Organizational Security
Personnel & Legal Considerations

Module 4

At the end of this module, you should be able to:

- Describe the System Admnistrator's role in an organization.
- Describe the role of an Information System in an organization.
- Understand the need for Resource Custodians.
- Understand information sensitivity and classification.
- Understand who owns the data that you create.
- Understand copyrights, piracy and describe the Digital Millennium Copyright Act.
- Understand how to handle hirings, firings, and layoffs when it comes to information security.
- Describe the concept of separation of duties and why it is important.
- Understand how to handle lost or stolen equipment.
- Understand why law enforcement interaction is important.

The System Administrator Role

What role does a SysAdmin play in Organizational Security?

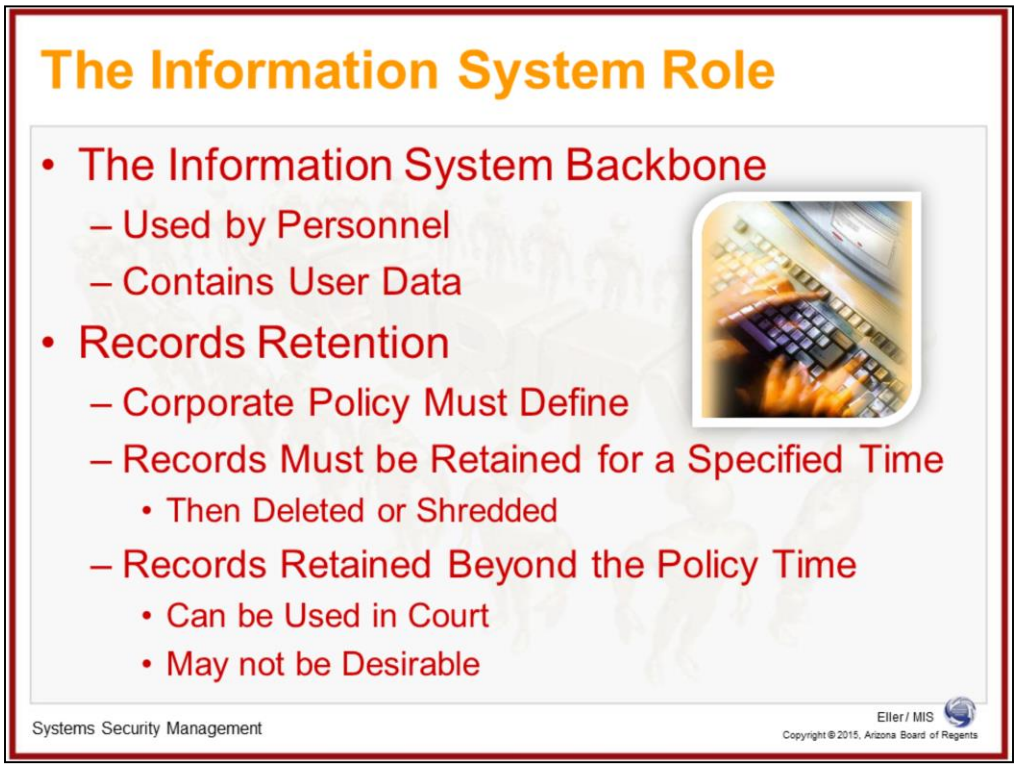
A SysAdmin's responsibility is to carry out organizational IT policy. What that policy is remains up to the organization to decide; however, in general the SysAdmin will be involved in the following:

Creation/Removal of Accounts – SysAdmins will regularly create user accounts for new employees and should be actively removing or disabling accounts for those employees who leave the company. This process is streamlined when the organization provides a policy that notifies the SysAdmin when an employee is hired or leaves. This helps the SysAdmin to provide new accounts in a timely manner and only keeps the accounts open for as long as the user is employed.

Assignment of Access Rights – Creating and removing user accounts is only one piece of the security puzzle. In order for a user to do their job they will likely need access to specific data or information on the network. The SysAdmin needs to know what the user needs access to in order to grant the appropriate access rights.

Provide Information to Management – Part of the SysAdmin's responsibility is to provide information to management. This information needs to be a high-level overview report of whatever information management needs. These reports may be requested by management from time to time, or specific reports may be required if defined within the organization's IT security policy.

Work with Law Enforcement – From time to time it may be necessary for the SysAdmin to work with local (or federal) law enforcement. This interaction can result from the theft of equipment or they could be called in due to a security breach. In the event a law enforcement agency seeks out the SysAdmin for assistance, a court order may be necessary in order for the SysAdmin to provide information.



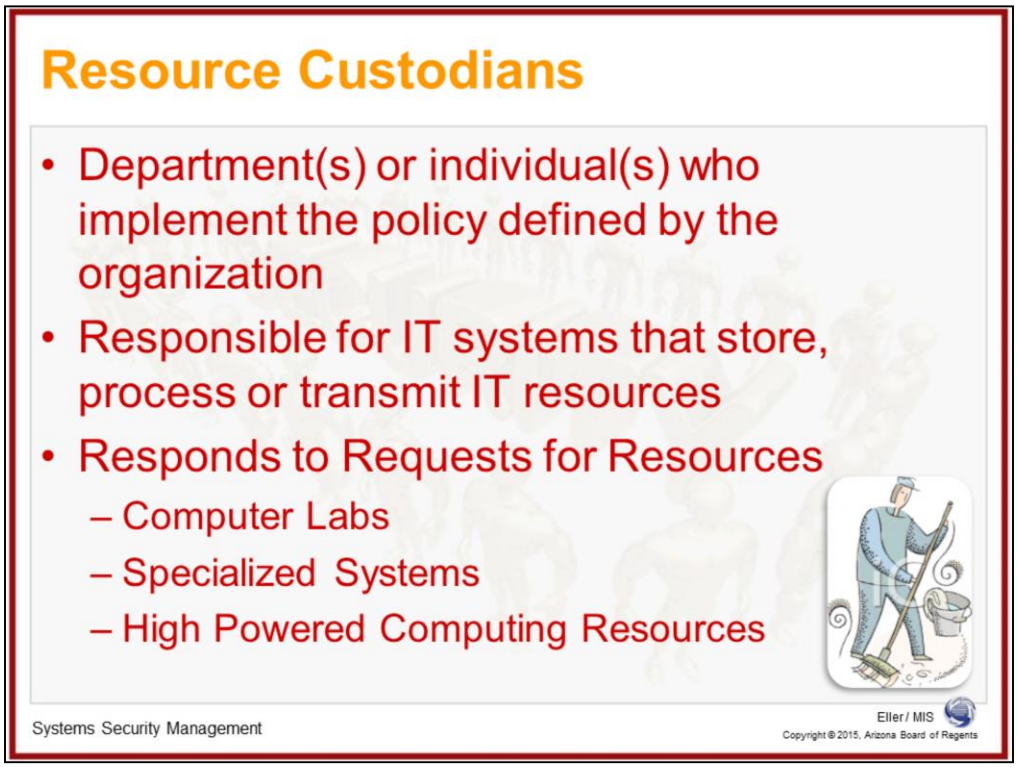
The Information System Role

The information system backbone is critical to the operations of many organizations. Information systems are used by personnel to store, retrieve, analyze, and manipulate user data in order to perform day-to-day operations. Depending on the organization, the information system may play a larger role than in others.

Records Retention

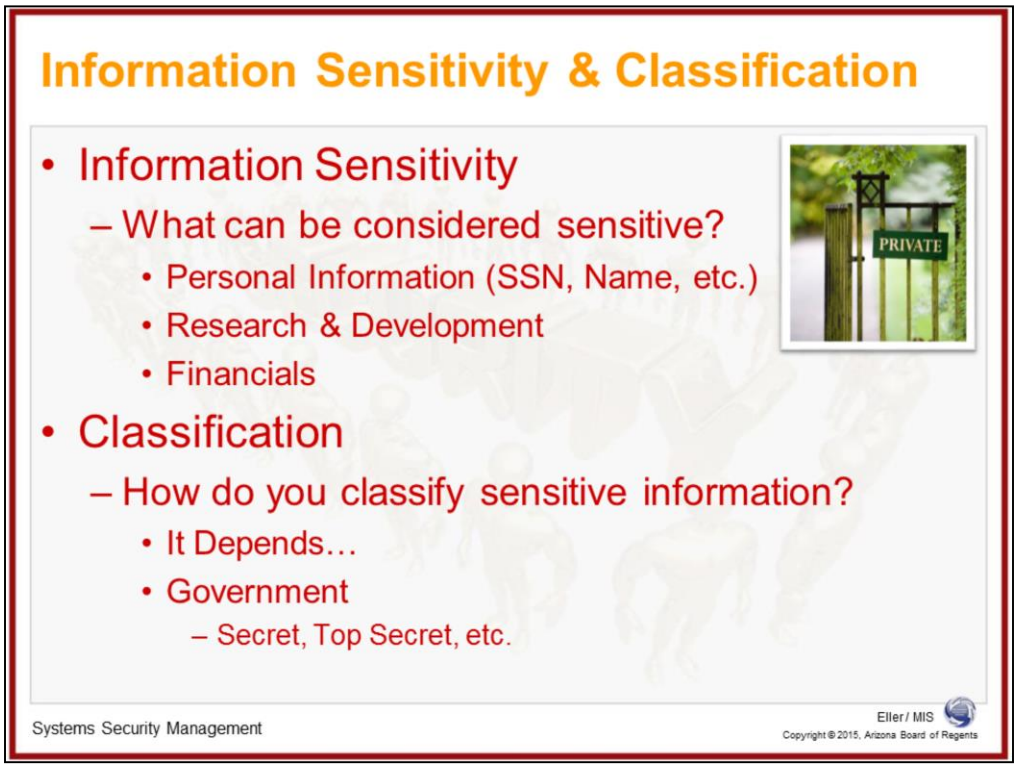
One of the most important aspects of information system maintenance and security involves records retention. Most organizations have a policy in-place for paper records defining how long the organization should keep its records for legal purposes and when the records should be destroyed. Some of these same organizations do not have a defined policy in-place for the retention of digital records, and this is something that needs to be addressed. Organizations need to define a digital records retention policy in the IT security policy in order to protect the organization's best interests.

In general, paper and digital records must be kept for a set period of time as defined by the organization's policies. This is because the government can subpoena an organization's records for legal proceedings. The problem for organizations is if records are not destroyed after the defined time period and still exist, the organization is legally required to produce them for court proceedings. By destroying the records after the defined retention policy, the organization is not liable for producing the requested records.



Resource Custodians

A resource custodian is a department or individual who implements the policies defined by the organization. The custodian is responsible for IT systems that store, process, or transmit IT resources across a network. In general, a resource custodian is usually a SysAdmin; however, this does not always need to be the case. In addition to these IT systems, a resource custodian will also respond to requests for computing resources, such as computer labs, specialized systems, or high powered computing resources (AKA supercomputers).



Information Sensitivity and Classification

Information Sensitivity

The reality in today's information age is some information is more sensitive than others. The question becomes, what information should be considered sensitive in nature? The answer depends on the organization and the data it collects. Personal information such as social security numbers, full names, and current addresses are all examples of personal information that identity thieves want to steal. Other potential examples of sensitive information in an organization might include research and development data or financial information.

Classification

How should an organization classify sensitive information? Well, the answer to that question is it really depends on the kind of information and how the organization needs to secure the information. Any personal information gathered by an organization should be protected in order to prevent potential identity theft. Other information may need varying degrees of confidentiality depending on the contents. For example, research and development information might require far more security than a copy of different press releases. The Unites States Government uses a classification system for securing information that you may be familiar with: secret, top secret, etc.

Data Ownership

One question that comes up every now and again involves data ownership. Who is the owner of an employee's work product? Network users in an organization may be the ones who create or collect the data; however, that does not give the users ownership over the data. SysAdmins are responsible for maintaining the systems where data is stored by the users, but again, this does not give SysAdmins ownership over the data. The bottom line is the organization owns all data and information collected and created while their users are employed by the company. Even research conducted at an organization such as a University does not generally belong to the researcher.

In general, organizational policy should dictate the ownership of data and information collected while the company is conducting business. More often than not, the company will own all work product generated, so if you have a personal project you want to work on, do not do the work on company time or systems.

Copyrights

A copyright is official ownership of information, ideas, and products, among others. In general, all someone must do is place a copyright symbol with a date and their name to copyright something. Officially, however, the person or organization should register the copyright with the federal government for additional legal protections.

Have you ever installed a piece of software on your computer and been presented with an End User License Agreement (EULA)? Have you ever read the agreement, or do you simply hit accept and let the software install? More often than not, the answer is the latter. Many people download or purchase software because they want or need it and since they must hit accept to install it, they do without hesitation. The problem with this occurs when something unexpected happens. For example, one software package available over the Internet would install the program you downloaded and would also install another piece of software that was construed as spyware. Many people complained when it became clear this second piece of software came with the original software install, but the company distributing the software had placed wording into the EULA stating the software would be installed if the user accepted the license agreement. How many of the people who installed the software do you believe read the EULA prior to accepting it and installing both pieces of software? Not many. Many companies use legalese in the EULAs because they want to cover themselves legally, full well knowing the normal user will not bother to read the EULA prior to accepting the terms. This is just something to consider, since EULAs are used by companies as a way to protect their copyrights.

Have you ever bought a music CD and ripped the music to your computer so you can play it on a portable music player? How about software? Have you made a backup copy of your software just in case the original is lost or damaged? Fair use is a concept that has been in existence for decades. “Fair use is a doctrine in United States copyright law that allows limited use of copyrighted material without requiring permission from the rights holders, such as for commentary, criticism, news reporting, research, teaching or scholarship” (Fair Use, 2010). This allows people to make backup copies of media or use pieces of other people’s written material for various purposes. Basically, it is perfectly within your rights to make a backup copy of software you purchased or rip your music to your computer so you can listen to it on a portable player. What is not ok, is sharing those copies with people who have not purchased the same software or music. This is where the Digital Millennium Copyright Act came into play.

Digital Millennium Copyright Act

The Digital Millennium Copyright Act, or DMCA, was signed into law by President Bill Clinton on October 28, 1998. The law was divided into five titles, the most important of which defined digital copyright protections. The U.S. Government realized that older laws governing fair use were out-of-date with newer digital media. In the past, fair use was cited as a reason for making copies of audio and video tapes and CDs. The thought process was the technology at the time could not make a perfect copy of the material, and every subsequent time the material was copied, the copy was a degraded version of the original. With newer digital media and the ability for anyone to make near-perfect digital copies of CDs or DVDs led to the creation of this piece of legislation.

This act has been law for more than a decade now and it is not uncommon for a SysAdmin to receive a DMCA notification from time to time. This law allows the owner of a copyright to search for DMCA violations and send a cease and desist order to whoever is found to be distributing the material over the Internet. On a University campus this is definitely not unheard of. In general, the DMCA notification is sent directly to the network owner where the material is hosted. The notification will identify the copyrighted material and the infringing network address of the computer used to share the material. The network owner is expected locate the computer in question and remove the infringing materials. Once this is done, the network owner must respond directly to the party who sent the DMCA notification, letting them know the material has been removed. If this is not done in a timely manner, the copyright owner has the right to begin a legal remedy to the situation.

On University campuses, sharing of copyrighted material happens from time to time (probably more often than we realize). Some Universities have added fees to student tuition that gives them access to a certain amount of downloadable music or videos from third party companies while others outright ban sharing entirely through the use of technology. Regardless, the DMCA has had a direct impact on ensuring a copyright holder's rights in the digital age.

Piracy

The bottom line: piracy is bad. Piracy, or copyright infringement, “is the unauthorized or prohibited use of works covered by copyright law, in a way that violates one of the copyright owner's exclusive rights” (Copyright Infringement, 2010). The image on the left is an old magazine advertisement from the 1980s discussing software piracy. The message of “if you are involved in software piracy then you are breaking the law” is a simple message. The image on the right is a more modern take on the same message. “Stolen loot was illegal then and illegal now. Don't be a pirate, respect copyright laws.”

Piracy (continued)

Piracy is a problem in general for copyright holders. This is a known fact. What some people do not realize is piracy in the workplace is even more problematic, because it creates liability for the organization. Organizations whose networks host pirated materials, if found, will be sent DMCA notifications, which if not dealt with quickly could result in a lawsuit. So, what kinds of pirated materials might you see on the network? Well, copies of software, movies, music, video games, and even books could all be copyrighted material that might be shared on a network.

In order to combat piracy in the workplace, the organization must have a set of policies specifically defining the use of copyrighted material and what can and cannot be shared on the network. The policy must also detail the consequences of piracy, which could include, and not necessarily be limited to, firing the infringing party.

Hirings, Firings, and Layoffs

Personnel Hiring

All organizations (small businesses or contractors not withstanding) have a Human Resources department (or group) responsible for handling the hiring or termination of employees. As such, these organizations normally have a standard set of policies governing the hiring and termination processes. Many of the policies governing HR should include the input of the IT department. The reason for this is simple, certain security measures need to be taken when someone is hired and others need to occur upon termination.

Hiring policies in particular should include a section discussing the notification of the new hire to the IT department. Information provided should include enough information to allow for user account creation and the type of system access granted to the new employee.

Personnel Firing and Layoffs

As with the hiring process, the termination process policies should also include the IT department. IT should be notified when an employee is no longer with the company. The policy should also dictate whether user accounts are deleted or disabled. In addition, the policy needs to dictate what should happen with the terminated employee's data, both on the network and on company-owned client systems.

Internal Controls

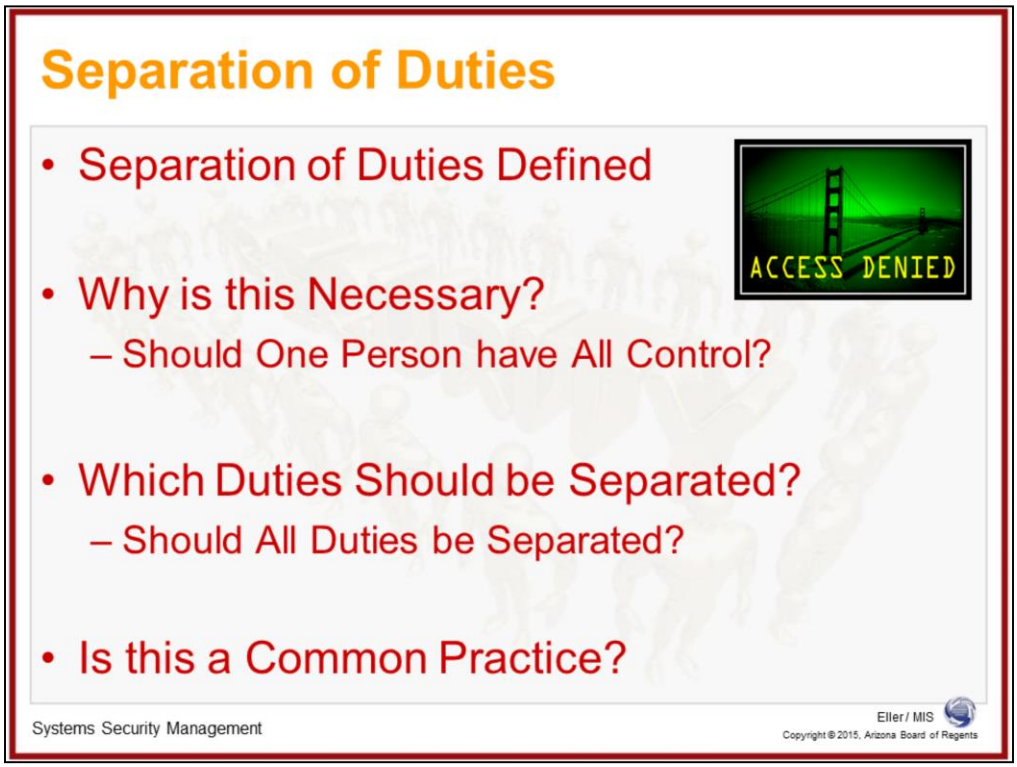
Internal controls are necessary in order to ensure the security of information systems on the network. Several areas where internal controls are necessary include:

Accountability, Authorization and Approval - Accountability exists when you are able to determine who has access to what data, why they need access to that data, what applications are authorized for use, and where sensitive, private data resides.

Security of Assets - This is the responsibility of the SysAdmin, as all network resources need to remain secure. Assets can include servers, printers, network storage devices, client computers, and network hardware such as routers and switches. Basically anything that can be accessed and used over the network to access, store, and transmit data needs to be as secure as possible.

Separation of Duties - We will discuss this specifically in a moment.

Review and Reconciliation - Ensures that transactions are recorded correctly, can be retrieved, and are safeguarded from improper modification.



Separation of Duties

Separation of duties is the idea that different people should perform key information system duties. Giving one person the sole responsibility for all tasks is a very bad idea. For example, the person who does payroll should not be the person who authorizes raises or promotions as this could be considered to be a conflict of interest. With regard to system management, the SysAdmin is generally responsible for all servers and network hardware in the organization; however, should this person also have the ability to control the types of software used by employees for their jobs? In general, the SysAdmin should be one of the most trusted individuals in the organization, especially when the organization handles sensitive information. Despite this, the SysAdmin should not necessarily know all the ins and outs of how specific software works. It can be especially dangerous for an organization if only one single person had all of the control over the information systems.

So, should specific duties be separated or should all duties be separated? This is a question best asked of the organization's IT and senior management. Certain duties such as payroll and raises/promotion authority should absolutely be separated, but sometimes certain IT functions should not be separated otherwise it might reduce the speed at which tasks are completed, such as user account creation and granting permissions for system access. Other IT functions such as the System Management tasks and an Application Administrator (someone who can support/train personnel in a specific application) should be separated otherwise the organization might run the risk of putting too many eggs in a single basket.

Separation of duties is a common practice for many aspects of day-to-day business operations. Depending on the organization, separation of duties in IT may or may not be something the organization is concerned about. It really depends on the size of the organization and if there are any regulations or policies that must be adhered to. A good test of the efficacy of this practice is the concept of "mandatory vacations". Ensuring that tasks are still accomplished and nothing untoward happens when an employee is on vacation is a good way to check that separation of duties is working as expected.

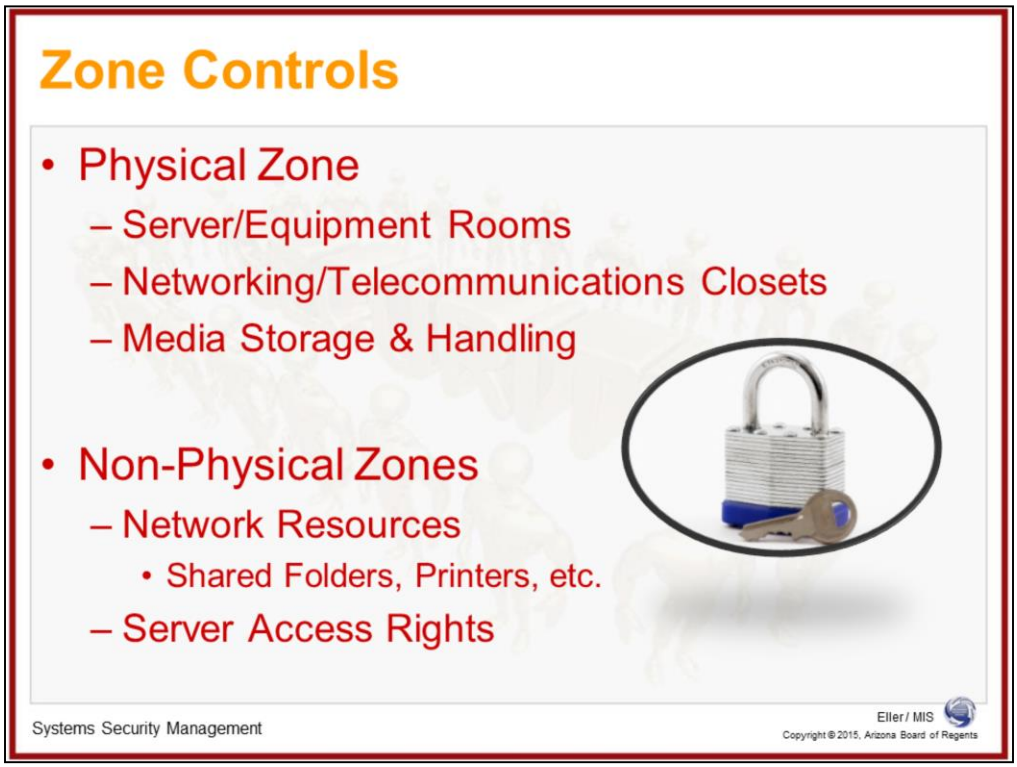
Due Diligence

With regard to organizational IT security, due diligence is the responsibility of the SysAdmin. The SysAdmin must ensure all systems are secure at all times, must review logs to identify potential security problems, and must respond quickly to security incidents should they occur. Basically, in order to maintain the security of the organization's network, the SysAdmin must be able to get information quickly and in a format which allows for fast response times.

Some ways in which a SysAdmin can ensure due diligence is adhered to would involve the constant collection and aggregation of information. Different investigative tools should be used to gather information, including evidence collection and information retrieval tools.

In the event a security incident is uncovered, the SysAdmin needs to adhere to organizational security requirements, which could include involving the human resources department, the legal department, and the IT department. Involving other departments when a security incident occurs will require the SysAdmin has adequate evidence of the incident. In order to deliver this information to the involved departments, the SysAdmin needs to ensure all systems are audited regularly and reports are generated from the audit data.

A formal incident response plan should be developed in advance of an actual emergency so there is a chain of custody for evidence and time isn't wasted trying to ascertain the next steps. This should be developed with Subject Matter Experts and have full buy-in from upper management so that when a breach is detected, the plan can be implemented as soon as possible.



Zone Controls

Zone controls are another organizational security measure designed to help ensure the security of information systems. From a physical zone standpoint, information systems should be housed in specialized server or equipment rooms with adequate locks and restricted access. Networking and telecommunications closets should also be locked and restricted in order to prevent unauthorized users from accessing network hardware. Finally media, such as backup tapes, should be stored in a specific location and policies should define how the media is handled.

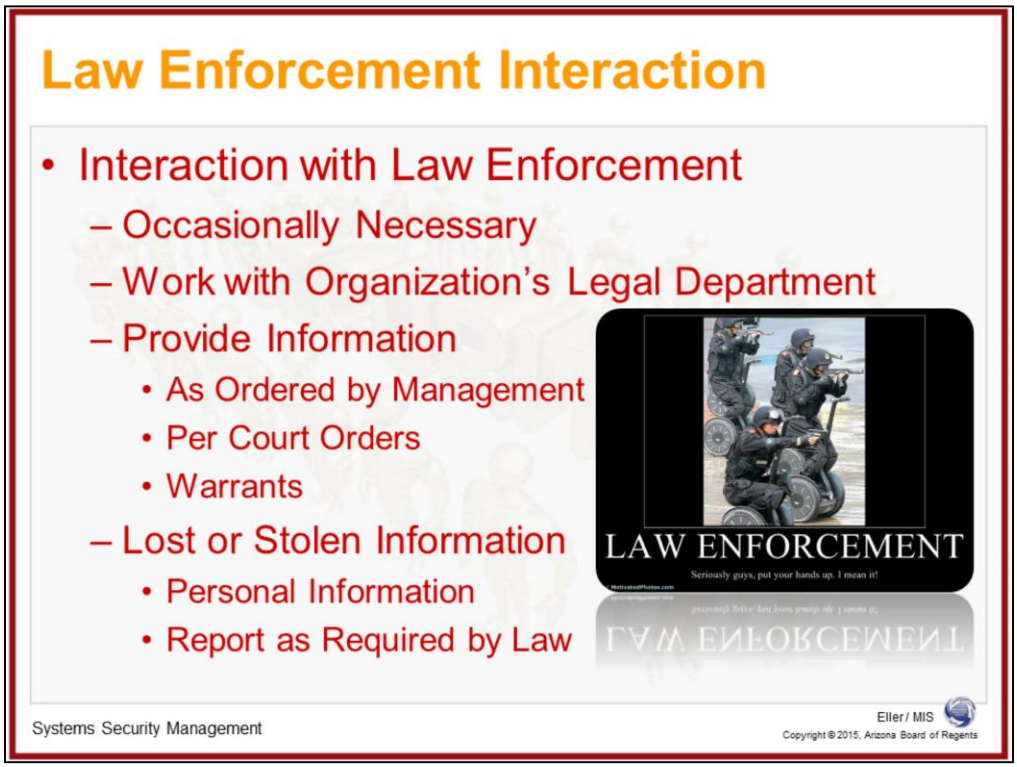
With non-physical zones, controls will usually include access control lists defining who should and should not have access to network resources such as shared folders and printers. Server access rights will also need to be strictly controlled in order to prevent unauthorized access to sensitive information.

Lost or Stolen Equipment

How do organizations deal with loss? It really depends on what is lost or stolen. With equipment, the loss or theft should be reported to law enforcement for insurance (or possible recovery) purposes. The loss or theft of personal information requires that law enforcement is notified, and may also require notifying those whose information has gone missing once they are identified. Sometimes it may be possible that equipment could disappear in an attempt at corporate espionage. How this and all losses should be handled must be defined in the organization's policies.

It is possible to put measures in place to deter theft. Many organizations adopt encryption solutions which allow IT to encrypt client computer systems, so if they are stolen there is little risk any data contained on the system would be recoverable. Other organizations adopt the use of "dumb" terminals, or systems which contain little to no information or software at all. These systems would need to connect to a network in order to provide an environment where the employee could work. If this type of device is stolen, there is no risk of losing data because nothing is kept on the local hard drive.

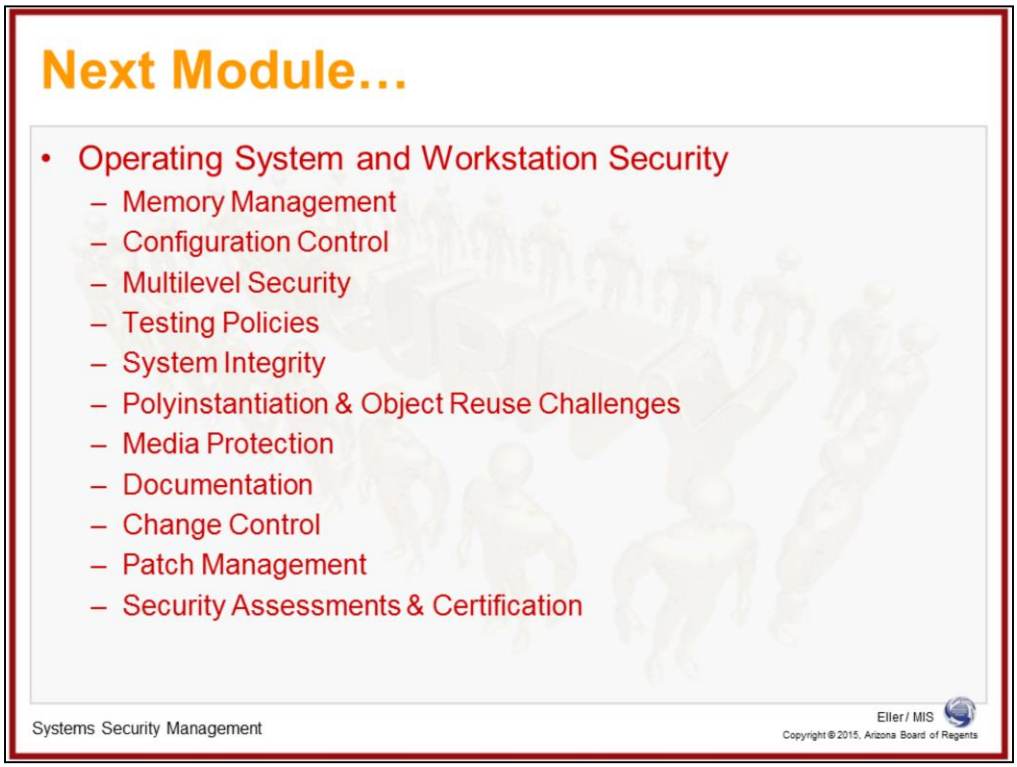
In general, with any loss, law enforcement involvement will likely occur.



Law Enforcement Interaction

At some point, an organization may need to work with law enforcement personnel. Organizational policy should dictate how this is handled; however, in general an organization will direct law enforcement to the legal department. In the event the organization is asked to provide information to law enforcement, this can be handled in several ways. Management can order the SysAdmin to provide the specific information that is requested. Alternatively, the organization can choose to require law enforcement to provide a court order or warrant for the information.

When it comes to lost or stolen equipment, the organization should report the losses as required by law and should only provide personal information if absolutely necessary.



In the next module we will discuss operating systems and workstation security, including:

- Memory Management
- Configuration Control
- Multilevel Security
- Testing Policies
- System Integrity
- Polyinstantiation & Object Reuse Challenges
- Media Protection
- Documentation
- Change Control
- Patch Management
- Security Assessments & Certification

References

Coleman, K. (2008, August 26). Muddied responsibilities create unwanted risk. Kevin Coleman says auditors may start labeling poorly defined IT duties as a material deficiency. *CSO Online: Security & Risk*. Retrieved from http://www.csoonline.com/article/446017/Separation_of_Duties_and_IT_Security.

Copyright Infringement. (2010, July 18). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Copyright_infringement.

Fair Use. (2010, June 17). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Fair_use.

Internal Control Overview: Information Systems. (2009). *Arizona State University*. Retrieved from http://uabf.asu.edu/audit_internalcontrols_is.

U.S. Copyright Office. (1998, December). Digital Millennium Copyright Act of 1988. Retrieved from http://www.copyright.gov/legislation/dmca.pdf.