Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementing a Local Security Program to Protect National Infrastructure System Companies and Facili

National infrastructure protection has received a great deal of attention and action since President Clinton issued Executive Order 13010 on 15 July 1996, establishing the President's Commission on Critical Infrastructure Protection (PCCIP) which "...was tasked to formulate a comprehensive national strategy for protecting the infrastructures we all depend on from physical and "cyber" threats."1,2 Numerous events since 1996 such as the terrorist attacks of 11 September 2001 have both justified and added further emphasis...

Copyright SANS Institute

Author Retains Full Rights

AD

DEEPARMOR®

SANS Security Essentials GSEC Practical Assignment (Ver 1.3)
Mark Loos
April 8, 2002
TITLE: Implementing a Local Security Program to Protect National Infrastructure System Companies and Facilities

INTRODUCTION

National infrastructure protection has received a great deal of attention and action since President Clinton issued Executive Order 13010 on 15 July 1996, establishing the President's Commission on Critical Infrastructure Protection (PCCIP) which "...was tasked to formulate a comprehensive national strategy for protecting the infrastructures we all depend on from physical and "cyber" threats."[1,2] Numerous events since 1996 such as the terrorist attacks of 11 September 2001 have both justified and added further emphasis to this effort. The purpose of my paper is to first review the macro-level issues involved in the need for a national level infrastructure protection program. In fact many of these major issues have already been very well examined in other SANS papers.[3,4,5,6] However, I want to transition from these macro-level issues and then focus on those pertinent threats and developments that drive the need for specific security programs at the local infrastructure company level. These key infrastructure elements include the gas, oil, water, electricity, and transportation companies which are the life blood of our country and commerce.

The central security issue of this paper and what many of these companies have in common is that their key industrial processes are managed by control systems such as Supervisory Control And Data Acquisition (SCADA) systems which were once closed industrial control systems, but are now largely computerized components designed for functional performance and information sharing, and not with security or current threats in mind. It is this remote access and connection of these systems to modems, to company networks, and/or to the Internet which make these systems very vulnerable.[7] In addition, local utilities face the challenges of limited resources and increasing demand for their services/products, changes in operations due to deregulation requirements, and pressures to cut costs and improve efficiencies in a mixed economic market, all the while facing an array of cyber, criminal, and terrorist threats.[8] After examining some of these specific threats and challenges seen at the local company level, I will present a generic and informational checklist which can be used for the development of a local security program. The purpose of this checklist is to enable management and network support personnel to work together in a cooperative effort to more effectively deal with the above cited threats and challenges, and to enhance the security and operation of these critical utility systems. Such a structured and tailored security program will be essential to individual utilities if they are to assure their ability to securely operate and provide essential services to their customers now and in the future.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

THREATS AND CHALLENGES

Changes in technology, Internet availability and use, government regulations and public availability of information, and the world and national political scene have radically changed the environment in which our infrastructure companies operate. On one hand, it has enabled infrastructure companies to improve efficiency through automation, computerization, and remote access, but has also significantly increased the risks they face and their need for a multilayed security program. I will examine each of the four threats/challenges cited above as I highlight the requirement for a security program, and then transition into a tutorial checklist that can be used to build a tailored security program for a specific company or location.

Changes in Technology - Infrastructure control equipment, energy management, and SCADA type control systems in the past were basically closed systems,[9] which unless one could gain direct access to the systems themselves or their control panels, one could not directly impact, change settings, or cause any sort of significant damage. The only remote damage one could reasonably expect to inflict was if one could shut down the electric power, source of fuel, environmental controls, and/or cooling that played a supporting role in the operation of the SCADA systems. These secondary damage efforts were high-risk, high-effort endeavors which in themselves were so difficult to achieve that they provided a degree of protection to the infrastructure company.

However, today we have seen a significant change in the technology and openness of the control systems themselves. Some of this change comes from the need to increase efficiency of operations and cut costs, and some of it comes from the technology itself.[10] The result is that many of these systems now incorporate computer and communication elements into their basic components and this enables a varying degree of access between and into SCADA equipment, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTU), IECs, company networks, and even business partners/customers via the Internet. This results in a once-closed system now being much more "open," and which may provide a fairly-low risk avenue or access for outside action by those not meant to have direct access to these key utility control systems. As stated by Paul Oman, Edmund Schweitzer, and Deborah Frincke in their article, *Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA Systems:*

> "Increasing reliance on automated control systems with remote access (via phone or Internet) and the growing global economy have expanded the number of potential attackers with access to substation controllers and SCADA systems, and therefore magnified the risk electric utilities have from sabotage and espionage."[11]

An additional complicating factor in this system metamorphosis is that as this more open and automated infrastructure control system has grown, the process of growth and change has not always been that intelligently thought out or well planned. Market forces and innovation may be great for increasing corporate and economic efficiency, but sometimes new products or modifications to existing systems are not fully thought out and there can

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

be numerous and unexpected consequences.[12] Such consequences can and have resulted in unexpected power outages, security "holes", or even accidents. As stated by Col. Alan Campen, in an article for SIGNAL Magazine in 1998:

> "The weakness of infrastructures lies principally in poorly understood and unforeseen consequences of interconnections for control--one to another and mutually--to the information infrastructure. Industry more quickly grasped the efficiencies and economics of SCADA centralized control, than it did the unforeseen consequences of a proliferation of interdependent and unknown interconnections. Rippling power blackouts that have darkened large areas of the country are examples of cascading when networks seek to isolate themselves from failures in neighboring systems. Another example of the risks of SCADA was a railroad accident in Maryland reportedly caused when switch controls for one rail system, controlled in Georgia, conflicted with those of another controlled in Florida."[12]

A related concern is the effect of mixing modern equipment, with their new computerized components, with old or legacy SCADA type equipment. Many times security retrofits are not an option[7], and as Joe Weiss, technical manager of the Enterprise Infrastructure Security Program at the Electric Power Research Institute recently stated: "...he remains concerned that the industrial sector as a whole hasn't yet addressed the fundamental cyber security challenges stemming from its use of legacy control systems."[13] Security and protective items such as Firewalls, Intrusion Detection Systems, etc., work well with modern networks and computers, but they are not typically designed to work with industrial control systems, and this limits their ability to be used as security retrofits.

To conclude our look at the technology impact and issues relating to infrastructure control items, one only has to check a number of the web pages of the builders of SCADA and related equipment to see firsthand the fusion of SCADA items and computers. I checked the home pages of two companies,[14,15] and saw an array of high-tech products designed to perform SCADA and SCADA related functions. All of these items highlighted such varied product sub-components as "...32 bit processor...600 I/O points...10-Base-T Ethernet connection...serial ports...capability to upgrade firmware and programs remotely."[14] There were RTU's with, "Advanced features and options such as built-in radio transceivers, dialup modems..."[15] I was impressed with the range, quality, and technology of the various products, but no security products, integrated security solutions, and/or encryption systems were highlighted or generally associated with the listed products. This was especially the case for those products with a capability to interact/support dialup modems and wireless communications. Dialup modems and wireless communications are two avenues of entry into a network or system that are notorious for hacker entry unless they are very carefully secured and protected. As I looked at the array of this obviously high-tech and very capable SCADA related equipment, technology has enabled a set of products that can greatly improve the efficiencies and economics of SCADA functions, but also provides a means for unauthorized and potentially hostile entry into the SCADA related networks and components of key infrasture companies.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Internet Availability and Use - Saying that the Internet has changed significantly since its inception as the ARPANET (Advanced Research Projects Administration Network), a computer project funded by the Department of Defense (DoD) in 1969, is an understatement. The ARPANET, which started out as a network of four computers, three in California and one in Utah, grew into an "Internet" in the 1980s. This net connected various educational and research sites funded by the National Science Foundation (NSF) with a number of DoD and DoD contractor sites.[16]

A key development during this time period was the development of the Transmission Control Protocol and the Internet Protocol, which have become commonly known as TCP/IP. The key design goals were to: one, ensure that as a communication protocol that it had to be independent of any specific hardware/software manufactures; and two, "it had to have good built-in failure recovery."[17] TCP/IP's capability to ensure communications and do so independent of hardware/software type has, in fact, been a major element in its success and the growth of the Internet. An additional factor in all this early Internet development was the ability to ensure successful communication. This in fact was the first priority, with not a lot of priority being given to security at that time. The majority of communication and network traffic was between government, government contractors, and university sites, and hacking and network intrusions were not a significant problem during this time period.

This early Internet continued to grow until 1990 when the DoD and NSF turned the oversight of the Internet over to commercially run networks that comprise today's Internet.[16] What followed was an explosive period of growth which has resulted in an Internet today of truly massive size. As cited in the CyberAtlas, the Worldwide Internet Population in 2002 is between 445.9 million (eMarketer figures) and 533 million (Computer Industry Almanac), with a projected growth to 709.1 million (eMarketer) to 945 million (Computer Industry Almanac) in 2004.[18] As we know today, the Internet is truly one of the World's key communication avenues supporting the communication and transfer of text, graphics, audio, video, and all means of commerce, industry and interaction.

Unfortunately, along with the positive has come some negative, and clearly, some of the negative includes network intrusion, hacking, and computer data theft. Although unfortunate, this should not really be all that surprising when we consider the sheer numbers of people involved in the Internet, human nature, and the sensitivity of some of the data that flows along the Internet communication channels. For example if we use the conservative figures of eMarketer of 445.9 million for today's Internet users, and if only one per cent of those people were involved in either data snooping or "recreational" hacking of some sort, you would have between four and five million people presenting some degree of computer nuisance or threat. Additionally, if only one in a thousand were actually involved in illegal and/or harmful action, you would still have some 400,000 to 450,000 individuals you would have to specifically guard against. Furthermore, if only one in 10,000 had what could be called criminal and malicious intent, then users of the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Internet would still face a malicious group of some 40,000 to 45,000. Whatever the exact figures, I believe this number review serves a useful purpose in driving home the point that the current Internet is not the Internet of the 1980's and early 1990's, but a much more dynamic and capable means of communication, interchange and commerce, but also one which presents a much more threatening environment. Anyone who ventures out into that communication environment, especially if they do so with any sort of important and/or valuable information/product, must take the appropriate defensive measures to protect their valuable product or important information. Additionally, not only are numbers a factor, but with every passing year, we see the Internet provide both a forum and avenue for the education of computer and Internet users so that many Internet users become more computer literate. This unfortunately includes the spread of hacker tools, techniques and methods.[8,11] Therefore, any infrastructure company manager and their network manager and/or security manager should take specific notice of the sheer size and opportunity for possible intrusions into their networks or control systems, and take appropriate protective actions. This includes implementing a computer security program as a component of their greater company security program. Failure to do so will only result in a greater opportunity for disaster in the future.

Government Regulations and Public Availability of Information - Both government regulations and the open society we live in have made available a great degree of information that complicates the protection of the control systems which play a key part in the operation of our infrastructure industries. Additionally, government regulations have also impacted the infrastructure industries in more ways than requiring the disclosure of certain types of information. It has also affected the business environment through deregulation and in ways that stress the employee environment, and this many times impacts company security.[8,11] Federal Energy Regulatory Commission Orders 888 and 889 resulted in major changes to the nation's public electric utility industry. "The first rule, Order No. 888, addresses both open access and stranded cost issues. The second rule, Order 889, requires utilities to establish electronic systems to share information about available transmission capacity."[19] What is particularly interesting about these rules is not just the deregulation actions they caused, which are significant, but also the guidance on sharing and dissemination of information embodied in Order 889, now known as the Open Access Same-time Information System Rule or OASIS rule. This OASIS rule stated some fairly specific communications protocol and standards requirements for the dissemination of utility company and pricing information to include support for HTML access by Internet browsers, support of ZIP compression standards, and to have a data rate of at least 28.8 Kbits per second.[20] What has resulted because of government regulation, business competition, and a growing use of the Internet is that we have a great deal of very sensitive utility company and infrastructure information out on the Internet. As stated by Ed Badolato, president of Washington-based Contingency Management Services, Inc. and former Deputy Assistant Secretary for Energy Emergencies at the DOE, "the amount of information about critical energy infrastructures available on the Internet provides a blueprint for terrorists. Most of the information was put there as a response to regulatory requirements and for business promotion purposes."[21] Another example of what is very likely too much information being posted

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

on company web sites was uncovered by Eric Friedberg, managing director at the New York based Stroz Associates, and former computer crime director at the U.S. Department of Justice. He stated:

> "Many Web sites constitute a gold mine for potential attackers," said Friedberg. Audits have found descriptions of physical locations of backup facilities, the number of people working at specific facilities, detailed information about wired and wireless networks, and specifications of ventilation, air conditioning and elevator systems. Other sites give graphical representations of floor plans, cabling connections, and ventilation ductwork, Friedberg said."[22]

A survey by riptech, a computer security firm and consultant to many of the US's largest utility companies, yielded another disturbing fact: some 70% of the operating manuals for SCADA related network control systems are available to the public.[23] This clearly provides rich source material of what to do for anyone who has ill intent if they are successful in hacking into a company's control system.

Furthermore, it's not just the specifics of what's on the company web site that must be taken into account today, such as the detailed information cited above, but many times the tone and content of a company's message(s) also bear review and assessment as to whether it may draw unnecessary attention by hackers, terrorists or other groups opposed to a company's policies or business. As stated by Eric Shaw, a former CIA psychologist and profiler who now works for Stroz Associates, "Companies are communicating very effectively with their internal audience and clients, but they don't realize how information from a public Web site can be interpreted differently, particularly by adversary groups."[22] The Internet and company web sites provide a great marketing and advertisement vehicle, but there is also a downside to this in that one's message is not only seen by customers and potential customers. Many others will see your message and common sense and security awareness dictate that company managers and security officials, as well as web site managers play a part in deciding what goes on the company web site today. A key issue in this discussion is balancing the public's right to know with security, both as it relates to national security of our key infrastructure utilities and of the country. Paula Scalingi, former Director of Critical Infrastructure Protection at the DOE and now a private consultant stated:

> "On the one hand, there is the natural, visceral and understandable drive to eliminate such information on the Net. On the other hand, there is a real need to know on the part of public- and private-sector organizations and individuals for safety, security and emergency response purposes...Maybe no one in the post 9/11 world wants to hear this message, but we need a cool-headed, systematic approach to the problem, rather than the current rush frenetically to snatch without question infrastructure-related information from public view."[24]

Clearly any company and location security plan needs to include both a realistic and balanced scrub of a company's web site. This balanced security, environmental and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

safety, and business assessment should include and retain information required by government regulations, and good business practices and necessity. However, it should also eliminate information that could aid or draw the unnecessary attention of computer hackers, criminals, and/or terrorists in carrying out malicious activities/actions against company property, personnel, and/or information. Company management needs to have an appreciation and understanding that the company web portal is not just a window to their customers or a means for remote and efficient control of their industrial components, but may well be a window to the world. They and their web site managers and company security personnel need to work together to eliminate as much as possible the security issues associated with this "window to the world."

One final point I want to highlight in this section is the impact that deregulation has had on the company worker/employee environment. The purpose of this paper is not a Human Relations or Personnel Management essay, but clearly deregulation and economic efficiencies have in some cases put considerable stress on the employee environment, and that can create disgruntled employees and result in the creation of insider threats.[8,11] This specific issue argues for a combined management approach that gets factored into a company's security policy. Prudent measures to reduce the impact of down sizing and employee layoffs and creation of insider threats need to be seen in the light of "pay now or pay later". There is one case of a disgruntled ex-employee of an electric utility who posted a note in a hacker journal that his knowledge of these systems could be used to shut down the regional power grid.[8] A combination of employee security screening, best possible employer-employee work environment, and retraining and job transition program need to be implemented to mitigate against instances where employees with critical system and facility knowledge are "dropped" from employment with little concern for what happens to them or what they do in the future. Sooner or later, a utility company may find that one of these discarded and disgruntled former employees is willing to use his/her insider information for malicious intent or revenge. Even at the local site or company level, the nation and world is a much changed environment and this has become more evident since 11 Sept 2001, and that is what we will examine in the next section.

World and National Political Scene Changes - In addition to the many issues highlighted above, terrorism and cyber crime are making their impact felt even at the company and local site level in North America today. Clearly, events of 11 Sept 2001 have highlighted that terrorism is a very real possibility in North America. Whether it is the domestic brand of terrorism, such as Oklahoma City, or the external brand, such as the first and second World Trade Center terrorist attacks, terrorism is a very real threat that must be taken into account in the security programs for critical infrastructure industries.

At both the global and national level, we are seeing selective terrorist groups, such as al-Qaida, radical anti-globalism groups, and even some of our domestic militia groups becoming more active in North America. Since the fall of the Iron Curtain and the defeat of Iraq in the Gulf War, the United States has become the single superpower in the world, and some terrorist groups such as al-Qaida believe that we are the root cause of many of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the World's or at least of their country's and/or culture's problems. Whatever one may think of this, at least in the eyes of al-Qaida, the US has become the target of both its rhetoric and hostile action. A complicating fact to this situation is that both the global economy with its worldwide economic interaction, and the world transportation system enable members of hostile groups to travel fairly easily on both a national and international level, and as the 11 Sept 2001 attacks demonstrated to actually use the means of transportation as weapons.

Although physical destruction still appears to be the greatest threat to our key infrastructure facilities today, the electronic and cyber threat is growing and requires significant defensive security action.[11, 25] As explained earlier in my paper, the reason for the growth of the cyber threat relates to a great degree to the growth of the Internet itself, the growth of the number of computer literate users, the growth of hacking or cyber tools readily available on the Internet, and the fact that the Internet enables global interaction on an even broader scale and is an easier "method of travel" than airline travel. Specifically, we are seeing a complex situation playing out in the world that requires us on both a national and company level to implement multilayed security programs to address both physical and cyber security. In this light, in June of 2001 a CIA official testifying before Congress on cyber threats warned that terrorists believe that "bombs still work better than bytes".[25] However, in a December 2001 article entitled, *The Cybercrime Threat*, by Lori Burkhart, one of the bottom lines she lists in her article is: "The PC is the most likely means of unauthorized access to utility systems. As utilities rely more on Web-based control and communication, the risk grows."[23] She further adds: "The National Security Agency long has warned that foreign governments are developing computer attack capabilities against critical infrastructures in energy, telecommunications, defense and government, with intents to damage and disrupt national defense and vital services."[23] However, not only are foreign governments involved in the cyber area, but also non-state groups such as terrorist groups as well. The Canadian government's Office of Critical Infrastructure Protection and Emergency Preparedness made the assessment in a November 2001 Threat Analysis Report, that although al-Qaida has not engaged in cyber attacks in the past, this organization has the financial resources to pursue such a capability, and that there is substantial, but unsubstantiated reporting that al-Qaida are sophisticated users of computer and telecommunications technology.[26, 27] Furthermore, Richard Clark, the head of the White House's Office of Cyber defenses, recently said: "that there is evidence that the terrorist group al-Qaeda [sic] was using the Internet to gather intelligence about critical facilities in the U.S. and that other terrorist groups and nations may be doing the same."[28]

Finally, to put this discussion into the context of critical infrastructure industries, riptech, in a presentation to the 2001 Energy IT Expo, stated on one of their slides entitled "Riptech Information Security Threat Report... "initial analysis confirms information security concerns of Power and Energy industry -- over 60% of companies suffered a "severe" attack during the past six months."[29] The cyber threat as well as the more traditional threats, are real threats to our key infrastructure utilities, and both must be addressed in a company or site security program. On the cyber front, I propose that what

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

we are seeing is the steady, but sure growth of a real cyber threat, like the airplane in WWI which started out as an observation vehicle, but eventually evolved into a major and significant weapon system. I think we are seeing the same transition with the computer and that this has already basically happened with hackers and criminals, and eventually will also occur with governments and terrorist groups. This will make it all the more important for our key infrastructure industries to implement multi-layered physical and cyber security programs, and to this end I plan to explain and highlight in next section a security matrix and checklist that can be used to build a tailored security program for an individual company or site.

SECURITY CHECKLIST

"I have said many times that security issues are industry issues and that solutions go beyond technology and involve people, processes and policies."[30] Howard Schmidt, Vice Chairman of the President's Critical Infrastructure Protection Board.

Each infrastructure company and facility location clearly has its own goals, policies, requirements, situations, resources and limitations that will drive the size and type of its specific company or site security program. Yet as the above quote by Howard Schmidt states, security issues require a comprehensive, and, I submit, full-time approach. As starting point, each infrastructure company should have at least some sort of trained security staff, and perform a detailed security and vulnerability assessment based on company goals, policies, objectives, and situations. They need to first: determine what is really critical to protect, what only needs superficial protection, and what requires no protection at all in light of their company or facility goals and requirements. Secondly, they need to determine what their security shortfalls and gaps are. Third, they need to tailor the best possible and affordable security program from a baseline of possible security actions to address and correct any shortfalls, and then implement that program to protect their assets. In the final analysis this is a balancing act between what one needs to do, what is appropriate to do, and what one's available resources are for security and protection. Each company must make the specific assessment of how much security it needs and can afford, but in the long run companies will find out the real meaning of "pay now, or pay later".

The following "tutorial" checklist should be used as a starting point of what a specific infrastructure company or site could use to implement a comprehensive, in-depth security program to protect their assets. It is not meant as the end all of a security program, but as a good, initial starting point:

Security Item/Action	Specific security actions to develop or take C=Completed; IW=In Work; N/A=Not Applicable	Status: C, IW or N/A
1. Identify,	Identify & appreciate essential company products,	

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Review & Understand Your Company Goals, Policies, and Overall Guidelines. What's your company or plant's bottom line and what should you protect?	resources, and processes. ID what is critical to your company's survival and success; what is of average value; and, what is of little or no value. Security policy & procedures should be constructed to provide an "inverted and integrated" process overlaid to the company's products, resources, and processes -- there should be more security & defense in depth for the most important/critical items & processes, less security for the average value products, resources, and processes, and little to no security for the items and processes of little to no value. It is imperative to integrate security into the key company & production processes, so it is seen by employer and employee alike as not just a cost center, but as a profit enabler & key resource protector which everyone needs to support & to do if they want their company & individual jobs to flourish. Your security program can be represented as: Risk,Cost=Threat X Vulnerability X Assets at Risk / Countermeasures Your security program is the specific countermeasures when taken as a whole, reduces the risk/cost to an acceptable cost or loss. The countermeasures can be adjusted to manage or respond to the risk(s). ID & List: -Company Central Function/Process _____ -Critical products, resources, and processes: _____ -Average value products, resources, and processes: _____ -Low or No value products, resources & processes: _____	
2. Establish Security Policy	Develop a local company/plant security policy using the following steps (these basic steps are taken from SANS Institute GSEC Course, Sect 2, Lessons 2,2a):[31] A. Clear statement of **Purpose and Goals** of the Security Policy. _____ B. **Reference Documents** - a listing of key policy & reference documents that drive the local security policy. If this is a local company and/or plant that is part of a bigger enterprise, then one of the key references should be the parent organization's security policy. _____	

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

C. **Cancellation** of prior security policy(s) - If this is a new and/or updated policy then this section will list changes from prior policy(s) and why/what the update was implemented. _____

D. **Background** providing more specific or detailed information explaining why an update to the security policy was implemented and/or why specific features of a security policy need to be implemented. Include only if it's required for clarification or to win over management and the average "company worker." _____

E. **Scope** - lists and explains to who, what and where the security policy applies. _____

F. **Policy Statement** - The central statement of what is to be done and why. It should be crafted to influence, guide, and drive management, security, network, and the average company worker in the implementing, carrying out, and/or updating a comprehensive security program. _____

G. **Responsibility** - State who is responsible for what. These should be broad statements of responsibility, but they need to focus on job categories such as management, network administration, physical and personnel security, and the work center levels such as for an infrastructure company - the power generation section, the power control room section, etc. These statements can then be used along with the Action paragraph below, to later develop Security procedures and checklists for each work center and individual work team as required. This section should also include guidance on metrics or methods to measure security policy and program effectiveness. This may also be the section for you to include a broad statement relating to possible action(s) that would/could happen to employees for failing to comply with company/plant security policy & requirements--needless to say any such statements would need the review and approval of management, legal, and human resources personnel. _____

H. **Action** - Specifies what actions are necessary and when they should be done. A natural attachment or sub _____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

element of this paragraph would be a listing of Security Procedures and/or Checklists tailored to each work center team or for a specific critical position such as the Duty Controller in Charge in a Power Plant Control Room - this checklist or procedure checklist would be a key reference during a major security incident and which should provide key responses to specific actions such as who to contact in what order, who to recall if not already on the job for specific actions to be accomplished, who to contact and get permission to take certain major actions (i.e. who has the authority to shut down the company computer network), etc. These procedures and checklists will need to be more flexible and changeable than the overall security policy itself, but will still need to be formal documents approved by management for two major reasons - 1) that company management understands and approves in advance actions that may happen on an expedited or emergency basis, and 2) provide protection and "top cover" for the employees who have to carry out the actions, and yet do so within a framework of actions that management knows about. Finally, ensure the policy is reviewed annually and after each major security incident to ensure further changes/updates are not required.

-Finally get management buy-in, approval, and signature on the Security Policy. You need to ensure the final product is clear, concise, achievable, and most importantly makes sense to those who must implement the security program. Then work with the Human Resources Department to distribute a formal copy of the Security Policy to Employees - one of the best ways is to include the policy or a summary of the policy is in the Company/Plant employee handbook.

3. Conduct an in-depth Security and Vulnerability Assessment.

An in-depth security assessment takes your security policy and program from the text level into reality. It's essential you do a baseline security assessment to really understand where your company/plant stands in the real world in regards to security, and what corrective actions (if any) need to be implemented to get to the level your company needs to be. Based on the current threat environment for infrastructure companies already highlighted earlier in this paper, such assessments

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

should be done on at least an annual basis. The security assessments should be a review of the three major categories of a security program - personnel (i.e. people) security, physical security, and computer and communications security. That said, common sense, safety, legal and policy guidelines, and expense will clearly enter into what is done during a vulnerability assessment. Additionally, there will be some areas like personnel security screening that may be done on a longer term basis, and other areas like checking the local computer system which should be done on a more frequent basis. Therefore, you will need to tailor your vulnerability assessments to your local company and plant requirements. Finally, security and vulnerability assessments are another area where you need to **have written management approval to conduct the assessment and for the areas/actions to be assessed**. Let's take a look at each major area requiring security and vulnerability assessments.

3a. Personnel Security

People are the center of any company and business, and they can also be the weakest security link. This can be because they are poorly trained, or because they do not care or are "disgruntled" and may fall into the category of the insider threat. Any company hiring process needs to legally screen people (the job of the Human Services Dept, but with the assistance of functional area experts) for not only their ability to do the job, or be trained to do the job, but also their suitability as an employee in a critical infrastructure company. Are they reliable, dependable, and can they be expected to obey company policies, rules, and not present a threat to the company, the company's product or customers, and/or their fellow employees? As a minimum, there should be an initial screening of new/potential employees, and then a rescreening in the future on anywhere from a one to five year basis. Some of this rescreening should be tied into other normal screening actions such as annual job ratings, complaint actions, etc., where a track record of employee performance demonstrates the reliability or unreliability of an employee. Such a program must not be just negatively based, but must also provide incentives/rewards for positive work and contributions, and training to overcome security threats. As an example, a major

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	computer security threat is social engineering[32], where hackers can use various techniques to try and convince people to provide them information about the computer systems they have access to, to include their passwords. Initial and annual follow-up security training for employees should be provided to provide them an understanding of the company's security policy & procedures, threats the company faces, and serve as a deterrent against hacker social engineering techniques. Finally, develop and implement employee termination and transition programs that are as "human" as possible. Yes, this will cost money, but it is good PR, good security, and will help mitigate instances of the disgruntled employee who has information or knowledge to sell or to use against your critical systems.	
	-Implement Initial Personnel Security Screening	_____
	-Implement Follow-up Personnel Security Screening	_____
	-Implement Initial Personnel Security Training	_____
	-Implement Follow-up Personnel Security Training & Incentives Program	_____
	-Implement an Employee Transition Program	_____
3b. Physical Security	Physical security ensures the company's or plant's key physical items, to includes its people, production equipment, and computers are safe and secure. Many key systems such as a network server's security settings may be bypassed if an unauthorized user can gain direct access to the console or the system can be damaged/destroyed because the server and its information is physically damaged/destroyed. Therefore, it is extremely important to ensure key company or site production and information systems are kept in restricted access areas, and only those employees who need direct and unescorted access be allowed such access.	
	-Based on the assessment of company critical items cited in Checklist Item #1 above, implement physical segmentation and protection as required by the criticality of the function your company/plant performs and of the importance of item(s) being protected. Such protection may include employee badging system, locks and entry control systems, alarms, fences, and guards and gated areas.	_____
	-Develop contact points and procedures to request	_____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

assistance from local law enforcement and emergency services for major incidents and disasters.

- Conduct security exercises to check access controls into your company's secure areas on at least an annual basis. _____

3c. Computer & Communications Security

"The greatest threat in terms of financial loss is insiders. Period, no questions. That said, the greatest number of threats is via Internet attacks."[33] You will need to implement a computer & communication defense in depth security effort which will not only guard against the above cited traditional insider and hacker threats, but also the developing cyber-terrorism and information warfare threats very possible in the near future. The following seven step program is a good starting point:

1) **Do a vulnerability assessment of your current computer, communications, and control network.** _____

-Make sure you have the written permission of management. _____

-Use vulnerability scanners such as Nmap, Saint, Nessus, CIS-Cerberus, SARA, and/or ScanPort to get a baseline of your computer network and its vulnerabilities. Use programs like Phonesweep and ToneLoc to search for unauthozied modem connections within your Firewall - these are particularly dangerous as they give someone the capability to bypass your Firewall. The same basically holds for any wireless and/or remote interfaces that are not encrypted. _____

-Check what information is publically available on your company's web site--is it really necessary to be there--does it provide too much of an insight into your physical plant layout, your computers and communication systems, your utility control systems? Remove information that really shouldn't be out on the net. _____

-Assess the interfaces between your computer network, your SCADA control devices, and the ability of an outside and/or unauthorized personnel to interject into your infrastructure control systems. Key items to look for include the ability to open and close switches and circuit breakers, to transfer power from one power grid to another causing overloads and cascading effects, and to turn on or off key support systems such as

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

systems which directly support and provide required heating/cooling for the actual SCADA control systems or power generation equipment.

-Ensure the resulting vulnerability "findings" are documented & you generate a written report of required corrective actions. _____

2) **Check security sites** such as Carnegie Mellon University's Computer Emergency Response Team Web Page at www.cert.org for various security related bulletins, and www.sans.org for their and the FBIs's Top 20 list of Cyber Threats.[34] Additionally, **look at participating in one of the Information Sharing and Analysis Centers** established by PDD-63.[35] Eight centers were originally identified in PDD-63, but 11 ISACs have been established or planned for. Each ISAC is focused on a particular sector of our Critical Infrastructure and is established with a lead Federal Agency in partnership with a given infrastructure sector's industry coordinator. ISACs include: _____

-Banking & Finance: www.fsisac.com
-Electric Power: www.nerc.com
-Emergency Services (Fire & Rescue): www.usfa.fema.gov/nfa
-Emergency Services (Law Enforcement): www.nipc.gov
-Emergency Services (Public Health): TBD
-Information Technology: www.itaa.org
-Telecommunications: www.ncs.gov
-Oil and Gas: www.npc.org
-Transportation (Surface): www.aar.org
-Transportation (Aviation): TBD
-Water: www.amwa.net

By utilizing the above web sites and ISACs, one can keep up to date on hacking trends and threats, and are better prepared to meet current and new threats.

3) **Harden your operating system**, and if you don't have an OS that is "security friendly" then look at migrating to one that is more secure. For example Windows 98 is much less secure than Windows 2000. _____

-Disable default settings, ports, passwords. Remove programs that you don't need and which are set to default/insecure settings. _____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

-Enable event and security logging, and keep a second copy of logs separate from the log on the computer you are tracking - this can be a great help to you if someone is entering your network and then changing the logs to cover their tracks. _____

-Disable or really scrub the settings of programs such as ActiveX, X-Windows, and PC Anywhere[9, 36] that allow remote access or could allow entry of malicious code. Use SSH instead of ".rhosts" style authentication to improve the security of authentication. _____

-Enforce strong passwords--at least 8 characters long with mixed characters (A, a, 1, @), and change passwords on a frequency required by the criticality of the information or system they allow access to. _____

-Implement and maintain currency on OS and program updates and patches, but ensure you check-out/debug program updates and patches on an off-line system before you do so network wide to ensure all checks out OK. Restrict user, group, and file attributes and access along job and work centered lines, and to the minimum needed. _____

-**The objective is to build a secure configuration for your Network OS.**

4) **Implement a multi-layered defense of Firewall, Intrusion Detection, and/or Virus Scanning software and systems.** Defense in depth is the operative phrase here as no <u>one</u> firewall, IDS, and/or Virus Scanner can do the full job of computer/network security itself. _____

-**Firewalls** are clearly one of the major means of network and host protection today, and come in many hardware and software versions. All basically perform the same function of blocking access to a computer or network based on certain rules. Firewalls can block both inbound and outbound traffic based on the rules you set. Firewalls can be broken into two major categories: protocol-level firewalls and application-level firewalls.[37] Protocol level Firewalls are faster, typically "packet-filter", and are used in many firewall hardware implementations. Application-level Firewalls are more complex and thorough, but slower because they do check more items/actions, they filter on program action, and are available for servers and large systems/networks, but not for stand alone systems. Numerous Firewall products exist and some of the _____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

options that are available are: Lockdown, Firewall-1, Cisco's Pix, Raptor, Proxy, and ZoneAlarm. You should be able to find one that meets your systems and affordability requirements.

-Intrusion Detection Systems (IDS): Programs designed to take a snap-shot of a computer system and then track changes on the system and sound an alert when certain thresholds/actions take place. IDS systems work at two different levels -- host or individual systems, and networked systems. Some IDS programs to check out include TCP Wrappers, Psionic Port Sentry, Shadow, NetRanger, NFR, Snort, ISS RealSecure, Nuke Nabber, and Black ICE. Tripwire is also a useful file and registry checking program.

-Virus Checkers/Scanners: Programs which check for viruses and malicious code. Develop a virus defense policy with written procedures. Today some 50,000 viruses of various types exist and it's vital that your computer and/or network be protected by a virus checker/scanner. Scan any program and/or file before it's allowed to be added to your network if at all possible. Virus programs need to be kept current, to include the virus signature profile. Run a virus system wide scanning check from once a month to once a week depending on your operation and criticality of system, or as soon as possible if you suspect your network or a given computer may have a virus.

5) **Use Encryption and Virtual Private Networks (VPNs).** This will "harden and protect" those of your communications that must go over the Internet, or allow access from/to your systems and the Internet. All encryption basically falls into two categories: symmetric, based on a single key or code that both parties to a communication must possess; and, asymmetric which is based on a public and private key or code combination. Both systems work, but the private key or code system tends to be very support intensive as there has to be a reliable and secure system of getting the codes securely transferred from one user to another. The asymmetric system uses a much easier to support system of private/public keys. Look into programs such as Pretty Good Privacy (PGP) which allow important data on your computers to be encrypted, as this is a further obstacle and deterrent to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

hackers. For commercial applications and transactions, look at using SET - Secure Electronic Transaction, which is designed to provide a secure means of conducting commercial business and passing of credit card information in response to commercial activity. SSL - Secure Socket Layers and TLS - Transport Layer Security are basically programs designed to ensure the secure communications of critical information and data. Finally, VPNs are programs which enable users to establish secure communications between computers/networks through the use of "tunneling" protocols, by the use of encryption, and finally by not allowing any other than authorized users to access the network. VPNs provide a cost-effective alternative to dedicated communication lines like T1 lines.

6) **Implement incident handling plans and procedures**. A good starting point is the six step incident handling process listed in the Sans GSEC course:[38] _____

-**Preparation: Prepare for incident(s) before they happen.** Develop procedures based on your security policy. ID team members, train them, and practice response actions. Get management approval of the Incident Handling concept and procedures. Develop & establish contacts with security, law enforcement and emergency response agencies/personnel prior to incidents happening. _____

-**Identification: Teach people how to recognize incidents**, how to respond, who to contact, and what initial steps to take as an incident is identified. _____

-**Containment:** Ensure trained personnel/experts are involved early in the identification and containment phases. **Secure the area and systems which are contaminated**, make a backup of all infected computer systems for follow-on analysis and evidence purposes. Change passwords on all infected systems, and pull systems off-line as required. _____

-**Eradication: Determine the cause, clean, and fix system(s)** before putting system(s) back online. Improve & adjust your defenses, running a vulnerability assessment to help/assist with this upgrade/update of your defenses. _____

-**Recovery: Validate the system(s)** and if you must restore the system(s) make sure you do not use _____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	contaminated/bad code or data. **Monitor system(s) performance to ensure fix is good.** **-Lessons Learned**: Draft a report with lessons learned and send recommendations to management for approval, action, and implementation. Arrange & do follow-up meeting to **get lessons learned out & focus on process improvement rather than any blame.**	_____
	7) **Implement a system of program/data backup and recovery**. If disaster does happen, whether man made or from an accident or nature, it's essential you have a plan to reconstitute your network and systems. A data backup and restore plan is critical -- you should have methodical backup plan that provides for at least a daily, weekly, monthly and annual backup plan, with a copy of tapes kept on your site, and a second backup copy stores off-site in a safe/secure location. Additionally, the on-site tapes should also be stored in a locked cabinet with only the minimum of management, security, and network administrative personnel having access to the tapes. You can look at your backup tapes as your last line of defense.	_____
4. "The Unexpected"	The one thing you can say about security and "the real world" is that as much as you may see many of the same crimes and security incidents - human nature being what it is, you will also see "the unexpected" -- this can relate to new technology, new threats, or the never ending ability of human beings to improvise and do the unexpected. Ensure your security policy and program is flexible and forward looking enough to deal with these new threats and the unexpected ones.	_____

CONCLUSION/SUMMARY

The current world, national, business, and technology environments in which our national infrastructure and utility companies operate today demand implementation of an in-depth, comprehensive security program. However, each company's situation is different and will drive the exact program which should be implemented and what one can be reasonably expected or afforded to implement. The above security matrix can be used as a starting point by company management, security, and network teams to structure and tailor a security program which best suites their particular requirements. The rewards for implementing such a comprehensive, in-depth and structured security program is the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

protection of an infrastructure company's most critical resources and assets, and the ability to operate in what can be a fairly challenging, and at times hostile business and Internet climate. Failure to implement a comprehensive and in-depth security program to protect these critical infrastructure plants and facilities is surely a recipe for eventual disaster.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

1. “President’s Commission on Critical Infrastructure Protection,” http://www.ciao.gov/pccip/index.htm

2. “Federal Register, Part III, The President, Executive Order 13010--Critical Infrastructure Protection,” July 17, 1996, http://www.ciao.gov/PCCIP/eo13010.pdf

3. “Protecting America’s Critical Infrastructure” by Kimberly Perez-Lugones, September 6, 2000, SANS Paper, http://rr.sans.org/infowar/protecting.php

4. “Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack” by Jonathan Stidham, September 26, 2001, SANS Paper, http://rr.sans.org/hackers/lights.php

5. “Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure” by Shannon M. Lawson, February 19, 2002, SANS Paper, http://rr.sans.org/infowar/us_critical.php

6. “Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy” by Frances Wentworth, September 26, 2000, SANS Paper, http://rr.sans.org/infowar/CIP.php

7. “Information Security Issues for Industrial Control Systems” presentation by Joe Weiss, September 10, 2001, Presentation to ISA, Houston, TX, http://www.isd.mel.nist.gov/projects/processcontrol/documents/ISA/issues.PDF

8. “SAFEGUARDING IEDS, SUBSTATIONS, AND SCADA SYSTEMS AGAINST ELECTRONIC INTRUSIONS” by Paul Oman, Edmund O. Schweitzer, III, and Jeff Roberts, Schweitzer Engineering Laboratories, Inc. Pullman, WA, USA, http://www.selinc.com/techpprs/6118.pdf

9. “Common Vulnerabilities in Operational Networks” presentation by Dion Stempfley and Joe Pendry, riptech, http://www.energyitexpo.com/presentations/stempfley.pdf

10. “Understanding SCADA System Security Vulnerabilities” , by riptech, January 2001, @2001, Riptech, Inc., http://www.riptech.com/pdfs/Power_WhitePapter_SCADA.pdf

11. “CONCERNS ABOUT INTRUSIONS INTO REMOTELY ACCESSIBLE SUBSTATION CONTROLLERS AND SCADA SYSTEMS” by Paul Oman, Edmund O. Schweitzer, III, Deborah Fincke, @SEL 2000, http://www.selinc.com/techpprs/6111.pdf

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

12. “National Vulnerability Intensifies As Infrastructure Reliance Grows” by Col. Alan D. Campen, USAF (Ret.), July 1998, @SIGNAL Magazine 1998, http://www.us.net/signal/Archive/July98/national-july.html

13. “Utility Companies Face Barrage of Cyberattacks” by Dan Verton, January 21, 2002, COMPUTERWORLD, http://www.computerworld.com/itresources/rcstory/0,4167,STO67581_KEY73,00.html

14. Control Microsystems Web Page, Products Listing, http://www.scadapack.com/pages/products.html

15. Industrial Control Links Web Pape, Products Listing, http://www.iclinks.com/Products/products.html

16. “The Internet for Dummies” by John R. Levine, Carol Baroudi, and Margaret Levine Young, 7th Edition, IDG Books Worldwide, Inc., @2000

17. “Network+ Study Guide” by David Groth, 2nd Edition, SYBEX Inc., @2001 SYBEX Inc., pg 135-136.

18. “The World’s Online Populations” by CyberAtlas Staff, http://cyberatlas.internet.com/big_picture/geographics/print/0,,5911_151151,00.html

19. COMMISSION ORDERS SWEEPING CHANGES FOR ELECTRIC UTILITY INDUSTRY, REQUIRES WHOLESALE MARKET TO OPEN TO COMPETITION” Http://www.converger.com/fercnopr/888_889.htm

20. “Environmental and Social Impacts of FERC Orders 888 and 889,” Talk To Me: Robert G. Pattridge, 7-01-96, http://www.isc.rit.edu/~rgp5877/ferc.htm

21. “Energy, Nuclear Infrastructure Exposed” by Dan Verton, February 11, 2002, COMPUTERWORLD, http://www.computerworld.com/itresources/rcstory/0,4167,STO68183_KEY73,00.html

22. “Web sites seen as terrorist aids” by Dan Verton, February 11, 2002, COMPUTERWORLD, http://www.computerworld.com/cwi/stories/0,1199,NAV47-81_STO68181,00.html

23. “The Cybercrime Threat” by Lori A. Burkhart, December 2001, puc.com, http://www.pur.com/Cybercrime%20Threat.html

24. “New York pulls sensitive data from state’s Web sites” by Dan Verton, February 26, 2002, COMPUTERWORLD, http://www.computerworld.com/storyba/0,4125,NAV47_STO68628,00.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

25. "Forum: U.S. must also prepare for attacks over the Internet" by Patrick Thibodeau, September 21, 2001, COMPUTERWORLD, http://www.computerworld.com/itresources/rcstory/0,4167,STO64132_KEY73,00.html

26. "Al-Qaida Cyber Capability," Government of Canada, Office of Infrastructure Protection and Emergency Preparedness, THREAT ANALYSIS, Number: TAV01-001, 2 November 2001, http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html

27. "Report warns of al-Qaeda's potential cybercapabilities" by Dan Verton, January 04, 2002, COMPUTERWORLD, http://www.computerworld.com/storyba/0,4125,NAV47_STO67092,00.html

28. "Official: Terrorists used Internet to get info on potential targets" by Patrick Thibodeau, February 13, 2002, COMPUTERWORLD, http://www.computerworld.com/storyba/0,4125,NAV47_STO68281,00.html

29. "Energy IT Expo presentation" by Tim Belcher and Joe Pendry, riptech, 13-15 Jan 2002, Hyatt Regency, New Orleans, http://www.energyitexpo.com/presentations/belcher.pdf

30. "Former Microsoft Exec Begins Federal Critical Infrastructure Protection Job" by Dan Verton, January 28, 2002, COMPUTERWORLD, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO67754,00.html

31. "SANS Security Essentials GSEC Study Guide", Sections 2-2 and 2-2a.

32. "SANS Security Essentials GSEC Study Guide", Section 1-1, Slides 18-20.

33. "SANS Security Essentials GSEC Study Guide," Section 1-3, Slide 2.

34. "SANS Security Essentials GSEC Study Guide," Section 3-6, Slide 41.

35. "Information Sharing and Analysis Center, Water ISAC, Eight Critical Infrastructures," http://www.amwa.net/isac/eightsectors.html

36. "Information Security Needs for Electric Power Applications," Presentation by Joe Weiss, EPRI, at the Real-time and Embedded Systems Forum, Austin, Texas, 18th-19th July 2001, http://www.opengroup.org/rtforum/jul2001/minutes.html

37. "SANS Security Essentials GSEC Study Guide," Section 3-6, Slide 16.

38. "SANS Security Essentials GSEC Study Guide," Section 2-4, Slide 9.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: November 19th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS London November 2017	OnlineGB	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced