Global Information Assurance Certification Paper

Defense in Depth for the Small Business - A Pragmatic Approach

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b - Option 1

Russell Morrison
June 23, 2004

Abstract

There are many papers that have been written on implementing and or improving small business security. Many of them are written with the assumption that the small business will be using a security consultant to implement the solution(s). Unfortunately, many small businesses do not have the time and or the funds to consult with security consultants or purchase hardened systems. Many of them will go to the local electronics vendor, purchase the system off the shelf, and put it to use. This paper considers this the rule rather than the exception. In following, this paper attempts to outline a series of a few simple common sense steps to achieve a more secure computing environment for the small business. The steps provided are broken down into time frames with immediate, short term, and medium to long term so the small business user is not overwhelmed with a whole pile of things to do immediately. Some additional research resources are provided at the end of the paper that should further help the small business if they have time to do some additional reading to better understand their risks.

Table of Contents

1 Introduction

The costs and complexity of computer hardware and software have significantly decreased in the last few years. When combined with the current ubiquity of the Internet, many small businesses have adopted computers, networks, and the Internet as strategic marketing and support tools. However, the over-simplification of the installation and configuration of current computer systems (through the use of default settings, configuration wizards, and graphical user interfaces) has left many of these systems "open" to (hidden and unknown) security risks. To date, many computer hardware and software vendors have not helped this situation as many ship their systems with many if not all default features/services enabled in order to make it easier for the end user to setup and operate their new system. This is compounded by the fact that as the software and hardware vendor change their new systems to be more secure, there are still many millions of systems running the old insecure configurations.

In addition, a great deal of information has been written about how businesses (and users) should securely configure their systems. In most cases, this information has been utilized by medium to large businesses to securely configure their computer systems as they have the financial resources and access to skilled staff to undertake this process. However, small businesses (and individual users) may have access to the same "security" information (from various sources) but for various reasons they don't utilize it. The reasons might include any of the following: limited understanding of the issues, limited financial resources, limited access to skilled personnel to properly configure their machines, trust in the vendor to properly configure the system for its intended use, and the use of default security settings right out of the box. As well, many small business systems are generally purchased as single systems (purchased as needed, not part of an annual budget) based on price and or features and are quickly deployed with the default settings. This has resulted in many small businesses having a variety of vintages of hardware and software in various states of configuration and security patching. These factors have (unknowingly) left many small businesses open to data theft/manipulation, and or malware.

There are a number of things that need to happen to make small businesses better understand these issues. Keeping in mind that the level of computer knowledge within many small businesses is generally very low, and the fact that many of them do not have established relationships with trained computer security individuals or companies, and many of them arrange and purchase their hardware as required and in many cases sourced from the local electronics store, the best approach may be to detail a number of very basic steps that all small businesses need to undertake to achieve a basic level of security. From that point, several more basic steps can be listed that can be undertaken over time to achieve an even higher level of security. At the end of this process, (the timeline of which is largely defined by each individual small business) the

business network is basically secured and moving towards a higher level with each new machine purchase.

The preferred security approach in any business is “defense in depth”. This is a phrase that has been used for many years in a variety of “security and risk” situations. This includes describing a defense strategy in military history (see an example here Link#1). It has also been used in “high risk industries” to describe failover precautions (e.g., nuclear power industry) (see an example here Link#2). It has also been discussed by many in the computer industry (see examples here Link#3 , Link#4 , Link#5 , Link#6), by several SANS students (see examples here Link#7 , Link#8 , Link#9 , Link#10) and has been defined by SANS as:

> **“Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.”**
>
> (See the SANS glossary here Link#11)

Defining “defense in depth” and establishing “layers of defense” in a small business can be a challenge as the “computer network” may consist of only one or a few systems (likely running different versions of potentially varied operating systems) and likely connected to the Internet on a high speed (i.e., broadband) connection. In addition, most small businesses are unaware of most security issues that may arise with their systems until something “bad” happens (and are prompted to bring in someone to clean it up) or they read about it in their local newspaper. So, any basic defenses put in place for a small business should be resilient enough to operate without constant administration or updating. It is important to note that the small business does not need to “see” or fully understand the concept of defense in depth but rather if they implement the various basic steps outlined later in this paper, they will have defense in depth.

Another preferred security approach is “default deny”. This means that all Internet traffic coming towards the small business network should be outright denied access unless specifically allowed. This is always the safest approach for all business firewalls. If some traffic is going to get past the firewall someone has to have intentionally configured the firewall or other routing device at the outer edge of the company network to specifically allow that new traffic to enter. This is a very safe default approach to take against new exploits on unknown ports. The steps outlined in this paper try to establish that default deny stance.

This paper tries to address the various security challenges faced by the small business by taking an extremely pragmatic approach (a definition for pragmatic has been provided here Link#12) to the above noted preferred security stance and in doing so suggests “target” settings and or configurations that would be most appropriate based on the systems and situations commonly expected in a small business. It should be noted that this paper does not demonstrate in detail the methods to configure all

possible desktops to achieve a specific “target” end result. There are too many variations with all the different operating systems, etc. currently in use by small businesses.

2 Basic Assumptions

Several assumptions have been made in developing the recommendations in this paper. The recommendations are aimed at the "small business" but can be utilized by businesses of all sizes (and also individual users). A small business for this discussion has been defined as a business with one or a small number of staff and limited assets and financial resources.

It is assumed for this discussion that the small business has data residing on their computer systems that is proprietary and they would like it to remain private. In following, it is also assumed that the small business does not knowingly "share" its computer systems with outside sources or parties (i.e., non-staff located outside the corporate network) and the computer systems are only for use by its staff or selected contractors. It is also assumed that the small business network does not have a file server and if there is more than one computer on the existing small business "network" that peer-to-peer file and or printer sharing is already in place.

It is assumed the small business has one or more "older" computers (i.e., more than 4 years old) (likely no longer supported by the hardware and or software vendor) along with maybe one or more "newer" computers (i.e., less than 4 years old). It is also assumed that the "older" systems are no longer eligible for any (or only for limited) bug fixes or security updates from the software vendor(s) (e.g., Microsoft Windows 95/98/ME, Mac OS versions prior to 9, Microsoft Office 97/98). It is assumed the small business has in place at least basic virus scanning software.

Since most small businesses do not have clearly defined policies on computer usage, it is assumed the small business systems will already have a variety of common "tools" and internet programs installed including email, instant messaging, streaming audio, and web browsers. It is also assumed that the small business has an "internet presence" meaning they have a web page and or email accounts that might be hosted on their own systems or on an external provider system.

For staffing, the small business does not have "IT staff" but may have one or more existing staff members who will "adjust" systems to make them work for the company needs. These individuals have full time roles elsewhere within the company and the "IT" role is a very part time low priority role as needed. This means the small business systems will not undergo any regular monitoring or updating and basically operate "as is" until something breaks, they are moved to a different role within the company, or the system is retired.

3 Recommendations

A series of recommendations are provided along with the suggested time frame for implementation. In subsequent sections, more details are given as to how each of these items should be implemented along with a very brief explanation as to why. It should be noted that given the rapidity that computer systems and software change and security exploits surface, the time frames have been made short to ensure that all basic security steps have been implemented within 6 months. In following, "long term" in this paper means longer than 6 months.

Steps	Immediate Recommendations	Implementation Time Frame
1	Reduce the number of "external" access points.	**Immediate**
2	Isolate the business network from outside access.	**Immediate**
3	No internal hosting of internet facing services.	**Immediate**
4	Install up to date versions of critical software.	**Immediate**
5	Establish basic computer usage rules.	**Immediate**
	Short Term and greater Recommendations	**Implementation Time Frame**
1	Establish external spam and virus filtering.	**Short Term**
2	Isolate the different systems on the internal network.	**Short Term**
3	Automate updating of critical software.	**Short Term**
4	Locate file and printer shares on newer machines.	**Short Term**
5	Establish authentication for accessing network data	**Short Term**
6	Implement some form of regular data backup.	**Short Term**
7	Phase out the older versions of software.	**Long Term**
8	Move to a fileserver based network.	**Long Term**

NOTE: Time frames provided are:
immediate=within 30 days
Short Term=within 90 days
Medium Term=within 180 days
Long Term=greater than 180 days.

4 Immediate Steps (Complete these 5 within 30 days)

These immediate steps will establish a basic level of computer and network security for the small business. The intent is close down (or very closely control) inbound traffic, barricade the company network from unwanted access, then try to establish some level of control over the internal traffic/activities. Subsequent sections of this document will provide follow-up steps that can be implemented as the small business moves forward in its more secure stance.

4.1 Secured Internet Presence and Usage

Steps	Recommendation
1 **CONTROL REMOTE ACCESS INTO THE COMPANY**	By reducing the number of external access points to one, it makes it easier to monitor and guard access to the business network and its data. This means removing or disabling all rogue access points into the network including modems (e.g., on a laptop or some desktops), wireless access (e.g., on a laptop), etc. while those machines operate in the office and having all outbound traffic traveling across one firewall ("gateway") onto one internet connection. This may also result in cost savings to the small business once unneeded dial-up connections, etc. are cancelled. As well, where feasible small businesses should stick to a wired network initially despite the apparent simplicity and convenience of wireless networking. There are currently too many ways to build an insecure wireless network. With a wired network, the small business has more physical control over what machines are connecting to its network and what traffic is coming into and going out of its network. If it is absolutely necessary for the small business staff to have remote access into the company network, the business should look into remote access tools hosted by others that are very well regarded for security (e.g., GoToMyPC) (Information is available here LINK#13). The small business should not be hosting remote access on their own systems (e.g., PCAnywhere) as there are too many security issues involved and it needs constant monitoring.
2 **NETWORK FIREWALL**	By confining the business network to wired only and isolating the network from outside access, this enables some level of traffic filtering and control. For a small business, there are two options. One approach is to have their internet provider establish a managed firewall or router downstream of their internet connection (this usually involves a monthly cost). Another low cost approach is a small-wired hardware "firewall" device that provides network address translation (NAT) and stateful packet inspection at the outside edge of the business network. Examples are the Linksys BEFSR41 or the SMC

Steps	Recommendation
	Barricade SMC7004VBR. Both are commonly available from many electronics vendors. Either type should drop all inbound traffic by default unless configured otherwise. This achieves the recommended default deny stance against inbound traffic. It should be noted that there are a large number of "hardware firewall" options with a wide range in pricing (including units from companies such as Nokia, Cisco, Symantec, etc.) but most are beyond the needs and the anticipated budget of most small businesses.
3 **NO INTERNAL HOSTING OF PUBLIC SERVICES**	The small business should not be hosting any sort of publicly accessible data on its systems or network. The small business should try to simplify their network model as much as possible to more clearly understand their security issues. The small business should outsource all "hosted" services they may use such as web pages, email, FTP, e-commerce, etc. to an "outside" hosting company. This is not to say the small business should not use these services or offer them to the internet public, but rather the small business should not run these services on their own network. The overall intent here is to limit the direction of traffic across the company firewall to outbound sessions only. This should be put into place at the same time that Item C above is implemented.

4.2 Clean up the Internal Network

Steps	Recommendation
4 **CRITICAL SOFTWARE**	Antivirus software on the desktop (and file server) is essential. This is the last line of defense against malware that has made it as far as the individual machine. This software should always be the most up to date version and the small business should always purchase a brand name product (e.g., Symantec, McAfee, Trend Micro, F-Secure, etc.) to ensure good product support during malware outbreaks.
5 **COMPUTER USAGE RULES**	The company should establish some basic computer usage rules as to what sort of materials/information should be opened or viewed on the business machines. Optimally, these rules should be written down. However, in the immediate term it might mean just sitting down with staff and explaining the intent. This should go a long way to reducing exposure to external malware. The company should make sure these "new" rules are followed by watching and openly discussing infractions with staff. This should be seen as educating the staff and not disciplining them since the business operated without any rules before so it may take a little time to sway them. The rules

Steps	Recommendation
	may be as simple as stating that “if anyone is unsure about a document or piece of data that arrives in an email, then ask the boss!” Once the rules are in place for a while and the staff begins to understand what are acceptable and unacceptable practices, they will require less input.

5 Short Term Steps (Complete these 6 within 90 days)

Steps	Recommendation
1 **EXTERNAL SPAM AND VIRUS FILTERING**	The small business should sign up with their internet provider or another external provider for spam and virus filtering on **all** inbound company email. Examples of external companies that specialize in filtering services include Postini (information available here LINK#14). Another alternative for unmanaged spam and virus filtering is a gateway appliance such as the ones supplied by BlueCat Networks (Information is here LINK#15) or Symantec (information is here LINK#16). However, the small business would be required to purchase the appliance, which may be a constraint.
2 **SYSTEM ISOLATION**	Isolating each of the systems on the internal network will help protect "clean" systems from "infected" systems should some malware become installed on one of the systems. The one limitation to this is peer-to-peer file sharing and how it is distributed around the internal network. Item I below discusses moving the file and print sharing to one or more "focus" machines. To help achieve this isolation, each system that is not hosting file or print sharing should have file and print sharing disabled in its network settings. In addition, a host-based firewall should be installed on each of these systems to limit unwanted inbound traffic. Good examples of small host based firewall products are Zone Alarm (information here LINK#17), BlackIce. (Information here LINK#18), Symantec (information here LINK#19), and McAfee (information here LINK#20). The Zone Alarm product is also available as a reduced feature free download, which will suit the financially stretched small businesses.
3 **AUTOMATE UPDATES**	Automate critical software updating for both antivirus and operating system updates where feasible to ensure that all critical bug fixes and security updates are downloaded and consistently installed. Automation can be avoided if the small business will manually update the critical pieces of software on a regular schedule. However, if there is any chance these updates will be delayed for any reason, the process should be automated.
4 **FOCUS ALL FILE AND PRINT**	The "newest" computer systems should become the only host(s) for the small business network file and printer sharing. This helps to protect and improve access to that data in a number of ways. The newest computer will generally be the fastest machine so file and print access times should improve. The newest computer will likely be running the newest version of the operating system and therefore, should still be able to access bug fixes and security patches which will help to protect this computer from malware that might target its file shares. The newest system is also most likely to

Steps	Recommendation
SHARING	have the largest and newest hard drive for storage and this newer drive is less likely to fail than the drives in the older systems. As a result of this move, all file and print sharing can be turned off or disabled on all other machines which helps to reduce the number of potential targets on the internal network.
5 **AUTHENTICATE USERS**	It is important to limit access to network accessible company resources. The file and print shares should be password locked where feasible. Optimally, the resources would require a valid username and password for access. This is quite easy to establish in common desktop machines such as MS Windows (information is provided here LINK#21). A basic policy or "rule" should be put in place to define "acceptable" passwords so that they are difficult enough so as to not be easily guessed. The passwords should be a mixture of characters, numbers, symbols, and should have mixed case and not be dictionary words (in any language).
6 **REGULAR BACKUPS**	It is essential for a small business to undertake backups of its computer data on a regular basis. If some catastrophic event should occur (e.g., fire), the small business needs to be able to recover from the event with its business plans and data still intact. This does not mean the small business needs to have tape drives, etc. as there are a number of backup options depending on the amount of data and the time to complete the task. Once the file and print sharing is focused on one or more newer computers, the company should insist that all company data be kept on those shares and not on local computer hard drives. This helps to centralize the backup needs to only a few target machines. A number of low cost options exist for backups including using a CD Writer, DVD writer, or a removable disk drive such as an Iomega JAZ. These formats will work well for total data amounts less than approximately 1-2 gigabytes. If the business has already exceeded that amount of data (or expects to exceed that amount within the short term to medium term), a small tape drive would be the easiest option. Again, a number of lower cost options exist from a variety of manufacturers. Low (or no cost) backup software to run the chosen device is provided with most operating systems in MS Windows (Information is provided here LINK#22).

6 Medium to Long Term Steps (Complete when feasible)

Steps	Recommendation
7 **PHASE OUT OLD SOFTWARE**	A small business will generally continue to use an asset until it dies or is no longer needed (i.e., the company has downsized or the system was replaced with a newer unit). Unfortunately, this means that very well built computer systems could last for many years (e.g., 7-10 years) operating very old (i.e., insecure) software versions. Short Term Step #2 (System Isolation) noted above will help to isolate these older machines from most issues but eventually the software just gets too old to support any version of the current security tools (e.g., host based firewalls). It is generally a good idea to define a system life cycle and clearly define how long a system will be considered useable before it is replaced. This helps to prepare the small business for future expenses (i.e., buying a replacement system in year 200X). A period of 5 years or less is a reasonable life cycle window for computer systems and supporting software. Most hardware support will last one year unless extended support is purchased which may extend the amount out to 3 or 4 years. Most software developers will commonly support software for up to 3 years, and then put it on extended support for maybe another year or two. In addition, most taxable depreciation on the system has completed within 5 years so the small business should consider new systems at that time if funding is available.
8 **FILESERVER SECURITY**	In the longer term, as the small business continues to operate (and the amount of company data continues to increase), the internal network infrastructure should be upgraded to accommodate a true file server. This step provides a more robust platform for file and printer sharing and in most cases allows for more fine-grained control over individual file security (information is provided here LINK#23 and here for Microsoft file servers LINK#24). The server platform could also be used for more rigorous network login authentication.

7 Follow-up and Additional Resources

Optimally, since a small business does not have the internal staff to undertake security issues on its own, it would contract out many of the network and or system revisions discussed above to a qualified computer security consultant. However, as was pointed out, many small businesses do not have the time (to either undertake the adjustments or locate a qualified consultant), the understanding for the need, and or the funding to pay for "secure" IT solutions. For convenience and simplicity (and maybe due to effective marketing), many small businesses resort to purchasing their "IT infrastructure" as needed from a local high volume electronics vendor. In addition, the new systems or components are quickly put to use before they have undergone any security hardening and before long they are (knowingly or unknowingly) infected with malware.

If the small business has the time and the funding (for professional services), it should seek out a qualified security consultant in their area and strike up a long term "as-needed" relationship just as they might with an accountant or lawyer. Obviously, they don't want to be convinced to purchase a bunch of inappropriate hardware or software (and this may be an ongoing fear by many small businesses when it comes to unknown subjects like computer security). So, the best source may be a referral from another small business that is pleased with a particular consultant's services. A more objective (though not necessarily complete) source would be an online website that lists security individuals or service organizations (information on the SecurityFocus services page is provided here LINK#25 as an example). Either way, the small business will need to take some time and discuss its needs with a few different consultants and determine what their solutions (and the anticipated costs) will be now and down the road.

Again if time allows, the small business should attempt to understand some of the security issues that may impact their computers and network. If they have some basic level of understanding, they should have a better chance at spotting "infected" machines and taking them offline before they impact other company resources. Below is a listing of online resources that will provide a variety of background information:

The SANS Institute website provides a variety of reference materials including research papers, links to other important security sites like the Internet Storm Centre, plus other computer security features. http://www.sans.org.

The Computer Emergency Response Team (CERT) Coordination Centre website hosted at Carnegie Mellon University Software Engineering Institute is a very good site for computer security information. http://www.cert.org/

The SecurityFocus website is also a very good source for security information on a variety of computer software and platforms: http://www.securityfocus.com/

The Microsoft Security website is a good source for Microsoft specific products:
http://www.microsoft.com/security/default.mspx

The Symantec website is a good source for Virus and malware information:
http://securityresponse.symantec.com/

The Apple website offers support for Apple products:
http://www.apple.com/support/

8 Summary and Conclusions

This document has provided a number of very practical common sense steps that all small businesses should implement in order to establish a basic level of security for their business computer systems. A number of basic assumptions went into developing these steps but the assumptions are very straightforward and should be applicable to a very large majority of small businesses. The overall intent is to help remove most small businesses from the malware and security incident "radar screen". If the small business is able to put in place all 13 steps, their network will have a very good basic level of security that will help to protect their company data and computer resources in the years to come.

9 References

9.1 URL Links provided throughout document:

Link#1
Military History Department, Stellenbosch University
Defense in Depth – Castle Fortifications
http://www.sun.ac.za/mil/mil_history/castles_defence.htm

Link#2
International Atomic Energy Agency
NUSafe Tutorials – Nuclear Installation Safety Net – Basic Safety Concepts
Defense in Depth Principle
http://www.iaea.org/ns/nusafe/tutorial/design/defdep.htm

Link#3
Weinberger, Joshua. "Five Steps to a Solid Security Foundation"
eweek Magazine, March 15, 2004
http://www.eweek.com/article2/0,1759,1549769,00.asp

Link#4
Muffett, Alec. IT Security: New Trends, Ancient Techniques
SUN Professional Services, 2004
http://www.clusit.it/infosecurity2004/muffett.pdf

Link#5
Adler, Steven. End to End Security
Microsoft Europe, April 2004
http://research.microsoft.com/collaboration/university/europe/events/AcademicDays/NE/0404 Oslo/Steven Adler - End To End Security(MSR Academic).ppt

Link#6
Symantec. Defense in Depth and Your Small Business
Symantec, 2004
http://www.symantec.com/smallbiz/library/depth.html

Link#7
Davoren, Sandra. GSEC Candidate
Security Considerations for Small Businesses to Achieve Defense in Depth.
SANS Institute, November 2003
http://www.giac.org/practical/GSEC/Sandra_Davoren_GSEC.pdf

Link#8
Harbour, Thomas. GSEC Candidate
Defense in Depth on the home front
SANS Institute, April 2003
http://www.giac.org/practical/GSEC/Thomas_Harbour_GSEC.pdf

Link#9
Taylor, David. GSEC Practical Version 1.3
Multi-Layered Approach to Small Office Networking
SANS Institute, 2002
http://www.sans.org/rr/papers/index.php?id=624

Link#10
Kadel, Lee.
Designing And Implementing An Effective Information Security Program: Protecting The Data Assets Of Individuals, Small And Large Businesses
SANS Institute, March 2004
http://www.sans.org/rr/papers/index.php?id=1398

Link#11
SANS Glossary of Terms Used in Security and Intrusion Detection
SANS Institute, 2004
http://www.sans.org/resources/glossary.php

Link#12
Roget's New Millennium™ Thesaurus, First Edition (v 1.0.5)
Copyright © 2004 by Lexico Publishing Group, LLC. All rights reserved
http://thesaurus.reference.com/search?q=pragmatic

LINK#13
GoToMyPC Remote Desktop
https://www.gotomypc.com/

LINK#14
POSTINI Spam and Virus Filtering Services
http://www.postini.com/

LINK#15
BlueCat Networks Meridius Spam and Virus Filtering Appliance
http://www.bluecatnetworks.com/products/meridius/index.html

LINK#16
Symantec Spam and Virus Filtering Appliance
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=142

LINK#17
Zone Alarm Pro Firewall Software
http://www.zonealarm.com

LINK#18
BlackICE Firewall Software
http://www.blackice.com (redirect to digitalriver online sales site)

LINK#19
Norton Internet Security Professional Software
http://www.symantec.com/smallbiz/nis_pr/

LINK#20
McAfee Internet Security Suite Software
http://us.mcafee.com/root/package.asp?pkgid=144&cid=10089

LINK#21
Microsoft. Set Up File Sharing
Microsoft Broadband Networking, 2004
http://www.microsoft.com/hardware/broadbandnetworking/10_concept_file_share_setup.mspx

LINK#22
Microsoft. Windows XP Back Up and Recover Your Information
Microsoft, 2004
http://www.microsoft.com/windowsxp/using/setup/getstarted/backup.mspx

LINK#23
Delaney, John R. & Lipschut, Robert P. "Servers"
PCMagazine, July 13, 2004
http://www.pcmag.com/article2/0,1759,1613592,00.asp

LINK#24
Microsoft. File server role: Configuring a file server
Microsoft Server Documentation, 2004
http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/file_server_role.asp

LINK#25
Security Focus Website Listing of Professional Service Individuals and Organizations
http://www.securityfocus.com/services

9.2 Other References Used

Association Vincotte Nuclear, Brussels. Nuclear Safety and Health Physics Defense in depth Concept
Association Vincotte Nuclear, no date
http://www.avn.be/uk/4_nucleaire/did_fr.asp

Bechtel, Ken. Anti-Virus Defense In Depth
SecurityFocus, April 2003
http://www.securityfocus.com/infocus/1687

Berry, Jonathon. Defense in depth: Preventing Going Hairless Over Wireless
SANS Institute, April 2002
http://www.sans.org/rr/papers/index.php?id=169

Computer Business Review. "Second skin"
ComputerWire, January 2004
http://www.cbronline.com/print_friendly/c7c5b5f1108fd6ef80256e680059b870

Davies, Jim. "Creating a culture of security"
Globe and Mail Newspaper, February 2003
http://www.theglobeandmail.com/servlet/story/RTGAM.20030224.gtkasten/BNPrint/Technology/

Ng Wei En. "Defence-in-depth: Companies need to look at various layers of security, be it in the physical environment or in operational processes"
Computerworld Singapore Newpaper - December 2001
http://www.computerworld.com.sg/pcwsg.nsf/0/1B6D3C6693D618BE48256B2F003A3397?OpenDocument

Northcutt, Stephen, et al. Inside Network Perimeter Security
New Riders Publishing, Indianapolis, Indiana. 2003 Pages 7-21, 231-280, 307-322

Rapoza, Jim. "Security Compliance is Good Business"
Eweek, April 26, 2004
http://www.eweek.com/article2/0,1759,1572292,00.asp

School of Computing, Information and Mathematical Sciences,

Edith Cowan University, Australia
Principles of Security and Risk Analysis
Edith Cowan University, 1997
http://www.soem.ecu.edu.au/units/scy1102/website/html/module_06.html

TechNet, TechNet's Corporate Information Security Evaluation for CEO's, "Preview Draft"
TechNet, December 2003
http://www.technet.org/resources/security_evaluation_new.pdf

Last Updated: May 27th, 2017

Upcoming Training

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