SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Security and IT Alignment

Ray Bernard, PSP, CHS-III

Originally Published in SecurityInfoWatch.com

August 2012

Security and IT Alignment

In the consulting work that my colleagues and I do, we almost always find simple steps that corporate and physical security departments can take to better align themselves with IT. However, I recently realized that it is wrong to think of the IT policies and practices as “rules to follow” or “hoops to jump through” — phrasing it this way conceals an important point: the IT policies and practices are what company management has approved and mandated for security and cost-effectiveness reasons.

Applying the IT policies to your physical security technology means improving how you do things for your department and your overall organization’s benefit. That’s what this question and answer relates to:

Q:I have been reading about the importance of aligning our security department with the IT department; but, since we don’t have any ongoing or upcoming technology projects, I don’t know whom to talk to about what. Are there any common starting points for such discussions?

A: There definitely are, and once you get collaboration going, you will find plenty of common ground.

IT departments have been dealing with computer and network technology for decades, and have learned — often the hard way — how to manage technology deployments and take care of the technology in place to get the maximum performance with minimum effort and cost. Using their policies can help you get more for your technology money, and help you obtain beneficial resources from outside your department — essentially they get more results with less effort. A good starting point is to find relevant IT policy documents and figure out how they can apply to electronic security systems and the data they generate.

Typically, each policy will spell out whom the document applies to, the roles, responsibilities, rights and privileges involved, along with any specific requirements. Usually, the documents contain a glossary clarifying exactly what IT means by a particular word or phrase — that data alone is valuable.

IT departments have become much more adept than most security departments at managing technology and ensuring that it performs the way it needs to, and managing enterprise-scale deployments in a cost-effective manner. This is because they have so much critical technology to deal with, and almost all of it is enterprise-wide in its use. This can make outage impacts enterprise-wide, having a much greater impact than, for example, a single card reader failing. This doesn't mean IT never has problems, but it does mean that they minimize the number and impact of problems that might occur.

The cost-effective aspect of technology deployment is an area where Security can usually make improvements. For example, many security departments don't have up-to-date, as-built drawings for its systems. As a result, troubleshooting and repairs take longer and cost more than they should. Planning technology changes (not rip-and-replace) is more trouble and takes more time, because all the information needed is not readily at hand.

Electronic physical security systems are classified as "critical systems" — if yours are not, they should be! Thus, there is an IT policy that can help improve technology deployments; in fact, there is usually at least one policy that actually makes it a company requirement to have updated as-builts, backups of system and device configurations, and so on. This IT policy is typically called Configuration Management or Production Change Control. It includes: keeping good records for and good control over what systems are in production use; and how to plan and manage updates and upgrades. Typically, correct application of this company policy will beneficially impact system documentation, maintenance contracts with service providers, and the planning and execution of technology updates and upgrades — all in the direction of making security technology deployments less troublesome and more cost-effective.

Your homework assignment for this column is to locate your IT department's Configuration Management policy, and find out how Security can benefit by getting compliant with this existing company policy. IT can

help you do this, and when initial costs are involved, IT can provide business-case support because they already know these practices save money in the long run. That's one reason such practices are company policy.

For the IT folks, it would be a welcome change to have an individual business function such as Security approach them to learn about their policies and ask for help in getting compliant! It is one way to start Security/IT collaborations off on the right foot.

There are often a dozen categories of IT policy, standards, practices and procedures that apply to physical security departments and their systems technology. They can include: how to use network resources; password policies; procurement practices; pilot testing; asset management; maintenance policies and lifecycle planning; compliance; and more.

Write to Ray about this column at ConvergenceQA@go-rbcs.com. Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. Mr. Bernard is founder and publisher of The Security Minute 60-second newsletter (www.TheSecurityMinute.com). For more, go to www.go-rbcs.com or call 949-831-6788. Mr. Bernard is also a member of the Content Expert Faculty of the Security Executive Council (www.SecurityExecutiveCouncil.com).

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com