

# Re: CISO/Security Team roles and functions

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-02/msg00042.html>

---

- *From:* "Sergii Khomenko" <[sergey.khomenko@xxxxxxxxx](mailto:sergey.khomenko@xxxxxxxxx)>
  - *Date:* Mon, 4 Feb 2008 18:51:35 +0200
- 

Hi Soul,

I recently (few monthes) joined information security management unit in telecommunication company and also had to go through the roles/responsibilities study. Here is what I found in CISSP all-in-one guide:

## The Data Owner

The data owner (information owner) is usually a member of management who is in charge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information. The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting.

The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

## The Data Custodian

The data custodian (information custodian) is responsible for maintaining and protecting the data. This role is usually filled by the IT or security department, and the duties include performing regular backups of the data, periodically

## Re: CISO/Security Team roles and functions

validating the integrity of the data, restoring data from backup media, retaining records of activity, and fulfilling the requirements specified in the company's security policy, standards, and guidelines that pertain to information security and data protection.

### The System Owner

The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

### The Application Owner

Some applications are specific to individual business units for example, the accounting department has accounting software, R&D has software for testing and development, and quality assurance uses some type of automated system. The application owners, usually the business unit managers, are responsible for dictating who can and cannot access their applications (subject to staying in compliance with the company's security policies, of course). Since each unit claims ownership of its specific applications, the application owner for each unit is responsible for the security of the unit's applications. This includes testing, patching, performing change control on the programs, and making sure the right controls are in place to provide the necessary level of protection.

### The Security Administrator

Anyone who has a root account on Unix or Linux systems or an administrator account on Windows or Macintosh systems actually has security administrator rights. (Unfortunately, too many people have these accounts in most environments.) This means they can give and take away permissions, set security configurations, and mess everything up if they are having a bad day. However, just because a person has a root or administrator account does not mean

## Re: CISO/Security Team roles and functions

they are fulfilling the security administrator role. A security administrator's tasks are many, and include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. (The security administrator should not actually approve new system user accounts. This is the responsibility of the supervisor.) The security administrator must make sure access rights given to users support the policies and data owner directives.

### The Change Control Analyst

As someone wise once said, the only thing that is constant is change. So, when change does take place, someone must make sure it's safe. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens&

### The Data Analyst

Having proper data structures, definitions, and organization is very important to a company. The data analyst is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. For example, payroll information should not be mixed with inventory information, the purchasing department needs to have a lot of its values in monetary terms, and the inventory system must follow a standardized naming scheme. The data analyst may be responsible for architecting a new system that will hold company information or advise in the purchase of a product that will do so. The data analyst works with the data owners to help ensure that the structures set up coincide with and support the company's business objectives.

### The Process Owner

Ever heard the popular mantra, "Security is not a product, it's a process"? The statement is very true. Security should be considered and treated like any another business process

## Re: CISO/Security Team roles and functions

not as its own island, nor like a redheaded step-child with cooties.

(The author is a redheaded step-child, but currently has no cooties.)

All organizations have many processes: how to take orders from customers; how to make widgets to fulfill these orders; how to ship the widgets to the customers; and how to collect from customers when they don't pay their bills; and so on.

An organization could not function properly without well-defined processes.

The process owner is responsible for properly defining, improving upon, and monitoring these processes. A process owner is not necessarily tied to one business unit or application. Complex processes involve many variables that can span different departments, technologies, and data types.

### The Solution Provider

Every vendor you talk to will tell you they are the right solution provider for whatever ails you. In truth, several different types of solution providers exist, because the world is full of different problems. This role is called upon when a business has a problem or requires a process be improved upon. For example, if Company A needs a solution that supports digitally signed e-mails and an authentication framework for employees, it would turn to a public key infrastructure (PKI) solution provider. A solution provider works with the business unit managers, data owners, and senior management to develop and deploy a solution to reduce the company's pain points.

### The Supervisor

The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security, distributing initial passwords, making sure the employees' account information is up-to-date, and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

## Re: CISO/Security Team roles and functions

### The Auditor

The function of the auditor is to provide a method for ensuring independently that management and shareholders of an organization can rely upon the appropriateness of security objectives as well as the information they are being provided with regarding the status of the organization as a whole. The auditor is brought in to an organization to determine if the controls that have been implemented by the administration for either technical or physical attributes have reached, and comply with, the security objectives that are either required for the organization by legislation or have been deemed necessary by the governance of the organization. Auditors can conduct either internal or external auditing of an organization and a combination of both will usually provide the most comprehensive and objective evaluation of the organization being evaluated. The biggest concern for auditors is the question of bias and objectivity. The use of a third party for reviews will typically alleviate that issue, and in some instances there are actually legal mandates and regulations that prevent even third-party auditors from working for too many years in a row with a single organization in order to prevent them from becoming too close and thereby compromising their objectivity in evaluations and audits.

### The Security Analyst

The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are "in the weeds" and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than an implementation level.

### The User

The user is any individual who routinely uses the data for work-related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

## Re: CISO/Security Team roles and functions

### Why So Many Roles?

A decision maker is not the proper role for the data custodian or system administrator in protecting system resources. They may have the technical knowledge of how security mechanisms should be implemented and configured, but they should not be put into a position of deciding how the company approaches security and what security measures should be implemented. Too many times companies handle security at the administrator level. In these situations, security is not viewed in broad enough terms. Proper risk analysis is usually not performed. Senior management is not fully aware of the risks the company faces. Not enough funds are available for security, and when a security breach takes place, there is no efficient way of dealing with it. As stated previously, security should work in a top-down fashion to be ultimately successful. A company's security is not tied only to the type of firewall installed and the timeliness of security patches being applied. A company is an environment filled with various resources, activities, people, and practices. The security of the environment must be approached in a holistic way, with each part of security addressed in a serious and responsible manner. Although most environments will not contain all of the roles outlined previously, all of these responsibilities still must be carried out.

I hope this will help you.

Sergey

On Feb 4, 2008 2:21 PM, soul <soul1273@xxxxxxxx> wrote:

Hi All,

In my organization, the IT security Team is in charge of risk management, security policies, and administration/management of access, rights and authorization for in some applications (SAP, SWIFT,...)and Firewalls administration for traffic authorization on the network. But the new network division chief said that the security team should only provide security policies but not firewalls administration. He want the network team be in charge of the Firewalls administration. He said firewalls administration is operational security and should be perform by network team. But, I respond to him that there is need of segregation of duties and responsibilities. the Firewalls are installed by Network team but the administration of firewalls is perform by IT Security team like for the applications.

What can or should be the roles and functions of a security team in an organization?  
There is a confusion concerning some terminologies: OPERATIONAL SECURITY,  
SECURITY ADMINISTRATION,....

thank you.

Re: CISO/Security Team roles and functions

Re: CISO/Security Team roles and functions

---

Ne gardez plus qu'une seule adresse mail ! Copiez vos mails vers Yahoo! Mail  
<http://mail.yahoo.fr>