BAUER
COLLEGE OF BUSINESS
UNIVERSITY of HOUSTON

ISRC Notes—October 2002

Security, Privacy, and Business Continuity Trends

Prepared by: Andrew Schwarz
under the supervision of Dr. Blake Ives

Based on a presentation by Mr. Al Decker, EDS

With the one year anniversary of 9-11, firms are reflecting upon how the world has changed the way in which they do business. Al Decker discussed the 9-11 legacy, arguing that businesses must implement a solid business continuity plan that encompasses the physical, cyber, intellectual, and financial areas of the firm while balances the privacy and security concerns of the individual. He concludes with six keys to success.

The Global Marketplace

While it is not new news, it is clear that the world is increasingly moving toward becoming a borderless society. Consider a few trends:

- Air travel is now cheaper and faster than ever before, enabling the average consumer to go anywhere in the world
- The evolution of the global community (through the United Nations and the WTO) and free trade zones (WTO, NAFTA, and the EU) has loosened country borders, enable free trade, and enabled global commerce
- Global consolidation has forced firms to focus upon competition from all areas of the world

Yet, this borderless society is not without challenges. In a post 9-11 world, security concerns are heightened, with enterprises needing to prepare for the "strong possibility" (Gartner 2001) of further attacks, including the possibility of cyber-terrorism. These threats have moved business continuity to the front of the mind of most executives.

One realization that has come out of 9-11 is the awareness by all firms that they are potential targets for disruptive threats. Infrastructure companies such as oil and gas, telecommunications, transportation, and utilities are fundamental to the economy and massive disruptions would occur if a business continuity event occurred. Core producers such as automotive makers, consumer product manufacturers, healthcare providers, high tech companies, pharmaceuticals, and process industries are significant participants in the GDP and are highly interconnected with other aspects of the economy; one catastrophe in core producing firms will cause ripples throughout the entire country. Firms that operate in highly visible industries, such as entertainment, gaming, leisure, the media, or sports are highly interactive with consumers and present the highest risk to end consumer safety. The net result: all firms must consider business continuity.

Beyond the business overall, IT must recognize the increasing threats and respond as well. While this may seem intuitive, several post 9-11 studies have found that business have not yet planned for the threats of the new world order:

- A study of 459 CIOs by Ernst & Young International found that just 53% of companies had business continuity plans, and less than half had IT security awareness and training programs for employees (Verton, 2002).

- Researchers at Gartner estimated last year that 60% of U.S. businesses - particularly those that rely heavily on their IT infrastructures - haven't spent enough on business continuity or disaster recovery to guarantee their own survival (Johnson, 2002)
- A poll by *CSO* magazine found that 59% of 1,000 chief security officers said electronic attacks pose a much bigger concern to their companies than physical ones (Johnson, 2002)

To prepare a business continuity plan, the first step is to understand the types of challenges facing post 9-11 firms today.

Overview of Today's Key Challenges

According to Al Decker, there are nine key challenges facing corporations today:

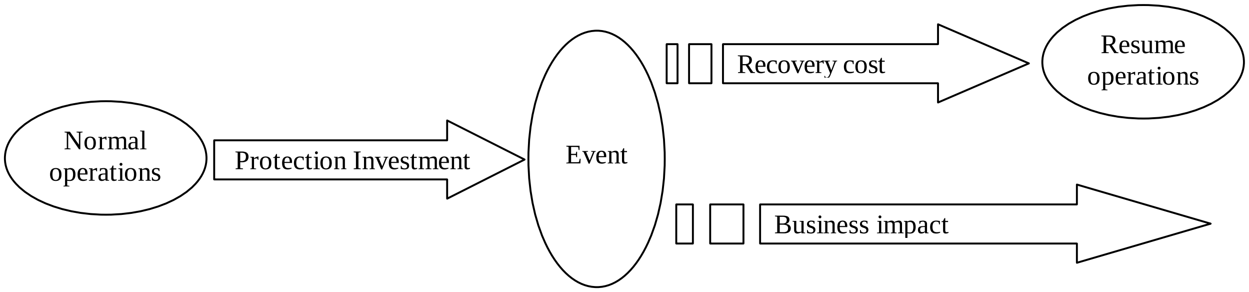
1. Cyber-terrorism
2. Physical security
3. Business continuity
4. Cross-border security
5. Disruption of business/supply chain
6. Fraud and cyber crime
7. Privacy issues
8. Regulatory compliance
9. Preserving trust in the marketplace

The key to handling these challenges is creating business continuity plans that manage the potential risk of occurrence. To accomplish this, executives must balance between costs, the likelihood of occurrence, and the potential business impact.

The Balancing Act

As firms engage in normal operations, they invest in certain protection mechanisms, incurring ongoing incremental expenses as they attempt to prevent disruptive events from occurring, prepare for the event, and develop an appropriate plan and response. However, this investment is balanced against the likelihood of the event occurring, the recovery cost to bring the firm back to normal operations, and the business impact. When assessing the recovery cost, firms must examine the performance during recovery, the time it will take to recover, and the scope of the recovery and the business impact must include lost revenue, customer/partner confidence, and regulatory/legal issues.

The figure below depicts the balancing act for firms.



For further information about this balancing act, we refer the reader to the 2000 ISRC White Paper entitled "Planning and Managing Information Technology in a Disruptive Environment" and the ISRC presentation on IS Disaster Planning and Recovery, held in February 2002.

The result of this balancing act is the creation of a business continuity plan.

An Integrated Business Continuity Plan

According to Al Decker, there are three essential elements to a business continuity plan: people, processes, and technology. Each of these constituents must be included in an integrated approach that crosses the four essential (physical, cyber, intellectual, and financial) areas of a plan. Each of the areas will now be considered in turn.

The physical area of a business continuity plan should include the people and physical facilities and equipment needed to locate, acquire, produce, transport, and deliver critical resources. Within EDS, physical area planning includes:

- The use of active asset tracking, or transponder technology used to locate and track people and equipment within the workspace
- A fragmented employee authentication environment to ensure secured access to entries, perimeters, and computer systems
- The use of biometrics to create a secured environment for the authentication, identification, and access of computer systems (For more information on biometrics, we refer our reader to our recent Future Technology Briefing on biometric technologies)

The intellectual area of a business continuity plan should include the knowledge and experiences of the employees needed to continue the creation of products and strategies. Within EDS, digital learning is protected using the Cyber Security Institute.

The cyber area of a business continuity plan includes how to protect the logical and physical aspects of information technology including the back office, CRM, wireless, and mobile technology. Some examples include:

- A solid security architecture that takes into account internal and external inputs and protects investments in computing hardware and software

- A fully-encompassing security strategy that includes the domains of network/infrastructure security, platform security, and application and data security
- A specific focus upon applications that are protected through access management and network identity

The financial area of a business continuity plan includes how to ensure supply chain continuity, policies, and the brand.

The Key to Success

For a business continuity plan to be successful and deliver value, it must create trust, ensure the privacy of individuals, and provide security. While individuals are increasingly sympathetic toward protecting their firms, they also fear losing their own privacy and security. Thus, technologies such as biometrics and asset tracking must take into account the rights of individuals as well.

With these recognitions in mind, Mr. Decker offers six suggestions:

1. You must develop, test, and implement the plans with periodic updates. With no test plan, 40% of all businesses fail immediately and only 8% survive in 5 years
2. You must recognize the signals that failure is occurring
3. You must be trained on how to react
4. You must design business processes with interruptions in mind
5. You must develop alternatives and redundancy when appropriate
6. You must have business and technical subject matter experts involved and committed

Conclusions

The post 9-11 world requires businesses to seriously consider new threats, while balancing security and privacy concerns. If firms recognize the six keys suggested by Al Decker, they are more likely to create a successful business continuity plan and be one of the 53% of firms prepared for the threats of the new world order.

For More Information

Johnson, Maryfran (2002). "Once Again, IT Responds." *Computerworld*, September 9, 2002. http://www.computerworld.com/securitytopics/security/story/0,10801,74090,00.html.

Verton, Dan (2002). "Sept. 11 lessons drive key aspects of Bush cyberdefense plan." *Computerworld*, September 19, 2002. http://www.computerworld.com/governmenttopics/government/story/0,10801,74359,00.html

Biometric future technology briefing: http://www.uhisrc.com/FTB/Security/Securityindex.htm.