



Career Corner

The Convergence of Physical and Cyber Security

By Joyce Brocaglia
Joyce@AltaAssociates.com

Introduction

Many people feel that the convergence of physical and cyber security is inevitable, but what is the reality in today's marketplace?

The current state of the industry is that the majority of companies have not yet combined the roles of physical and cyber security. Most do not have a chief security officer responsible for both sides of the house. I believe this is because security is a lot more than just armed guards and encrypted networks. It involves hard problems and complex issues like privacy, risk management, regulatory compliance, policy creation and enforcement and investigations.

Companies realize that there are significant challenges involved in combining the roles. Many executive management teams are not yet ready to commit to the level of strategic planning and communication required to bring these under one roof. A few of the most difficult challenges are establishing new reporting structures and finding an executive qualified to lead both organizations. In terms of the staff, physical and information security professionals have very different upbringing and cultures. There is a reason why they are best at what their specialty is, and it may not be effective to try and change their expertise. This is compounded by the fact that each individual and department has staked claim to their own fiefdoms, resulting in turf wars that may take years to settle.

What Companies Want from Information Security Officers

So, if combining physical and cyber security is not yet prevalent in most companies, what is it that companies are requesting from their information security officers? The most common trend that we see involves the following three points:

1. Building stronger relationships with your physical security peers. Companies are requiring their CISOs to build relationships with their physical security counterparts. This can be initiated by simply attending an ISSA or ASIS meeting together to facilitate the recognition of touch points and to determine areas in which to collaborate your efforts.
2. Begin creating integrated solutions
At RSA, I attended a dinner that had a panel discussion with Kevin Mitnick, the notorious hacker; Mary Anne Davidson, chief information security officer of Oracle; and Jeff Moss, founder of Black Hat. They all agreed that the most effective hackers were those who combined physical and cyber techniques to gain access. Now that the threats

are intertwined, it's all about developing a comprehensive asset protection program and not just a cyber security program.

3. Security and awareness

It is important that every employee understands that they are individually responsible for the security of their company. Employees need to be provided with training that will make security second nature and make them more aware of the consequences of their actions.

What Are Corporations Doing?

Although corporations have not fully integrated their security functions, it is certain that our future will require increased collaboration. Technology

The current state of the industry is that the majority of companies have not yet combined the roles of physical and cyber security.

is rapidly moving into areas that were previously supported by physical security solutions.

In an effort to manage the convergence of physical and IT security, Computer Associates (CA) announced the creation of the Open Security Exchange at the RSA 2003 conference. According to their frequently asked questions, "The Open Security exchange is a cross-industry forum dedicated to delivering vendor-neutral interoperability specifications and best practices guidelines in the areas of security management. The physical and IT security management convergence specifications promote organizational and technical integration between the physical and IT worlds to maximize operational security while reducing operating costs. These specifications are intended to provide the ability to Audit Data Across Systems; provide Strong Authentication and the ability to Provision Users."

The founding companies are Computer Associates, HID Corporation, Gemplus and Software House, a member of Tyco Fire & Security. Each company provides products that offer integrated security solutions. Computer Associates eTrust 20/20 bridges the gap between physical and IT security by collecting, correlating, analyzing and displaying security events. The convergence specifications will be built into CA's Security Command Center, currently in beta. The Command Center centrally manages an organization's security infrastructure, providing situational awareness and full command and control.

As more corporations join the forum and collaborate on developing interoperability standards and best practices, it will become easier for companies to customize and adopt an integrated solution that meets the needs of their organization. I believe that this may be the type of framework that CISOs and CSOs can build upon in restructuring their enterprise security programs.

Conclusion

In conclusion, the threats are intertwined, the solutions are beginning to be integrated, best practices are being developed, and vendors are now creating products to support a cost-effective integrated solution. Some degree of convergence is absolutely inevitable; the question is *when* and *how much*.

Joyce Brocaglia is the CEO of Alta Associates, the Human Capital Risk Managers specializing in information security recruiting. www.altaassociates.com