

Rethinking Your Business Protection

– Linking Critical Components

A coordinated, robust business protection plan is essential for both corporate governance and productivity. Protecting business components such as intellectual property, information flow and all aspects of the supply chain is vital to maintaining customer and stakeholder confidence. Rethinking your business protection policy and infusing information technology security and supply chain risk into corporate philosophy ensures they will be part of the overall business planning strategies. Frequently they are overlooked, leaving corporations at risk for unforeseen events.

The American Society for Industrial Security (ASIS) Alexandria, VA, "*Chief Security Officer (CSO) Guideline*" released November 24, 2003 stated, "Today's business risk environments have become increasingly more severe, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business. Boards of Directors, shareholders, key stakeholders, and the public correctly expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functions to mitigate or reduce those risks. In addition, there is an expectation that management will respond in a highly effective manner flawlessly to those events and incidents that threaten the assets of the organization. A proactive strategy for mitigation of the risk of loss ultimately provides a positive impact to profitability and is an organizational governance responsibility of senior management and governing boards."

IT Security Awareness

IT security benefited from the overall increased security awareness that resulted after September 11, 2001 and the \$2.4 billion clean-up costs from the Nimda and Code Red computer worms in 2001. In the wake of these devastating physical attacks and cyber exploits, many corporations began to seriously look at their existing security plans and then dedicate resources to both understanding new threats and their procedures and programs to defend against them. There has been a near daily onslaught of viruses, worms, Trojan horse programs, identity theft scams and the ever increasing volumes of unwanted spam e-mail reaching corporations.

Legislation such as Graham-Leach-Bliley, the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes Oxley each contain security, internal controls and privacy components which prompted additional scrutiny of security controls and raised security challenges to the CEO and Board level.

A substantial improvement has been seen during these reassessments. Corporations began for the first time to look seriously at more than just external

vulnerabilities and threats. Many organizations came to realize that IT security risks can (and do) also originate from internal trusted users.

Room for Improvement in IT Security

Although IT security has seen an increase in awareness and management focus during the last three years, there are still some substantial areas for improvement.

In many cases, IT Security still remains detached from overall security planning within Corporations. A large number of companies have moved or are moving towards a consolidated “ownership” for the majority of security issues by the creation of Chief Security Officer/Chief Information Security Officer positions. Frequently, though, critical security support roles and responsibilities remain delegated to numerous departments within the corporation. Prime examples would include physical security and business continuity support services which may still be the responsibility of Facilities Management or Human Resources, or primary responsibility for Sarbanes-Oxley Section 404 compliance being tasked to the Legal or Compliance offices. The complexity of today’s business environment and the increasing reliance on IT infrastructure necessitates tight coordination of *all* security related roles within the Corporation with an objective of bringing together all departments with security responsibilities for discussions of staff coordination, resource sharing and viewing risk from different points of view. This can be accomplished by creation of a Security Steering Committee or Security Council with Management Team participation or oversight. The Corporation’s Security Operations Plan should be expanded to reflect a wider range of security challenges and coordinated methods approved by the Corporation’s Management to address these challenges. According to research conducted by security firm Vormetric, by November 2003 more than half of the Fortune 500 had formally appointed a Chief Security Officer or Chief Information Security Officer. By comparison, in July 2004 few members of the Fortune 500 have taken the follow-on step of creating a Steering Committee or Security Council.

Implementing New Technologies Is Not Sole Answer

Network security issues, primarily the proliferation of viruses, worms and other malware and denial of service attacks, have continued to plague corporations that rely on their IT networks for business operations. Defenses against these threats are clearly reflected in the budgets of nearly all corporations. According to a June 2004 survey by the Meta Group, IT security spending now accounts for an average of 4% of all IT spending by Global 2000 companies. Unfortunately, a large number of companies still see these challenges as being overcome by simply implementing new security technologies. Technologies and next generation security products are simply tools in the toolbox – necessary to get the job done, but not without master craftsmen who know how to best use them.

Effective network security begins with people – skilled technicians, superior security management, and most importantly, well informed users who know it's not acceptable to do certain things on the Company network. Coupled with well written and easy to understand policies, security education and training can be among the best investments of security dollars.

Being Lucky Is Not Enough

A declining but still substantial number of Corporate Management Teams believe that they are simply not at risk – primarily because they have been lucky enough to not have had a major incident. A growing body of evidence confirms that IT related attacks remain a major source of risk for business operations. The Computer Security Institute's 2004 Computer Crime and Security Survey, conducted with the participation of the U.S. Federal Bureau of Investigation, revealed that the threat of computer crime and information security breaches remains a real factor affecting today's businesses. The annual survey, the ninth conducted by CSI/FBI, included responses from 494 organizations that reported losses of more than \$141 million. The most expensive attacks against these organizations were Denial of Service (DoS) followed by theft of proprietary information. A survey conducted in April 2004 by Chief Security Officer (CSO) magazine with cooperation from the US Secret Service and security experts at Carnegie Mellon University found that cyber attacks cost businesses an estimated \$666 million in 2003.

Are You Ready?

Certainly with business dedicating such substantial financial resources and the potential and magnitude for loss, the threat is considered credible enough to warrant the effort to orchestrate a high level enterprise approach.

Improvements in IT security during the last three years have in many cases included establishment of professional security teams, upgrades of perimeter and desktop security products and/or creation of enterprise wide security programs and policies. However, effective security requires constant review and sustainability. Procedures and tools must be reviewed on a continual basis to ensure that they are still credible in a rapidly changing threatscape.

This became painfully clear on January 25, 2003 when the Slammer worm caused worldwide disruptions in network connectivity and ultimately more than \$2 billion in damages and clean-up. Although many corporations had instituted anti-virus and anti-worm countermeasures, they were not prepared for the exploit of a relatively obscure vulnerability in a popular server software package and the speed at which the worm spread. The worm caused flight disruptions at a major airline's East Coast hub, shut down corporate and commercial e-mail systems and even took a network of automated teller machines off-line. Many organizations admitted that they knew of the vulnerability but had neglected to

patch the systems and had no procedures and/or patch verification measures in place.

One way to avoid complacency is to seek trusted third parties to assess the security of the organization and, if warranted, conduct real world penetration testing to ensure that best practices for IT security have been fully considered. In addressing sustainability of key business support systems in the event of a crisis, the security program, though often overlooked, must also be considered often as was the case with the Slammer worm.

Supply Chain Risk: Increasing Awareness

Threats to the continuation of an enterprise exist in other quarters. One substantial area of business protection remains nearly untouched - Supply Chain Risk.

Until very recently, the term Supply Chain was usually defined in rather simplistic terms, addressing only the “upstream” raw materials for a production operation. But today’s definition is quickly evolving to include a wider range of activities and a broader array of increasingly complex business models. A more appropriate definition of Supply Chain could easily be “...all materials, information, facilities, equipment, people, finance, and logistics to produce, store, transport, and sell goods or services”. Supply Chain analysis now takes into account business sectors other than manufacturing and looks at *all* key steps in a sector’s operations. New unforeseen elements are adding complexity to Supply Chain planning. For example, a product such as vehicle tires or Freon may need to be closely tracked even beyond the point of sale to account for the continued cost of disposal or recycling based on environmental or social issues. Likewise, a product may have “post use” value such as precious metal recovery from older electronics.

Supply Chain’s Impact on Corporate Profits

The increasing complexity of the Supply Chain has resulted in increased risk to many corporations. There is a growing body of evidence with numerous examples of instances where Supply Chain related issues had a significant negative impact on corporate profits. A joint study performed by Georgia Institute of Technology and the University of Western Ontario, revealed that supply chain disruptions can directly impact corporate stock prices by nearly 9%, with losses mounting to 20% months after the event.

Supply Chain risk and the potential for major losses made world headlines in March 2000. A Philips semiconductor plant in Albuquerque, New Mexico that supplied Nokia and its competitor Ericsson with specialized microchips for mobile phones was damaged by fire after a lightning strike. These chips were critical

components and not available from other sources. Nokia had a history of close communication and supply chain monitoring of its suppliers that allowed them to respond rapidly to the issue. According to information reported in the press, Erickson was not even aware of the event for several days. Nokia's business processes and contingency planning paid off. Shortly after learning of the fire Nokia made rapid changes to its designs, substituted other similar components and increased its market share of the rapidly growing mobile phone market. Ericsson reported both short and long range production shortfalls and posted a \$1.7 billion loss in that year's handset division.

Natural catastrophes can clearly impact the Supply Chain. But increases in supply chain risk can be traced to many man-made sources, including "just-in-time" delivery efforts, intercontinental and global procurement, third party outsourcing, increased border security controls, cost reduction efforts and ever increasing client expectations. These factors are driving progressive business planners to incorporate Supply Chain issues into their short and long range risk planning.

Even minor disruptions in a company's supply chain can have devastating consequences. Wal-Mart's strong market position has allowed the company to have particular influence over their major suppliers. Wal-Mart often requires commitments on delivery, pricing, and compliance with their processes. Vendors are required to meet Wal-Mart demands or face significant loss of market share. Vendors whose shipping methods break down even for a short period of time may face the loss of preferred vendor status. The potential loss of Wal-Mart as a customer can drive a small or even modest sized company from the market. Like IT Security, many companies have or plan to leverage technology to solve their supply related problems. In the case of Wal-Mart, this has included very specialized electronic order systems, customized product packaging and markings, and a recent mandate to apply radio frequency identification (RFID). This new reliance on electronic systems, however, presents its own exposures as the high degree of specialization enhances the impact of Information Technology disruptions and IT Security issues.

As noted above, IT security has elevated its level of visibility in the corporate hierarchy and has been afforded increased resources due to the magnitude and frequency of actual events that impact business operations. Although Supply chain disruptions are much less frequent than IT security incidents, their impact can be extreme. Natural and man-made factors that impact the increasingly complex Supply Chain may now raise the occurrence of actual loss and concurrently raise the general awareness of Supply Chain Risk. However, management focus on Supply Chain Risk is still in its infancy.

Supply Chain Risk Lies Below Corporate Radar

The management reporting structure for Supply Chain risk clearly lags behind the level now found in IT Security. Senior managers or directors are rarely directly responsible for Supply Chain issues and certainly not for supply chain risk. Supply chain issues are normally the responsibility of manufacturing managers who typically hold mid to upper level positions and a wide range of responsibilities to go with that role. In some corporations, Supply chain concerns may very well be delegated even further from the levels of strategic decision making. The creation of Chief Risk Officers in some corporations is a clearly positive trend, but Supply Chain risk still lies well below the radar screen of many corporations.

Sarbanes Oxley and Supply Chain

Supply Chain risk and its potential impact on corporate profits have recently caught the regulator's eye. Some enlightened agencies and auditors now consider supply chain risk to fall under the auspices of the Sarbanes Oxley Act. Other government regulations both assist and complicate the supply chain risk issues. For example, regulated industries such as pharmaceutical, communications and aviation have various government agencies (FDA, FCC, FAA) that strive for product safety but at the same time often have conflicting requirements to assure continued supply chain reliability. Recently enacted port security programs initiated by the department of Homeland Security have tightened up on vessels in USA ports but these border controls can slow or even stop entire operations. A single incident can shut down an entire port resulting in serious downstream difficulties for multiple companies. This occurred in July of 2004 when aggressive comments made by a ship captain resulted in disruptions at the Port of Philadelphia.

IT Security and Supply Chain Risk planning now constitute established and growing pillars of an effective Business Protection plan for corporations of all sizes. Coupled with a robust Business Continuity/Disaster Recovery effort, IT Security and Supply Chain risk planning go well beyond the "what if?" and lead to effective and tested methods to quickly recover from a wide range of profit draining mishaps.

Successful Solutions

Virtual Corporation Offers a Comprehensive Look

An innovative, coordinated business strategy links risk identification and asset protection to assure long term customer satisfaction while simultaneously driving profits. These efforts complement efficient business practices resulting not only in protection, but return on investment. Proven methodologies and tools provide business planners with quality insights and solutions.

Virtual Corporation is a world leader in Business Continuity and Disaster Recovery planning services and has provided expert assistance to numerous major corporations since 1994. Virtual can uniquely leverage its exceptional expertise and proven methodologies in Business Continuity Consulting to ensure that every program is sustainable, well documented and effective. Virtual's combined expertise in IT Security, Supply Chain Risk and Business Continuity ensures the development of a comprehensive business protection program or a stand-alone implementation in a single practice area.

Virtual's services include Information Technology Security, Supply Chain Risk Management and Business Continuity Services to provide a comprehensive and unique approach to identify and mitigate risks across an entire corporation.

Virtual Corporation, Flanders, NJ • 973-927-5454 • www.virtual-corp.net
Winner of PMI – NJ Chapter – “Project of the Year Award 2004”

.