Implementation of a Configuration Management Plan Overview

An important function of the IT department is to maintain information systems and upgrade, enhance, and revise those systems as necessary. Information systems are subject to many changes and modifications due to system patches, new technology or functionality, correction of process errors, or system failures. The IT department must be able to manage change in order to support business operations and ensure the security of the systems.

The problem is that change poses a significant risk to the organization. Because of changes systems may fail, functionality may be lost, security vulnerabilities may be introduced, and data integrity may be compromised. This requires the development and implementation of a change management process that avoids business interruption and enforces the documentation, testing, and approval of all changes.

Configuration Management

An organization may mandate the configuration of equipment through standards and baselines. The use of standards and baselines can ensure that network devices, software, hardware, and end point devices are configured in a consistent way and that all such devices are compliant with the security baseline established for the organization. Compliance scanners may be used to validate that all equipment is compliant with those standards and baselines. Discovery scanners can detect if any unauthorized devices have been connected to the network. If a device is found that is not compliant with the security baseline, it may be disabled or isolated into a quarantine area until it can be checked and updated.

The purpose of configuration management is to manage the configuration of the devices, networks, applications, and projects of the organization. A subset of configuration management is change management. Change management manages change to the configurations. Change management requires a process to manage change so that it does not adversely affect business operations.

The Change Control Board

One way to manage change is to implement a change control board (CCB). In some organizations, this may be called a change management board or other name. The CCB is responsible to review all proposed changes and approve or reject the changes, oversee the implementation and testing of the changes, and to enforce the process of documenting, testing, and approving all changes. The CCB represents the interests of the business and should ensure that changes are implemented in a timely manner (especially critical security patches) and at a time least likely to affect business operations.

The change control process should be a formal process often comprising the following steps:

- Change request (documented)

- Review of the request for approval (depending on impact on other projects or security)
- Approval of the change request
- Development of the change
- Testing of the change
- Scheduling of the change
- Implementation of the change
- Notification of the completion of the change

Having a formal change control process can avoid the problems of scope creep or the introduction of unauthorized changes.

Change management also supports separation of duties to ensure that the developer cannot move a change into production directly. Some organizations will require the approval of a senior manager prior to permitting any changes. This process, known as systems authorization, is used to protect the entire organization from the implementation of an insecure system. The senior manager that authorizes the change accepts the risk associated with the change.

Version control is an important part of change management so that a record is kept of all versions of, and changes to, the product. This can protect the integrity of the product and minimize the risk that a latter change overrides a previous change unintentionally. Version control can also be used to track all of the changes made in a version and to identify if any changes were made that were not a part of the authorized change request.

Patch Management

Patch management mostly applies to software and hardware devices that are subject to modification. These patches may be needed to address a vulnerability or to improve functionality. The challenge for the security practitioner is being aware of all patches since they can come at irregular intervals from many different vendors. Some patches are critical and should be deployed quickly, while others may not be as critical but should be deployed since later patches may require the implementation of the previous patch. Standards such as PCI-DSS may also require security patches to be deployed within a certain timeframe.

The problem of patches that do not work or that disable systems is legendary. Many organizations have been affected by a flawed patch from a reputable vendor that disabled other systems or system functionality. Therefore, an organization should test the patch before rolling it out across the organization. This is often complicated by the lack of a testing environment that matches production. Few organizations have the budget to maintain a test environment that is an except copy of production. This means that the testing will not be able to test everything, and problems may appear in production that were not apparent in the test environment. But as much as possible, the patches should be tested to ensure they will work correctly in production.

Rollout

The change should be scheduled at a time that will have minimal impact on the organization. This may be during off-hours or on a weekend. Each rollout should have a back-out plan so that if the change does not work, there is a plan to resume operations. The rollout of the change may be done as a pilot, a phased rollout, a parallel process, or an abrupt cutover.

Once the change has been made, all systems should be checked for correct operation and feedback from the users requested. The final step in the change management process is to notify management of the completion of the change.

System documentation should always reflect the current state of the system. Network diagrams, application documentation, project documentation, and hardware configurations should all be “living documents” that are updated with all changes and provide a record of the changes that have been made to the system over the years.

Detecting Unauthorized Change

Unauthorized changes pose a serious risk to an organization. For this reason, annual or spot check audits should be conducted to match all changes made on a system to the approved change request. A change that has been made without the correct supporting documentation should be investigated. Unauthorized changes may be symptoms of system compromise such as the installation of a rootkit.

File integrity checkers can be used to detect whether a change has been made to a file without the knowledge of the owner or administrator.

Summary

Configuration management is an important part of information security and is critical to support and protect information systems. Changes should always follow a formal process that requires the documentation, testing, and approval of any changes.

Participate in Physical (Environmental) Security Operations Overview

Physical and environmental security are often the responsibilities of other departments such as the physical security department or the facilities management group, but these areas play an important role in providing resilient and reliable information systems to the organization. The security practitioner may be required to work with these other departments to ensure the requirements to support information systems with electrical power, fire protection, physical access security and protection from theft, natural events, and surveillance are met.

It can even be said that physical security overrides most other forms of security such as passwords, firewalls, and procedures. If an adversary can gain access to a server room, then the adversary can bypass all of the other forms of control and circumvent the security defenses. An adversary in a server room or wiring closet can install a wireless device or sniffer, cut or re-route cables, and disable equipment among other things.

Layered Defense

Physical security is an excellent example of layered defense. The first obstacle for an intruder is to gain access to the property, and this may be restricted by use of a fence, security guard, or wall. Depending on the level of risk to the organization, a low fence may be there just to discourage people from walking across the property, or it may be there as a large obstacle that would require a determined effort to climb. Sensors may also be placed on the fence or in the area immediately inside the fence to detect a possible intruder. These sensors may be light beams, motion sensors, or a fiber optic cable that would detect the vibrations made by an intruder climbing the fence or walking on the ground near the buried cable. A fence requires maintenance and surveillance to ensure it is not damaged or cut.

Placing gates across roads and walkways will control traffic onto the facility as well. These gates can be automatic or manned by a security force that

would prohibit unauthorized personnel from accessing the facility.

Lighting and Cameras

Two of the best security controls available are lighting and cameras. Lighting can deter crime and also support surveillance. Lighting should be protected from damage and provide a wide range of coverage. Lighting should also be arranged to support the use of cameras and avoid “blinding” a camera. In some cases, lighting may also be used to “blind” an approaching vehicle or person so that the security guards can see the approaching vehicle, but the personnel in the vehicle cannot clearly see the security guards. This is called “glare” or “projection” lighting.

Lighting may be used on the outside of a building to prevent dark corners or areas where an intruder might hide. This lighting can shine down the wall of the building. Parking areas and doorways should also be lit for safety and security.

Inside of a building, lighting can be used to indicate emergency exits, work areas, and hallways. This lighting may come on only when there is motion in the area (trip lighting) or in the event of a power failure (emergency lighting).

Cameras provide one of the best physical security controls available. Cameras provide surveillance, incident detection, and response capabilities. A security guard may be able to monitor a large area through the use of multiple cameras. Once an incident is detected, the guard can respond more effectively by seeing the scope and nature of the incident. A fire will generate a different response from a medical emergency for example.

By designing cameras to be able to pan (move laterally), tilt (move up and down), and zoom (move in to a closer image), the security guard can effectively oversee a situation. The cameras can also record an incident for later review and analysis.

Like lighting, cameras need protection from damage and require proper maintenance. The use of a trained security response force is also needed to ensure the activity in the lighted area, or activity detected by a camera is noticed and responded to effectively.

Doors, Windows, and Buildings

Once a person has entered the grounds of the facility, the next layer of defense is the building itself. Access to the building may be restricted through securing doors, windows, and other access points such as loading docks and elevator and ventilation shafts. Further inside the building, security controls access to work areas, server rooms, wiring closets, and other sensitive areas of the facility. This may be done through the use of locks and security guards.

Doors should be properly secured to prevent unauthorized entry and the spread of fire. For this reason, a solid door is preferable to a hollow door, and the door itself should be installed correctly to avoid being able to "pop" the door open or remove the door by removing the hinges. Emergency exits should be kept clear and marked.

Windows

Windows are important parts of a building's infrastructure. They allow light, fresh air, and access in some cases or are sealed and secure in others. The types of glass used in the windows are dependent on the risk faced by the organization. Plate glass is cheap and common but also very dangerous in the event of a windstorm or explosion since the glass may break into many sharp shards of glass that pose an extreme risk to health. Tempered glass is designed to protect against the risk of flying glass shards by breaking into many small "pebbles" of glass. This is what is used in the side windows of a car and bus stops or other areas where glass may frequently be broken. Laminated glass is two panes of [usually tempered] glass with a plastic sheet in between them. This holds the glass together in the event of breakage. This is used in the front windshield of a car. Polycarbonates are bullet resistant and can stop a small caliber bullet in most cases. Glass may also be protected through the use of solar films that reflect the sun and prevent it from overheating the inside of the building and bomb blast film that will hold the glass together in the event of an explosion.

To protect themselves from an intruder breaking in through a window, the organization may have glass breakage sensors or other motion sensors installed to detect an attempted entry.

Buildings

Ideally, buildings should be located in an area not threatened by natural events, such as flooding or tornado; however, this is not always possible. Buildings have to be built to withstand adverse weather and natural events as much as possible. (It is nearly impossible to mitigate the damage from an F5 tornado). Locating buildings close to airports, railways, or highways also poses a risk as a major derailment or accident could damage the facility or restrict access to the area.

The organization may also choose to limit the signage of the building to avoid identifying the types of operations being run at that facility. A secure facility should also work with local emergency services to enable an appropriate response in case of an incident.

Locks

There are several types of locks in use:

- Keyed locks
- Combination locks
- Biometric locks
- Cipher locks
- Card key locks

A keyed lock is one of the most common locks in use. The keyed lock uses a key that inserts into a tumbler. The cuts (grooves) in the key are set to the exact depth of the pins in the tumbler. With the correct key, the tumbler will turn and allow the lock to open. Keyed locks require key management and inventory. The problem is that many keyed locks are “pickable,” using torsion wrenches and picks or through key bumping. It has sometimes been said that the purpose of a lock is to slow the intruder down until a response can be activated.

Combination locks use a series of numbers to open the lock. The problem is preserving the secrecy of the combination. A person entering the combination may be observed using a camera.

Biometrics locks use a person’s physiological characteristics to identify and authenticate them. Biometrics may be based on a fingerprint, PAM scan, iris scan, retina scan, or other unique feature. These devices are expensive to install, implement, and maintain since the biometric information of all users must be obtained and stored securely.

Cipher locks use a push button combination for access. These may be “pickable,” using a camera, and a failure to change the combination may make the keys in use shiny.

Card key locks are used in many facilities using either a proximity-based card or a contact card that would be “read” by the reader. The card key locks can be re-programmed when a card is lost or stolen and can also record the times of entry if desired.

Fire

The security practitioner should be alert to preventing, detecting, and responding to the threat of fire. Common fires are often the result of several factors coming together—fuel, oxygen, and heat. Some models also add in a fourth element—a trigger. Removing one of these factors usually prevents fire.

Once a fire has started, it is important to detect the fire quickly before it can spread to other areas. Smoke, heat, or flame detectors can be used to detect a fire. The detection of a fire should initiate the emergency response where the first priority is life safety, but the second priority is to contain the incident and limit the amount of damage.

The way to respond to a fire depends on the type of fire.

A Class A fire (wood, paper, common combustibles) is usually extinguished using water to reduce the temperature or carbon dioxide or other agent to remove the oxygen. In some cases, it may also be possible to remove the fuel (fire doors, fire breaks).

A Class B fire (oil, gasoline) may be smothered through the use of dry powder or the displacement of oxygen using carbon dioxide or inert gas.

A Class C fire (electrical) is extinguished using a dry chemical. This class of fire is not used in some countries.

The best advice in most cases is to evacuate the area, seal off ventilation and fresh air supplies (close doors), and call emergency personnel. Fighting the fire may pose a serious risk to the employee and even hinder a professional response.

Electrical

Information systems and technology reply on a clean and steady supply of power. These systems are easily affected by fluctuations in voltage or interruptions in supply. For this reason, most organizations will run IT equipment on an Uninterruptible Power Supply (UPS) that will maintain power supply to the equipment in the event of failure and may help absorb the fluctuations in power that can occur. Surge protectors are also used to divert a surge of voltage to ground (earth). This can protect against lightning strikes or crossed lines. The UPS may be sufficient to keep all systems operational, or it may only be sufficient to allow for the graceful shutdown of non-critical systems.

In the event of an extended outage, the organization may use a backup generator to provide power.

The common electrical problems are:

- Fault—momentary loss of power
- Blackout—extended loss of power
- Spike—brief increase in voltage
- Surge—increase in voltage (often of longer duration than a spike)
- Sag—decrease in voltage
- Brownout—decrease in voltage (often caused by insufficient supply)

Power systems need regular review to ensure that the UPS systems and generators can provide sufficient power to maintain operations. Generators and batteries also need maintenance and upkeep to ensure reliable operation.

Other Physical Security Considerations

The security practitioner should have an eye for other physical and environmental security problems or issues. Information technology relies on the supporting infrastructure necessary to ensure that equipment is protected from theft, alteration, or damage—whether from human, natural, or circumstantial (facility-related) causes.

Water

Water presents a serious hazard to IT equipment. A leaking roof, flood, broken water pipe, or condensation can short circuit electrical equipment and cause catastrophic failure. Server rooms are often located below ground level, and this makes them susceptible to all forms of leakage and flooding from higher levels.

Humidity

A computer room should maintain a steady humidity level as much as possible—usually between 40% and 60% relative humidity (humidity is relative to temperature). Low humidity can cause static discharge, which can seriously harm equipment. High humidity can cause condensation and corrosion of contacts and connectors.

Summary

Physical and Environmental Security are important factors in maintaining a reliable information systems infrastructure. The security practitioner should be aware of risk and threats associated with these areas to ensure physical security of equipment areas and adequate infrastructure support with adequate power and fire protection.

Security Awareness Overview

Security awareness training is probably the best security control available to the security practitioner. The purpose of security awareness is to ensure that all staff is aware of security issues, policies, and threats. This empowers staff to be watchful for potential security incidents and able to take action to prevent, detect, and notify security personnel about the suspicious activity.

Security awareness sessions should be held at least annually, and all staff should be [strongly] encouraged to attend. The content of awareness programs may change over time to address current threats and explain new security policies or procedures.

The awareness program should ideally be customized according to the responsibilities of staff and thereby address the issue that each staff member should know. People will quickly lose interest if the content covered in the program is not relevant to them.

Terminology

A common problem with security awareness is the lack of understanding the language used by security people. Security people use terms in a way that is misunderstood by most listeners. For example, the term “security” itself is often poorly understood and may have a completely different meaning for a manager or a user than it does for a security practitioner.

Discussion: What is the Meaning of the Term "Security"

How would a security practitioner define the term “security?”

How do users interpret that term? How do managers interpret the term?

Review: The Meaning of the Term “Security”

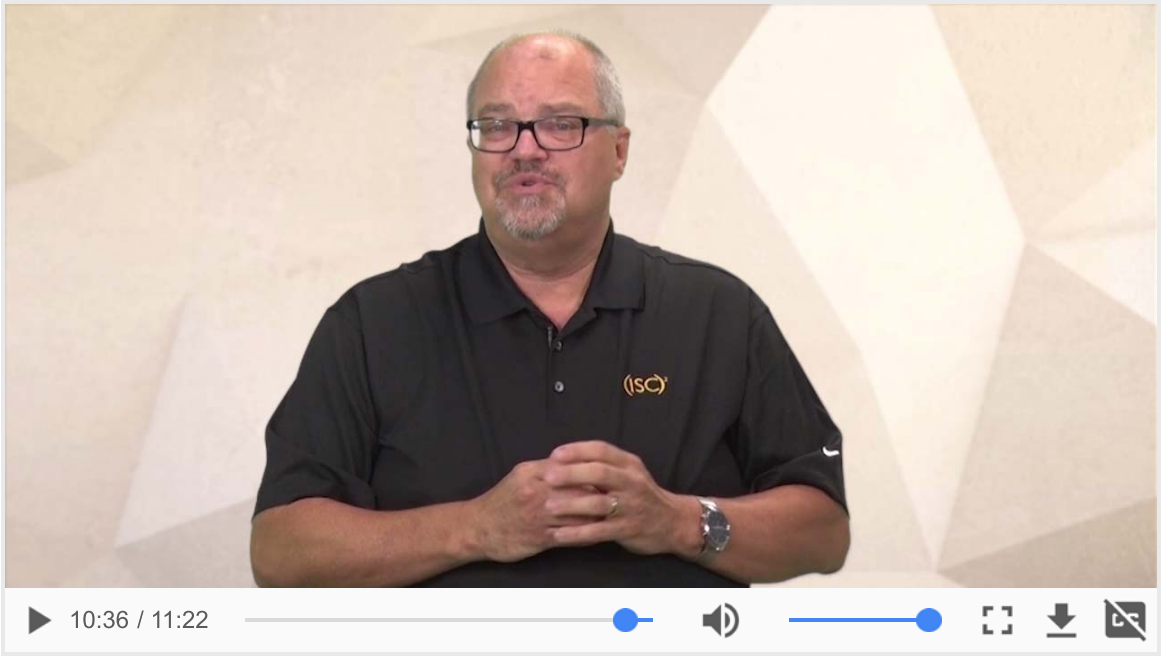
We can see that the same word has a very different meaning for many people. While a security practitioner sees security as a benefit and safety, the user often see security as a hindrance, while a manager may perceive it as a cost. It is important to present clear definitions for terminology so that everyone is thinking of the term in the same manner. It is also important that security moves from an obscure, emotional condition where people wonder “are we secure or not?“ or “are the hackers smarter than us?” to a point where security is seen as a measurable and possible condition. Everyone attending a security awareness session should leave with the confidence that security is working and that continuous progress is being made to thwart the attackers and mitigate the risk. If people leave the awareness session believing that security is possible and that what they do can make a difference in protecting the organization and themselves, then they will be much more likely to support and comply with the security program.

Delivering a Security Awareness Program

A security awareness program is a short but valuable time to pass on useful and timely information to the employees and contractors of an organization. We are also seeing more organizations, such as banks, deliver security awareness messages to their customers to help them avoid becoming a victim of fraud.

The program needs to have a clear message that resonates with the audience and makes them think. An old adage used to describe an effective presentation was to “Make them laugh, make them cry, and make them think.” This is especially important in a security awareness session. It must have energy, content, a clear message, seriousness, and a challenge. The message should be delivered in different ways—posters, web sessions, lectures, and mementos (wristbands, lanyards, and pens). Everyone has different learning styles and to deliver the same message in the same dry, repetitive manner will only work for a short time and only for a limited number of attendees. Posters are great, but they soon become wallpaper. Lectures are good, but they can be hard to arrange for remote workers. Web sessions may be hard to ensure anyone is paying attention, and the answers to a quiz at the end may be shared by the first person to complete the program.

Delivery of a program through a message based on Fear, Uncertainty, and Doubt (the “FUD” factor) tries to scare people into action, but this often works for a short time and can desensitize staff into not paying attention in future sessions.



▼ Transcript

Hi. Thank you for having attended this SSCP course. As you have learned to be a security practitioner, you have learned many things about how to design, implement, operate and maintain a security program. There's one area, though, that's especially important. That is the area of security awareness training. In this short, little video, we're not going to talk about a security awareness course itself. We're going to talk, rather, about how to deliver a security awareness program. Security awareness is probably the most important and most effective control that we have. In fact, we could easily say that security is a people problem, and as a result, it's also a people solution. Knowing how to deliver an effective security awareness program is critical to helping you establish an entire team of security people comprised of everybody in the organization. Without a doubt, security is dependent on awareness. And having security awareness will help us to be able to ensure that everyone knows how security is a part of their responsibility.

The first thing we have to remember when we deliver a security awareness program is that the attendees of the program are not the enemy. We're not to speak to the people in the audience as if they are the problem. No. They are the people that make the company work. They're the people that make money. They're the people that help the organization meet its mission and objectives. And we as the security team must get them on board to understand how they can incorporate and integrate security into their daily business practices. We must never treat them as if they are the problem. No. Instead, we have to understand where they're coming from. We have to understand their world and, from that perspective, learn how to help them to

understand the importance of our viewpoint on security and why it's important also for them.

The first thing when you deliver a security awareness program is to have credibility. Are you believable? Are you a person that has, then, the authority and, in many cases, the expertise to be able to deliver that program? This means that, of course, you should introduce yourself and how you are a part of the team and helping the company to succeed. Then talk about why this course is important, why they need to be here, and how you want to help empower them to actually protect their jobs and the organization from the many breaches that happen today.

The idea here is that security is everybody's problem, not just the problem of the security department. We depend on everyone to be able to resist phishing attacks, to be able to defend against ransomware, to be able to protect our organization, as well as to know how to respond when there is an incident. There are subliminal messages we want to send as well. That is the fact that the security awareness program is not just an option, it's a necessity, and we need them on board as a part of then the security team.

We can see here that the important part of public speaking is to, first of all, know what you want to say. Know the message. The more comfortable we are with the message, the more believable the message is for us. Our passion and our credibility will then shine through. One of the secrets to a good program is to know exactly what you want to say so you have a core theme that then gets across during that presentation. We also say that a good presentation should make them laugh. Put in a bit of humor. Make them cry. A little bit of seriousness and why this is important. But also, and most importantly, leave them with something to think about. What is it that we want them to leave the room having thought about and considering how this applies to their daily responsibilities? The other thing we have to remember is that we use a lot of terms that may not be familiar to the people we're speaking to. And in fact, the very terminology we use should be explained and defined. Many people don't know what a demilitarized zone is and why we would use such a term. They don't really understand what a firewall is and the purpose of it. We need to define security in ways that they can understand and relate to, even things like identity theft. The term gets thrown around many times, but very few people really understand what we are referring to when we talk about it. That way, we should always define these terms, explain what they mean, and use examples that people can relate to. There are three things we want to make sure as we work on the theme of the security awareness program: that it's relevant, that it's realistic, and of course we want to make sure it's riveting. It captures their attention.

Something which is relevant means we talk about what security means to them in their position. If we're talking to an IT staff, quite often messages can be quite different than if we're talking to users or if we're talking to management. So, customize the program according to the audience we're speaking to.

We should make sure that everyone understands the importance of policies and procedures, why we have them. The subliminal message with that, of course, is that policy is a requirement, not just an option. Everybody needs to understand and know the policy in order to be able to be compliant with it. We should discuss the laws and regulations that apply to our industry and why it's important that we are compliant with those. We discuss the problem that if something goes wrong, there could be disciplinary action. So, people are reminded of the fact that this is not just a nice theme or a nice discussion that it's really an important part of their daily responsibilities, and they're accountable for following the policies and procedures we have.

One of the things we should make sure is always in every message is the theme of social engineering. Social engineering is the manipulation of people to do something that they shouldn't have done. We need to ensure that everyone is aware of the types of social engineering: intimidation, name dropping, as well as appealing for help, and the many types of technical social engineering such as phishing attacks. By telling people about these and making them aware of those problems, we give them an inoculation to protect them from them becoming a victim of these types of attacks. In all of these things, remember to make the program relevant and adjust it according to the audience that we're speaking to. It's important that it is realistic. Very often, we deliver a security awareness program that is completely thrown away by the audience because we can't even do that. It's not even realistic. Bruce Schneier once wrote, "You have to remember to think like the people in the audience." We tell them, "Choose a strong password, something which would be impossible to remember, but never write it down." Immediately, the audience is going to reject that. It's not realistic. We have to make security simple. We have to make it possible. We have to deliver the program that's something they could just incorporate into their behaviors. Not because we put pressure on them, but because they realize this is just the right thing to do. It's realistic. So, it's good to use examples: What's happened to other industries in the same area that we are, the same geographic area, the same industry sector. Use examples of what has happened so we don't have the same types of mistakes. It's often good to use examples of what the cost of a breach would be if we were to have one. Of course that theme make security simple, but also let your passion for

security come through. Make the program riveting, interesting, not just the same, boring old message where we bring the people together and berate them for having bad passwords. No. Find ways to make it creative and innovative. In all of this, bring in variety in how you bring the message across.

It's good sometimes to have rewards as well. Of course, appeal to people's different learning styles. Some people like posters. Some people like explanations. Some people like examples. In all of these things, try to find ways to make the security program something they want to attend. So the theme is tell them what you're going to tell them. Tell them and then review it later. There's a reason for this. Then, we can ensure through measuring the security program did the message come across? Did they hear those three keywords we wanted? Something which is, of course, realistic, something which is, of course, relevant for them, and something which is riveting. In summary, try to make your security awareness programs interesting and an event that everyone wants to attend.

Training the Hackers

The question about how much information should be disclosed to the attendees of a security awareness program is difficult to answer. Some people believe that if we tell people how attacks are conducted and explain the methods of an attack, then we train people in how to become hackers themselves. Other people believe that sharing information about hacks and attacks can help the attendees to be more aware of and alert for issues.

Analogies and examples may be excellent ways to present security concepts to make them understandable and relevant. Examples of what has happened to other organizations (especially those in the same industry or geographic region) may demonstrate the reason for and value of the security program.

The Message

The security awareness session should be short and impactful, delivering a clear message to the attendees. This means that the program should be focused to ensure that everyone leaves the session clearly knowing the core message that was delivered. Instead of covering many various points, this may require a short list of three (for example) key points that needed to be brought forward.

The purpose of security awareness training is to affect the behavior of the attendees and addressing their belief systems does this. If the attendees believe the message they are hearing, then they are more likely to align their behaviors with those beliefs. For this reason, it can be good to explain why certain security controls are necessary and the goal of the security program.

A security awareness program should be reinforced by policy and should refer to the policies of the organization as applicable. Adding in references to international standards, laws, and industry baselines may also legitimize the security program.

The program should also be measurable to weigh whether or not it is working. The measurement of the program may be through a quiz, observation, or monitoring for changes in behavior as a result of attending a session.

Social Engineering

One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. Social engineering is the manipulation of people to do something that they should not have done. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.

Ethics

Ethics are based on a person's personal beliefs of right and wrong. Ethics are a complex area that may be influenced by many factors such as culture, law, tradition, or religion. People may have their own criteria for determining what is or is not ethical. This makes it complicated for an organization that wants to set an ethical standard for the conduct of their employees. It cannot be assumed that everyone should just "know" what is and is not acceptable. This can be applied to the area of gifts, for example. Should an employee be allowed to receive a gift from a vendor or supplier? If so, to what value? Do they have to declare it to management? Setting an ethical standard for the organization means that everyone should know what they can and cannot do in relation to gifts. This avoids conflict and confusion and perhaps can protect a person from an investigation. The ethical standards of the organization should be communicated and explained during security awareness sessions.

Some organizations and individuals may also be bound by a code of ethics related to their occupation—such as medical professionals and financial advisors. These people must be aware of their ethical obligations.

As an SSCP, the security practitioner will be subject to the (ISC)^2 Code of Ethics. These ethical standards are a requirement for certification:

Code

All information security professionals who are certified by (ISC)² recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code"). (ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. (ISC)² members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)² member that breaches the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

There are only four mandatory canons in the Code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Code of Ethics Preamble

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principles.
- Advance and protect the profession

Summary

Awareness is a critical part of the security strategy of an organization. It ensures that people are aware of security issues and their responsibility to follow policies and procedures. Communicating ethical standards and expectations to all employees is important to create a stable and safe work environment.