SIEMENS

Technical Article

Zug, April 30, 2015

# Corporate security, a challenge for companies

Enterprise security concepts must be as diverse as the companies, markets and industries they serve. When it comes to implementation of such solutions, they have one thing in common: The human factor plays a critical role in the success of any technology deployed. With the increase of employees, visitors or contractors moving throughout the enterprise, this becomes even more significant. Keeping this in mind, viable physical security solutions merged with organizational and technical measures need to be implemented in such a way that they are accepted by everyone throughout the company, allowing for day-to-day operations to be carried out simply and easily.

*By Megan Miller, Market Manager, Siemens Building Technologies*

Security concepts have been around for as long as businesses have existed. In the past, security measures were relatively straightforward, using security guards or physical barriers such as fences. The main goal has always been the same: effective protection of people and assets to avoid specific risks and threat scenarios. Today, however, Corporate Security Officers (CSOs) face new and especially pressing challenges.

**Globalization**

As enterprises become multinational, their locations, divisions and branches span the globe, each with their own specific needs, including local security requirements or government regulations. At the same time, employees are increasingly mobile and often no longer tied to a fixed company location. This necessitates security standards which are aligned across the enterprise in order to meet local requirements as well as corporate governance policies that may need to be managed remotely.

**Siemens AG**
Communications and Government Affairs
Head: Stephan Heimbach

Wittelsbacherplatz 2
80333 Munich
Germany

### Cybercrime and IT security

Data is one of the most valuable assets of a company – and in many cases the most vulnerable. Studies show that more than 50 percent of all organizations that lose critical information go out of business in less than two years. With a shift from physical to information-based assets and a growing trend toward online data storage, IT security is becoming increasingly complex. This has a clear impact on traditional enterprise security as many security violations pertaining to data, networks and IT infrastructure originate internally. Even the most powerful firewall cannot protect an enterprise from this type of insider threat or espionage. Security solutions need to precisely coordinate and correlate physical access with IT processes to bring together physical and logical security.

### Competitive pressure, image and compliance

In today's competitive environment, companies rely more than ever on maintaining business continuity and managing their reputation with key stakeholders. Every security incident must be handled carefully to avoid damage to the corporate brand. Relevant incidents demand a quick response to maintain an adequate level of security locally or globally. Prolonged downtime is unacceptable under any circumstance, and all unauthorized access to customer data or information must be avoided. In addition, all triggered events and measures need to be documented for reporting and must be traceable for auditing purposes to comply with government, industry or local regulatory requirements.

### The human factor

Corporate security officers are meeting such increasingly demanding scenarios using holistic security concepts built on a standardized risk analysis, always keeping users in mind. Since people still remain one of the major weak points that lead to potential risk, it is important to know the stakeholders and align processes and policies as part of risk management strategies. Only when employees at every level of the company see themselves as part of the security concept will it be possible to close security gaps that cannot be addressed solely with technology.

### Technology must be suitable for day-to-day operations

Security solutions are an essential part of a security culture but must be aligned with business processes and requirements. Technology must help employees comply

with security standards in their day-to-day operations. Access management is one practical example of this. If the solutions deployed are not simple to use in everyday life, employees will find ways to circumvent the current standards and regulations. In addition, problems can arise when a variety of access solutions are deployed in various buildings or locations. Access cards or keys can easily get lost or stolen; if this goes unnoticed for a long period of time, it opens up the enterprise to new risk. However, if the right technology is in place – intuitive, modular and easy to operate – employees will automatically use it correctly as part of their normal routine.

Today's CSO needs to accommodate shifts in technology and ensure that investments are future-proof. A crucial factor is the right technology; it has to provide flexibility as the enterprise evolves and offer automation capabilities to support users. Another aspect is the acceptance of the security controls that are in place. In other words, what matters isn't so much the technology itself but rather how it will be utilized by the users.

**Corporate security as a concept**

In many companies, security solutions or disciplines are managed individually or siloed, which causes an increase in resources and costs. Historically, this has often been the result of a merger or acquisition where systems are "inherited" by the existing enterprise. Many times it is also because individual departments or locations have varying requirements. Silo-type solutions are still common, which leads to a loss of security standards and an increase in expenses for administration, maintenance and training.

Siemens has responded to these heterogeneous landscapes with a holistic approach to corporate security. These solutions focus on large international companies with widely dispersed locations as well as customers in a competitive market space who place a high strategic value on security issues. Siemens offers customized, integrated security solutions and services that support the complete framework from risk analysis, consulting and planning to implementation, maintenance and future upgrades. This provides companies with universal security standards which can be deployed throughout the enterprise, worldwide.

To implement this type of security solution it is important to understand the business first and follow with a company-specific strategy. Local conditions and specifications need to be taken into account to ensure the overall global strategy does not interfere with applicable privacy or other data protection regulations. The course of development begins with understanding the company's core business, followed by an analysis of corporate processes and policies. The next phase is the identification of specific threat scenarios and the risks which need to be taken into account. After all this has been defined and documented, technical, structural and organizational countermeasures are precisely tailored to individual situations and the actual requirements. The key is to create a corporate-wide security culture that encompasses all stakeholders at all levels.

**Central security structures**

In an international security market study performed by Siemens, 83 percent of the CSOs surveyed recognized the trend toward centrally organizing corporate security solutions. The move to strategically orient and centrally align corporate security cannot be adequately realized using isolated technologies or silo-type solutions. A holistic approach allows security practitioners at the operational and strategic level to gain momentum and increase their capability as needed in order to respond quickly and easily should an incident occur.

One example of a holistic approach is the One Card concept for enterprise-wide access control: A single multifunctional employee ID card supports the needs of visitors, employees and contractors. The card serves as an electronic key to all entrances, doors and gates and can also be used for self-service options such as cashless payment for the cafeteria, access to sensitive software applications or files and many other specialized needs. Employees readily accept technology when it gives them added value and allows them to be more independent within the enterprise. The One Card solution also offers extra security on an as-needed basis for critical facilities, resources or infrastructures which need a uniform and centralized software approach.

In very large companies, One Card solutions from Siemens facilitate the movement of employees throughout the enterprise at every location and allow for secure access to networks and information. The system manages all identities and

authorizations, thus eliminating manual processes. Cardholder data needs to be entered only once and is automatically synchronized with the corporate database in real time, saving time and money. Individual branch locations may decide to independently manage their security solutions or disciplines but can elect to centrally configure them to encompass multiple locations. Should an ID or access card get lost or stolen, the user's data can be retrieved immediately from a central database, allowing security personnel to quickly delete the credentials and create a new ID. This minimizes both security gaps and administrative efforts when issuing a replacement ID and prevents duplicates.

**Case study: corporate security at Vodafone**

German mobile phone provider Vodafone, a subsidiary of the international Vodafone Group, implemented a comprehensive, integrated corporate security solution at its new headquarters in Düsseldorf. The state-of-the-art site is one of the largest and most modern office buildings in Europe. The challenge was to create a sustainable and highly integrated security infrastructure here and in other European locations. Siemens met this challenge by deploying a security concept that combines both active and passive security systems.

One focus for this facility was a multi-site access management solution for more than ten thousand employees throughout Europe. Companies with a large workforce like Vodafone need to be able to efficiently manage access credentials, keys or access cards – a complex task especially when credentials are lost, exposing the company to security risks and expenses. For its new campus, Vodafone decided to deploy and operate an access control and lock system which uses a single end-point with Near Field Communication (NFC) technology.

With this technology, access authorizations are stored on a mobile phone equipped with an NFC SIM card. In preparation, Siemens had already added NFC functions inside the card readers and lock cylinders throughout the campus. Switching from cards or company IDs to NFC-enabled mobile phone end-points requires no replacement of the technology.

Since all functions run in real time, a real-time server can handle 100,000 events per second compared to a conventional door control unit which processes only 100

events per second. Having a real-time access control system in place allows the company to locate and track individuals on the campus or inside a building. Above all, a real-time system provides up-to-date and reliable data at all times, allowing for quick intervention when necessary.

This technical article is available at
http://www.siemens.com/download?PR00377
Press pictures are located at
http://www.siemens.com/download?PR00374
http://www.siemens.com/download?PR00375
For further information on the Building Technologies Division, please see
www.siemens.com/buildingtechnologies

**Contact for journalists**

Catharina Bujnoch
Phone: +41 41 724-5677; E-mail: catharina.bujnoch@siemens.com

**Siemens AG** (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for more than 165 years. The company is active in more than 200 countries, focusing on the areas of electrification, automation and digitalization. One of the world's largest producers of energy-efficient, resource-saving technologies, Siemens is No. 1 in offshore wind turbine construction, a leading supplier of combined cycle turbines for power generation, a major provider of power transmission solutions and a pioneer in infrastructure solutions as well as automation, drive and software solutions for industry. The company is also a leading provider of medical imaging equipment – such as computed tomography and magnetic resonance imaging systems – and a leader in laboratory diagnostics as well as clinical IT. In fiscal 2014, which ended on September 30, 2014, Siemens generated revenue from continuing operations of €71.9 billion and net income of €5.5 billion. At the end of September 2014, the company had around 343,000 employees worldwide on a continuing basis. Further information is available on the Internet at www.siemens.com.