



The Convergence of Physical and Network Security

Will the Trend be a Best Practice?

A Phare Consulting White Paper—November 2004
By Rich Anderson, President

Contents

Contents	1
Abstract.....	2
Introduction	3
Driving Forces Behind The Merger	4
Not All Forces Are Created Equal	6
Outlook	7
About the Author	8



Abstract

This white paper provides a high-level overview of the movement to combine the organization's which provide physical and network security. It includes and analysis of the key forces driving this trend, both for and against, such as technology and organizational issues. Finally, we will review the likely outcome of this movement.

“Many companies have two security directors—one for physical security and one for information security. Does it make sense? How is it changing? These individuals represent two different security industries, each speaking a different language, but both serving the same customer concurrently. Until recently, these two groups barely acknowledged each other. Only lately are emerging the advantages of their working together to view the ‘big picture’ of a corporation’s security.”

- Jim Spencer, Access Control & Security Systems Integration, November 2000

“Physical and information technology should be treated as inseparable bed-fellows.”
- silicon.com, March 2003

Introduction

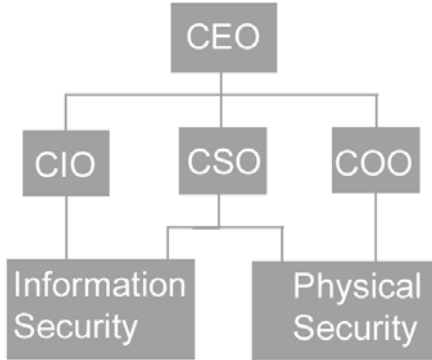
Convergence of Physical and Network Security

If there is a topic that has excited the security trade press of late, it has been the merger of physical and network security. The concept first appeared in articles dated in 1997, but has really taken hold in the wake of 9/11. The idea is simply this: in most companies, physical security and network security have operated as two separate departments, most often reporting to two different branches of the organization. They have selected different systems, different types of people, and often viewed their jobs as completely unrelated. As many in the press have pointed out, there are a number of reasons to increasingly view these groups as having more in common than not. In particular, the argument goes, there are a number of areas where cooperation would reduce corporate risk, while cutting expenses at the same time. Ultimately, both departments

would merge under the management of a single CSO.

Is It Really Happening?

There is no question that a large segment of the world's companies have hired CSOs and placed all forms of security under their responsibility. In fact, CSO Magazine estimates that 54 percent of corporations with \$1B in annual revenue have one. It is also fair to point out, however, that not all of those have full responsibility for both physical and network security.



While there is clear movement toward a single department for security, it is not by any means a stampede. In fact, many industry experts doubt the long-term viability of this trend. This paper examines the driving forces behind the trend, and sheds some light on the likelihood of this movement becoming a best practice.

“Physical and IT security convergence seems just one leap away...and may remain that way.”
- Information Security Magazine, June 2004

Driving Forces Behind The Merger

In order to gauge the likelihood of this convergence gaining momentum, let's look at the driving forces behind it. As with any change of this type, there are some forces, which accelerate the change, and others, which slow it down.

PRO Political Climate Favors Hiring Chief Security Officers

In this post-Enron world, there has been a tremendous focus on corporate governance. Members of the board of directors are feeling more pressure than ever to watch the store. From their view, having a single throat to grab is comforting. In the medical or banking arenas, it may be required. As legislation such as HIPAA, GLBA, and Sarbanes-Oxley enter the picture, the risk of not having an anointed high level leader whose mandate is to create a security culture, may simply be too high to accept. In the words of one industry wag, an advantage of having a CSO is to centralize blame.

From a convergence point of view, the impact of having a CSO is clear. Even if he or she chooses to maintain separate groups for physical and network security, there will be tremendous pressure to view the problem holistically, and establish a culture that encourages cooperation and discourages wasteful duplication. Ultimately, while having specialists can be justified, it may be difficult to defend having two departments.

PRO Technology Merging

Today's security systems are based on IT technology, with network based panels, high-end servers, and enterprise level databases. As we move toward tomorrow, with IT based cameras, network video servers, and "appliance" based

systems, security systems will require the full knowledge of an IT group to administer. That knowledge, and the cost that goes with it, may be beyond the means of even the most diehard "control your own destiny" physical security director.

PRO Similar Threats

While the technologies used for protection may be different, most attackers won't see it that way. A company's data can get stolen by someone breaking through a firewall and entering a database, or breaking through the door and stealing a hard disk. Industrial espionage can occur by breaking a window, or by reactivating a stolen ID badge. Attackers will take whatever path is easiest to compromise your company. Since your threats are not isolated along IT and Physical lines, there will be a strong argument that your approach to minimizing the risk should be tightly coordinated and holistic.

PRO Activity Overlaps

Most companies have already made some of the obvious moves in this area. It is rare for a security department to host its own servers or install proprietary networks today. That said, there are still plenty of opportunities for synergy in at least three areas. First, both groups do "identity management". Often, the physical security group has built a database of all employees and contractors, listing their permissions to enter buildings and areas. Similarly, the network security people have built a separate but equivalent database listing what

applications those same people can log into on the network. Add in the issuance of badges, the use of biometrics for log in, and auditing the database, and the overlap is huge.

Secondly, investigations are a significant workload for both departments. While the tools may be different today, the underlying investigative logic is not, and the threats have a great deal of commonality. In addition, there is a significant amount of work in process to provide tools that combine the audit trails of the two areas. The ability to see both physical and network violations, combined with CCTV records in one log, will simplify many investigations.

Finally, there are many opportunities to use each others existing infrastructure to save time and effort. Areas such as database backups, hardware status monitoring, and patch administration, are often done poorly or not at all on physical security systems. Conversely, it is not at all unusual for server rooms to have no log of physical access, and no CCTV coverage.

CON Dramatically Different Culture

The lack of respect that is often found between the Physical and IT security groups is legendary. This one issue can often be the most difficult part of reorganizing to co-manage these groups. Still, the first step is to make sure that both groups understand the consequences of poor security in either arena; information can vanish, confidential data can be stolen, and people can die. Mutual respect will come from working together, but often only with significant time and effort and sometimes only with personnel changes.

CON Different Knowledge Set

On the surface, it seems simple. The physical guys don't know how to configure a VPN, and the IT guys don't know how to body tackle an intruder. In reality, the knowledge gap is generally deeper and wider than most think. We all know the IT guys have the technology edge, but even they don't have the background that the Physical guys do in door hardware, camera placement, lens selection, etc. Neither group is in a position to take over the other's responsibilities in the short term.

CON Loss of Control

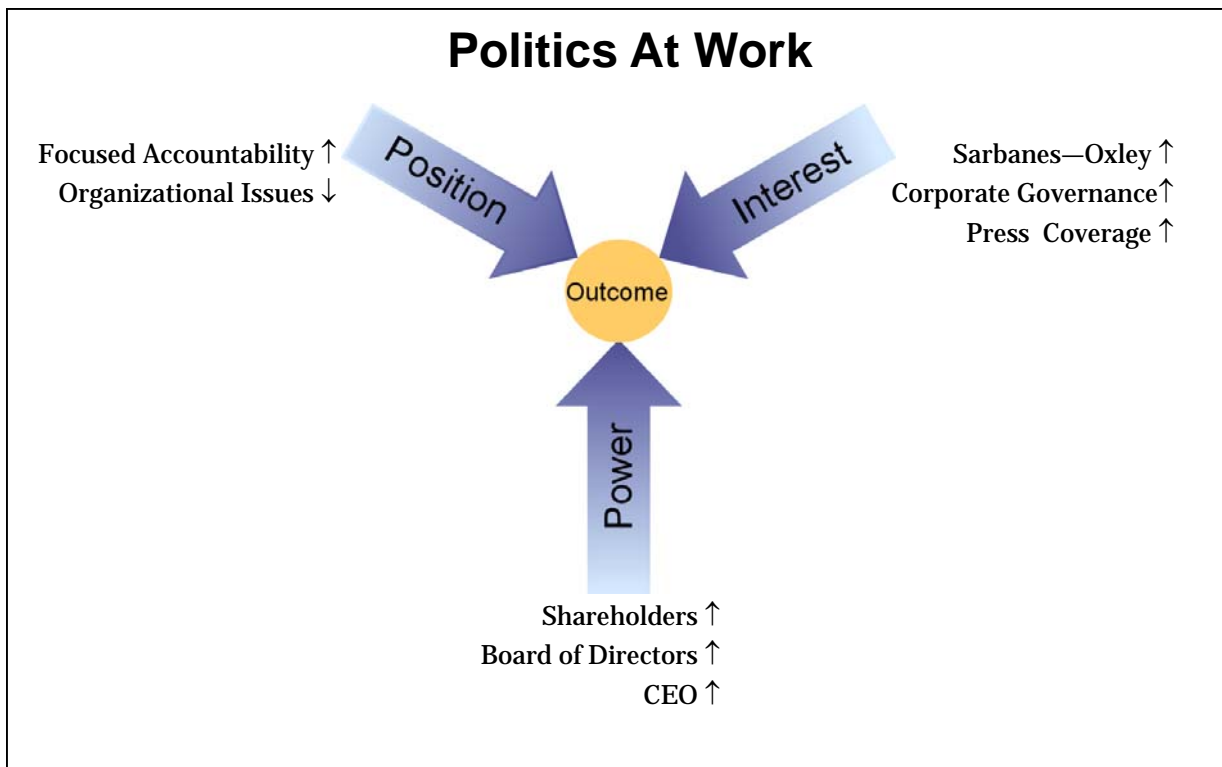
One of the biggest fears from both sides seems to be a loss of control. While there is a level of paranoia on the IT side regarding anyone but the chosen few maintaining network attached hardware or changing permissions, the bulk of the sensitivity is often on the Physical side of the house. It is often a result of not being viewed as a mission critical application, and therefore, not deserving of special planning during network maintenance or a high priority for system upgrades. In particular, a loss of budget control could easily mean being at the bottom of the capital spending list.

CON Politics

The fear of a loss of control from the physical side, or an increased workload and responsibility level from the IT side, has produced some very biased behavior. Sometimes the turf war has been so bad that it was uncontrollable even when both groups reported to the same CSO. While these games can go on for a long time, eventually the pressure for simultaneous risk and expense reduction will force decisions to eliminate duplication.

Not All Forces Are Equal

The classic studies on how to predict the outcome of a political situation will tell you that there are three major factors to consider. First, of all the people involved, what are their positions on the matter? Secondly, how much do they really care about the issue? Thirdly, how powerful are those people within the organization? The current political environment seems to map out like this. A number of powerful people in the organization such as the Board of Directors and CEO are becoming involved in the issue of corporate security. Their interest level is rising, not only because of legislative issues, but also due to the high profile corporate governance cases that have hit the media. Those same powerful and interested people also tend to push for results and accountability. Roll all of this together, and there is a strong bias which favors the forces that are attempting to merge these groups together under one management team.



The Relevance Of Sarbanes—Oxley

Since IT underlies the very business of recording and reporting all financial activity, it follows that a lack of control over either physical or network access of the IT system would imply a lack of control over the organization's financial reports, in direct violation of Sarbanes-Oxley section 404. This will be an audit item.

Outlook

Is it right for your company? Depends... In order to work, all the key ingredients must be present. Those elements are:

- ✓ Strong leadership and a belief in the concept at the CEO level.
- ✓ The availability of a CSO that understands the management of both worlds.
- ✓ A middle management team that understands why this makes sense
- ✓ A viable plan to make the transition

Next steps? Here are our recommendations:

1. Start by making your current organizational structure as good as it can be. Having a CSO is not a requirement for cooperation.
2. Most companies should have an impartial “outsider” do an assessment of the current status of both security efforts, and the opportunities for synergy. Develop a plan and then push it hard.
3. Befriend your security partners. No matter what the organizational structure, IT and Physical security now need to work together, and that requires trust.
4. Consider whether your current organizational structure is getting in the way of minimizing risk for the company. If so, you need to be supportive of a change.

No matter how you count, there are more forces pushing the IT and Physical security groups together than there are pulling them apart. This doesn't mean, however, that the majority of companies are rushing to smash the two together under a CSO. The obstacles can be significant. That said, we have clearly entered an era where a lack of cooperation between the two groups will be obvious and intolerable. Will a merger be the best practice of the future? The odds say yes. The opportunities to provide better security at less cost are too tempting to pass by.

“Organizational reputation, the uninterrupted reliability of the technical infrastructure and normal business processes, protection of physical and financial assets, the safety of employees, and shareholder confidence all rely in some measure upon the effectiveness of an accountable senior security executive.”

**- CSO Guideline
ASIS International, January 2004**

About the Author

Rich Anderson is the President of Phare Consulting Inc. Rich has served as both the VP of Marketing and the VP of Engineering for GE Security's Enterprise Group. During his 25 years of senior positions in the high tech arena, and his 14 years in security, he has managed a variety of challenges, from organizational design to product design, and process analysis to market analysis. Rich has a BSEE from Case-Western Reserve University and an MBA from Baldwin Wallace College.

About Phare Consulting Inc.

Phare Consulting is a Boca Raton, Florida based management consulting firm focused on the development of successful strategies and organizations. Our business is helping to make companies grow. With an extensive background in high-tech B2B companies, and a particular emphasis on the electronic security industry, Phare is uniquely positioned to deliver results - not just reports - to our clients. Learn more today by calling 1.561.962.2770.



Phare Consulting, Inc.
2385 Executive Center Drive
Suite 100
Boca Raton, Florida 33431
561.962.2770
info@phareconsulting.com
www.phareconsulting.com