

# True "convergence"

Bar Biszick, (csqa, cissp, cisa)

September 6, 2004

An article in the April 15, 2004 edition of CIO Magazine explored the debate over security "convergence." The term, as it is currently used, represents the merging of physical and information security responsibility. The article tried to expose the pros and cons of this issue by obtaining opinions as to whether policy as it relates to information security should remain with the CIO or be moved out of IT, presumably under a CISO who is usually also accountable for physical security. Thus, convergence would take place.

There are good reasons to centralize your security policy management. However the article also spoke about transferring responsibility and accountability as well, and this is why the article slightly missed the mark for me, as it did with other readers. While the article provided good hints on strategies for bringing information security together with physical security, it fundamentally failed by focusing mainly on the location of the responsibility--which is only nominally important--rather than fully explore the nature of the responsibility of security--which is paramount.

Security is an organizational risk responsibility, whose factors for success are multi-dimensional and cross-disciplinary. Threats cannot be neatly assigned to one division or another in an organization. For instance, hackers can obtain a user password by applying brute force technology tools as in a dictionary attack. Countermeasure responsibility usually lies with the CIO who sets system password policy. But it can also be obtained by physically stealing a remote user laptop. Given unlimited access to the box, the password will likely be broken. Countermeasures against asset theft are the responsibility of the Physical management team, who might require desktop locking devices for all laptops used on site. But a password could also be obtained through Social Engineering. An unsuspecting user might hand over their password when asked by someone posing as a network administrator who has seems to have a legitimate need for it. In this case, countermeasures are the responsibility of management who should provide appropriate HR orientation for new hires, and periodic security awareness training. So clearly the problem of information security exceeds the scope of the CIO. It is an organizational problem, not an IT problem. But transferring responsibility for those aspects a CIO and his organization can control is entirely the wrong approach.

We now know that firewalls will never be 100% secure, that sophisticated viruses move far too fast for detection and response to be of any real use, that no amount of security awareness will deter a dishonest or disgruntled employee, and that secure coding classes are often not much more than a refresher in coding 101 (50% of coding problems are about quality, not security--the remainder being too specific to the technology and infrastructure to be taught). In this atmosphere, our attention must be on minimizing damage, maximizing awareness and professionalism, and optimizing security budget. You don't do that by just shifting fragmented security responsibility around in an organization. You do that implementing good security process, which can succeed even in the absence of named security roles.

The real root cause of security problems aren't the hackers, or the disgruntled or dishonest employees, or naive users--notwithstanding the fact that most of the cost of security problems stem from these. Most security problems stem from having a fractured security model that compartmentalizes security efforts across an organization (which leads to redundant security controls working at cross purposes), one that does not provide effective means for comprehensive security effort coordination (which causes confusion and diversity of perceptions), one that fails to quantify business risk (leading to uninformed business decision making), and fails to measure against clear security objectives (which leaves project and operations groups unable to determine how much security attention and budget should be

applied). In other words, the root cause of most security problems is the failure to effectively coordinate security efforts across the entire organization using a comprehensive framework that articulates, validates, and documents organizational security acceptability for every given case.

So I don't see convergence as being an all or nothing proposition. Whether you place policy management in the hands of a single person or entity, such as a CISO or Security Group, we should keep Information Security responsibility with the CIO, Security Awareness training with Corporate Communications, and Security Policy making with the policy makers. Instead, what is needed is an Enterprise Security Coordinator, responsible the formalization and stewardship of the Enterprise Security vision and for assuring that that management's security vision is appropriately implemented by all participants in their respective area.

Companies serious about security know that, and also know that ultimately, security is a business risk, and the stewards of all business risk are collective senior management. Companies that assign all security responsibility under one individual in any capacity other than as enterprise coordinator for all organizational security efforts fail to recognize the complexity of the problem and its solution. Ultimately, the single entity named for responsibility and accountability becomes the security "sacrificial lamb," when something goes wrong.

What characteristics would make a good Security Coordinator? One could argue that, while preferable, the Security Coordinator need not necessarily be a seasoned security specialist. Skills in communication and risk management are at least as important and a mix of these, along with at least a strong overview knowledge of security principles is probably preferable. Other complimentary disciplines include audit and compliance, standards, process analysis, quality assurance and change management.

Feasibility of any change to the IT infrastructure should require consideration of audit, legal & regulatory constraints, security policy and procedures, inputs from tactical operations personnel, risk management personnel, and IT management. Without some entity coordinating the process, CIOs, Project Managers, Developers, QAs and Operations personnel cannot make sound judgments as to how much security, optimally, should be built into the system and its supporting processes. A steward of the organizational security vision would be able to negotiate and coordinate required resources from other sectors, ultimately delivering a core set of security requirements that represent executive management's security acceptability for any given project. Such an individual would assure that due diligence is performed for security prior to any significant change of the IT infrastructure. He would coordinate the review of current security policies, processes and procedures and obtain proof that the infrastructure can accommodate the proposed changes without undermining existing security measures, He would facilitate the real time investigation of changing legal and regulatory issues and threats, would ensure that breach history is reviewed, that business criticality and security levels are not overlooked, and that enterprise programs that relate to security are appropriately updated—those for business continuity, disaster recovery and training.

It makes good sense to consolidate security policy to ensure consistency and compatibility of policies that serve different parts of the organization. But it makes no sense to offload security responsibility and accountability outside of the divisions that know best what is prudent and practical, and are ultimately responsible for implementing security policy. Instead, let's expand the notion of convergence to encompass the entire security effort—not just those connected to IT and Operations--and place someone at the helm to guide all security efforts across the entire organization.