Global Information Assurance Certification Paper

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.

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 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.

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 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 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 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 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 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, Review & Understand Your Company Goals, Policies, and Overall Guidelines. What's your company or plant's bottom line and what should you protect?	Identify & appreciate essential company products, 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.	_____ _____ _____

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 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.

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

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

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.

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
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 Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
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
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
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
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
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive