Securing large commercial facilities

By Allyson Koekhoven.

How do you secure locations where people are supposed to be working, socialising and moving about freely?

How do large commercial facilities secure their premises without hindering the passage of legitimate visitors and employees? What role do the technological and human elements play in the equation? *Hi-Tech Security Solutions* spoke to a major manufacturing operation's on-site compliance and risk control investigator and a chief of safety and security within the hospitality sector.

Leo Nardi, who is based at the manufacturing facility, is the contracts manager and electronics advisor at Justicia. "We believe in providing a holistic, integrated security environment. Points to consider from the outset revolve around the integration design, the effectiveness of the proposed solution and maximising any return on investment. It is also important to understand the practical implementation of additional integration design to ensure that any probable future upgrades to the system are accounted for proactively."

Within the manufacturing operation where Nardi is based, CCTV is operated on a separate network to the IT function. "This is typical of pre-IP installations. One needs to decide whether to merge the two networks or to retain them as standalone entities.

"One of the major considerations is the large amount of bandwidth and storage capacity required by a high-end IP solution. Often the volumes can exceed those of the other business communication and data requirements. Successful integration of systems is critically important and one needs to employ forward-thinking IT personnel who can see the potential around IP systems and their logistical requirements," Nardi continued.

"I manage a safety and security department like a business within a business. All decisions must make sound business sense and most importantly, benefit the sustainability of the business, its customer base, all stakeholders and staff members in one or more ways. Safety and security is an expensive business that does not directly generate profits for a business and therefore it is important to always make well-educated decisions," said Radisson Blu Hotel's chief of safety and security, Marthinus Baumbach.

"It is a big responsibility to manage the safety and security of a property worth a staggering amount of money and more importantly, all the lives within it. I do not take anything for granted. I keep my finger on the pulse of the operation; taking shortcuts is not an option and all safety and security systems are continuously tested and meticulously maintained," he said.

Silositis (the disease of division) versus integration

Nardi said that he has observed many examples in industry where projects are not signed off with the inclusion of a security / integration expert and there is little or no communication between various entities on the ground level. Security is a classical grudge purchase and often an afterthought.

"Justicia employs a philosophy of including security in all aspects of business decisions. When you factor integration into the equation, this is definitely not an afterthought. Factors such as the various service level agreements from different suppliers within the system also need to be carefully considered. Ensuring that systems are integrated wherever possible ensures easier management and flexibility of the entire facility."

"I manage the safety and security operation in a multi-storey, high-rise building with several other tenants within the complex. The layout poses challenges of its own. A small portion of the safety and security systems are integrated with a management platform but the majority of the systems run independently from each other. No doubt, this is more labour intensive, time consuming and arguably a bit more expensive. I do, however believe that the advantages outweigh the disadvantages," countered Baumbach.

Continued on page 28

Continued from page 26

"CCTV is an ideal starting point for integration to other systems but one must remember that it is only one portion of the whole security, and indeed business system. Another point to remember is that cameras are no longer just used for security purposes. There is an increasing trend to deploy them as part of the manufacturing monitoring process. Because of their analytical value, they can be programmed to concentrate on specific events. For example, certain processes within this manufacturing facility are served by a traffic light (stack light) system. When the red light is displayed, the camera sends an alert to the control room that immediate attention is needed in the process," explained Nardi.

Integration will become even more prominent in the future. Even large IT systems are becoming more integrated within themselves and are trending towards virtualised machine environments. One need not fear integration. A well-designed system will not over complicate. The integration platform can be viewed as a component attached to many other components. A well thought out design will factor in a high degree of redundancy and eliminate single points of failure. A component that fails will not bring the whole system down. Integrated environments provide many advantages where the sum of the whole is greater than the sum of the individual parts.

"We prefer to look at the entire infrastructure and plan for future expansion and how this would impact on bandwidth and storage. Policies and procedures are paramount to ensure compliance and successful application," he added.

"Our control room monitors all safety and security systems around the clock and data is processed and analysed in real-time. I prefer to keep the various systems separate from each other, just as in the same way governments and big corporate organisations do not allow people in key positions to travel together in the same car or on the same plane. I actually take this a step further by having a different service provider for the maintenance, repairs and technical support of each system," said Baumbach.

"If all systems are integrated and there is a problem with the management platform, it will affect each and every system in the operation. If all systems are down simultaneously, it may have far-reaching consequences. It is much easier to implement interim measures if only one system is down instead of several. For this reason I prefer to keep systems separate from each other," he continued.

Man versus machine

"Technology needs to complement the human element in any security installation," said Nardi. "I firmly believe that there are three areas of oversell in the security industry when it comes to CCTV. Firstly, video analytics. This is a great tool but it cannot completely replace the human element. Secondly, third-party integration is often sold as first-party integration. This is not the same thing and can end up with the client incurring unforeseen costs and complications. Finally, megapixel cameras have a definite role to play but, by understanding that they also have limitations, they can be deployed more effectively. Their use can also be maximised by assigning them to a specific area as you would a human counterpart."

"Technology will never replace the decision-making skills and senses of a human being. Being in the hospitality industry, human interaction is invaluable and irreplaceable. The guard force forms the backbone of my security operation, with technology undertaking the supporting role. The key is to have an exceptionally well trained security team capable of using the technology at their disposal effectively," said Baumbach.

"Technology is only as good as the person monitoring, analysing and interpreting the data, so the two complement each other all the time. To achieve the balance between humans and technology, training remains one of my priorities.

"One must be cautious not to change technology just for the sake of change. I still use an old-fashioned manual system that is incredibly effective and dependable. Having said this, technology enables us to work smarter and has paved the way to process and react to vital, up-to-date information immediately," added Baumbach.

"Technology empowers my guard force to make accurate assessments and to take correct decisions. It is interesting to see how quickly technology becomes outdated and obsolete. I use a conservative and low-risk approach by using technology that has been tried and tested," he said.

Leo Nardi

Marthinus Baumbach

"Technology can be used to assist and complement the functions of your security personnel. For instance, technology could save time and effort by automatically raising booms or spikes. This frees the security guard up for a more important function. A security guard could also monitor several locations simultaneously by viewing a CCTV console. These are simple examples and an in-depth analysis of more complicated environments is beyond the scope of this discussion. Technology can also be used to provide accountability for the guard's actions and to minimise the element of human fallibility, which is inherent in all of us. Adequate training of both guards and control room operators is crucial and should never be negotiated," added Nardi.

Securing information

"Information security has become a priority in recent years, especially for government departments, the military, financial institutions and larger corporate organisations. Information and the access to it, is the lifeline of many organisations," according to Baumbach.

"To mitigate risk and for insurance purposes, I find it beneficial to outsource to an IT department. That way, a company has recourse should issues arise with the service provider. The use of up-to-date anti-virus, anti-spy and firewall software is vital for any organisation to effectively secure information. Although readily available, but not commonly used yet, the utilisation of encryption and decryption software may become standard practice in the corporate environment in future," said Baumbach.

"Within the compliance department, reports are correlated to ensure that each event is prioritised. The incident management system provides a chain of evidence that is shared across a common platform. However, to be successful, this needs to be properly managed and protected. One needs to ensure that only those people who have received clearance to access the information, can do so. There are also legal implications to consider when it comes to personal information and the protection thereof," said Nardi.

"In conclusion, an effective operational security system should not only consider the security elements within the organisation, but should also actively involve other sectors such as occupational health and safety, IT and production departments to provide a successful solution," Nardi concluded.