Organizing for Security: Trends and Best Practices

Executive Directions, Security & Risk Strategies, Security Infusion

Tom Scholtz

FOCAL POINT
While the emphasis on information security, risk management, and regulatory compliance continues to drive increased investment, the pervasive nature of these activities results in complicated organizational challenges.

CONTEXT
From an enterprise perspective, the information security discipline touches all aspects of day-to-day business operations. The close interrelationship with other important functions such as corporate risk management, regulatory compliance, and audit means that information security (infosec) accountabilities (the “who”), responsibilities (the “what”), and organizational positioning (the “where”) require close scrutiny. As with all organizational dynamics, there are no silver-bullet solutions, and standardized templates run the risk of oversimplifying the challenge. However, organizations should consider several trends and best practices when addressing their own unique infosec organization planning.

What Are Organizations Currently Doing?
META Group research indicates that about 60% of organizations have dedicated information security teams. About 28% have centralized teams, while another 28% have some blend of centralized and decentralized functionality, and 4% have structures with absolutely no centralized or corporate responsibility. In the 40% of organizations without dedicated infosec teams, responsibility for information security functions is typically allocated informally among IT staff members.

Of the organizations with a dedicated information security team, 62% report to the CIO/IT management, 12% to the CEO, 10% to the CTO, and 7% to the CFO/finance director. We believe these reporting lines will continue to change during the next two to five years as information security is moved out of the IT line of responsibility (see “The Reporting Structure in a Perfect World” section).

We expect staffing numbers for security teams to continue growing for the next 12 months. This growth will be especially fast for smaller organizations (<10,000 employees). Although the supply of people with technical and subject-matter skills is still fairly strong, a shortage exists for people with both security and business knowledge as well as effective executive communication skills. To this end, we are increasingly seeing individuals with no infosec background being appointed to lead infosec teams. This is generally a good strategy, as long as these people can establish a meaningful rapport with both the subject-matter experts (SMEs) in their new teams and their business audiences. Staff certification (e.g., CISSP) is becoming increasingly popular as a means of staff selection, but should not be used as a primary criterion. With many economies starting to pick up, organizations should institute strategies for retaining key resources and formalize staffing plans and hiring strategies as soon as possible.

The Basics: Non-Negotiable Roles and Associated Responsibilities

The starting point for any security organizational planning is to identify all the primary roles and associated responsibilities. META Group research indicates there are five such primary roles (see Figure 1), of which four should preferably be part of a dedicated (i.e., centralized or federated) infosec team.
• **Leadership:** This role entails a strong personification of information security and the enterprise security charter within the organization. Duties include executive-level relationship building, line management of the centralized security resources, and coordination of decentralized resources. This role also drives security strategy and the security program (see GNS Deltas 1086, 1084, and 973).

• **Analysis/design:** This is the traditional security specialist role, the main function of which is to support resource owners in developing relevant security policy and appropriate policy enforcement mechanisms. The effectiveness of this role predicates an important principle, that of the ultimate accountability of information security resting with business owners of the information, not with the security team. Indeed, the security team (and other functions such as internal audit) exists to support the business in shouldering this accountability.

• **Security operations:** This role is responsible for the day-to-day monitoring (i.e., operational audit) of the information security state of the business (see GNS Deltas 989 and 1038). Process ownership includes research, monitoring, scanning, response, forensics, and reporting.

• **Awareness communication:** Successful information security primarily depends on the cooperation and behavior of executives, users, and IT staff, hence the importance of an effective awareness communication and training program, managed by people with marketing and communications skills (see GNS Delta 922). This role includes the function of security coordinator, a person appointed within line-of-business (LOB) departments to act as interface between the security team, department management, and users.

• **User life-cycle management (ULM):** Increasingly called “user life-cycle management,” this role is responsible for the steps (provisioning, maintenance, and termination) associated with managing digital access rights of users. This role should preferably be as close to the business as possible, hence it usually reports within the LOBs. In such situations, however, it must have a tightly matrixed relationship with the rest of the security team, given the critical link between user life-cycle management and effective authentication and authorization. Furthermore, a consistent process and toolset is a prerequisite for efficiency, usually predating centralized system ownership.
Because the security team does not operate in isolation (see Delta 2336), ancillary roles are important. These include governance (as embodied in a security steering committee), audit, architecture, application development, and technical support (typically responsible for installing and managing security tools such as firewalls, VPNS, access control systems, and encryption tools).

**So What’s in a Title Then?**

The prevailing nomenclature in the US for the leader of the information security team is chief information security officer (CISO) or chief security officer (CSO). The situation is less standardized in Europe, with a number of titles being prevalent — e.g., director of information security, IT security manager, corporate information security officer, IT risk and security manager.

In larger organizations (especially European ones), differentiation is often made between the chief information security officer and the chief IT security officer. The former typically has a broad scope that includes all information and business applications, whether electronic or not, with the latter taking responsibility only for the IT infrastructure and systems.

Titles are less important than ensuring that all responsibilities are accounted for. Ideally, leadership titles should map to a logical taxonomy of control. At the pinnacle of this taxonomy is responsibility for corporate risk management (see Table 1). From this anchor point, responsibility for various risk and security management functions can be extrapolated. Given the current diversity of titles, responsibilities, and reporting structures, we use the term “information security principal” to indicate the role that assumes the respective leadership and management functions.

The leadership titles and associated responsibilities cannot be divorced from the evolutionary maturity and functions of the information security organization. In most organizations, the reporting link between corporate risk management (if it exists) and information/IT security has not yet been established. Indeed, the relative immaturity of the information security discipline has resulted in some organizations recently actively severing pre-existing reporting lines between corporate risk management and IT security (see “Some Contrary Strategies” section).

**Table 1 — Security Management Responsibilities, Titles, and Reporting Lines**

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>Representative Titles of the Information Security Principal</th>
<th>Typical Reporting Lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>All corporate risk management activities, including compliance, business risk management, and information risk management</td>
<td>Chief risk officer (CRO), director of corporate risk management (DCRM)</td>
<td>Board or CEO/managing director, sometimes the corporate services executive</td>
</tr>
<tr>
<td>All corporate security matters, including physical and logical security</td>
<td>Chief security officer (CSO), director of security (DoS)</td>
<td>CRO/DCRM, sometimes corporate services executive or CFO/finance director</td>
</tr>
<tr>
<td>All information security, whether electronic or not</td>
<td>Chief information security officer (CISO), director of information security (DIS)</td>
<td>CSO/DoS, sometimes direct to CRO/DCRM (when CSO/DoS function does not exist)</td>
</tr>
<tr>
<td>All IT-based information security, and security of all IT systems</td>
<td>Chief IT security officer (CITSO), director of IT security (DITS)</td>
<td>CSO/DoS, or sometimes the CISO/DIS</td>
</tr>
<tr>
<td>All IT-based information security, and security of all IT systems</td>
<td>Information/IT security manager</td>
<td>CIO/director of information services, director of network operations, IT facilities manager</td>
</tr>
<tr>
<td>Business-unit related information security functions</td>
<td>Information/IT security manager: LOB unit</td>
<td>LOB management, LOB IT management</td>
</tr>
</tbody>
</table>
As the security discipline matures, the team will require closer integration with corporate risk management and physical security. This will result in the security team falling under the auspices of the chief risk officer/director of corporate risk management (which will have responsibility for all corporate risk management efforts, including, among others, business continuity and disaster recovery). In the few organizations without a corporate risk management function, the security team will report directly to the board or the corporate services executive.

The chief security officer/director of security takes responsibility for all security aspects, including physical security. From the IT perspective, the next ranking executive is the chief information security officer/director of information security, who takes responsibility for all logical information security aspects. Depending on the organizational structure, the chief IT security officer/director of IT security, responsible for systems and IT-based information security, is either a peer position to that of the CISO or reports to the CISO.

In many organizations where the information security discipline is still viewed as a low priority, the principal reports into an IT functional unit, typically facilities or network operations. Also, in smaller organizations (<3,000 users), resource limitations result in all or most of the responsibilities identified in Table 1 being vested in one individual, typically called the CSO or DoS, and reporting to the CIO.

**The Reporting Structure in a Perfect World**

At the risk of both oversimplifying the organizational dynamics of information security and appearing prescriptive in the reporting structures, Figure 2 illustrates what META Group believes to be an important principle in the organizational position of the information security team. It indicates that, in a perfect world, the infosec team should not report into the IT organization, but rather into a separate risk management and/or compliance management function.

![Figure 2 — Preferred Reporting Structure](image)

This structure reinforces the understanding that information security is not just an IT issue, but rather a core component of overall corporate risk management. It also implies a somewhat higher corporate profile, with a senior authority level supporting more effective awareness communication. As indicated above, most security
teams still report into the IT function, but we believe that as these teams mature (in terms of policy management, communication, and appropriate technology adoption), they will increasingly be moved out of IT.

The Pros and Cons of Different Reporting Structures

The reporting level of the information security principal, while dictated by organizational realities and history, has a direct bearing on the effectiveness with which that individual can execute his/her duties. Although the rule of thumb is for the "position" of information security to be as high as possible in the corporate hierarchy, the various authority levels have their own advantages and disadvantages that should be kept in mind.

Table 2 — Advantages and Disadvantages of Reporting Lines

<table>
<thead>
<tr>
<th>Information Security Principal Reports Into:</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| CEO/Board                                   | • Indicates requisite level of executive attention and control  
• Provides power and authority throughout the business | • Potential lack of integration with corporate risk management  
• Viewed as "ivory tower" by IT and the business | |
| Corporate Risk Officer/CFO                  | • Optimum solution in most organizations — good executive exposure and close interrelationship with other risk management disciplines  
• Provides power and authority throughout the business | • Can result in lack of attention to immature security technologies and disconnect with IT infrastructure developments  
• Can be seen as an "ivory tower" | |
| CIO/Director of Information Services        | • Reasonable level of executive attention  
• Power and authority in IT | • Security potentially still projected as an "IT" issue only  
• Limited power and authority outside of IT — can be mitigated via relationships and strong local security coordinators | |
| Chief Information Technology Director       | • Well, at least it still reports to a "C" function … | • Security treated as a technology issue, disregarding the behavioral and cultural dimensions.  
• Limited power and authority outside of IT | |
| Corporate Facilities Management             | • Potentially some executive exposure  
• Apparent logical fit | • The relative immaturity of the information security discipline compared to physical security  
• The different skills and cultural approaches of the human resources | |
| IT Functional Management                     | • Well, at least there is a security team, right … | • Complete lack of executive awareness or support — worst of all possible worlds, indicating a serious disregard for the importance of information security and associated risks  
• No power or authority, not even in IT |
Other Factors That Influence Organization Design

Because all organizations are different, specific realities will influence the organizational dynamics of the infosec team. The following factors must be considered:

- The risk affinity of the organization impacts the importance of information security. The more sensitive the organization is (or individual operating units are) toward risk, the higher the profile (and subsequently the organizational level) of the information security team.

- The corporate structure (centralized vs. decentralized/federated, hierarchical vs. flat) and culture (prescriptive vs. democratic/collaborative) must be reflected by the structure and nature of the information security team. A prescriptive, hierarchical security structure will be as unsuccessful in a flat, democratic organization as a collaborative/collegiate approach will be in a hierarchical organization.

- Geographic issues influence organizational dynamics, and likewise must be reflected in the infosec team. Particular challenges associated with geographically distributed organizations include communication, catering for local business, cultural and regulatory requirements, and balancing these with the need for standardization and leverage of common principles and solutions.

- The organizational home of business continuity planning/disaster recovery planning must be considered. Even though conceptually BCP/DRP is often viewed as part of the infosec discipline, in many organizations it reports separately into the IT operations function. Given the commonality of processes (risk assessment, asset valuation/data classification, business impact analysis, policy management), an argument can be made for moving the BCP/DRP team closer to the infosec team (see Figure 2).

A Model for Decentralized/Federated Organizations

Organizations that have decentralized structures, with reasonable levels of autonomy delegated to the decentralized units, require more complex management and coordination structures, usually predating some kind of matrixed management relationships. Figure 3 depicts the typical model required for such organizations. The CSO function is a small, corporate function, typically consisting of a single person, or a small team for larger organizations. This function fulfills the corporate leadership role, coordinates enterprise-wide strategy and awareness communication, and manages those strategic processes (e.g., policy management, risk assessment) and projects that encompass enterprise-wide security initiatives (e.g., identity management). Depending on the level of decentralization, an enterprise security operations function can also be operated at a corporate level under the direct auspices of the CSO.

The business-unit CISOs take the leadership, communication, strategic, and operational process responsibilities for their respective units. The actual detail about levels of activity ownership between the respective management roles will differ from organization to organization, primarily influenced by prevailing political and cultural realities of the organization. A key success factor to the effectiveness of the specific dynamics becomes the level and maturity of process design and implementation within the organization (see GNS Delta 997).
Such a decentralized management construct requires numerous different governance and communications forums to make it work. Typical forums include the following:

- **Corporate information security steering committee**: This group is responsible for executive governance and for enterprisewide policy and investment decisions (see GNS Delta 929). Membership typically consists of LOB executives, the CSO, and selected CISOs and IT management (e.g., CIO, network manager).

- **Information security advisory board**: This is the tactical cooperation forum and, to a certain degree, the “brain trust” of all security activities across the enterprise. It facilitates the sharing of best practices and experiences, and acts in an advisory capacity to the steering committee. Typically meeting monthly or quarterly, its members are the CSO and all the CISOs.

- **Information security communications forum**: This constitutes the operational communications platform, usually an e-mail list and occasional meetings (typically once a year). The members are all information security staff — i.e., those whose roles and duties are primarily focused on information security activities.

- **Information security program**: This facilitates the strategic coordination of all security activities, and should be vested as an initiative under the auspices of the corporate information security steering committee. It sets the common vision, strategies, principles, and practices; guides the utilization of common management tools; and governs all the security projects. The members consist of a program manager, the CSO, CISOs, project managers, and appropriate staff (e.g., legal experts, HR representative, subject-matter experts).

META Group research indicates that in some extremely federated organizations, or organizations going through tough M&A activity (typically indicated by diverse corporate and national cultures having to be integrated), there is an explicit need for even more “facilitation and coordination” forums. These are responsible for fostering collaboration in activities such as standards development, advice and knowledge sharing, and assurance/validation of security controls. While some of these bodies have a semi-permanent nature, many others are more transient — i.e., they exist primarily to mitigate corporate cultural clashes and facilitate integration in the short term.
Another feature emerging in some decentralized organizations, especially those with very slim corporate functions, is the adoption of centers of excellence (sometimes called centers of competence) within business units. The objective is to leverage scarce resources around process optimization that can be leveraged by other business units, without undue (politically incorrect?) bolstering of the centralized corporate resources. Such COEs are typically constructed around processes such as risk management, monitoring, and incident response, forensics, awareness communication and liaison, and solution development.

Some Contrary Strategies

While this META Practice articulates a distillation of current and recommended best practices in infosec organizational strategies, it is worth noting that there are some organizations adopting strategies that can be interpreted as being contrary to current best practices and common wisdoms. These include the following:

- **Separating the IT risk management team from the infosec team:** The IT risk management team (whose purview goes beyond just information security to include such areas as vendor, technology, and sourcing risk) articulates the risks, while the infosec team (among others) addresses these risks. The logic is that the strategic risk management processes are different from the actual risk mitigation processes, and that information security processes are relatively more mature than IT risk management processes. Within the context of specific organizations, such an approach enables a closer linkage between IT risk management and business risk management.

- **Moving the infosec team from the corporate risk function “back down” into IT:** This is done as an interim measure to reverse a perceived dilution of information technology focus in a rapidly evolving technology environment. This is most commonly seen when a security program effort is perceived by upper management as having failed during its first three years.

These contrary strategies are typically based on valid arguments, and highlighting them serves to reiterate that information security organization design is far from an absolute science. Indeed, while organization design should focus on minimizing the seams between security processes and functions, yet still maintaining the principles of separation of duties (see Delta 2375), it should always be done within the context of the prevailing realities and needs of each organization.

**Bottom Line**

Security organization design should integrate best practices and principles with organizational and cultural reality.

*Business Impact: Failure to institute clear information security responsibilities within an appropriate organizational profile impedes effective awareness communication and investment, resulting in untenable risk.*