Lou Magnotti, *CIO, U.S. House of Representatives*

Liz Lancaster, *Director of Member Services, Security Executive Council*

Lorna Koppel, *Director-IT Security/CISO, Kohler Co.*

John Masserini, *Information Security Officer, Dow Jones & Co.*

What are the characteristics of a good relationship between Corporate Security and Information Security?

There is nothing more important than communication in any effective relationship; it is the foundation of competency.

The communication between Corporate Security and Information Security must be open and candid, while maintaining a professional respect for each other's knowledge, areas of responsibility and experience.

Looking back at my 28-year career, the current emphasis on convergence of physical, industrial, operational and information security seems almost like a step back in time. During the late '70s and early '80s, we were all one multi-disciplined security department. But the computer security folks, myself included, fought hard to be recognized as a separate security discipline.

Moving forward, we can have the best of both worlds and really make a difference if we remain committed to communication, operate from understanding our business requirements and develop risk mitigation strategies as a team. The relationship must typify the fighter pilots' slogan ... "I've got your six (back)!"

Over the last several years, there has been a push to collaborate among security groups to identify, manage and mitigate risk as a collective effort. Rather than "owning" risks to business, security leaders (and their groups) are evolving into subject matter experts that provide consultation related to risk mitigation to the rest of the organization.

This push is shifting security responsibilities to individual stakeholders in an ongoing effort to make security part of everyone's corporate responsibility.

A good relationship between Corporate and Information Security involves listening to issues of peer groups, providing a sounding board and meeting face-to-face. Awareness evolves from gaining an understanding of risks to each business unit in your respective areas. Innovate by sharing ideas and information. Define risk management roles together based on skill-sets. Demonstrate leadership in areas of expertise.

Drive program success together, and measure and communicate that success to senior leadership.

Working together successfully means you can pick up the phone at any time and discuss concerns, ideas, etc., and work on solutions without fear of turf politics getting in the way.

Either area should be able to lead initiatives and be trusted that they will look out for the interests important to the other team and know when to bring them in. Trust means leaders and staff at all levels feel comfortable communicating honestly and openly across organizational lines.

Both areas must take a shared approach to protecting the company because, frankly, risk mitigation overlaps both areas. There should be respect for each other's unique skills and acknowledgment of inherent weaknesses.

Information Security can help Corporate Security work through IT processes. Corporate Security has access to resources and specific training in areas with law enforcement, interrogations, investigations and overall personnel security that Information Security folks do not have.

A strong relationship between Information Security and Corporate Security is critical for the success of both and goes far beyond the asset management/loss prevention realm.

Being a global organization, we rely on our Corporate Security counterparts to enforce policies on behalf of Information Security.

With offices ranging from five to 2,000 people, reliable physical security of data center and office space access allows development of technology solutions with less restrictive risk profiles, thereby enabling our user population to drive business. Additionally, The Global Information Security Office owns Business Continuity, Disaster Recovery and Crisis Management planning — all which are dependent not only on Corporate Security but Facilities Management as well.

Our success in planning is directly linked to the support and execution of the plans by Corporate Security groups around the world. A strong level of trust between the two organizations and constant communication enable both groups to complement each other to drive down risk.

Next Month's Question: How can I best protect my organization's intellectual property?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.
The information in this article is copyrighted by the SEC and reprinted with permission. All rights reserved.