Global Information Assurance Certification Paper

How to Effectively Launch and Maintain Security Policies

Vince Fitzpatrick
January 21st, 2004

Abstract:

Every organization experiences security issues. These could be as small as an event in which someone inappropriately attempts to access the network or as large as an incident in which an attacker brings down your organization's website. When Senior Management is privy to these issues and feels the threat is sufficient, one direction they may take is to implement new security policies. Once the command is given, the race begins. Employees rush to update current policies or to create new ones. When this response is complete, the company has many more policies which are written in a variety of formats and which unfortunately are sometimes lost within the organization, never to be seen again.

Writing clear and concise security policies is extremely important and also time consuming. But, creating the policies is only one piece of this program. The policies must be effectively implemented and maintained. The best-written policies are worthless if there is not proper support or if no one knows where to find them. The goal of this paper is to provide guidelines on how to effectively launch and maintain security policies.

Why implement any policy, let alone security policies?

Before defining what a policy is, let me explain why security policies should or should not be implemented. There are several reasons why policies should be implemented, including strategic initiatives, legislation and business best practices. Though it is a good practice to reference a particular security event to help explain why a policy was implemented, a security event alone should not be used as the sole reason to implement a policy. A security event cannot properly support a policy since often it is an undocumented story whose facts will change with each telling. Satisfying documented requirements such as strategic initiatives, legislation and business best practices are the best reasons to implement security policies.

One of the reasons policies are implemented is to support strategic initiatives which are directed by Senior Management. These initiatives help guide the organization to accomplish its mission statement. These initiatives should be documented. Documented strategic initiatives are known as the organization's Programs. I recommend that Senior Management communicate their Programs via concise one-page Program Statements. A Program Statement is a high level policy which is defined later in this paper. Management then creates policies to fulfill the requirements of these programs. An example is an Information Protection Program, whose corresponding policies would then deal with

Information Classification or Non Disclosure Agreements. It is not important what your organization calls these high level policies. What is important is that Senior Management sets expectations by documenting the highest-level policy, which supports the rest of the policy infrastructure.

Today, many security policies are born from legislation such as the Gramm-Leach-Bliley Act of 1999 (GLBA), the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA). In today's security environment these are three very important acts that spawn many security policies.

The Gramm-Leach-Bliley Act of 1999 (GLBA) requires that financial institutions maintain secure and confidential customer data. The Health Insurance Portability and Accountability Act sets similar requirements for the healthcare field to protect the confidentiality of patient records. Because of these acts, organizations must create appropriate Programs and Policies such as an Information Protection Program that in turn leads to an Information Classification Policy.

The Sarbanes-Oxley Act holds senior executives accountable for their organization's data. This act forces the creation of policies regulating how employees handle company information. In response to this act organizations create Business Continuity Plan (BCP) Programs that produce Data Retention and other related Policies. To safely lead their organization in the correct path, management should be aware of what laws apply to their organization and then create the appropriate programs and policies.

Another reason why policies are implemented is to follow business best practices such as ISO 17799. ISO 17799 is an internationally recognized security standard. Presently, ISO 17799 provides a high-level security guideline. But in the near future there will be an ISO 17799 certification track. Organizations will desire to be ISO 17799 certified, just as manufacturing organizations sought ISO 9000 certification in the 1980's. This certification will become a market differentiator. Best practices are also a valid reason to create security policies. So, you should choose the appropriate best practice model for your organization and then implement the corresponding Programs and Policies.

Whether it is strategic initiatives, legislation or business best practices, addressing why a security policy is created is very important. The best way to show that a policy is important to the organization is to demonstrate that the policy has Senior Management backing. The best way to do that is to link your policies back to a Program Statement. The Program Statement documents why the policy was implemented. Look at the Security Programs your organization currently follows. See if these programs can validate all the Security Policies your organization requires. If not, speak with management regarding how to implement the appropriate Security Programs.

What is a policy?

The goal of this paper is not to explain how to write a good policy. Rather, this paper will focus on the implementation and maintenance of a policy while briefly addressing the technical aspect. The technical aspect of writing a good policy is a skill and deserves the necessary attention. This paper will only briefly define what a policy is and what are its supporting documents.

The term policy means different things to different people. So, it is extremely important that everyone in your organization has a consensus of what a policy is and is not. They should also understand the difference between a statement, policy, and control.

Policies are clear, concise, documented rules that are laid out by management. In general terms, a policy states what needs to be accomplished but not how to accomplish it. A policy is mandatory, measurable and enforceable. If a policy is not mandatory and enforceable, it is not a policy but a guideline. Good policies are written with an understanding of the organization's culture. Michele D. Guel, a former federal IT security official who currently leads security policies for a large technology company, states, "The bottom line for policies is they must take into consideration the balance of protection with the level of productivity hit." (1) If a policy is too much of a hindrance to productivity, a productive employee will either circumvent or ignore the policy. Make certain that every employee in the organization understands the organization's definition of a policy.

It would be excellent if your organization had a standard policy format for writing any type of policy, whether it relates to security, legal or human resources. A standard policy format helps to bring consistency to your organization's policy infrastructure. An employee in the Marketing department should be able to read an IT policy. If possible, standardize a policy format for your organization before you implement any policies, including security policies. This will enable all employees to work from the same set of definitions regarding your organization's policy infrastructure documentation.

The policy's format should be fewer than 2 pages, but there are always exceptions. The format should not contain any legalese. At a minimum, it should include the topic, scope and owner of the policy. It should state the consequences of non-compliance and also state when exceptions are permitted. It should reference why the policy was implemented, such as strategic initiatives, legislation or business best practices. There are many websites and publications that provide excellent policy formats and sample policies, such as SANS. You can find this information at http://www.sans.org/resources/policies/ . Most importantly, never start from scratch when creating your security policies. Always reference other security policies before implementing your own. You may only need to tweak someone else's policies to meet the requirements of your organization.

Policies are general rules outlining how to accomplish a standard. Standards, guidelines and procedures are the documented controls used to accomplish a policy. A standard is an organizationally accepted hardware, software or process. Deviating from the standard would be a policy infraction. A guideline is a recommendation regarding hardware, software or a process. Since a guideline is a recommendation, not following a guideline does not indicate a policy infraction but may still be unacceptable to management. A procedure is a detailed process that shows an employee how to satisfy a standard or guideline.

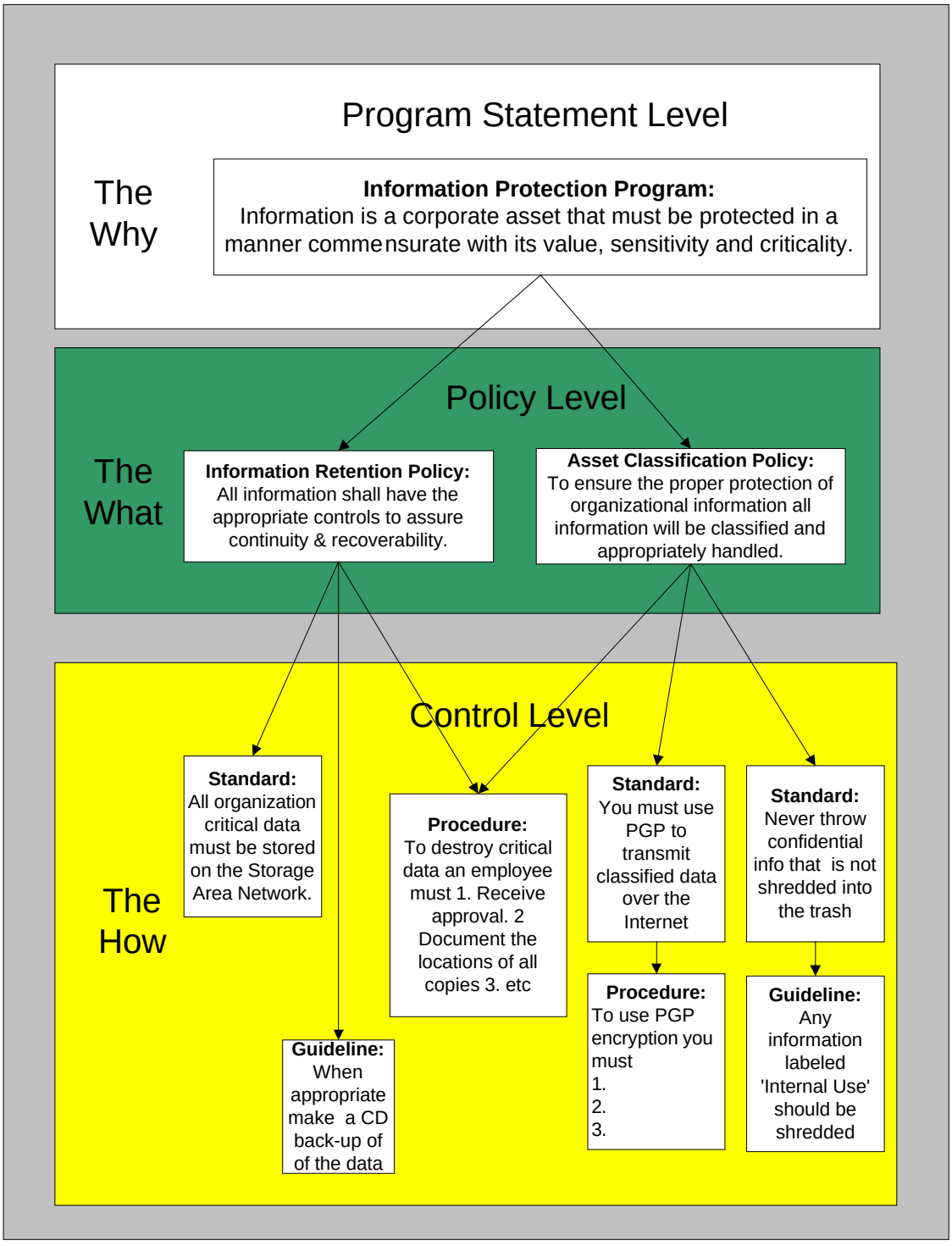
Since the policy is general, a control is used to provide more focus. One policy may reference many controls. Also, a control may support many policies. For example, a policy could state that information is the property of the organization and all employees have the responsibility to protect this property. This policy may reference a control stating that only the Marketing department performs any communication with news medias. An example of a standard would be if your organization only sanctioned the use of PGP to transmit confidential data across the Internet. A procedure would state how to use the standard. It could state what steps to follow to encrypt and decrypt the data. (Reference the chart on next page.)

The amount of trust you are allowed to have in your employees is inversely proportional to the number of these controls you need to implement. These controls, consisting of standards, guidelines and procedures, should be documented. If you are a large financial organization you may need to implement many controls. Make certain there is a consensus regarding your organization's definitions for these documents.

Your organization's policy infrastructure is composed of controls, policies and the high-level program statements. Maintaining this hierarchy and all the relevant documentation is essential to maintaining your security policies. Remember that a policy without controls does not provide guidance.

Note: Per SANS Security Essentials training, "Security policy must always be in accordance with local, state, and federal computer crime laws as well as other applicable government statutes, such as US export regulations". [(2)]

Below is an example of the policy hierarchy which links Programs, Policies and Controls.



What are the roles?

There is no need to restructure your organization to implement and maintain security policies. But you do need to compose the necessary teams to design, implement and maintain your policy infrastructure. It is important that these teams understand their responsibilities. Document your procedures to implement a policy. To maintain focus you do not want everyone and anyone implementing policies. The team that will oversee these procedures is the Security Council. Name your team whatever is appropriate for your organization. You may want to call this team the Security Policy Team or possibly the Security Policy Council. The name is not important. What is important is that this team understands their responsibility is to facilitate the security policies infrastructure.

The Security Council receives its authority directly from Senior Management. The council is composed of senior members from a cross section of the organization, including members from Legal, Human Resources, Audit, Business Units and IT. Since documentation is a key deliverable, include in this team someone with excellent writing skills. Using the high level Program Statements, the Security Council will create and maintain the organization's security policies. This council is also responsible for policy maintenance and enforcement. The size and culture of your organization will dictate the size of your council. The council may begin meeting on a weekly or bi-weekly basis until the key policies are implemented and then move to a quarterly review cycle.

It is important to work with the Legal and Human Resources departments since these departments customarily maintained employee policies. There are some security policies that the Legal and Human Resources departments may consider their realm of expertise and responsibility. Since Legal, Human Resources and the Security department may hold different views regarding security, you may need to be flexible on the level of control the security policies will have. You may also try to first educate these departments regarding the current security threats. A good working relationship with these departments is important. If there is not a good working relationship, you may spend more time dealing with politics than with security.

The council makes recommendations regarding the policies' controls, standards, guidelines and procedures. But these documents are implemented and maintained at the managerial level. Managers must determine what policy documents are relevant for their departments and then implement and maintain them. If there are any issues or questions, the manager is responsible for resolving these with the Security Council. The manager also works with Human Resources when there is a policy infraction.

A great deal of documentation is created when implementing your security policy infrastructure. To maintain focus make certain that all organization levels solicit

feedback from the levels above and below them. Someone in another level of the organization may easily see flaws in a policy document that the creators did not notice.

The most important role belongs to the employee. The employee is the keystone. It is vital that the employee provide constructive feedback regarding the controls, standards, guidelines and procedures. A policy is useless unless the employee understands why the policy is being implemented and how to satisfy the policy's requirements.

Since each organization is different, each organization sets up their roles differently. To properly manage your security policies make certain that employees understand their responsibilities and how their role links to the complete policy infrastructure process. Every employee has a role to play when securing the organization.

Where to store the policies?

After the security policies have been written and approved, a company wide communication announces the implementation of these policies that will securely steer the organization to success. Management provides their endorsement, the policy writers are congratulated, there is a sigh of relief that the project is complete and the policies are printed and/or stored on a network share. But was the project an actual success? Will employees utilize the policies? Often after policies are implemented no one ever references or remembers the policies. So as new policies and procedures are created they are stored in a different location than the original policy documents. Thus begins the demise of your policy's hierarchy. Policies become departmentalized. Inevitably after the next security incident the policy creation process will begin again.

It is important that you store the policies somewhere visible. This is not to say you should have a printed version sitting by the front door, but they should be somewhere easily accessible and maintainable. My recommendation is that all your policies, including security policies, be stored on a document management system such as Documentum or SharePoint.

Many organizations become information fiefdoms. You need to befriend the keeper of the information to obtain any information they own. This is extremely unproductive. Do not let your security policies fall into this situation. If only the Security Council knows the location of the policies, there are no longer policies, just an expensive wish list.

If your organization does not have a document management system, you may want to begin a larger initiative regarding where and how all your critical documents are stored and maintained. Spend the appropriate time to plan the

document management interface to reflect the needs of your organization. Then store all your policies on this site, not just your security policies. An employee should have a single location to reference all such information.

If you use a document management system you can easily link together your statements, policies, standards, guidelines and procedures using HTML links. The HTML links allow employees to quickly reference supporting documents and bypass information they do not need. Policies properly stored on a document management system will be easily accessible. You could also use your document management system to track the policy infrastructure document's life cycle from draft to implementation. These systems can also track the frequency a document has been accessed. This will help you determine if employees are referencing your policies. But one drawback of using HTML links is that they are useless in a printed format.

Policies should be stored in both a topical and organizational view. Storing the information topically makes it easier for the employee to find a specific piece of information. An example is if an employee desires to know the procedure to physically move a production server from one location to another. In this example, the employee would go to your organization's document management system, click on the Physical Security Program Statement, then the Production Hardware Security Policy, which would reference the procedure for moving a production server. Storing the information in an organizational view makes it easier for employees to locate information pertinent to their role. A field sales employee may want to see all the policies that apply to a portable laptop user, or the new desktop support administrator may desire to see all the policies that apply to the desktop support team. Having all your policies accessible from both a topical and organizational view requires a great deal of planning on the part of the Security Council, but it makes it much easier for employees to find the policy they are looking to reference.

The main policy infrastructure page on your document management system is an excellent place to document your organization's definitions of a Program Statement, Policy, Control, Guideline, Procedure or any other Policy Infrastructure document. The page would also include the names of the members of the Security Council, state how to make a recommendation and explain how to ask a question.

If you do not have the resources to implement a document management system, implement the appropriate solution for your organization. Whether you store your policies on a bookshelf, a network drive or a document management system, keep your security policies in the spotlight by continually referencing them. Even policies stored on robust document management systems are useless if no one ever references them. Take the time to decide where to store your policies. Each organization will have different requirements. Implement a solution that you will be able to maintain.

How to get the word out?

Once the decision regarding where to store your policies is finalized, you will need to begin planning how to communicate to employees where the policies are located and what their responsibilities regarding these policies will be. Pointing employees to the policies is the easy part. Having them accept responsibility is the hard part. This requires education because most employees will see these policies as a hindrance. You need to educate employees about how policies help to better the organization and accomplish its mission statement. Many times in our lives we follow rules, whether legal or social. If you look at the rule microscopically it appears a hindrance, such as the traffic regulations. Many times you may feel that a red light or a one-way street is a hindrance to your progress, especially when you are in a hurry. But imagine that there were no traffic lights, stop signs or parking regulations. Gridlock and accidents would bring traffic to a screeching halt. So you can't look at the policy microscopically. This is not easily accomplished and requires some re-education. You must view it in terms of its overall goal and outcome. So, spend time educating your employees regarding your security policies.

Experts, such a Patrick McBride, recommend that 40% of the security budget be spent on security awareness and that half of that be spent on training IT professionals on policies, procedures and standards. Security awareness training is an excellent avenue to let employees know why policies are important. Interactive training lets the employee become involved in the security process. This interaction will allow the security team to see if the employees understand the policies and the reasons why they are implemented. This feedback is extremely important. Security professionals can easily become focused on securing the environment and lose sight of the business. This training can be another check to verify that your security policies are not a hindrance to your organization's mission.

Since training time is valuable, it is essential that this time be properly used. Because it is impossible to review every security concern during a Security Awareness training session, I suggest you pick several key policies, explain why these have been implemented and tell some related stories. If you can validate a couple of policies in the employees' eyes, it will be more likely they will accept the remaining security policies.

This is an excellent time to explain your organization's definitions of statements, policies, standards, guidelines, controls and procedures. Inform the employees where they can forward any additional questions regarding the security policies. If you can maintain a constant dialogue around your security policies it is more likely that employees will take ownership of these documents and then your security programs will succeed.

Once you have an initial round of security awareness training that highlights your policies, it is important to keep the message alive. You can do this through new hire orientations, newsletters and follow-up training sessions. Try keeping security in the spotlight, and whenever possible reference the security policies. Proper training is the way to reeducate your employees to view security policies as a help and not a hindrance.

How to keep you policies alive and well

The job is never complete when working with policies. Policies must change as technology and business processes change. But almost never will someone volunteer to update any document relating to a policy. Each statement, policy, procedure, standard and guideline must have a designated owner. It is that person's responsibility to maintain her policy documents. This should be documented in the job descriptions for that role. The Security Council must meet regularly to discuss the effectiveness of the documents and when appropriate make the necessary changes. Audit will play a vital role in the success of your policies. Internal audit will examine the effectiveness of your policies and should make recommendations. The more your policies are examined and reviewed the better.

As stated above in the 'How to get the word out' section, training is an excellent way to help sustain the life of your policies, but there are those who, no matter how much education is provided, will still break the rules. So, you must use both technical and process tools to catch policy violators and then dispense the appropriate response. Enforcement must be consistent and fair. Employment termination should not be the only result of policy infractions because there are instances where breaking the rule is necessary. Work with Human Resources to establish appropriate levels of discipline for policy infractions. You must enforce your policies to retain their validity. Employees will soon realize if no one is paying attention to the organization's policies. Once this happens the policy is dead. So, to avoid your policy's demise, make certain there is a procedure in place to enforce your policies with the appropriate response for infractions.

Try coordinating with Human Resources so that the employee's yearly evaluation and compensation review is tied to a review of the current policies. The employees will need to review each policy appropriate to their position and sign off on such. Making the policy review the key to unlocking an employee's yearly performance review is a very effective way to help keep your security policies alive.

Whenever possible refer back to a statement or policy. Keeping your policies in the spotlight will help to keep your organization on the correct path and also help to keep your policies current.

Conclusion

To effectively launch and maintain security policies remember that policies cannot exist on their own. The policy is only a piece of the puzzle. Create the appropriate policy infrastructure containing Statements, Policies and related Controls. You must have all the pieces above and below the policy to successfully implement and maintain your organization's security program.

It is important to ensure that your organization is working from the same set of definitions. Everyone should understand your organization's policy hierarchy, where to find these documents, and why they have been implemented.

Do not expect your policies to maintain themselves. Your organization's Security Council must consistently review and update the documents with corresponding training and company communications.

Lastly, do not overwhelm your employees with new security policies. Plan, start slowly, and keep moving.

References

1. Guel, M. “A Short Primer For Developing Security Policies”; SANS Institute; Copyright 2001; On-line. 12 Dec. 2003; <http://www.sans.org/resources/policies/Policy_Primer.pdf>; page 9

2. Cole, E. Fossen, J. Northcutt, S. Pomeranz, H. SANS Security Essentials with CISSP CBK Ver. 2.1; pg. 347

Bibliography

Andress, M. “Effective security starts with policies”; InfoWorld; 16 Nov. 2001; On-line. 12 Dec. 2003; <http://archive.infoworld.com/articles/tc/xml/01/11/19/011119tcpolicy.xml>

Armstrong, I. “Policy that lives: Enforcing security in spite of the users”; SC Magazine; July 2003; On-line. 12 Dec. 2003; <http://www.scmagazine.com/scmagazine/2003_07/feature_1/>

“Best Policies for the Countywide Information Security Program”; California County Information Services Directors Association California Counties; April 2003; On-line. 12 Dec. 2003; <http://www.misac.org/state_library/ccisda_security_best_policies.doc>

Bosworth, S. Kabay, M. Computer Security Handbook; Copyright 2002; pg 28.2

Buffington, J. “Where is DR headed?’; SC Magazine; April 2003; On-line. 12 Dec. 2003; <http://www.scmagazine.com/scmagazine/2003_04/cover/>

Cole, E. Fossen, J. Northcutt, S. Pomeranz, H. SANS Security Essentials with CISSP CBK Ver. 2.1

Cunningham, K. ‘Cyberterrorism: Are We Leaving the Keys Out?’; SC Magazine; Nov 2002; On-line. 15 Dec. 2003; <http://www.scmagazine.com/scmagazine/sc-online/2002/article/51/article.html>

Guel, M. “A Short Primer For Developing Security Policies”; SANS Institute; Copyright 2001; On-line. 12 Dec. 2003; <http://www.sans.org/resources/policies/Policy_Primer.pdf>

“IT Controls and Objectives for Sarbanes-Oxley”; IT Governance Institute; Online. 12 Dec. 2003: <http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

McBride, P. “How to Spend a Dollar on Security”; 9 November 2000; On-line. 12 Dec. 2003; <http://www.computerworld.com/securitytopics/security/story/0,10801,53651,00.html>

SANS; On-line. <http://www.sans.org>

“Site Security Handbook”; Request for Comments: 2196; Network Working Group; September 1997; On-line. 12 Dec. 2003; <http://www.ietf.org/rfc/rfc2196.txt?Number=2196>

Vaeth, S. “Shackled by the rules? Unlock the opportunities”; SC Magazine; Feb. 2003; On-line. 12 Dec. 2003; <http://www.scmagazine.com/scmagazine/2003_02/cover/>

“Why Security Policies Fail’, White Paper; Control Data; Copyright 1999; On-line. 15 Dec. 2003; <http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf>

Last Updated: May 29th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event