Physical Security and IT Convergence

For over 30 years security has been a camera, a monitor and thousands of miles of coax or a couple of contacts wired to an alarm system. The post 911 era has brought the issue of physical security to the forefront of new technologies development and set a collision course with Information Technology (IT). Since technological convergence does not automatically provide for a parallel organizational convergence - the change brought up confusion and frustration from both the IT professionals and the traditional asset managers. IT and Physical Security departments have been scratching heads over an uneasy task of trying to figure out how to solve the problems that keep appearing - how big are the companies that have the issues? How do we resolve these issues? Which side is responsible for physical security technology? Where is technology going?

The Critical Infrastructure

Although the initial trend was for physical security technology and physical security systems to incorporate information technology components and infrastructure, today many security technologies and systems do more than incorporate those elements. Whether large or small, the security and surveillance systems are completely based upon them.

A good example would be CCTV surveillance. The type of CCTV cameras that are used for facial recognition today have been around for more than 30 years. The more recent advancements in their use were spurred by the introduction of computers. Until affordable computer technology could be utilized to make CCTV monitoring and recording manageable (becoming widespread around 10 years ago), their usefulness was limited and manpower intensive. Today, the advancements in information processing technologies have made possible a variety of tasks, including, but not limited to, video based smoke and fire detection, facial recognition, and many types of advanced situation-based alarm monitoring based upon pattern recognition and behavior recognition. Not to mention video analytics and video content analysis where relevant data can be stored in a database and searched for tendencies and trends or abnormalities.

It’s not just security anymore

New security capabilities are also providing benefits outside the realm of security, and that has complicated the picture significantly. For example, *Shipping and Warehousing operations* can be monitored remotely by CCTV. If a critical shipment is due to go out early in the morning, the video management software can be used to point a camera at the shipment material and set an alarm that will alert a manager or executive when the containers are moved or if they are not moved within a specific time period. At the same time video management software can be used as a supervisor tool for schools and educational institutions during the day and secure the school from vandals at night. *Card or biometric based access control systems* can provide electronic time card functions, generating time and attendance records for the *Payroll Syste*m. *Human Resources* can review video recordings to verify the effectiveness of employee training, and document the results for management. While it’s great to have increased Return-On-Investment (ROI) for security expenditures, the non-security benefits raise complex procurement and budgetary issues: Whose budget will pay for the extensions to the security network for operational purposes – IT, Security or Operations? How do you divide up the bills for installation, ongoing maintenance and upgrades on CCTV cameras that perform triple duty (security, operations monitoring, and training)? Should Operations and HR have a say in the procurement process? Who will resolve disputes over competing departmental interests? Should security system traffic even be allowed to travel on the business network for non-security purposes or visa versa? These questions only touch upon the wide array of organizational complexities that are being introduced by the IT-based expansion of physical security systems.

The obstacles

There are five aspects of the technological convergence that have created problems and conflicts for Security departments and IT departments:

ƒ **New security systems require knowledge that is beyond security's domain.** Electronic security systems incorporate information technology elements (such as databases and computers) and require information technology infrastructure (such as local and wide area wired and wireless networks). Most of these elements have complex configuration and setup steps that must be performed by a knowledgeable person. Thus the procurement, deployment and maintenance of most security systems now require IT knowledge and skills. Security departments now must look to the IT department for help with many aspects of security projects. Unfortunately, there is a large communication gap, because the Security personnel don't know the IT domain, and the IT personnel don't know the Security domain. This is compounded by the fact that today many companies have not worked out an up-to-date and easy-to-understand Security Plan and Security Emergency Response Plan. Having these plans would help IT get an understanding of the purpose and activities involved in Security during normal business, off-hours, and emergency operations.

Compounding the problem is the turf war. Like most industrial convergence there is fear of loss of power or control to the other side. Both IT departments and Asset Managers do not wish to lose control of their domain and are reluctant to give the other a foot hold. Of all aspects of technology convergence this is one that is the most unpredictable and the most difficult to overcome.

ƒ **Security systems offer many non-security benefits.** These are the new stakeholders throughout the organization, whose use of the systems requires extending the information technology elements and infrastructure of the physical security systems for non-security purposes. This introduces complex issues for budgeting, procurement, deployment and ongoing use of the systems. It also significantly expands the privacy issues.

ƒ **The IT elements of security systems are used differently than the same IT elements of business system**s. For example, the usage patterns for networked security workstations are very different from what is typical for business systems of networked PCs. This leads IT departments to misestimate the requirements for information technology elements and infrastructure of the security systems. This is most apparent in calculation of network bandwidth requirements, which is almost always significantly underestimated. Security departments, on the other hand, not being familiar with the IT domain, do not realize that these differences exist and usually fail to adequately, if at all, educate IT personnel about them.

ƒ **Using technology blinders.** It is very important when engaging in security analysis, and when discussing security with people outside of Security and IT, that enthusiasm for new high-tech security systems and products doesn't create blinders that keep low-tech solutions out of view. This is a risk for those in both IT and Security who are immersed in technology on a daily basis.

ƒ **There are no standards.** For 30 years we had VHS cassettes as the core medium for recording video which made it very easy to select a product. Today, there are literally 1000s of products in the market with hundreds of digital formats. What is even worse is that no two products are a like. They all have nuances that set them apart. How do you choose? This is where a Security Emergency Response Plan will help even more.

What is the Solution?

It's no surprise that companies who are most effective in implementing good security programs are those companies who have an executive at a high level that is a "security evangelist." It requires a high-level address to organizational security issues to set priorities for items that extend across the entire organizational spectrum, especially when non-security benefits are involved. Security leadership must be strong, active and ongoing in order to achieve real results. Whether the label "security evangelist" is used or not, someone at executive level has to take on that role. It's not an option or a temporary involvement.

The consideration and establishment of organizational security requires participatory collaboration. It sometimes requires "executive muscle" to provide the needed support to Security Asset Managers and IT departments. Additionally, it often takes executive savvy to deal with competing resource allocation issues and to set appropriate budget priorities. Executive insight can be required to evaluate security measures and initiatives in light of the big picture, and to envision the optimum scenarios for their implementation. Sometimes there are campaigns that can be utilized to introduce or support an initiative that will help to align the efforts with overall business objectives. Experience shows that there is no adequate replacement for having a security-minded senior executive. Don't always go for the big initiatives. Small "baby steps" are less disruptive, and are also less demanding on organizational

resources. Use what you have now. Discover what you can do right away with existing resources. Usually there are very basic measures that can be taken to help bridge the gap. Get outside help. Simple and inexpensive solutions are not available for every security need. When they are, they are often obvious only in retrospect. This underscores the value of consulting with people outside the Security and IT departments, and even outside the organization, who can view things in a fresh perspective. Choose a company that has deep roots in both physical security and IT.

Who is responsible?

For most organizations, the roles and responsibilities regarding security must be expanded not just for Security and IT personnel, but for most managers and executives. To make sure that security initiatives are fully accomplished and that security policies and procedures also remain in place requires that managers and executives have enough security knowledge that they can exert effective control in their own areas where security issues are involved. The also need the knowledge to be able to evaluate the relative importance of security issues. Sometimes lapses in security are a result of people not really understanding the role that a security measure plays, and why it is important. Informed managers and executives must see to it that their people are adequately informed, whether this occurs through formal training or ad hoc briefings or instructions. Whatever your own responsibilities are in the security picture, it is your job to see that you know what you need to know to carry them out. Those of the executives and managers, whose areas would benefit from security technology, whether it's for security or operational purposes, are stakeholders in the deployment of security systems.

Both the Security and the IT departments must be able to engage in real dialog with them. Security and IT must be able to summarize and clearly explain the security initiatives and any technology under consideration, in terms of how it would affect each area of the organization and the organization overall. This includes being prepared to explain the relevant risk assessment work upon which any security recommendations are based.

Success!

To achieve full success with organizational security requires effective recognition and handling of these problematic organizational situations, which, in turn, requires knowledge of the organization itself, and the purpose and activities of each part of the organization. While that may sound very matter-of-fact, often Security personnel and IT personnel do not possess or find it difficult to get access to this knowledge. Many executives can't articulate their purpose and function in relation to the overall business. The purpose of security is to protect and support the functions of the business. This requires a clear understanding of each area of the business. To get a handle on security, you first have to get a handle on what each area of the business is doing. To set security priorities, you have to know the priorities of the business. You have to understand the big picture, so that you can put things in their proper perspective. Each executive must be able to correctly answer these questions, 'What are we in the business of? What are we going to do?' It is enlightening and often surprising to hear the wide variety of answers from within the same organization."

Additionally you have to understand that security isn't just physical security or logical security; it includes the human element and all three elements must be addressed. This must be understood outside the Security and IT departments in order for an organization to be effectively proactive about security, which is the only way success in security will be achieved. Don't wait for something to happen. Hawkeye Vision Inc. is here to help. We are a technology company that has deep roots in both physical security and IT. Whether it is IT working with Asset Managers or visa versa, we are your bridge to the other side.

Hawkeye Vision Inc.
10415 J St.
Omaha, NE 68127
800-959-9148