InformationShield

The Importance of Defining and Documenting Information Security Roles and Responsibilities

By Charles Cresson Wood, CISSP, CISA, CISM

Many organization's information security efforts are characterized by a surprising amount of chaos and unnecessary internal politics. At an increasing number of organizations, lack of clearly articulated roles and responsibilities has become one of the most serious impediments to information security progress. This paper discusses the major reasons why an organization should establish clear information security roles and responsibilities, and how to increase management awareness of the information security staffing requirements.

[Material for this paper is excerpted from Information Security Roles and Responsibilities Made Easy]

The Labor Costs of Security

The total cost of ownership (TCO) models developed by a variety of industry analysts such as the Gartner Group indicate that labor represents anywhere from two-thirds to three-quarters of the on-going cost associated with information technology. In this context, on-going costs include system configuration, administration, maintenance, training, and the like. Information security is just one of many niche areas within the information technology field, but its costs are also dominated by labor. In spite of what information security vendor sales representatives may tell you, the information security field is still in an embryonic state, and many essential activities have not yet been automated, or have not yet been automated to any significant extent. This means that all organizations, no matter how sophisticated they happen to be, will be critically dependent on the work of people to achieve a truly secure information technology environment.

If your organization has not yet clarified information security roles and responsibilities, then the organization is much less likely to be successful with other tasks related to information security. For instance, if the responsibility

for information security training and awareness has not yet been assigned, the probability is high that are this job is not being done, or at least it's not being done adequately.

For example, workers at your organization may wonder whether this work should be done by the Human Resources Department, the Training Department, or the Information Security Department. Thus, it is not an exaggeration to say that clear roles and responsibilities are an essential prerequisite for all information security activities. To genuinely be effective in the information security arena, every organization needs to consciously specify and coordinate the activities of a team of people, each with different information security roles and responsibilities.

Why Should You Clearly Document Roles & Responsibilities?

There are a number of key reasons why an organization should define and document information security roles and responsibilities. Even if roles have been defined, in this era of emphasis on corporate governance it is critical to document them as well. If information security roles are not clearly defined in your organization, and a roles and responsibilities clarification project is still missing in your organization, you are encouraged to use the following discussion to write a project justification memo to management.

Garner greater respect and greater resources for the information security function

Having specific documented role and responsibility statements is advisable for every organizational unit, not just the information security group. Those organizational units with fully developed role and responsibility statements will enjoy greater respect and greater resources. At many organizations, information security is a new or still-undeveloped organizational function. This means that these same organizations are often missing documents that cover information security job descriptions, mission statements, and reporting relationships. When these roles and responsibilities are documented and approved, the information security function will be increasingly recognized as a legitimate and on-going organizational function, worthy of respect and its own share of organizational resources.

Demonstrate top management support for information security

One of the most important reasons to document role and responsibility assignments is to demonstrate top management support. Information security specialists often feel as though many people oppose what they are trying to do. Occasionally information security specialists must take an unpopular position, for example, postponing the cut-over to a new software application until appropriate controls can be included. If the information

security specialists aren't going to be outvoted, outmaneuvered, and otherwise overruled, clearly documented top management support for the information security function must have been documented. Thus, with documented and approved roles and responsibilities, information security specialists can prevent or expediently resolve many arguments, and then get on with their work.

Establish formal communication channels with top management

At many organizations, the information security function has been repeatedly moved from department to department. Many of these departments may not have known what to do with the information security function. These departments often treat the information security function like an unwanted foster child that really never had a home. As a result, departmental management may not have seriously considered the recommendations offered by information security specialists. Consequently, management may have postponed or failed to fund a number of important information security projects. But when roles and responsibilities for the information security function are specified and approved by top management, all this can quickly change. Then the information security function will have a real home, in other words, it will know where it fits into the organizational structure. In the course of defining a formalized and permanent home for the information security function, the ways that this function works with other internal groups will be defined. Then the information security function will have formal communication channels with top management that can be used to help get important projects underway.

Foster coordinated team effort to safeguard information as it travels around

One additional important reason to document information security roles and responsibilities involves overcoming an erroneous viewpoint that information security is something that can be handled by specialists in the Information Security Department working alone. The job is way too big and way too important to be left to the Information Security Department. When roles and responsibilities are documented, specific people inside and outside the Information Security Department will be held accountable, and this in turn will cause them to become proactive. Without this accountability, in many cases they will wait until there is a problem, and then do their best to handle whatever has taken place. Today, organizations can no longer approach information security with a "fix on failure" mentality. Research studies show that information security is ten times less expensive when it is built into application systems before these same systems go into production use, as opposed to when security is added-on after these systems have already been placed into production operation. Said a bit differently, when it comes to information security, proactive planning and management is considerably less expensive than reactive repair and correction efforts.

Enable management to better allocate organizational resources to outsourcing firms, consultants, etc.

Many organizations are now turning to outsourcing firms to handle their information security needs. While some management responsibilities such as making final decisions about information security policies should ultimately rest on the shoulders of internal management, a considerable amount of the security work can be outsourced. If roles and responsibilities are not clearly established at the time that a contract is negotiated, the organization that contracted the outsourcing firm may find itself in a difficult spot. The outsourcing firm may claim that the requested service (such as forensic investigation of a system break-in) is not in the contract, and that the customer must pay an additional fee. All this of course assumes that the outsourcing firm has technically-competent people available at the time they are needed.

Of course, other consulting firms can also be called in, but with any of these options, precious time will be wasted negotiating fees, defining the work to be done, etc. While all of these ad-hoc business arrangements are being made, a hacker could be on the loose inside the internal network at your organization. To keep losses to a minimum, it is absolutely essential that roles and responsibilities for all important information security activities be defined in advance in outsourcing contracts (this topic is explored at length in the chapter that covers "Outsourcing Firms" in *Information Security Roles and Responsibilities Made Easy* [1]).

On a related note, if management wishes to outsource some or all of the information security function, or if management wishes to retain contractors, consultants, or temporaries to assist with information security, then roles and responsibilities must first be specified. Unless roles and responsibilities have been clearly defined, management will find it difficult or even impossible to adequately draw up requests for proposals, legal contracts, outsourcing agreements, service level agreements (SLAs), and other documents with these third parties. Thus clear roles and responsibilities can be a significant enabler which allows management to better allocate organizational resources.

Minimize the costs associated with the provision of adequate information security services

A related business management reason to establish clear roles and responsibilities is that, in so doing, management will reduce costs to adequately handle information security. Through the specification of job descriptions, management can select and retain people who are adequately qualified, but not over-qualified. This will in turn help to keep salary costs down. Likewise, a number of organizations are increasingly taking the

security tasks performed by Systems Administrators and assigning these tasks to new information-security-specific positions like Access Control System Administrator. Not only does this change provide better separation of duties, it also allows the organization to lower costs because the security-specific jobs often pay less than the Systems Administrator jobs. On a related note, when clear roles and responsibilities documentation exists, management will know exactly what types of training programs it should send internal staff to, and this will help avoid wasting resources on training that is not directly relevant to the jobs that the involved individuals perform.

Reduce chance that information security staff will be single point of failure

Rather than eliminating the need for human involvement, the new information systems that organizations are using today (such as Internet commerce systems) are increasing the reliance on certain types of people with specialized skills. For example, if a critical technical person were to abruptly leave his or her employer, the organization might be hard pressed to continue certain technical computer operations without this person. This increased reliance on people with highly specialized skills and training can be reduced by backup personnel, cross-training, sharing job responsibilities, documenting the work, and other tasks associated with the development of clear information security roles and responsibilities.

The information security field is still embryonic when compared to the marketing or accounting fields. While some interesting new technological solutions to information security problems are now on the market, in most organizations the achievement of effective information security critically depends on people. At this point in the evolution of the technology, there are many information security problems that can only be handled by people. For example, there is no commercially-available technological solution to the social engineering (masquerading) threats that all organizations face. All too often, the people within organizations don't understand what management expects them to do, and this in turn will prevent the achievement of information security goals. Only after roles and responsibilities have been clarified and documented, and after selected people are then appropriately trained, can these same people participate as essential members of the team that handles information security.

Demonstrate compliance with internal policies, as well as laws and regulations

Another good reason to document roles and responsibilities is to demonstrate compliance with internal policies as well as external laws and regulations. Auditors and government examiners are impressed with documentation. It gives them the feeling that things are under control. A surprising number of

modern laws include the requirement that information security roles and responsibilities must be specified. For example, within the United States, the Health Insurance Portability & Accountability Act (HIPAA) [2] requires that firms in the health care industry document information security related roles and responsibilities. *(See Table 1 for a list of laws and security frameworks that require specific documentation of security roles and responsibilities.)*

On a related note, with clear documentation defining information security roles and responsibilities, an organization can show that it is operating in a fashion which is consistent with the standard of due care. Being able to demonstrate this consistency may be very important in terms of reducing or eliminating management liability for losses and other problems. Such documentation may help with a variety of liability concerns including computer professional malpractice and breach of management's fiduciary duty to protect information assets. One example of an authoritative statement of the standard of due care, which includes the requirement that information security roles and responsibilities be clearly specified, is entitled "Generally Accepted Information Security Principles" (GASSP) [3]. Demonstrating compliance with the standard of due care can help shield management from negligence and related liability claims.

Increase worker efficiency and productivity by eliminating confusion

Perhaps the most significant reason to establish and document clear roles and responsibilities involves increasing worker productivity. Statistical studies of business economics indicate that about half of productivity growth over time comes from more efficient equipment, and about half comes from better trained, better educated, and better managed labor. Thus the clarification and publication of information security roles and responsibilities can have a substantial positive impact on productivity, and thereby markedly improve profits. The information security field is a new area, and there is still great confusion about who should be doing what. For example, when a worker has his or her laptop computer stolen, who should this event be reported to? Should a notice be sent to the Information Security Department, the Physical Security Department, or the Insurance Department? Maybe the notice should go only to the worker's manager? Without clear roles and responsibilities, users will unnecessarily spend time figuring out the answers to questions such as these. Likewise, if roles and responsibilities are clarified and documented, employees will not waste their time trying to figure out who to invite to certain meetings or who needs to sign-off on certain proposals.

Table 1: Regulatory and Industry Framework Requirements for Establishing Information Security Roles and Responsibilities

Regulation/Framework	Industry	Specific Requirements
Sarbanes-Oxley Based on CobIT (Contol Objectives for Information Technology) Version 4.1	**All – Publicly Traded Companies**	4.0 Define the IT organization and relationships 4.4 Roles and Responsibilities, 4.6 Responsibility for Logical and Physical Security,
PCI-DSS Payment Card Industry Data Security Standard Version 1.2	**Payment Card Industry**	PCI 12.5 Assigned information security management responsibilities.
HIPAA Privacy and Security HIPAA (Health Information Portability and Accountability Act) Final Security Rule	**Healthcare**	Section 164.308(a)(2) - Assigned Security Responsibility In the Privacy Rule, Administrative requirements (section §164.530) requires personnel designations for such roles as Chief Privacy Officer.
FISMA/NIST NIST SP 800-53	**U.S. Federal Government**	NIST: Personnel Security (PS) "Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?" [Reference FISCAM SD-1.2]
NERC/FERC Cyber Security Standards for Critical Infrastructure Protection	**Energy/Infrastructure**	CIP-003-R R2. Cyber Security Leadership "The Responsible Entity shall also define ***the roles and responsibilities*** of Critical Cyber Asset owners, custodians, and users."
ISO/IEC 17799:2005 (ISO 27002) Code of Practice for Information Security Management	**All**	6.0 Organization Security 6.1.3 Allocation of information security responsibilities. 8.0 Personnel Security 8.1.1 Roles and responsibilities
GAISP Generally Accepted Information Security Principles (GAISP) V 3.0	**All**	Section 2.1 – The Accountability Principle "Information security accountability and responsibility must be clearly defined and acknowledged."

Conclusion

Information security is inherently inter-disciplinary and inter-departmental, and at many organizations, it is fast becoming inter-organizational. For example, an effective communications encryption system requires a mix of human resources ideas (such as training), computer science ideas (such as mathematics to determine key length), and management ideas (such as procedures for key recovery when a key is lost). In addition, to have an encryption system such as a virtual private network (VPN) work with business partners, these same people must work with their counterparts at other organizations. All this complexity requires a great deal of coordination if it's going to be effective. The roles and responsibilities of these individuals and organizational units must be clearly delineated if significant confusion and serious security lapses are going to be avoided.

Information Security Roles and Responsibilities Made Easy by Charles Cresson Wood provides additional justification for clearly establishing and documenting information security job functions. It also includes pre-written job descriptions, mission statements, and reporting structures which organizations can use to help build an effective security organization.

About the Author

Charles Cresson Wood, CISA, CISSP, CISM, is an independent information security consultant based in Mendocino, California. He has authored six books and over 300 technical articles dealing with information security. His best known book is entitled *Information Security Policies Made Easy* and contains over 1300 pre-written security policies with valuable implementation advice. His most recent book, entitled *Information Security Roles & Responsibilities Made Easy*, contains ready-to-go job descriptions, mission statements, and reporting relationship diagrams. In the field since 1979, Mr. Wood has done consulting work with over 135 organizations in over 20 countries. He specializes in organizational infrastructure projects related to information security including architectures, policies, guidelines, standards, procedures, and organizational designs. In 1996 he received the Computer Security Institute's Lifetime Achievement Award. He can be reached at ccwood@ix.netcom.com.

References

[1] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood, CISSP, CISM. Published by Information Shield, Inc. 2002-2008. [http://www.informationshield.com]

[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule. Department of Health and Human Services; Published in the Federal Registrar. [http://aspe.hhs.gov/admnsimp/index.shtml]

[3] Generally Accepted Information Security Principles (GAAP). [http://web.mit.edu/security/www/gassp1.html]

[4] ISO/IEC 17799:2005 (ISO 27002) – Code of practice for information security management - Published by ISO and available at BSI [www.bsi-global.org/]

[5] Payment Card Industry (PCI) Data Security Standard, Version 1.2 – Published October 2008, PCI Security Standards Council. [www.pcisecuritystandards.org]

[6] NIST Special Publication 800-53, Security Self-Assessment Guide for Information Technology Systems, November 2008 - Published by the National Institute of Standards and Technology (NIST). [www.nist.gov].

[7] Information Security Policies Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. 2002-2005. [www.informationshield.com]

informationshield.com

2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365