June 11, 2001

An eRisk Primer: Executive Summary

ECOMMERCE: GREAT RISK, GREAT REWARD

Xenia Ley Parker

*The following is an excerpt from **An eRisk Primer** by Xenia Ley Parker.*

Hard to ignore

Although using Internet as a primary way to do business was thought too risky a few short years ago, people are so comfortable with the concept that electronic commerce (EC) is ubiquitous. Today's children don't even know what the world was like before computers. One of the fastest growing segments of the new user population is "seniors," demonstrating that technology has penetrated all age layers of society. Current EC activity is Internet-based, with the World Wide Web so widely used in business to consumer (B2C) transactions that credit card companies are racing to put out emoney cards and secured products with guarantees to any still-wary consumers that their transactions will be safe.

EC has an open technology infrastructure and an ever-increasing extent to which its components are digitized, with "digital" used more often as the term for EC products instead of electronic. Different types of EC place different demands on those components. Players, products/services, and transactions can be physical, as in ordering products over the Internet, or purely digital, as in downloading software, music or ebooks, or any combination of the two.

Using the free Internet unleashed EC's potential for business-to-business (B2B) as well as B2C transactions. EC is the enabling technology for competitive advantage as businesses connect legacy and other back office systems through Intranets or Extranets, then further linking those systems to those of new alliances and partnerships. A fast-paced area, from five to seven times larger than B2C, industry analysts' predictions for the B2B market range between $1.3 and 2.5 trillion dollars by 2003, up to $5.7 trillion by 2004. The B2C market is growing as fast, but with its typically smaller transaction size, is expected over $100 billion by 2004. A perhaps more startling statistic from the Strategis Group in Washington, as reported in a Sunday supplement to the Bergen Record in October 2000, is that automobile-based subscriptions to Internet services, at 1.2 million in 2000, will soar to 16 million in 2004.

Considering this explosive growth, it is easy to see why many organizations are playing catch-up to reach the consumer market. Features of the Internet and EC activities determine characteristics of the "e-Conomy" a global, digital, high velocity market economy. Worldwide expansion means reforming old markets and exploring new ones as the market becomes more dynamic, reflecting real-time supply/demand changes. Soon the world of business will become ebusiness, and perhaps at some point the "e" will go away. As Jack Welch, CEO of GE said recently: "This is not some activity outside the business, this is the business."

Impact

What does the phenomenon of the Web and emerging Internet technologies really mean to the enterprise? Great opportunity, great risk. Despite all the hype, as EC becomes commonplace, conducting ebusiness can create real exposures. Changes in economic, industrial, operating and regulatory conditions mean new problems. Hoards of malefactors are out there in cyberspace, seeking systems to misuse. New viruses challenge information systems; keeping virus-scanning

software current is even more difficult, with updates needed almost daily. Bugs or errors in immature systems threaten survivability and profitability of EC business.

The Internet puts EC businesses at greater risk:

1. Interconnectivity and openness make attacks and unauthorized access easier
2. Digitization adds special problems for digital information and transactions
3. Globalization and virtualization enlarge the scale and scope of risks
4. Computing power, connectivity and speed can spread viruses, allow system break-ins or compound errors in seconds, possibly affecting interconnected parties
5. Ever-changing environment changes risks so solutions may lose effectiveness
6. Hacking techniques never stop evolving, so new tools mean new vulnerabilities

At the Critical Infrastructure Assurance Conference in September 2000, New York's US Senator Charles E. Schumer, talked about Internet risks as a national security issue. He covered a range of threats, including the growing ability for foreign nationals and governments to wage "Net War". While we are building traditional defenses against physical threats, the real threat is being ignored. Calling for a partnership with the private sector to address vulnerabilities at the cyber level, he said that government couldn't do it alone.

Hard to control

Because the Internet was not designed for business, it's not surprising that it was not designed to control and manage business risks. For over two decades its use was restricted to researchers for shared computing/communications. All that changed with the user-friendly, graphical World Wide Web. A network of networks, the Internet's major characteristic is openness, due to common standards and protocols for system interaction, allowing client and server applications to function independent of hardware or operating systems. Absent such open protocols and standards, proprietary systems cannot interact without special interfaces. This common technology ground allows user applications to be mixed and matched with relative ease. Conducting financial and other transactions over the Internet is taking over. Moving beyond secured technologies like Electronic Data Interchange (EDI) over proprietary value added networks (VANs) into areas such as market research, knowledge management, product selection, production, ordering, payment, delivery, and more, EC is expected to replace many of the more traditional methods altogether.

Before the Internet, the information infrastructure was primarily proprietary. Resource sharing, distribution, scalability, concurrency, transparency and fault-tolerance are features of Internet distributed client/server style computing. These very characteristics, in many cases, are the reason for dramatically increased risks. Hackers and crackers--who auditors used to stress were not as big a threat as a company's internal users—have been able to increase their activities due to businesses using the Internet with technology that has security holes, and unprotected back office systems. The 1999 FBI/CSI (Computer Security Institute) Information Security survey found the threats are now equal, not because internal threats were lower, but that external ones had grown so high.

Anyone can set up shop on the Web, configuring computers to use TCP/IP and connect over the Internet. Corporate Intranets and Extranets use the underlying Internet protocol, TCP/IP, to package proprietary protocol-based messages and transmit them to other remote networks, as do virtual private networks (VPN). However, in part due to weaknesses as a result of its origins in the UNIX operating system, TCP/IP is inherently insecure. Thus, reliability of basic communications over the Internet is questionable, absent additional protective technologies.

Add in the technology risk due to the Internet itself. Along with the staggering increase in use over

the last decade came Internet congestion, due to a lack of resource allocation mechanisms based on accepted rationales. This problem is hard to solve. A victim of its own success, current IPv4 is running out of its 32-bit IP addresses, as the supply of .com names is similarly being exhausted. IPv6 expands the possibilities with a seemingly unlimited 128-bit address space, and seven new domain names were just announced in November 2000.

As each host becomes a new link in the seemingly endless Internet chain, each is also subject to the possibility of huge problems that can occur as owned sites crash, or as some believe, whole segments of the Internet itself might collapse. Then what will happen regarding survivability of businesses that have moved everything onto this unregulated public network?

From a content perspective, the growing risks include business information disclosure, misuse of intellectual property, and violation of copyrights, trademark infringement, libelous statements on web sites, privacy violations, reputation damage, and more. Add in the 'usual' technology risks of errors due to human or system problems, and deliberate sabotage like denial of service attacks, and you have a good idea of the problems to which an organization is exposed. Current insurance policies, in almost all cases, are inadequate to cover the potentially disastrous losses.

From an audit perspective, it's important to note that using the 'free' Internet is purchased at a price - lost control afforded by proprietary network protections, agreed-upon formats, and VAN service level agreements. New application service providers (ASPs) and Internet Service Providers (ISP's) are providing many of the Web development and hosting tasks, but also raising questions about reliability, availability, authentication, and security.

Traditional assurance services are being re-vamped to meet the new challenges. As a body of data is developed, these services, along with improvements in firewalls and intelligence being built into routers, third party certifications, trusted certificate authorities, digital signatures, and encryption using public key infrastructure (PKI) and the like will all combine to improve controls over EC. Applying business and control requirements during development will enable better security as the Internet is used for an ever-wider range of transactions.

Strategy

In EC, commerce fundamentals remain--players, products/services, transactions, and information infrastructure--but how they interact and are controlled changes, sometimes dramatically. Internal auditors need to understand how these truly paperless business events affect internal controls.

EC business strategy has to be re-created constantly in the ever-evolving world of cyberspace. For success, a new paradigm--spelled out in a long range plan, no matter how many times it needs to be updated--is required to exploit EC's potential. For each enterprise, questions exist about how to develop the new business models, market strategy, what to do first, what to do next, and how to proceed. The answers are not always intuitive, and may not be reached the first time out. An on-going, iterative innovation process must co-exist with strategy and technology initiatives for EC to reach fruition.

This monograph provides an overview of the key issues in EC. These are described in the following sections: Part One is an Introduction, covering EC background and potential; Part Two focuses on the impact on the enterprise, including strategic and business risks; Part Three focuses on the technology, related risks and controls; and Part Four focuses on risk assessment, the audit and assurance role, including the changes in system development warranted by EC.