SIEMENS

Technical Article

Industry Sector
Building Technologies Division

Zug (Switzerland), July 4, 2011

Security in an IT world

There is a move towards more integrated solutions in security, with security management software being employed to provide a greater degree of situational awareness. This means that IT will have an increasing role to play in the security world, and this raises challenges.

One challenge is the need to ensure that the solution providers and system integrators have a good understanding of what the expectations are from an enterprise or corporate customer. For the system integrators, this requires a strong focus on developing security software that meets the standards of an enterprise organization. Another challenge is to develop the resources to implement the solutions, recognizing that it is a very different world in which the vendors now operate. All those involved in the security equation, from the software developers through to those selling the solutions, the installers and commissioners of the systems, have to complement their current expertise with the right set of IT skills.

It is a very different scenario looking at a one building, one site application based on securing the location through traditional physical security measures than it is addressing a campus or multi-site location where the software component is much more critical. While in the first case it may well be a conversation with a single security manager or facilities manager responsible for that one location, in the latter it might involve discussions with C-level executives so that a different skills set is required.

Legacy issues

Increased situational awareness is a benefit of an integrated approach. With all the security disciplines of video surveillance, access control and intrusion detection co-existing and co-operating on a single platform, the safety and security of a site is optimized through centralized management and alarm handling. Another benefit is that the solutions now available are more flexible, customizable and scalable.

Siemens Schweiz AG
Industry 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

For any system integrator with a large installed base, it is important that the move to newer solutions and to the new breed of equipment takes account of the need to enable migration of the older installations. This is achieved through an open architecture based software approach. A complete migration plan can be developed which removes the need to rip out the existing infrastructure and start again, instead using the software to maintain and work with older style field devices and hardware and complement those with newer equipment.

There are obviously still a number of analogue security components in use. With the likes of IP encoders enabling, for example, the integration of analogue cameras and using cabling already in place, it is possible to reuse a significant amount of existing hardware when looking to employ security management software to convert from an analogue to a digital solution.

Returning to the flexibility afforded by a software led approach to security integration, this certainly applies to the different configurations that are possible. It removes any tie to physical location. This can be important, particularly in greenfield sites and those where new software is being introduced, since the customer may not initially have a fully developed idea of how the systems are going to run. Even with comprehensive planning, actually experiencing in practice how the systems are fitting in with operational procedures could lead to changes from the initial configuration. As a site develops, its security requirements are also subject to change. Accommodating such changes is very easy to do if the integration is software based.

The virtualized world

The virtual aspect of computing can bring benefits in terms of investment. A lot of companies are moving towards virtualization of their hardware, particularly in light of the current economic climate. Constraints are common now with capital expenditure (capex) but not so much with operating expenditure (opex), and this IT-led approach is conventionally dealt with as an opex. Within this virtual world, maintenance, service and many other associated costs are reduced simply because there is not the requirement to maintain hundreds of servers but rather a much smaller set of base hardware. This has environmental benefits too as data centers focus on reducing their power and energy consumption.

Large scale corporations also have the opportunity to offer security based services. IT departments in such businesses are expected to provide a range of services – email, file services, remote connections etc – to individual departments, with each department paying a given amount a month, for example, for a mailbox or data storage facility. With the move of security onto the IT infrastructure, many IT departments want to maintain this service-led approach but without having to administer things such as cards for access control systems. While some will take responsibility

Siemens Schweiz AG
Industry 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

for access card management, others will prefer to look after just the IT aspect and ensure everything is working, offering this as a chargeable monthly service to the security facilitator who will be responsible for card management.

This points to some crucial questions to be answered for any installation: Who manages the networking structure and who manages access to that infrastructure? Who creates the users and who manages them? In small businesses and SME's, it may be a single department looking after everything. But certainly in larger organizations, two or three different departments can be involved, one taking care of the network infrastructure and another running the data center servers and video storage infrastructure. Coupled with this is the issue of cyber security and the need to prove how secure systems are. Regulations will have to be developed to which software companies can work in terms of proving their degree of security compliance.

Integration: security devices and beyond

In terms of integration, the main focus initially was to pass simple information between the main disciplines of physical security and to have a level of control over the sub-systems. For most solution providers this started by loosely coupling their different platforms together to give the users the perception of having an integrated system. The Siemens Siveillance Fusion security management solution has a different approach: the software was based on a single platform that integrated the devices through the different proprietary protocols of their own devices and those of their partners. This has been extended to cover standard open interfaces which significantly increases the number and types of devices that can be integrated.

This goes beyond the main base applications, integrating into enterprise systems as well and being able to pool data. A good example is human resources where personnel data can be integrated with the security system, thereby enabling organizations to have self-service portals through which visitor access can be completely controlled.

This goes back to the need for complete situational awareness. For many organizations knowing exactly where people are located is useful, particularly so in large operations. There are two aspects to this: the safety requirement where such information is invaluable if, for example, an evacuation of the building is required in the event of an emergency, and then the security requirement where the location of an incident needs to be pinpointed, as well as the people involved.

With older technology, it may well have been just an alarm generated to say somebody has passed through a door. Now, the option is available, through integrated systems, to take information from

Siemens Schweiz AG
Industry 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

access control, intrusion and video surveillance devices to get a much clearer understanding of the situation in real time and therefore respond much more effectively. It is no longer just a case of knowing that somebody has passed through a door but that the room is still occupied because the PIRs are still in active mode, and people can be identified through real time video images. Taking it a stage further, through integration with other software systems, it is possible, for example, to identify that somebody has plugged into a network access point – back to the cyber security issues referred to earlier which are becoming an ever increasing factor in security threats.

And to the future…

From a software point of view, open protocols is certainly the way to go. The more software developers have to accommodate proprietary integration, the more time is consumed and therefore the greater the costs. Some people labor under the misguided belief that a proprietary approach brings greater security and that open protocols reduce security levels. In fact, the more security solutions companies are able to integrate with other systems, the more information can be gleaned and the greater the situational awareness provided.

Now that security is operating very clearly in the IT arena, nearly all protocols are open so the ease with which such information can be fed into the security process is improving. The data is often sitting there, under-utilized in terms of how it can enhance security measures. It is a case of tapping into that resource and recognizing what information can help to improve security levels. Looking ahead, the currently high profile issue of cloud computing will certainly have a role to play in future integrated solutions, particularly given the potential cost savings it offers. There is some maturity required in the cloud world, including security reliability and privacy issues to be resolved, before it is taken up extensively. However, if such issues can be successfully addressed there is certainly the potential for use of the public cloud, as well as the opportunity for the creation of private clouds for the bigger enterprises to realize the benefits of embracing cloud technology.

Author

Mark Mooney, Head of Product Line Corporate Security, Siemens Building Technologies Division

Siemens Schweiz AG
Industry 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

The **Siemens Industry Sector** (Erlangen, Germany) is the worldwide leading supplier of environmentally friendly production, transportation and building technologies. With integrated automation technologies and comprehensive industry-specific solutions, Siemens increases the productivity, efficiency and flexibility of its customers in the fields of industry and infrastructure. In fiscal 2010, which ended on September 30, 2010, revenue from continuing operations of the Industry Sector (excluding Osram) totaled around €30.2 billion. At the end of September 2010, Siemens Industry Sector had around 164,000 employees worldwide without consideration of Osram. Further information is available on the Internet at: www.siemens.com/industry.

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world's leading provider of safe, secure and energy efficient solutions for buildings („Green Buildings") and building infrastructure. As a service provider, system integrator and product supplier Building Technologies offers building automation, HVAC, fire safety, security, low voltage power distribution and electrical installation technology. With around 42,000 employees worldwide (September 30), Building Technologies achieved a turnover of €6.9 billion in fiscal year 2010. www.siemens.com/buildingtechnologies.

Siemens Schweiz AG
Industry 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