Which Comes First, Business Continuity or Security?

Mary L. Carrido, President & CEO
MLC & Associates, Inc.

I am frequently asked which comes first, Business Continuity or Security. There are proponents from each industry that argue for one over the other. From my perspective, a broad strategic view is needed to fully address the issue. What I have found is that most practitioners start with a narrow tactical approach and spread out from there. Also, there is also a lack of common understanding regarding the terms Business Continuity and Security.

In my opinion, Business Continuity is a program that includes multiple components:

- An Emergency Operations Center/Crisis Management Team (executive decision-making and control)
- Emergency Response (people issues)
- Business Resumption (process issues)
- Information Technology (technology issues)
- Disaster Recovery (facility issues)

Furthermore, tools and support mechanisms for Business Continuity must include a current Business Impact Analysis and Risk Assessment, ongoing training, and simulations. The entire program is managed by a Business Continuity Office (at minimum a Director or Vice President).

A comprehensive Security program is similar in that includes People, Processes, Technology, and Facilities and in response to an incident. The difference between Business Continuity and Security is that the Security program is managed by a Chief Information Security Office or CISO and the primary control point is the Network Operations Center (NOC) or similar IT focused group and location rather than an EOC.

In both Business Continuity and Security programs if any of these four components (People, Processes, Technology, and Facilities) are missing or de-emphasized, then there will be gaps that can lead to serious failures.

People – Knowledge, skills, and capability form the basis for the success of any organization. For Business Continuity, people provide the means for ensuring the ongoing viability of the organization. People are assets that provide value to support the ongoing continuity of operations. For Security, people are also the basis for the organization but are often segregated into two major groups (1) monitors and (2) users. The monitors are analogous to the organization's "police force" that support and maintain controls in order to safeguard the organization. Users on the other hand are the "citizens" that are expected to follow the "law" and conform to a set of established rules.

Processes – Processes can be thought of in terms of operating procedures, policies, standards, and established organizational norms. Both Business Continuity and Security incorporate normal and contingency processes into their programs. The main difference here is that for Business Continuity processes are the object of recovery where as for Security processes are used to control behavior and limit risks.

Technology – In Business Continuity technology is often the object of recovering from an unplanned event and also provides a means for maintaining ongoing operations. In Security, technology is generally the focal point of the program. Technology is a two-edged sword that provides the means for protection as well as disruption of services.

Facilities – In Business Continuity facilities is a critical component since most organizations depend on facilities in order to maintain or resume normal operations. In Security, Facilities are also a key requirement but are also a focus for developing preventive controls to limit access and reduce the level of threat.

The case for Security as the overall driver that includes Business Continuity stems from the fact that physical and logical security are essential to the ongoing operation of organizations. Security is a "gatekeeper" that protects the organization from internal and external threats. It is argued that Security is so fundamental that it encompasses Business Continuity in terms of backup procedures and practices as well as recovery planning. From this standpoint, Security is the "big box" that holds the various components that are essential for ongoing operations. These smaller components include Business Continuity as well as physical security (premises security), secure data storage, encryption, access controls, wired and wireless security, security protocols, practices, and procedures.

This emphasis on the fundamental nature of security leads to a "Security First" attitude. At the extreme, all decisions include a consideration of security and all projects or even the strategic direction of the entire organization can be impacted.

The risk of a "Security First" approach is that so much emphasis is placed on security that the ability of the organization to carry out day-to-day tasks is hindered. For example, a "Security First" mandate may refuse to allow remote access services to the organization's systems. While this does provide a means for reducing the threat of an outside attacker gaining entry into the network, it limits an organization's flexibility in increasing employee productivity and greatly reduces the options for Business Continuity. While this is an extreme example, I have worked with some organizations that take this stand to one degree or another. In general, most large organizations have reached a compromise position wherein a secure VPN is provided that includes multi-level security controls.

The case for Business Continuity as the umbrella under which Security practices reside is made by numerous practitioners in the Business Continuity field. The logic here is that a true Business Continuity approach is an enabler that is designed to safeguard the ongoing ability of an organization to operate in terms the collaborative blending of People, Processes, Technology, and Facilities. Consequently, Security is one of the

basic requirements for the delivery of value. In this case, Security provides “means” value rather than “ends” value. In other words, Security is necessary and assists the organization in providing its “product” (e.g., goods and/or services) to end users but is not the driving criteria.

One of the risks here in terms of Security is that not enough attention is placed on securing the organization and some controls may be modified or limited to allow for greater flexibility in terms of Business Continuity capabilities. For example, a “Business Continuity First” viewpoint may require the on-line transmittal of confidential company data from one site to an online backup repository located in another geographic area. While off-site storage is a good practice and a necessary component of any Business Continuity Program, security vulnerabilities can be exploited as data travels through the public network or even via private networks. In order to reduce this risk, most organizations that transmit confidential data utilize various sets of controls including encryption, strong passwords, and certificates to authenticate valid users.

So what does come first, Business Continuity or Security? The answer is not immediately clear. It is often the case that the culture of the organization and the approach used. An organization that actively promotes Security but provides less than full support to Business Continuity will find that Security will drive decisions, standards, and practices. On the other hand, an organization that promotes Business Continuity but provides less than optimal support to Security will find that Business Continuity is the logical driver.

After many years of experience and considering numerous diverse positions on the topic, in my opinion the ideal is to take a holistic approach that incorporates both Business Continuity and Security. If this level of maturity is reached, I believe that Business Continuity is the main strategic umbrella and Security is one of the fundamental requirements for a truly comprehensive approach. This is not to say that Security takes a subservient position or is in any way lessened in importance. In fact, Security is a cornerstone of any best practices or world class Business Continuity

Program and is integral to all organizations. What it does say is that there is a need to bring all stakeholders together and reach a common understanding in order to make the combination of Business Continuity and Security efforts successful on an ongoing basis.

****