and to long recovery times.
- *Employee ignorance, negligence, or malfeasance.* Employees who do not know or care how to avoid risk and employees bent on destructive or criminal acts create failures and breakdowns of security and privacy.
- *Systems that are blind to dangerous activities.* Systems that fail to detect or prevent dangerous activities abet management inattention by removing a potential layer of automated warning and protection. Automated controls are particularly important when the enterprise allows key employees considerable authority to act autonomously. For example, appropriate levels of automated controls at Barings Bank might have detected the activities of Nick Leeson, whose unauthorized trades in violation of company rules lost \$1 billion over nine months and bankrupted the institution.¹¹

Ineffective governance, uncontrolled complexity, and inattention to risk create an environment of pervasive IT risk. Pervasive risks cannot be fully controlled by asking technicians to perform technical tasks differently. The risks are intrinsic to the way the company does business, not just to the way it manages IT. Further, risk factors reinforce and compound one another, so addressing individual risks that particular managers see does not address the full range of risks implicit in a given situation.

In short, having an excellent IT staff is not enough to control IT risk. Managing IT risk requires everybody involved to think differently. The CIO must make the business consequences of IT risk clear to business executives and provide a decision-making environment in which those executives can discuss and make decisions about IT risk in business terms. Business executives must ensure that the CIO has

implemented risk management and must actively participate in the tough decisions and culture changes that IT risk management entails.

IT Risk as Business Risk and Business Value

Because IT risk is now business risk, with business consequences, enterprises must change the way they manage it. Businesses can no longer afford to assume that IT risks will be contained within the walls of the IT department, or even of the enterprise. They must replace technology-driven approaches and fragmented views of IT risk with an integrated view that starts with an understanding of the business risks and consequences that flow from IT decisions. Then they must take action.

This is essentially what Tektronix did after its rude awakening to IT risk in 1996. Led by the CFO and CIO, with strong support from the CEO, Tektronix redesigned its business processes and replaced its jumble of complex systems with an enterprise resource planning package. The initiative demanded committed leadership to make the case for change, convince skeptics to adopt standard processes, and discipline remaining holdouts. Not only did the information systems have to change—the undisciplined variety of business processes that produced the risk-ridden systems morass had to change as well.

The process was painful—it took three years and about \$55 million to complete—but it was ultimately successful in many ways. Tektronix was at last able to acquire and divest divisions flexibly. The changes reduced other IT risks and improved business performance significantly as well. More accurate information, delivered faster, enabled higher inventory visibility, faster credit approvals, and a five-fold increase in the percentage of same-day shipments. In the end executives had better information to support strategic decisions, and more agility to implement those decisions.¹²

In our research we have encountered many companies that have turned around dangerously risky situations by building IT risk management capabilities incorporating two key elements:

1. They have adopted an integrated view of IT risk that allows them to make rational, informed trade-offs about IT risk in business terms.
2. They place careful emphasis on three core disciplines for managing risk: simplifying the IT foundation, creating a risk governance process, and fostering a risk-aware culture.

These elements work together. Without an effective risk management capability, enterprises cannot have useful conversations about IT risk. Without a common language that conveys IT risks in business terms, business executives cannot make informed decisions about these risks.

Managing an integrated business view of IT risk via the three core disciplines reduces IT threats while increasing business value derived from IT. If IT risk is handled as a compliance or avoidance issue, then it's just a cost to be managed. But if IT risk is handled in the right way, as business risk and capability, business value is created in three ways. First, there are fewer fires to fight, and the enterprise can focus on more productive activities. Second, the IT foundation is better structured and less costly, freeing resources for more productive activities. Third, the enterprise can pursue valuable opportunities that other firms would consider too risky to attempt.

Structure and Intended Readers of This Book

Many books have been written about specific elements of managing risk, in both business and IT. But, to our knowledge, this is the first book to provide rigorous research-driven advice and tools for build-

ing a comprehensive view of IT risk as business risk. As such, it should be read by business executives and IT executives alike.

If you're a business executive or board member, we provide ideas, frameworks, and advice to help you meet your fiduciary responsibility of managing IT risks as effectively as you manage other risks.

If you're an IT executive, we provide step-by-step advice and tools to help you build an IT risk management capability. We provide information in a practical form to help you start the program, find the right specialists for each element, and engage both business and IT people in the right roles.

Chapter 1 presents our key framework linking IT risk and business priorities. Contrary to the technical and compartmentalized way in which most enterprises manage IT risk, we argue that IT risks are best summarized in terms of four key business objectives: availability, access, accuracy, and agility. Technical risks can be best managed in terms of costs, benefits, and trade-offs among the business objectives—the same way executives make all their key decisions.

Finding a way to discuss IT risks in natural business terms is only the first part. Enterprises also must have the capability to identify, prioritize, and address the risks they face. Chapter 2 starts the enterprise on this path with a discussion of the three core disciplines of effective risk management:

1. A well-structured, well-managed *foundation* of IT assets, people, and supporting processes
2. A well-designed *risk governance process* to identify, prioritize, and track risks
3. A *risk-aware culture* in which people understand causes and solutions for IT risks and are comfortable discussing risk

Enterprises generally start with and emphasize one of these disciplines, but they must ultimately be capable in all of them. Over time, an enterprise may choose to change its emphasis as its capabilities mature.

Chapters 3–6 represent the heart of the book and offer a blueprint for developing effective risk management capabilities. These chapters have been written for IT executives, who will be responsible for implementing the practices, and should be skimmed by business executives, who will participate in the processes and charge their CIOs with implementing those processes. Chapters 3–4 describe how to improve the IT foundation of applications, infrastructure, people, processes, and controls. In these two chapters, we describe the IT risk pyramid and how executives can use it to manage the right risks in the right order.

Chapter 5 shows how to establish the second core discipline, the IT risk governance process. An effective IT risk governance process is coordinated by a risk officer, conducted by managers in each functional area, and overseen by executives at higher levels. The chapter includes processes and tools to make risk governance effective.

The final risk discipline, a risk-aware culture, is the topic of chapter 6. No process can be effective and no foundation can be protected if the enterprise is afraid to talk about risk. A risk-aware culture starts at the top with business executives who set direction, model risk-aware decision making, and reward effective risk management behaviors. The goal is a culture in which risk is discussed openly across the organization and actively managed to tolerable levels.

Chapters 7–9 bring the focus back to the business executives who are so critical to the success of IT risk management. IT risk has serious business consequences, and business executives have important roles to play in managing IT risk effectively.

Chapter 7 describes how to assess each discipline—the foundation, risk governance process, and risk-aware culture—in your organization and bring each up to at least a competent level. Although enterprises must become competent in all three disciplines as fast as possible, they often choose one focal discipline as the rallying point to continuously improve all three well beyond the competent stage.

We present diagnostic tools to assess the pros and cons of different focal discipline choices in your organization.

Chapter 8 is about looking forward to anticipate strategic risks. Much risk management is about identifying and resolving risks in the present or near future, but executives have a duty to make sure that the enterprise is viable for the long term. Accordingly, in this chapter we describe how to incorporate risk management into the firm's considerations of likely future strategic changes.

Chapter 9 concludes the book with a summary of key themes and an executive call to action. It highlights the ten ways executives can improve their IT risk management.

