



TenStep Supplemental Paper

12 February 2004

Company Security Requires Coordination from Many Groups

Many years ago, companies began to realize the importance of a coordinated and comprehensive security policy. In the mid-eighties, it was not unusual to walk in the front door of many companies and visit whomever you wanted without any challenge. Some of these were huge companies. One company in particular started to require salespeople to register with the central receptionist. However, this was not done in the name of security, but was a response to complaints from managers about all the salespeople knocking at their doors.

For good or for bad, those days are pretty much gone. Over the past 15 years, companies have become more conscious of the need for security at all levels. Of course, this trend accelerated with the events of September 11. The days of open doors and open access are gone. More sophisticated security will be the rule. The goal is to allow all employees to have access to everything they need to do their jobs – and not one thing more!

Many groups are responsible for aspects of security

Security is a broad term, and the development of your overall security policy requires help from many different organizations. Let's look at some of the players who are involved.

Facilities. Your Facilities Department is typically responsible for the physical safety and security of the people in the company. This includes things like making sure that spills are cleaned up to avoid injuries and conducting fire drills to make sure people know what to do in an emergency. Facilities is also typically responsible for having guards at the front of the building, establishing a reception area where all visitors wait, issuing badges to authorized employees and contractors, setting up badge reading equipment, etc. All of this is to ensure a safe and secure working environment for everyone at the facility.

Human Resources (HR). HR has two main roles in security. First, they develop policies for how people interact with each other. From a safety and security standpoint, this includes policies on workplace harassment, threats, retribution, etc. Second, they help determine the consequences associated with unwanted and careless behavior related to security. For instance, workplace harassment should result in immediate termination, regardless of how "valuable" an employee is in their job.

Auditing. Your internal and external auditors are typically interested in making sure that you have good, sound security policies in place – and that you are following them. The best laid plans are meaningless if they are not executed, and auditing makes sure that security is in place and enforced appropriately. Auditing is also very interested in separation of duties. This means that different people or groups are involved in various parts of a process to ensure that one or two people cannot collaborate for personal gain. This includes making sure that people cannot approve their own expense report. On the IT side, it means that business users cannot directly manipulate production data and that developers do not approve their own source code changes to be moved to production.



TenStep Supplemental Paper

Business Units. Each Business Unit needs to have security policies that cover their business information, raw data, reports, trade secrets, etc. For instance, certain financial reports may need to be designated “Highly Confidential” and kept in locked drawers when not being used. On the other hand, certain Human Resources information, such as the company benefits package, may be accessible by all employees (although not necessarily available to outside parties).

Network administration. Different companies have different names for this group, but they are the ones responsible for the security, reliability and integrity of the computer network. This group makes sure that the entire network is safe from hackers, firewalls protect the network from outside access, and data and databases are protected and secure. They also watch over the email system to be diligent for viruses, and respond quickly if a virus gets onto the network.

IT development. The development group must build the proper level of security into the business applications. This can include passwords to gain access into applications, as well as making sure that people only have access to the business information they need for their job. This responsibility is in partnership with the Business Units. The Business Units define the policy for their applications and their data. The development group needs to rigorously enforce that policy in the applications they develop.

Central coordination

Most companies have a person or a group that has overall responsibility for security. As you can see, there are many groups involved with the various aspects of security. However, this Security Group is vital to coordinate the various activities and make sure that everything is consistent and coherent. One of the primary roles of this group is also to build awareness. In many cases, security breaches are not the result of malicious acts, but are the result of people not understanding the implications of their actions.

Everyone’s role is to follow the policies and suggest improvements

Everyone in the company has an obligation to understand the security policies that affect them and to implement the policies in their jobs. IT people need to be especially diligent since they sometimes have ways to circumvent security rules if they choose.

IT people especially should resist the urge to bypass security policy. If you think the policy impedes your ability to do your job, voice your concerns and work to change the policy. Remember that security is not only designed to protect your company assets from outside parties. It is also meant to protect company assets from you.