SIEMENS

Technical Article

Infrastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), August 28, 2012

Protecting data – a key element of business continuity

By Urs Iten, Market Manager Data Centers, Siemens Building Technologies

While establishing company-wide safety and security policies enterprises need to retain agility and flexibility on the ground to cope with location-specific risks and operational goals in relation to their buildings, assets and employees. In the modern world data is at the heart of business. As such, business continuity and disaster recovery plans often originate from a corporate data center position since an incident here has such far-reaching consequences. Central to this is the provision of effective safety and security. In a data center context, security is primarily focused on protection of the integrity and privacy of data. However, physical security measures are also key, as is fire safety, if that data is to be protected from both external and internal threats.

There are many threats to a corporation's business continuity but IT is at the top of the list. Many of the business interruptions in a data center – an estimated 75 percent – are caused by human intervention, either accidental or malicious. These interruptions could be symptomatic of inadequate access policies or technologies or, if they are in place, to low adherence or acceptance of them. It is important to understand the reasons before the situation can be improved. It could be that the policies are unsuitable for the day-to-day business, or that an employee culture exists where risk is ignored or misunderstood.
According to the well-respected German industrial insurer and security systems consultant HDI-Gerling, manufacturers operating a 'just-in-time' supply service often suffer a complete breakdown in their ability to carry on operating within 24 hours of losing all their data processing function. Banks and similar commercial organizations statistically last just one and a half days longer.
For many institutions such as banks and healthcare facilities, the non-compliance issues of poor access management are clear. But it goes beyond the physical threats, contributing to the potential for data to be deleted, stolen or manipulated. In a pharmaceutical business, for example, manipulation of research data could be catastrophic, from delays in production to quality issues

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

Reference number: TA ICBT201207e Business Continuity.doc

leading to product recalls. Regulation and compliance rank among the top risks, with the highest rankings in the banking and life science sectors. Such events can severely impact on a company's reputation, its long term innovation capability and, of course, its revenues.

Integrating systems

Electronic security and safety solutions can help protect a data center and in doing so protect an organization's application availability, its confidentiality, its integrity and, ultimately, its ability to function. As already indicated, access control policies are fundamental and systems need to be in place through which violations can be identified and reported. Enterprise access control solutions, combined with dedicated access rights, help to ensure that people have physical access to the right areas across multiple sites, including the data center. Integrating these systems with visitor management systems can also help with on-site vendor and contractor management, a particular for data centers with their sometimes complex maintenance schedules due to 24x7 operations. Integration of security and safety measures is, in fact, one of the prime methods of enhancing business continuity through protection of business-critical data. Central management of operational systems provides a more efficient and dynamic use of resources, focusing them when and where they are needed. Fire safety and security can be integrated through danger management stations. This allows for centralized supervision and alarm handling from a number of different sources, including fire detection, video surveillance, access control and intrusion detection.
The benefits of integrating fire safety and security are numerous. Video surveillance allows the danger zone to be viewed immediately, offering a visual means of verifying and assessing the situation. Integrated access control provides monitoring of escape routes and the means to quickly open or close doors, an important part of the evacuation process. Integrated intrusion detection means that data and electronic equipment are protected not only from the threat of fire but also against unobserved theft or sabotage. All of this can be achieved through a single, centralized station which guides personnel through the step-by-step processes to be followed in the event of an incident. This integrated view of what is happening not only helps to resolve an incident but also provides the capability to learn from incidents which is crucial in enabling process adaptation in the very dynamic risk landscapes which characterize today's business environments. Although safety and security are not a direct part of IT operations, they definitely help to ensure the business continuity environment of a data center.

Moving towards Intelligent Response

This adoption of integrated systems is a trend which is bringing about an increasingly 'intelligent' response to safety and security. At the same time, open architecture is very much a focus at the moment, with a move towards standardized protocols to allow different systems, often from different manufacturers, to work together. This can include security, life safety – including

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

notification systems –, heating, ventilation and cooling, and lighting, as well as power management systems. Convergence is currently a widely used term in security, referring to convergence in terms of the systems that cooperate in open architectures, as indicated above, but also between physical and IT security. Technological advances in video management, network cameras, recording devices, intelligent access control and management software have helped security applications to take advantages of the IP network.
Response systems of the future – Siemens calls them Intelligent Response systems - where the system in place involves a variety of fully integrated, multi-modal technologies, will take integration further still. With systems capable of analyzing all relevant data collected from the thousands of sensors and field devices and the various management systems operating throughout a building, a 'demand controlled' response to incidents will be possible. This data will automatically trigger the relevant system response mechanisms in relation to the nature, size and criticality of the incident. Furthermore, it will enable the automated provision of dynamically updated and targeted instructions to everybody concerned, from guiding them quickly and efficiently to a place of safety to providing relevant situational information for swift and efficient intervention.
The benefits of such solutions are multifold and are vital in helping a business to continue to operate. Intervention is faster, through the support from comprehensive situational information; mitigation is more targeted and efficient as the right systems are triggered automatically to e.g. extinguish a fire; and collateral risks are minimized e.g. a quicker return to a secure building situation is achieved, access controlled doors are locked etc. In addition, an audit trail of actions taken and sequence of events can provide leverage to facilitate the post-incident and recovery activities. Insurance claims and liability risk management are examples of such activities. Continuous improvements with regards to security and business continuity policies and workflows can also be effected.

Coherent risk management

Events rarely occur in isolation. A fire or civil unrest can become a security exposure while a natural disaster can bring a whole range of issues into the equation. Many events have significant knock-on consequences, often triggering a chain that multiplies the exposure. Businesses need to understand these relations between events to gain a full understanding of their risk exposure and to put in place systems which can respond to potential events. Intelligent Response will provide the means through which such events can be managed more effectively, thereby reducing risk and providing the opportunity to maintain business continuity in the face of even the most severe of incidents.
Data centers are at the heart of business continuity efforts and rightly so given the fundamental role that data plays in almost all business operations. Corporations do need to consider the wider landscape and look for technology partners that can assist in combining company-wide policies

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

and processes across different multi-sites with the local agility required to adapt to localized risks and to implement response mechanisms accordingly.

The **Siemens Infrastructure & Cities Sector** (Munich, Germany), with approximately 87,000 employees, offers sustainable technologies for metropolitan areas and their infrastructures. Its offerings include integrated mobility solutions, building and security technology, power distribution, smart grid applications, and low- and medium-voltage products. The Sector comprises the Divisions Rail Systems, Mobility and Logistics, Low and Medium Voltage, Smart Grid, and Building Technologies. For more information, visit www.siemens.com/infrastructure-cities

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world leader in the market for safe and energy-efficient buildings (“green buildings”) and infrastructures. As a service provider, system integrator, and product vendor, Building Technologies has offerings for building automation, heating, ventilation and air conditioning (HVAC), fire protection and security. For more information, visit www.siemens.com/buildingtechnologies

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com