Global Information Assurance Certification Paper

Application of Project Management Techniques within the Security Office
Keith A. Fear
March 23, 2002
SANS Security Essentials GSEC Practical V1.3

Summary
The course material used within this certification program did a good job of covering the basic knowledge needed to begin identifying, assessing, managing and responding to security threats. However, one area that was not covered is how to manage the processes, procedures, and response plans that make up a modern Security Office. Within this document I will attempt to explain how modern Project Management strategies complement the security strategies we just covered in this course material. This document will not attempt to teach Project Management, just explain how to apply some of its strategies to the Security Office.

I will cover how to apply modern Project Management skills to representative samples of tasks performed within the modern security office. This will include writing a Security Policy, and create hardening procedures for various systems. Hopefully at the end of this document you find that the application of these strategies assists in bringing the Security Office in line with the rest of the Information Technology organization, and additionally provides a sound methodology for applying the security strategies we have just learned. A consistent, uniform approach to the application of Security Strategies will provide for a more secure environment allowing the security officer greater visibility and potentially allow for quicker identification and response when a threat does occur.

Areas of Focus
Within the modern Security Office, there are several areas that must be focused on. In summary those areas are:

- Risk Mitigation – The creation of a security strategy, ensuring that all systems are hardened. Installation, maintenance, and usage of firewalls and intrusion detection systems are all examples of this focus area.
- Threat Response – The methods and processes used to respond to an attack, or a perceived attack make up this area of focus.
- Education – While we may not like to believe it, a very large portion of the Security Offices time is, or should be, tied up in education. Education of end users on good password practices, education of management on why the dollars are needed for security are both examples of this area of focus.

In reality, there are not many other areas of focus that draw the attention of the Security Office. All of the tasks the Security Office is asked to perform, fall into

the above three categories. Project Management also has its areas of focus. Those areas of focus can really be broken down into 2 areas:

- Risk Mitigation – Just as with the Security Office, it is necessary for all project managers to attempt to identify and mitigate risk. Some examples of risk mitigation in project management might be purchasing insurance or the addition of 10% to the budget and time table for unforeseen risk items.
- The Trilogy – Within project management, there are three areas of focus beyond risk mitigation. They are Time, Resources, and Money. If someone broke down where a project manager's time is spent, well over half of his/her time would be spent managing these three items. Items that make up this area of focus would include managing the budget, team member's availability, and managing outside contractors.

If you look at the two sets of focus areas, it is very apparent that there are areas of overlap. This is just at the very highest of levels. With these overlaps noted, there are several Project Management skills that can be employed to make the implementation of these focus areas much easier, and more consistent. The skills we will discuss and employ are:

- Creating a Scope Document – Within Project Management, this skill is used to create and execute accurate projects. In short, it defines the running rules of a project. If an item is not covered in this document, it is not part of the project unless a Scope Change is completed.

- Creating a Work Breakdown Structure – This is what many people consider a project plan within Microsoft Project. In reality, a project plan includes many things, only one of which is a Work Breakdown Structure. This document is simply a list of work to accomplish, when it will be done, how much work will it take, and who does what.

- Managing Schedule – For all tasks, projects, and initiatives within an organization there are timelines. Usually these are predetermined, but occasionally, we have the luxury of assigning our own.

We are going to focus on applying project management skills to the risk mitigation focus area. People new to security are probably also not well versed in project management. I chose to merge these skills within the risk mitigation area of focus in order to provide new entrants with a method for immediate application of what I consider to be the key aspects of security; security planning, and system hardening. If we are unable to succeed in these two areas, we will never succeed in more complex areas.

Risk Mitigation

Within this area of focus, we are going to apply basic project management strategies to two examples. The two examples are the creation of a security policy, and the standardization of server hardening strategies. Once we have completed the primer with the security policy example, the remaining area will employ all of the same techniques with the addition of packaging for repeatability. In short, if one can master the skills discussed in this section, the rest is gravy.

Security Policy

A security policy, in short, defines acceptable risk. Acceptable risk to one company will be entirely different to another. Some examples of items that might be in a security policy are Executive Summary, Purpose, Related Documents, Cancellation, Policy Statement, Actions, Responsibility, and most importantly an Authority Statement.[1]

Making the assumption that there is no existing security policy, we need to create a scope document that details the process for creating this document. "The purpose of a scope document or statement of work is to clearly define the deliverables or services to be delivered by a project. It should include a description of the deliverables, the resources to perform the development of the deliverables, the budget allocated to the project and time frame. It should list all assumptions, policies, constraints, and standards that affect the project. It should clearly identify deliverables that are not included in the project. It may incorporate a Governance Agreement in the content or may refer to a Governance Agreement."[2]

While a complete scope document sample is beyond the scope of this document, below is a selection of critical areas within a scope document and what information should be contained within those sections. A complete sample can be found at http://www.processimpact.com/process_assets/vision_and_scope.doc.[3]

> Executive Summary – This section is crucial to the overall approval of this project. When this document is handed to senior management, they will

---

[1] Sans Security Essentials Course Material, "Basic Security Policy", 2-4, Contributing Authors Doug Austin, Alexander Bryce, Rob Dinehart, Brian m. Estep, Stephen Joyce, Carol Kramer, Randy Marchany, Stephen Northcutt, John Ritter, Matt Scarborough, Arrigo Triulzi, Eric Cole. (March 23, 2002)

[2] UC Davis Project Management Office, Definitions and Templates, http://pmo.ucdavis.edu/document.htm#Scope%20Document%20or%20Statement%20of%20Work (March 23, 2002)

[3] ProcessImpact.Com, Scope Document Template, http://www.processimpact.com/process_assets/vision_and_scope.doc, if prompted for user name and password, press Cancel, it is not required. Copyright © 1999 Karl E. Wiegers (March 23, 2002)

read the Executive Summary first. Some senior management may not even read beyond this section. Therefore this section must communicate what senior management needs to know about this project and its goals. This section should include a high level overview of the objectives of the project, not of the policy, as the policy hasn't been written yet. It additionally should communicate an overview of the approach that will be taken, and the high level deliverables that will be completed during this project.

Deliverables Section – Within the deliverables section, one must define what the deliverables of the project are. First and foremost, the primary deliverable should be a useable Security Policy document that is approved by management. However, there might be other deliverables that are incorporated into this project. Some examples might be standard password policy, acceptable usage policy, acceptable Internet usage policy or others. The deliverables section should detail the information that will be contained within each deliverable. For example, according to the University of Queensland Security Emergency Response Team, a completed security policy should include at minimum; an Abstract, Context, Philosophy and Function, Definitions, Governing Policies, Authority, Distribution, Review, Risk Analysis, Rights and Responsibilities of Users and of Resource Providers, and Violation sections.[4] By including a definition of what will be contained in the finished deliverables in your scope document, you will make it clear to everyone involved what will be researched and defined. Should changes need to be made, a scope change can always be executed, but at least by attempting to create clarity within the project up front, you should minimize rewrites and thereby save time.

Resources Section – The resources section details what resources are required to complete this project. Keep in mind that resources include people, systems, and money. If you are defining personnel resources, you must clearly define what skill sets are needed, when they will be needed, and for how long they will be needed. If the resource required is budget, then one must clearly define how much is needed and when the funds will be required. Additionally, you might be required to clarify exactly where you expect to spend the funds or with what vendor.

[4] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

Once the Scope Document has been created and approved, you must create a Work Breakdown Structure (WBS) for your project. This document is a detailed work plan for the entire life cycle of the project. While you may or may not know at every level of the WBS what specific detail work will be accomplished, you should have a good general idea of what work is necessary to complete each deliverable. It is necessary to point out that according to The Project Management Institutes Project Management Body Of Knowledge, each project must have 5 phases. These phases are Initiation, Planning, Executing, Controlling, and Closing.[5] Therefore, your WBS should be broken down into those 5 phases as well.

The initiation phase should include project setup information. Items such as project approval and scope creation are included in this phase. The planning phase includes items such as creating the detail time line, assigning detail work to resources, conducting a kick off meeting and other final planning and detail assignment tasks. The execution phase is a detailed task list of everything that must be done to complete each deliverable. The single most important line in this section is to have the completed policy signed by the highest-level person possible within the organization. As we have learned, failure to do so could open you up to real problems ranging from termination to prosecution. The controlling phase discussed the command and control aspects of the project. For example, how will staff report status, when will they do it, and how will scope changes be handled. Finally, the closing section defines how the project is closed and when it can be closed.

Below is a task list for the creation of a Security Policy. This is a portion of what will be included within a WBS, but it is the task portion and short notes of the WBS only. Resources and timelines would be added if this were a complete plan:

1.Initiation Phase

1.1. Create scope document - This should have been created prior to the WBS being created, therefore this is really a completed task from the very beginning.

1.2. Get approval for scope document - This must be signed off on as a plan by the highest level of management within the organization that can be reached. Given the potential impact, the higher level the signature the better.

[5] Project Management Body Of Knowledge,
Project Management Body of Knowledge, PMI Standards Committee, Copyright © 1996,
ISBN 1-880410-13-3 (March 23, 2002)

1.3. Get approval to begin project - This must be signed off on as a plan by the highest level of management within the organization that can be reached. As stated above, the higher level the signature the better.

2.Planning Phase

2.1. Complete draft WBS - We are creating a draft WBS right now. It should include as much detail as possible so that it may be presented to the project team.

2.2. Assign resources to tasks - These resources should be chosen for their understanding of the particular issue they will be working on, and for their ability to document their item accurately and completely.

2.3. Assign timelines to tasks – This will vary depending on any timeline restrictions presented by management, and the size of the organization.

2.4. Conduct kickoff meeting – Below are items that should be covered in the kick off meeting.

2.4.1. Confirm vacation schedules – Confirm when various team members have vacations scheduled.

2.4.2. Discuss scope document – Review the entire scope document that was created with the team. Allow input and feedback. If there are any areas of concern or issues, now is the time to find them.

2.4.3. Discuss deliverables – Review any deliverables that are planned. If you have any samples, present them so the team has a grasp of what you plan to accomplish.

2.4.4. Discuss timelines – Discuss deadlines for various tasks and review any concerns with those timeframes.

2.4.5. Discuss procedural issues – If you have specific procedures that must be addressed for your project, now is the time to discuss them. For example if there are access hours issues to specific secure areas, notify the team as appropriate.

2.4.6. Discuss any issues raised – If specific issues or concerns are raised by the team, discuss them and resolve them before moving on. Issues unresolved now will become worse issues later.

3.Execution Phase

3.1. Create security policy document – Notes about each sections contents are included for reference from Australian CERT recommendations. [6]

3.1.1. Abstract – "The abstract should set out what the document is and the organization for whom it has been written." [6]

---

[6] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

3.1.2. Context – "This section should outline the context within which the resources under the control of this policy operate. For instance, a private company may not be connected to any network outside of its own domain, or on the other hand it may be connected to banks throughout the world. The context effectively determines what the governing policies are of the security plan and influences the philosophy and procedural guidelines set out in the rest of the plan."[7]

3.1.3. Philosophy and function – "The writer of a security policy will inevitably be faced with several alternatives when deciding on a particular policy for a particular issue. The classic instance of such a dilemma occurs when one determines that a compromise of a computer system is actively in progress, and that the compromise possibly includes a violation of law does the system manager take steps to reduce the impact of the compromise (by, for example, disconnecting the compromised network from the source of the compromise), or does the system manager allow the compromise to continue in an attempt to identify the attacker at the risk of damaging or losing resources permanently? The basic philosophy that should be used when constructing policies that may be used for making non-deterministic decisions should be outlined in this section. One should also outline the functions that the plan is expected to serve within the organization. Similar to the philosophy behind the plan, the functions that the plan will serve will affect the content." [7]

3.1.4. Definitions – "The key to writing an effective plan is accurate and precise definitions of terms. Any term that may have any ambiguity attached to it must be defined in a precise manner. Any loopholes left in this section or in the sections regarding the rights and responsibilities of users and resource providers may be exploited by people in order to circumvent the plan." [7]

3.1.5. Governing policies – "The plan may only make mention of policies that directly affect it, rather than get bogged down in all policies that may indirectly affect the document in varying degrees for pragmatic reasons." [7]

3.1.6. Authority under which this policy is created and executed – "In order to be effective, the plan must be the product of a directive from an influential and authoritative person within the organization. It is important to define the driving force behind the

[7] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

development and implementation of the policy. Furthermore, this section must outline the person who has ultimate authority in the interpretation and application of it to a particular situation, particularly in lieu of any issue that may be addressed in subsequent sections. Another consideration when writing this section is that of allowing for flexibility. That is, decision makers may need a clause in the policy that allows for a policy statement to be temporarily waived from time to time by a person of authority under certain conditions or guidelines. Such a clause allows those in authority to act with initiative (and still within policy boundaries) should unusual situations arise".[8]

3.1.7. Distribution – "The organization should formally define the standards it will adhere to ensure that the people affected by the policy are appropriately informed of its contents (as is its moral responsibility)." [8]

3.1.8. Review characteristics - "A plan that is prepared in a final form and never reviewed for the appropriateness of its contents during its lifetime may quickly become a document that is either cumbersome or useless. This section should formally set out periodic" [8] and required review procedures and signoffs.

3.1.9. Risk Analysis and Response – "This section outlines the assets that must be protected," [8] how, and to what extent. "This is necessary to provide the underlying logic for the following sections which formally define the rules that apply to the use of those assets." [8] Additionally, this section should define response tactics allowed and those not allowed. It should clearly define the criticality of various systems and which response techniques are allowed for each type of resource.

3.1.10. Rights and responsibilities of users – "This section (and the next two) are the heart and soul of a plan. It can be difficult to draw distinct lines between the rights and responsibilities of users and the resource provider, since many issues may be considered to be in the domain of either (privacy being one such issue). The key to writing this section and the next is to make a firm decision on which issues belong in which section (e.g. by preparing a detailed table of contents) and thus avoid duplication and complexity. Issues that could be addressed in this section" [8] could include; "(a) Account use, by both the account holder and the resource provider. Special conditions may apply to the use of

[8] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

normal user accounts, and public access accounts (like anonymous FTP), and these conditions could be expressed here. (b) Software and data access and use, including sources of data and software. (c) Disclosure of information which is potentially harmful, such as password information or system configuration information. (d) Etiquette, including acceptable forms of expression (e.g. non-offensive expression expected for unsolicited electronic mail), and unacceptable practices (such as the forging of electronic mail and news articles). (e) Password use and format. (f) Rights to privacy, and the circumstances under which the resource provider may intrude on the files held under or activities practiced by an account. (g) Other miscellaneous guidelines regarding reasonable practices, such as the use of CPU cycles and temporary general access storage areas. Copyright issues may also be discussed here." [9]

3.1.11. Rights and responsibilities of resource providers – "There is a myriad of information that could be placed in this section. The content of this section assumes a large degree of importance (indeed, probably more than the previous section) when one considers recent statistics regarding the proportion of crimes involving computers that are committed by people internal (or recently internal) to the organization. Some (but by no means all) issues that could be addressed here include: backups, contact, information, dial-up access, host configuration guidelines including: allocation of responsibility, network connection guidelines; authentication guidelines, authority to hold and grant, account guidelines; auditing and monitoring guidelines, password format, enforcement and lifetime guidelines; and login banners, network construction, configuration and use guidelines including: allocation of responsibility, supported protocols, network design principles, address allocation and authority guidelines; and use of network management and other equipment, physical security guidelines and privacy guidelines." [9]

3.1.12. Violations – "A stated function of a security plan is to form a framework for deciding what action to take in particular circumstances. In the event of a security breach, a CSP needs to offer to those who must take action, necessary guidelines as to what authority they have in order to minimize the impact of that breach. Furthermore, after the breach, the policy must provide

[9] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

guidelines for courses of action to take in order to prevent further or repeated breaches, and also regarding the identification and discipline of the people responsible (in whatever capacity) for the breach. It may be desirable to also offer guidelines for liability of personnel with regard to security breaches. Such policies may tend to encourage people who are the victims of ignorance but honest intent to offer information that can be used constructively to prevent future incidents, rather than attempt to hide details of a breach that they may have (somewhat innocently) been involved in. This section also needs to discuss, in some detail, guidelines regarding investigation of incidents and courses of action that could be taken by decision-makers based upon details of the security breach. Such guidelines may include guidelines about referral of various matters to law enforcement agencies, as well as internal investigation and disciplinary principles. There should be some emphasis placed upon not only minimizing the impact of and recovering from a security breach, should one occur, but also in learning any constructive lessons possible from an incident. The way in which this can be done is to carry out a post-mortem of incidents. Requirements for post-mortem procedures and reports could be outlined in this section. Such a post-mortem could include preparation of reports containing details like cause and effect of the incident, side-effects of the incident, costs involved in terms of losses and recovery, and possible repulsion and impact minimization strategies should a similar incident occur in future." [10]

4.Controlling Phase

4.1. Specify status reporting – During the execution of a project, it is important for the team to routinely report status to the project manager. As the project manager, you will need to determine when and how this status should be reported.

4.2. Specify change management procedures – Should the scope of the project need to change, a standard method for applying for and granting scope changes should be created. This should include items such as a standard form, budget and time impact for a requested change and an approval or disapproval section.

5.Closing Phase

[10] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

5.1. Specify how the project is to closed – This should include how to turn the deliverables over to production, location of the original documents, and budget reconciliation.

Now that the WBS has been created, and the scope document has been created, it is time to execute the project. The WBS gives you a script to play from. Simply follow the guidelines within the WBS that you have defined for yourself and you should end up with a very functional and usable Security Policy. An example of a Security Policy can be found at http://www.irm.state.ny.us/policy/tp_971.htm[11]

Server Hardening Strategies

Within the previous example, we built the foundation upon which all of our future strategies are to be built. We defined how to create a scope document, and a work breakdown structure. These two documents are the basis for most projects. If these documents are created using careful estimating, and a conscientious approach to requirements setting you should be successful in creating the previously mentioned security document.

Moving on to server hardening strategies, we are going to assume the same skills are applied and that the previous security document is created and well written. Within a well written Security Policy, there will be a section that describes basic hardening of systems that is required to be accomplished for any new and existing system within production or to be added.

As part of creating our scope document on hardened systems, we should define the types of systems we will be attempting to harden. Making the assumption that we will be hardening Cisco Routers, we should begin our WBS by defining what needs to be hardened, and how best to accomplish this goal. For example, when determining what Cisco products to use for our security architecture, and how best to secure them, we can consult the "Cisco Safe: A Security Blueprint for Enterprise Networks"[12] white paper. This white paper discusses how to design the architecture, minimize expected threats, and configure systems in such a way as to consider them hardened. Once we have created a detailed task list of items we want to change on our routers to harden them, we can use this information to complete our WBS for our Cisco Router hardening exercise. The task list of items to change on our routers to harden them might look something like this:

[11] State of New York Office For Technology, Technology Policy 97-1 http://www.irm.state.ny.us/policy/tp_971.htm, (March 23, 2002)

[12] Cisco Safe: A Security Blueprint for Enterprise Networks http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm, (March 23, 2002)

- Apply current release of firmware
  - Ensure has SNMP exploit fix applied
  - Ensure I have reviewed current security exploits
  - Ensure I have reviewed release notes on this release of firmware
- Turn off unnecessary services
  - "No ip domain-lookup" [13]
  - "No cdp run" [13]
  - "No ip http server" [13]
  - "No ip source-route" [13]
  - "No service finger" [13]
  - "No ip bootp server" [13]
  - "No service udp-small-s" [13]
  - "No service tcp-small-s" [13]
- Enable logging
  - "Service timestamp log datetime localtime" [13]
  - "Logging xxx.xxx.xxx.xxx" [13]
  - "Snmp-server community xxxxxxxx ro xx" [13]
- Set passwords and encrypt them
  - "Service password-encryption" [13]
  - "Enable secret xxxxxxxxxx" [13]
  - "No enable password" [13]
- Add Message of the day
  - "Banner MOTD #
    This is a secured system operated for and by XXXXXXXX
    Authorization from XXXXXXXX is required prior to using this system
    Use by unauthorized persons is prohibited
    #" [13]
- Apply access lists to minimize unnecessary traffic – assuming this is an edge router, I would apply access lists to restrict traffic to only that traffic that must enter my DMZ, for example Port 80, and Port 25. Assuming I am not using SNMP V3 and cannot confirm the current SNMP vulnerability is fixed, I might also not enable SNMP. Additionally, I might restrict communications to and from this router across my DMZ. Depending on my design I might configure an access list that only allows communication between my firewall and this router on the DMZ. Assuming this is a WAN router internal to my network, I would not impose the same restrictions, although it would be beneficial to use access lists to restrict traffic across the WAN to only that traffic that must be present.

Assuming that these are the only items I want to set on my router to harden them, I would execute these settings and test this router to verify there are no

[13] Cisco Safe: A Security Blueprint for Enterprise Networks
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm, (March 23, 2002)

unforeseen consequences. Once I am confident that all of the settings are exactly the way I want them, I would deploy this router. Additionally, I would save a copy of this configuration on a secured server and additionally, burn one to CD for offsite storage in accordance with my disaster recovery plan.

The new project management technique we are going to employ in this section isn't really a technique at all - it is more like basic common sense. If I know I need to repeat a process several times, I should focus on making that process repeatable or reusable. In other words, we are going to package this project so we can repeat it when and where needed. As part of creating and executing this project, I should keep in mind that I want to package this solution at its completion. Therefore I should ensure that I create a reusable scope, project plan, document set, and relevant procedures that can be packaged and handed off to anyone that might need to use it in the future. If I have packaged this correctly, anyone should be able to complete this project as needed. When I couple this with a quality control process or peer review process, I now have a repeatable process that I can be comfortable is always executed the same way. This should provide for a more stable, secure environment.

Closing

In closing, we have discussed two basic security strategies, security policies and hardening. We have also discussed how best to apply basic project management techniques to those strategies to provide a more secure robust environment. The marriage of these two practices within IT organizations is going to become more important as time progresses. As is stated by the SANS Institute Resources Security Project Management Survey Results,[14] most organizations are in project purgatory as it relates to security. In Project Purgatory "the fire is hot; the good news is that you are still in the frying pan. When it comes to competent project management, your organization doesn't have a clue."[14] We all know the hackers are out there. They are well organized, and they are methodical. Isn't it about time, our response is just as well organized and methodical?

[14] Sans Institute Resources Security Project Management Survey Results http://www.sans.org/newlook/resources/pm_survey.htm (March 23, 2002)

References

[1] Sans Security Essentials Course Material, "Basic Security Policy", 2-4, Contributing Authors Doug Austin, Alexander Bryce, Rob Dinehart, Brian m. Estep, Stephen Joyce, Carol Kramer, Randy Marchany, Stephen Northcutt, John Ritter, Matt Scarborough, Arrigo Triulzi, Eric Cole. (March 23, 2002)

[2] UC Davis Project Management Office, Definitions and Templates, http://pmo.ucdavis.edu/document.htm#Scope%20Document%20or%20Statement%20of%20Work (March 23, 2002)

[3] ProcessImpact.Com, Scope Document Template, http://www.processimpact.com/process_assets/vision_and_scope.doc, if prompted for user name and password, press Cancel, it is not required. Copyright © 1999 Karl E. Wiegers (March 23, 2002)

[4] Australian CERT Recommendations, http://secinf.net/info/policy/AusCERT.html, Information Technology Services, Griffith University, Australia, Security Emergency Response Team, Prentice Centre, University of Queensland, Australia (March 23, 2002)

[5] Project Management Body Of Knowledge, Project Management Body of Knowledge, PMI Standards Committee, Copyright © 1996, ISBN 1-880410-13-3 (March 23, 2002)

[6] State of New York Office For Technology, Technology Policy 97-1 http://www.irm.state.ny.us/policy/tp_971.htm, (March 23, 2002)

[7] Cisco Safe: A Security Blueprint for Enterprise Networks http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm, (March 23, 2002)

[8] Sans Institute Resources Security Project Management Survey Results http://www.sans.org/newlook/resources/pm_survey.htm (March 23, 2002)

Last Updated: September 20th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event