

Risk management in the digital age

The growth of e-business and the widespread use of computer networks have spawned digital risk. **Rick Davis** advises how to manage it

Over the past few years, an increasing number of companies have found themselves hitting the headlines as victims of "digital risk" – one or another of the disparate risks associated with doing business in a networked environment. Some are undoubtedly hyped-up scare stories, but others offer a glimpse of a menacing and very real side of the digital world.

The emergence of e-business has created a new set of risks, as corporations and other institutions face growing threats from inside and outside their organisations. The risks take myriad forms: denial-of-service attacks, social engineering, website defacement, espionage, financial fraud, insider abuse of Internet access and virus contamination, to name a few. Consider these statistics:

- According to *Computer Economics*, computer viruses and worm attacks cost business \$17.1 billion in 2000, compared with \$12.1 billion in 1999. In addition to the direct technical implications, viruses have a significant negative impact on the productivity of system users, support staff, helpdesk staff, and other staff that assist 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 the FBI. For example, although nearly all of the 538 respondents representing various US corporations, government agencies, financial institutions and universities control access to their computer systems, 85 per cent still reported unauthorised use. The study also found that 64 per cent of respondents reported their organisations suffered

direct financial loss because of security breaches, and only 35 per cent could accurately determine how much was lost.

- The CERT Coordination Centre (CERT/CC) at Carnegie Mellon is a federally funded research and development centre that studies Internet security vulnerabilities. CERT/CC recently issued its 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 second-quarter 2001 is 1,115 versus 1,090 for all of 2000.

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 companies fall victim to such assaults.

How do such risks manifest themselves? There are plenty of stories in the public domain, and scattered through this article you'll find three scenarios that illustrate how a minor technical problem can escalate into a serious business risk. These stories are fictional – but events similar to them have occurred, and continue to occur, in the real world.

As the Internet continues to evolve as a business tool, stakeholder accountability will be the prime motivator for companies that 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 organisation was allowed to operate autonomously in a 'ready, aim, fire' mentality. The mantra for the future must be strategic, operational and technical alignment, a simple business fundamental. Now, more

Scenario 1: Pride goes before a fall

- The chairman of the board of a major international bank publicly announces that his bank is becoming a clear leader in online financial services. Unknown to him, however, a hired consultant, assisted by a trusted employee, is using inside information to break into the bank's network, working up to eventually breach sensitive back-end systems.
- The attackers steal millions of dollars and several gigabytes of confidential customer information. The hack is kept confidential, but is eventually leaked to the international press and the bank is soon answering calls from reporters, clients and auditors around the world questioning its information security policy, due diligence and operational procedures.
- After cooperating with law enforcement, the criminals are caught and the bank recovers nearly all of the stolen money. But online acquaintances of the perpetrators then gain access, open several new accounts and perform financial transactions in the names of some of the bank's most trusted customers. Worse still, the bank discovers that confidential customer information and sensitive account numbers have been published on publicly available websites around the world.
- The bank suffers the largest 12-month asset withdrawal in its long history and many users refuse to use the online banking system the bank invested so heavily in.

than ever, companies need to get back to basics. In the digital world where click-wrap and click-through agreements have become common, it's important to remember that organisations 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 organisation has with its stakeholders – employees, customers, suppliers, shareholders, creditors and the general public – depends largely on the type of business model and network model employed. It's important to understand that as much as we strive to create risk management and information security standards, there is no single magic solution.

An interdisciplinary approach

The capacity to connect to customers, suppliers, partners and remote workers using public and private networks has become critical to most businesses. The line between business and e-business is fading, and the continuing rapid proliferation and evolution of business models (the dotcom meltdown notwithstanding) poses significant risk management challenges. It is imperative that the focus moves from information security, essentially a one-off systems design issue, to digital risk management – a continuous practice that demands ongoing attention.

Constant re-engineering 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. Just as industries have reorganised their operational processes and procedures to address computing environments, so they must also reorganise and re-engineer corporate risk management.

The traditional organisational structure for risk management (static and 'silo-based') is

ineffective when dealing with the new digital risk environment, as are the methods used to make strategic, operational and technical decisions. Why? Because risk managers, who are usually found in the financial silo, are disconnected from technical and operational managers, and decisions regarding pre-emptive security measures remain at a distance from traditional risk management and insurance decisions.

The technical and organisational com-

“It is business relationships, public perception and corporate trust that need protecting. Technical infrastructure is merely a facilitator”

plexity associated with e-business initiatives makes it clear that decision makers relying on traditional risk management strategies will fail to keep pace with the demands of digital risk management. While most information security decisions focus primarily on technical exposures, technology alone cannot guarantee security, as shown by the continuing flood of headlines reporting hacker and virus exploits. And business line input is critical: relatively small technical problems can turn rapidly into enormous business problems, as the scenarios illustrate. Ultimately, it is business relationships, public perception and corporate trust that need protecting. Technical infrastructure is merely a facilitator.

Technology decisions can no longer be made in a vacuum, set apart from other business decisions, as the scenarios testify. By connecting to the Internet and engaging in e-business, business leaders put their

corporate assets in the care of others, and also take responsibility for assets belonging to others. These steps should not be taken on the basis of technical considerations alone.

What's needed is an interdisciplinary, multi-dimensional framework that can properly address the full range of complex digital risk issues: an enterprise-wide, top-down methodology to manage digital risk. Such an initiative must combine expertise from the worlds of insurance, traditional risk management, business consulting and information security.

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 electronic marketplace. The emerging breed of digital risk management professionals must work closely with business leaders to maximise the return on investment in information security while transferring residual risk to an insurer.

With guidance from senior executives and due regard to 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.

Such an initiative by its nature requires heightened levels of trust and accountability among all the parties involved. For example, the risks of outsourcing can be enormous, because the decision places outsourcing 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 that the organisation provides. This assurance can only be accomplished with an

Tacit and explicit digital risks

Tacit digital risk management	Explicit information security
STRATEGIC (80%)	TACTICAL (20%)
PRIMARY considerations →	SECONDARY considerations
MACRO decisions lead to →	MICRO decisions
Within this FOREST →	Exist these TREES
<ul style="list-style-type: none"> Proactive/built-in Corporate governance Organisational/human relations Stakeholder relationships Trust Reputation Opportunity Standard of due care Corporate policy Regulatory compliance Perception Expectations Privacy Liability Accountability Fiduciary responsibility Market capitalisation Intellectual property 	<ul style="list-style-type: none"> 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

executive-sanctioned, enterprise-wide digital risk management programme, which skilfully combines information security practices with traditional risk management, strong corporate policies and specialised insurance.

Shared responsibility for risks

Facing up to the interdependent nature of digital risk is a challenge for any executive team in any industry. When business decision makers think about digital risk, it is imperative that they understand the interdependencies inherent in e-business operations and attack the issues in a coherent and integrated manner.

E-business models inherently combine enterprise-wide financial, technical and legal risks that can leave even the most savvy traditional risk managers perplexed and ill-equipped. Typically, neither the corporate risk manager nor the information security manager is capable of addressing the risks that the multi-faceted and multi-dimensional electronic business landscape weaves through all strategic and functional decisions. So corporate officials must juggle their traditional risk management responsibilities and their new e-business risk management responsibilities (see the table on page 5).

As noted above, corporate risk management functions are traditionally largely carried out within separate corporate silos, each with their own process and goals, and each speaking their own functional language. It's now widely accepted that this approach does not capture many of the risks faced by an organisation.

This is particularly true in 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 organisation's service level agreement (SLA). Whether as a customer receiving an SLA, or as a vendor providing 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, and is the policy that governs all operations, strategy, and tactical decisions between the organisation and each stakeholder relationship.

Tacit and explicit risks

Until now, digital risk management initiatives have largely been driven by technically oriented information security practitioners, who have attempted to control electronic environments using electronic means. But like all other management challenges, digital risk exposures and solutions will always begin and end within the rela-

tionships, expectations, communication and frailty of humans, not machines.

Creating an effective digital risk management environment requires senior managers and decision makers to elevate the tone of conversation from that of tactical, information security techno-speak to one of corporate governance and enterprise-wide accountability. When it comes to enterprise-wide e-business governance, stakeholder perceptions often dictate business realities. A key part of managing digital risk is managing stakeholder trust, expectations, communication and knowledge. If the organisation fails to communicate expectations and set the tone for managing relationships consistently, it puts its digital risk initiatives at risk of failure.

So the primary driver in digital risk conversations and initiatives must be business and stakeholder considerations. Technical security conversation cannot be the sole driving factor. Driven by a corporate culture where senior managers continually communicate and demonstrate norms of behaviour, expectations, motives and consequences, the business risk considerations and human risk interactions should always create the contextual reference point for subsequent technical risk decisions.

Another way to think about this shift in

focus is to think of it as a movement away from the management of explicit technical exposures and towards the management of the tacit socio-cultural elements of risk. What do these terms mean?

- **Explicit:** Objective, measurable and quantitative risks related to the technology, inventory, physical facilities and process aspects of the enterprise;

- **Tacit:** Subjective, qualitative risks related to socio-cultural factors such as organisational roles, relationships, and structures; formal and informal modes of communication; norms of behaviour; and unintended consequences.

To date, experience suggests that Pareto's 80/20 rule is in full effect in the digital risk world. While we have traditionally focused the majority of our efforts on the explicit technical exposures that in themselves cause only a small amount of damage, the tacit risk factors that contribute most to the severity of a given problem have received nearly no attention and go largely unchecked. It is failure to manage these tacit risks that allows relatively small failures or oversights in information security – explicit risks – to snowball into major business problems.

This inadequate attention to the tacit risk elements is the essence of the current flaws in digital risk management based on information security, and a significant paradigm shift must occur if we are to realise the potential of electronic commerce and e-business safely.

As we've already said, technology alone cannot fix the problem. The 'zero tolerance' information security strategies once popular in government environments, which played a large part in shaping today's digital risk culture are not appropriate for relationship-based businesses, or even achievable by them.

Stakeholders today are exposed to digital risk and always will be, regardless of the technical approaches taken. It is therefore senior management's job to determine

Scenario 2: Somebody else's problem

- A fast-growing online retailer relies on outsourced partners to provide the website's technical infrastructure. As the site accepts credit card payments over the Web, it demands encryption of each transaction during processing, but the hosting partner doesn't encrypt the credit card numbers and sensitive customer data once the transaction is complete.

- A 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 hacker, who demands 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 3: The weakest link

- An academic research centre has been chosen by an industrial giant to conduct top-secret trials for a breakthrough technology. On hearing of the opportunity, a corporate espionage professional, working for a rival, masquerades as a janitor and gains physical access to the centre'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 12 months, the agent secretly accesses the centre's systems from a remote location and passes sensitive information to the competitor.

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

how the organisation and its stakeholders perceive this exposure, and to manage the ongoing risks to the best of their ability. Tacit, unquantifiable risk factors such as reputation, marketability and stakeholder trust are powerful 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.

While the natural instinct in technology intensive environments is to focus on managing explicit technical risk, it is actually tacit risks to long-standing business relationships that demand senior managers' attention.

The importance of stakeholder relationships can never be overstated. It is safe to say that the manner in which an organisation protects its most valued stakeholders is a primary indicator of that organisation'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 organisation's more quantifiable explicit risks such as credit, liquidity and profitability.

Digital risk reaches farther

The importance of stakeholder management when dealing with risk is not unique to digital risk. Many famous risk management disasters are more the result of stakeholder disillusion than of the actual risk 'event' – a small loss can suggest that management doesn't know what it's doing, and lead to a broadly based sell-off by investors.

Where digital risk management differs from other varieties of risk management, though, is that there is, in principle (and sometimes in practice), no upper boundary on the potential stakeholders in an e-business operation. That means the potential commercial exposure and loss of goodwill

A. Inter-disciplinary digital risk management

Decision maker	Traditional risk responsibilities	Digital risk responsibilities
Board of directors	Strategic corporate governance	Service level agreements (SLAs); enterprise-wide due diligence
Chief executive officer	Market opportunity; corporate execution; communicate internal expectations; leadership by example; revenue	SLAs; communicate external expectations; profitability
Chief legal counsel	Contract requirements; strategic planning; corporate ethics	SLAs; online liability; regulatory compliance
Chief financial officer	Corporate budget; balance sheet	SLAs; market capitalisation; access to capital
Chief risk officer	Internal insurance; internal physical facilities	SLAs; external insurance; enterprise risk; technical risk
Chief operations officer	Internal procedures; internal human resources; vendor/supplier pricing	SLAs; 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	SLAs; external systems; external networks; external users; external project management; vendor/supplier operations
Chief information security officer	Internal computer security; internal users/attackers	SLAs; external computer security; external users/attackers; physical security/facilities; corporate policy; training & education
Chief marketing officer	Market perception; public relations; branding	SLAs; stakeholder privacy

for stakeholders and customers in the network economy are unlike any seen in the past.

The capability of the Internet to connect individuals and organisations all over the world means that a given organisation can become responsible to an increasing number of stakeholders every day. While a traditional business risk such as 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.

If a company's network becomes a point of compromise for harm done to others, there will be consequential loss ramifications that spread far beyond the plausible boundaries of a traditional business loss.

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. It is not hard to envisage a scenario in which a single organisation could be blamed for being the source of a propagating threat.

What's more, digital risk exposures affect all organisations connected to the Internet,

regardless of how they use that connection, and regardless of whether or not they sell or transact directly with customers online. Potential risks include:

- **'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 or of harbouring legally sensitive, unprotected e-mail content;
- **Website exposures**, which can happen when a site becomes unavailable or is maliciously altered to include erroneous information; and
- **Data theft**, which involves insiders or outsiders stealing sensitive information and intellectual property.

Digital risk assessments must therefore address fiduciary accountability for all corporate stakeholders that may be affected, whether customers whose personal information is compromised or business partners whose networks are attacked via vulnerabilities in your system. And digital risk controls should begin with information security controls, not end with them. In the case of email, for example, good corporate culture should not only stop embarrassing internal memos coming to light, but stop them from

being written in the first place. And legal disclaimers can reduce much of the financial (if not the reputational) risks of spreading viruses.

Only the most obvious first steps have been taken in addressing most digital risks. Loss of trust between an organisation 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 safeguard the financial and technical security of its online relationships.

Creating competitive advantage

If digital risk management is to further the strategic goals of the organisation, its primary drivers must be sales and marketing, along with the quest to create competitive advantage. In the wake of the dotcom 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.

Regulations and codes of conduct such as those addressing privacy and security issues (such as HIPAA in the healthcare sector and Gramm-Leach-Bliley in financial services), make it 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 that are 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 towards 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: significant, long-term, financial loss; damaged digital assets; lawsuits and damaged reputations.

By now the message should be clear to all senior management teams seeking to safeguard their business' survival in the digital age. The dangerous new world of e-business comes with mind-numbing exposures that require dramatic new solutions. 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 the technical fixes needed to avert a single potentially disastrous event such as the Y2K problem, effective digital risk management is a 'best practices' process that never stops evolving. In order for today's e-businesses to survive, it is therefore mandatory that all organisations

adhere to best practices and proper planning, not just internally but also between interdependent trusted partners.

If current and future business models are to survive and achieve their financial objectives, corporate boards and senior leadership teams must be constantly vigilant in the quest for trust, stakeholder accountability, and proper corporate governance. Given 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 (rickdavis@digital-risk.com) is principal advisor at Atlanta-based risk management consultancy DigitalRisk Advisors. He was one of the original players in the digital risk insurance market and created the DigitalRisk ScoreCard Methodology. This article is adapted from a white paper available at: www.digital-risk.com

B. Insurance is mandatory

A COMPREHENSIVE insurance programme that covers major e-business exposures needs to be part of every organisation's digital risk management plan. Digital risk insurance helps to 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 defence 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

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 commercial general liability?

Coverage for major stakeholder groups?

Coverage for acts by internal and external parties?

Standard form vs. manuscript form?

sources, digital risk losses can cause significant downgrades in market valuation, lost business, damaged reputation,

and lost opportunity. An adequate insurance programme must be there to pick up the financial pieces. ■