An Introduction to Risk Management in the Digital Age

A Call to Action for an Enterprise-Wide,
Top-Down Approach to Digital Risk Management
and Corporate Governance

A White Paper from DigitalRisk Advisors

Introduction

Digital risk management is about re-defining corporate governance to meet the new demands facing electronic business. New regulations and recently updated Federal Sentencing Guidelines create mandatory corporate governance environments where business leaders are potentially held personally responsible for privacy and information security violations that occur on their watch.

The heightened level of vulnerability and exposure created by e-business necessitates a brand-new level of digital risk sensitivity directed by a hyper-aware board and senior management and permeating throughout the extended organization.

Network-dependent enterprises must create a proactive and systematic enterprise-wide framework for addressing change management and disaster preparedness. Lowering corporate negligence and liability in the digital age is a complex responsibility that requires significant coordination and maintenance.

The Reality of Digital Risk

The following scenarios are based on accounts of real incidents:

SCENARIO 1

- The Chairman of the Board of a major international bank publicly announces that his bank is dedicated to becoming a leader in delivering on-line financial services. A hired consultant, with help from a trusted bank employee, uses inside information to break into the bank's wireless LAN, eventually breaching sensitive back-end systems.

- The attack team steals $15 million and several gigabytes of confidential customer information. The hacking incident is leaked to the international press and the bank is answering calls from reporters, clients and auditors around the world regarding the bank's information security policy, due diligence and operational procedures.

- The perpetrators open several new accounts and perform financial transactions in the names of your most trusted customers. After cooperating with the law enforcement and recovering nearly all the stolen money, it comes to the bank's attention that confidential customer information and sensitive account numbers have been published on publicly available web sites around the world. The bank suffers the largest twelve-month asset withdrawal in its 150-year history and users refuse the online banking system the bank invested so heavily in.

SCENARIO 2

- The CEO of a high-profile on-line consumer auction site with a custom transaction-processing engine and multi-billion dollar market capitalization has to explain why a routine software maintenance procedure exposes a widely known security hole that a former disgruntled employee then uses to hack into the firm's back-end systems.

- The attacker takes over production systems and noticeably impacts traffic and transactions on the company's web site. The hacker taunts his former employer by boasting about his achievements on message boards and web sites around the globe. Calls begin to overwhelm customer service staff. After the interruption continues for several days, the media begins to claim that the site is not ready for prime time and that users should be cautious when visiting.

- Once the system is back to normal operations, the media continues its barrage on the firm's corporate culture and managerial inadequacies. Within 90 days of fixing the problem, the firm's stock valuation drops by over $ 3 billion and loses 25% of its subscriber base.

SCENARIO 3

- The fast-growing on-line music retailer relies on outsourced partners to provide the web site's technical infrastructure. As the site accepts credit card payments over the web, partners demand encryption of each transaction during processing but the hosting partner fails to encrypt the credit card numbers and sensitive customer data while it sits in the database once the transaction is complete.

- A Russian hacker attacks a known hole in the web commerce server and steals the unencrypted credit card and customer information. The CEO gets a midnight call at home from the Russian demanding a multi-million dollar payment in return for the stolen information.

- The international media learns of the incident, and the third round of funding doesn't come through because the venture capital community is concerned about the mounting adverse publicity.

SCENARIO 4

- A large, well-respected medical center that is heavily involved with ongoing HIV research has been chosen by a multi-national pharmaceutical giant to lead the process of assisting with top-secret clinical trials for a breakthrough vaccine. Upon hearing of the opportunity, a professional corporate espionage professional, working for a rival of the pharmaceutical giant, masquerades as a janitor and gains physical access to the center's internal systems - there are no access controls or physical monitoring of the facility.

- The agent easily creates an account with Administrator rights and also creates a secret backdoor accessible through an existing modem. Over the next twelve months, the agent secretly accesses the center's systems from a remote location and passes sensitive information a competitor.

- Once the patent process is underway, the pharmaceutical company's patent team finds that their main competitor has already filed a brand new pharmaceutical patent that looks very similar to their design; the only real difference is that the competitor's design is better. Through an investigation, the medical center's system was found to be the point of compromise and the pharmaceutical company holds the medical center liable for the lost market opportunity.

Stakeholders are Exposed

These four simple scenarios offer a glimpse of a menacing but very real side of the digital world. Given the increase in multi-million dollar cyber extortion, the growth of identity theft, and the widespread prevalence of questionable online business practices, there is no doubt that something fundamental has to change if business leaders are to avoid seeing their company become the central character in one of these scenarios.

As the Internet continues to evolve as a business tool, **stakeholder accountability** will be the prime motivator for companies who have learned from the past. This new commitment to stakeholder accountability requires that top-level support and attention to detail is a mandatory decision-making driver for all strategic, operational, and technical initiatives.

Gone are the days of "irrational exuberance" where each part of the organization was allowed to operate autonomously in a "ready, fire, aim" mentality. **Strategic, operational, and technical alignment must be the mantra of the future.** This is simple business fundamental, and now, more than ever, it's time to get back to basics.

Organizational Stakeholders @ Risk

- ❒ Employees
- ❒ Customers
- ❒ Suppliers
- ❒ Shareholders
- ❒ Executives / Board of Directors
- ❒ General Public

In the digital world where click wrap and click-through agreements have become commonplace, it's important to remember that organizations enter into default contract relationships with each stakeholder group whether governed by written documents or common-law practice.

The type of contractual relationship that an organization has with its stakeholders depends largely on the type of business model and network model that is employed. It's important to understand that as much as we strive to create risk management and information security standards, there is no silver bullet and one size does not fit all.

An Interdisciplinary Approach to Digital Risk Management

Just as industries have reorganized operational processes and procedures to address computing environments, so too must we reorganize and re-engineer corporate risk management. Looking at the traditional organizational structure and analyzing the methods for making strategic, operational, and technical decisions, we see that the static silo-based organizational structure is ineffective when dealing with the new digital risk environment.

In the wake of increasing technical and organizational complexity facing today's e-business initiatives, it is clear that decision makers relying on traditional risk management strategies are failing to keep pace with the digital risk demands. Why? Risk managers, who are

usually found in the financial silo, are disconnected from technical and operational managers, and decisions regarding preemptive security measures remain at a distance from traditional risk management and insurance decisions.

What's needed now is an interdisciplinary, multi-dimensional framework that can properly address all of the complex digital risk issues simultaneously. As evidenced by sensational hacker and virus headlines, technology alone will not guarantee e-business security. While most risk-based decisions and budgeting focus primarily on the technical exposures**,** what's needed is an enterprise-wide, top-down methodology to manage digital risk.

These solutions combine expertise from the worlds of insurance, traditional risk management, business consulting and information security and must focus on the strategic e-business initiatives before making technical network security commitments. It is business relationships, public perception, and corporate trust that we are protecting; technical infrastructure is merely a business facilitator.

The partnership of information security with traditional risk management is a strategy that blends strong corporate policy and proven risk management practices with the realities of information security in the emerging e-marketplace. The emerging new breed of digital risk management professionals must work closely with e-business leaders to maximize their information security ROI while transferring residual risk to an insurer.

With guidance from senior executives and due regard to the overall strategic goals, true digital risk management professionals will integrate all aspects of information security (risk identification, protection, control, and reaction) with traditional risk management (risk analysis, avoidance and transfer) to ensure that the complex demands of the e-business strategy are adequately met.

Digital Risk Management is a Process, not an Event

Continuous Life Cycle Approach - *Kaizen*

- ❒ Knowledge Transfer – *Advise*
- ❒ Identify / Analyze – *Baseline*
- ❒ Protect / Avoid Risk - *Implement*
- ❒ Detect / Control – *Inspection & Compliance*
- ❒ React/ Transfer - *Support*

Connecting to customers, suppliers, partners and remote workers using the Internet and World Wide Web has become a critical capability for most businesses. It is clear that all business will soon become e-business. While e-business models continue to rapidly proliferate and evolve, there are significant risk management challenges within this new business paradigm.

Constant reengineering in the quest to take advantage of new technologies and new business models is not new to modern corporations. However the distinctive needs of digital risk require a unique and binding partnership between business and technology decision makers.

A brief trend analysis shows that e-business is a complex landscape:

Technology Trends:	**Industry Trends:**
Web Services	Outsourced IT
Web to Backend Transaction Processing	Web Hosting / Co-location
Great Global Grid	Marketing Hype
Distributed Computing	Focus on ROI
Authorization	Confused Buyers
Strong Authentication	Overwhelmed Users
Mass Data Storage	Remote Access
Handheld Clients	Life Sciences / Biotech
Mobile Handsets	Mobile Commerce
Thin Clients	Security / Privacy
Wireless	Liability / Fiduciary Responsibility
Broadband	Personalization / 1 - to - 1 Content
IPv6	Identity Theft
Mobile IP / Internet Roaming	Lack of Standards
Automatic Location Identification	Lack of Knowledge / Unqualified Staff
Peer 2 Peer	Open Source vs. Proprietary Code

Application Trends:	**Social Trends:**
Enterprise Application Integration	Internet user acceptance rising
Personal / Corporate Portals	Electronic transaction become mainstream
Web Enabled ERP / ERP II	Virtual Communities
e-Banking / e-Financial Services	Virtual Affiliation / Loyalty
On-line Banking	Virtual Education / Dist Learning
Virtual Wallets	Global Village/ Shrinking Planet
e-money	Home Based Workforce
On-line Auction Marketplaces	Privacy / Tracking Concerns
CRM / 1 - to - 1 Marketing	
Remote Admin / Support	**Gov't / Legal Trends:**
Application Service Provider Utility	Legal Liability
Pay for Service	Insurance
Data Storage / Digital Vault	e-Sign legislation
Remote Synchronization	HIPAA
	GLBA
	European Union Privacy Act

As web site e-business strategies transform to become multi-enterprise Internet strategies, it is imperative that we migrate our focus from information security and begin talking about digital risk management. Managing enterprise-wide digital risk, as opposed to managing information security, is a continuous practice that demands immediate attention. But in the rush to create e-business initiatives at warp speed, digital risk management is often ignored.

With losses to the Love Bug virus estimated at a staggering $8.7 billion, followed by the Code Red attack that exceeded $2.6 billion, it is clear that technology decisions can no longer be made in a vacuum apart from other business decisions. The chasm that exists today within the executive suite is something all business leaders must deal address. By connecting to the Internet and engaging in e-business, business leaders have put their corporate assets in the care of others while also taking responsibility for assets belonging to others.

The DigitalRisk Paradigm

- ❒ Risk Management must Evolve Moving from Brick & Mortar to Brick & Click
- ❒ "Prudent Man" Rule Still Applies
- ❒ Enterprise-wide Controls must be Consistent with Business Model
- ❒ Managing Perceptions & Stakeholder Expectations is Critical
- ❒ Consistently support "Trust and Accountability" Behavior
- ❒ Intangible assets / knowledge process become the focus

By its nature, a **multi-enterprise e-business initiative** requires heightened levels of trust and accountability among all the parties involved; at any given time each e-business partner has care, custody, and control of another's tangible and intangible assets. For example, the risks of outsourcing can be enormous because the decision places outsourced vendors in ultimate control of critical business relationships. And with every strategic and technical decision, stakeholder relationships become weakened or strengthened according to the level of assurance, safety and accountability the organization provides.

That assurance can only be accomplished with an executive-level sanctioned, enterprise-wide digital risk management program, which skillfully combines information security practices with traditional risk management, strong corporate policies and specialized insurance.

Digital Risk Considerations

- ❒ Untested Business Models
- ❒ Rapidly Changing Technology
- ❒ Corporate Restructuring
- ❒ Rapid Growth / Market Pull
- ❒ Reactionary Impulses vs. Proactive Planning
- ❒ Working on "Internet Time"
- ❒ Increased Sensitive Information Handling
- ❒ Extended Enterprise Creates Uncertainty
- ❒ Liability of Outsourced Business Operations
- ❒ Communication Gap Between Business and Technology Decision Makers

Digital Risk Insurance is Mandatory

A comprehensive insurance program that covers the major e-business exposures needs to be part of every organization's digital risk management plan. Digital risk insurance serves to help absorb the soaring financial losses that we should all anticipate.

First-party insurance absorbs direct losses that policyholders sustain to their information assets while third-party insurance helps to pay for losses policyholders cause others. An important element addressed by **liability** insurance is the rising cost of defending against stakeholder claims and litigation, which places an increasing burden on even the most robust e-business initiatives. According to recent published reports, lawsuits brought against e-businesses are on the rise and defense costs and defamation awards are rapidly escalating.

An all-inclusive, top-down digital risk management strategy must also include insurance solutions that protect against **direct losses** including hardware failures, software bugs, downed telephone lines and overloaded networks. The goal is to protect corporate stakeholders, clients, customers and the general public against financial loss due to failures in e-business initiatives.

Whether stakeholder losses result from internal or external attacks, are accidental or malicious in nature, or originate from known or unknown sources, digital risk losses can cause significant downgrades in market valuation, lost business, damaged reputation, and lost opportunity. Therefore, an adequate insurance program must be there to pick up the financial pieces.

First Party Digital Risk Insurance

Property, EDP, Fidelity, Computer Crime

Addresses business recovery, lost revenue and direct damage suffered by the policyholder as a result of a covered incident.

Coverage Concerns: All Risk vs. Named Peril Coverage?
Coverage for Acts by Internal and External Parties?
Standard Form vs. Manuscript Form?

Third Party Digital Risk Insurance

D&O, Media Liability, Intellectual Property, Copyright, Patent, E&O, Contractual Liability

Addresses business recovery, lost revenue and damage suffered by someone else and caused by the policyholder.

Coverage Concerns: Any Coverage under CGL?
Coverage for Major Stakeholder Groups?
Coverage for Acts by Internal and External Parties?
Standard Form vs. Manuscript Form?

Interdependent Nature of Digital Risk

When business decision makers think about digital risk, it is imperative that they understand the standard interdependencies within e-business operations and attack the issues as a coherent and integrated team. E-business models inherently combine enterprise-wide financial, technical and legal risks that render even the most savvy traditional corporate risk managers perplexed and ill-equipped. No longer the sole domain of the traditional corporate risk manager position or the information security manager, the multi-faceted and multi-dimensional electronic business landscape presents risks interwoven throughout all strategic and functional decisions.

Corporate officials must simultaneously juggle their traditional risk management responsibilities and their new e-business risk management responsibilities. Facing the interdependent nature of digital risk is a challenge for any executive team in any industry. Past corporate risk management functions were largely carried out within separate corporate silos, each with their own process and goals, and each speaking their own functional language.

That contrasts with electronic business environments where risk management responsibilities begin to blend into each other and real-time coordination becomes the only path to success. The communications gap that exists between the top decision makers is a daunting hurdle that all senior management teams must overcome if they are to be successful. The digital risk paradigm requires senior executive teams to begin defining proactive risk management strategies and solutions in a common way using a common language that stresses **enterprise-wide awareness, knowledge sharing, and training.**

The interdisciplinary, enterprise-wide nature of digital risk management communication comes to life in the organization's **service level agreement (SLA)**. Whether as a customer recipient of an SLA or as vendor provider of an SLA, it is imperative that senior managers become proficient in managing these important business documents. The SLA sets the tone for what will happen in the business relationship**,** matching strategy, expectations and execution. This is the policy that governs all operations, strategy, and tactical decisions between the organization and each stakeholder relationship.

This space intentionally left blank

	INTER-DISCIPLINARY DIGITAL RISK MANAGEMENT	
Decision Maker	**Traditional Risk Responsibilities**	**e-Business Risk Responsibilities**
Board of Directors	Strategic Corporate Governance	Service Level Agreements Enterprise-wide Due Diligence
Chief Executive Officer	Market Opportunity Corporate Execution Communicate Internal Expectations Leadership by Example Revenue	Service Level Agreements Communicate External Expectations Profitability
Chief Legal Counsel	Contract Requirements Strategic Planning Corporate Ethics	Service Level Agreements On-line Liability Regulatory Compliance
Chief Financial Officer	Corporate Budget Balance Sheet	Service Level Agreements Market Capitalization Access to Capital
Chief Risk Officer	Internal Insurance Internal Physical Facilities	Service Level Agreements External Insurance Enterprise Risk Technical Risk
Chief Operations Officer	Internal Procedures Internal Human Resources Vendor / Supplier Pricing	Service Level Agreements Stakeholder Privacy External Procedures External Human Resources Vendor / Supplier Operations
Chief Technical Officer	Infrastructure Lifecycle Internal Systems Internal Network Internal Users Internal Project Management Vendor / Supplier Pricing	Service Level Agreements External Systems External Networks External Users External Project Management Vendor / Supplier Operations
Chief Information Security Officer	Internal Computer Security Internal Users / Attackers	Service Level Agreements External Computer Security External Users / Attackers Physical Security / Facilities Corporate Policy Training / Education
Chief Marketing Officer	Market Perception Public Relations Branding	Service Level Agreements Stakeholder Privacy

Tacit Risk vs. Explicit Risk: Power, Perception, Human Behavior

Achieving an environment where true digital risk management exists requires that all senior managers and decision makers raise the level of conversation from that of tactical, information security techno-speak to one of corporate governance and enterprise-wide accountability. Driven by a corporate culture where senior managers continually communicate and demonstrate norms of behavior, expectations, motives, and consequences, the business risk considerations and human risk interactions will always create the contextual reference point for subsequent technical risk decisions.

Pareto Rule: Technology is just the tip of the Digital Risk iceberg……

20% - Explicit / Objective / Measurable / Quantitative risk related to the technology, inventory, physical facilities, and process aspects of the enterprise

80% - Tacit / Subjective / Qualitative risk related to the socio-cultural factors such as organization roles, relationships, and structures, formal & informal modes of communication, power, norms of behavior, and unintended consequences

When it comes to managing enterprise-wide e-business governance, stakeholder perception and reality is often the same thing. The primary driver in digital risk conversations and initiatives must be business and stakeholder considerations. **Going forward, the technical security conversation cannot be the sole driving factor.**

Managing digital risk includes managing stakeholder trust, managing expectations, managing communication, and sharing knowledge. If the organization fails to communicate consistent expectations, and set the tone for managing relationships, all digital risk initiatives are at risk of failure.

Until now, digital risk management initiatives have been driven by technically oriented information security practitioners who have attempted to control electronic environments using electronic means. But just like all other management challenges, digital risk exposures and solutions will always begin and end within the relationships, expectations, communication and frailty of humans, not machines.

Experience shows that Pareto's 80 / 20 rule is in full effect in the digital risk world - while we have traditionally focused eighty percent of our efforts on the explicit technical exposures, the **tacit risk elements** that comprise the bulk of the problems received nearly no attention and go largely unchecked. **This inadequate attention to the tacit (intangible, unquantifiable risk factors) is the essence of the current information security problem and a significant paradigm shift must occur if we are to move electronic commerce and e-business toward its potential.**

"Zero-tolerance" information security strategies once popular in government environments are not acceptable for relationship-based e-business. Regardless of the technical approaches taken, stakeholders are exposed today and will always be exposed. Therefore, it is up to senior management to determine how the organization and its stakeholders will perceive this constant exposure and manage the risks to the best of their ability. **Tacit, unquantifiable risk factors such as reputation, marketability and stakeholder trust are powerful human condition motivators that cannot be left to chance, and using digital risk management strategies to demonstrate stakeholder value and respect has become critical in the course of e-business survival .**

THE DIGITAL RISK TACIT / EXPLICIT SPECTRUM	
Tacit (New Focus) **Digital Risk Management**	**Explicit (Traditional Focus)** **Information Security**
STRATEGIC (80%)	**TACTICAL (20%)**
MACRO decisions lead to →	→ **MICRO decisions**
Proactive / Built-In Corporate Governance Organizational / Human Relations Stakeholder Relationships Trust Reputation Opportunity Standard of Due Care Corporate Policy Regulatory Compliance Perception Expectations Privacy Liability Accountability Fiduciary Responsibility Market Capitalization Intellectual Property	Reactive / Add-On Point Solutions Technical Procedure Network Assets Physical Security Firewalls Public Key Infrastructure Intrusion Detection Anti-Virus Biometrics Virtual Private Networks Access Control Single Sign-on Encryption Digital Signature File Integrity Disaster Recovery

While the natural instinct in technology intensive environments is to focus on managing technical risk, it is actually the long-standing business relationships that demand the primary risk management attention of senior managers. **Defining business stakeholder relationships as "any person or group of persons that the organization needs in order to survive," the importance of stakeholder relationships can never be overstated; it is safe to say that the manner in which an organization protects its most valued stakeholders is a primary indicator of that organization's long-term success.**

When you consider that stakeholder groups include private investors, public markets and regulators, it is easy to see how demonstrating tacit digital risk due diligence and stakeholder trust management has a direct impact on an organization's more quantifiable explicit risks like credit, liquidity, and profitability.

Real Threats, Real Losses

The emergent e-business paradigm has created a totally new set of digital risks, as corporations and other institutions face growing threats from inside and outside their organizations. Denial of service attacks, social engineering, web site defacement, espionage, financial fraud, insider abuse of Internet access, and virus contamination are just some of the dangers today's organizations are exposed to.

Consider these statistics:

- According to **Computer Economics**, computer viruses and worm attacks cost business $17.1 billion in 2000 compared to $12.1 billion in 1999. In addition to the direct technical implications, viruses have significant negative impact on productivity of system users, support staff, helpdesk staff, and other staff responsible for assisting internal end users, IT staff, and customers worldwide.
- Growing security risks are also reported by the **2001 Computer Crime and Security Survey**, which is conducted annually by the Computer Security Institute (CSI) and FBI. For example, although nearly all of the 538 respondents representing various U.S. corporations, government agencies, financial institutions and universities utilize access controls, eighty five percent still reported unauthorized use of their computer systems. The study also found that of sixty four percent of respondents reporting their organizations suffered direct financial loss because of security breaches, only thirty five percent could accurately determine how much was lost.
- The **CERT Coordination Center (CERT/CC) at Carnegie Mellon** is a federally funded research and development center a center that studies Internet security vulnerabilities. CERT/CC recently issued their vulnerability statistics for the first two Quarters of 2001 showing a dramatic increase in digital risk activity. The number of security incidents reported to CERT/CC so far in 2001 is 15,476 versus 21,756 for all of 2000, while the number of security vulnerabilities reported to CERT/CC through 2nd Quarter 2001 is 1,115 versus 1,090 for all of 2000.

Unprecedented Reach and Scope

Within the e-business risk paradigm, the evolution of digital risk management inevitably combines corporate policy, specialized insurance, information security, and loss control / forensics. Given the swift and severe nature of network-based attacks, the losses endured can't be strictly safeguarded *after the fact*. The potential commercial exposure and loss of goodwill for stakeholders and customers in the Internet Economy are unlike any seen in the past.

The capability of the Internet to connect individuals and organizations all over the world means that the number of stakeholders that a given organization may become responsible for injuring increases immeasurably each day. If a company's network becomes a point of compromise for harm done to others, that compromise will have consequential loss ramifications that spread far beyond the widest conceivable boundaries of a traditional business loss.

While a traditional business risk like fire is relatively containable in the physical world, network-based security breaches can inflict damage and losses on others linked to a corporate network through the Internet at an uncontrollable rate and with an undeterminable reach.

A recent example of the rate and reach of digital risk damage is offered by the **Cooperative Association for Internet Data Analysis (CAIDA**). After significant analysis, CAIDA found that the "Code Red" worm affected more than 359,000 servers in less than 14 hours. They also determined that at the peak of the infection frenzy, more than 2,000 new hosts were infected each minute.

Digital risk losses must address fiduciary accountability for all corporate stakeholders that may be affected, from customers whose personal information is compromised, to suppliers attacked via your system. Loss of trust between an organization and its stakeholders (investors, customers, partners, suppliers, and public) could be catastrophic to any well-meaning e-business initiatives. As a result, the days are numbered for any e-business that can't guarantee the financial and technical security of its on-line relationships.

Electronic exposures can affect all organizations whether or not they sell or transact directly with customers on-line. Any organization connected to the Internet, regardless of how they use that connection, must be concerned with several potential points of compromise, such as:

- **"Island hopping",** where attackers can gain access to an insecure computer network and use it to launch attacks on the other networks. By compromising security weaknesses at multiple points, attackers can use victim hosts as "zombies" to target denial-of-service assaults that are traceable back to the victim's IP address.

- **E-mail compromise**, which places companies at risk of unknowingly spreading a virus and harboring legally sensitive unprotected e-mail content.

- **Web site exposures**, which can happen when a site becomes unavailable or is maliciously altered to include erroneous information.

- **Data theft**, which involves insiders or outsiders stealing sensitive information and intellectual property.

Creating a Compelling Competitive Advantage

In order for digital risk management to operate according to the strategic goals of the organization, sales & marketing and the quest to create competitive advantages must become primary drivers. In the wake of the dot-com crash, business decision makers should view their digital risk management plan as a strategic competitive weapon and an opportunity to raise the bar of best business practices and standards.

Struggling to comply with privacy and security regulations such as **HIPAA** in the healthcare sector and **Gramm-Leach-Bliley** in financial services, it's imperative that e-businesses establish a proactive, unified risk management solution across their entire extended enterprise.

Significant effort should be made to involve senior management in making digital risk decisions. Board Members, CEOs, CFOs, CIOs, Information Security Officers and Risk Managers accountable for both operational performance and achieving strategic objectives need to understand the direct alignment of digital risk with the strategic business goals of the enterprise. Adopting a comprehensive digital risk management strategy can go a long way in ensuring the security and longevity of your business in the next phase of the Internet marketplace.

The interdependent networked world has changed everything about business risk management. E-business initiatives are designed to streamline operations and create competitive advantages but conducting e-business can expose companies to unforeseen, business-ending risks. Inadequate protection and attention to exposures can eventually destroy even the strongest e-business models. Poorly managed risk profiles are all doomed to suffer the same fate: meaningful long-term financial loss, damaged digital assets, lawsuits, damaged reputations.

Sustaining DigitalRisk Management Effectiveness

- ❒ Speak in Digital Risk Management language
- ❒ Focus on stakeholders, 3rd Party liability is most damaging
- ❒ Some intangible exposures are not insurable
- ❒ Commit to Operational Excellence
- ❒ *Kaizen* - Continuous Improvement
- ❒ No Risk, No Reward
- ❒ Dare to Learn New Ways of Thinking
- ❒ Hire Smart People
- ❒ Never Say Never
- ❒ Consultative vs. Transactional Approach to Risk Management

By now the message should be clear to all senior management teams who face business survival in the Digital Age. The dangerous new world of e-business comes with mind-numbing exposures that require dramatic new solutions. Like any chain, e-business environments are only as strong as the weakest link. Where constant life-cycle vigilance is a necessary strategy and technical directions mirror business realities, executive teams have a duty to implement digital risk initiatives that include cost-effective safeguards and business-focused loss controls across the virtual enterprise.

Quite unlike a single event like the Y2K problem, effective Digital Risk Management is an ever-evolving “best practices” process that never ends. In order for today’s e-businesses to survive, it is therefore mandatory that all organizations adhere to best practices and proper planning both internally and between interdependent trusted partners. It is an undeniable fact that if current and future business models are to survive and achieve their financial objectives, it is essential for corporate boards and senior leadership teams be constantly vigilant in the quest for trust, stakeholder accountability, and proper corporate governance.

Knowing that your e-business success, longevity, and reputation are at stake, anything less than a total digital risk management solution is not a solution at all.

Rick Davis is Principal Advisor at the Atlanta-based risk management consultancy DigitalRisk Advisors. As a veteran digital risk management practitioner, Rick is one of the original players the digital risk insurance market and the creator of the DigitalRisk ScoreCard Methodology.

Please visit DigitalRisk Advisors on the Web at www.digital-risk.com for speaker info, newsletters and current services information. Contact Rick directly by e-mail at rickdavis@digital-risk.com or by phone at 770.587.5990.