# Global Information Assurance Certification Paper

# Elements of a Remote Access Security Architecture

**By Joann Nieman**



**GSEC Practical Assignment**
**Version 1.4b Option 1**

Submitted: 28 Jan 04

***Abstract***

Globally the numbers of teleworkers increases dramatically each year. Along with that increase is an increase in requirements for remote access to the internal network and a proportionate increase in risk to the network. Risks include loss or theft of data, exposure to malicious content and hackers. These risks increase if personally owned systems access the network or broadband is used for access. Mitigation of these risks require strong authentication, encryption, a strong anti-virus and operating system patch management program, firewalls, virtual private networks (VPN) and in some cases policy enforcement software to build a remote access security architecture. As much as possible, prohibit personally owned systems. When unavoidable, processes and user training can reduce the risk of personally owned systems.

***Remote Access Requirements on the Rise***

Telecommuting, Telework, Road Warriors or whatever you call them they are beating on the Network Managers door. They want full access to the organization network resources and they want it now. Teleworkers range from the employee who works full-time from home to employees who work regularly scheduled days at home to the employee who requires remote access on an ad-hoc basis. In addition, let us not forget the employees whose jobs require extensive time on the road. Their very survival depends on reliable and fast network access.

Who wouldn't prefer to work from home? In many U.S. cities, workers spend hours each day commuting to the office. The commutes not only increase the commuter's personal costs (gas, car wear and tear and insurance) but also increase commuter stress. Arcati Limited estimates that nearly 30 million American workers (nearly 20% of the workforce) work from home at least one day of the week. Two-thirds of the Fortune 1000 companies have formal telecommuting programs. Of course, in today's global economy the U.S. is not alone in this phenomenon. In the United Kingdom, the Office of National statistics recently reported teleworking increased 70% from five years ago. Many other European nations report even higher proportions of teleworkers.[1]

Because of section 359 of Public Law Number 106-346 of October 23, 2000, the U.S. Federal Government is required to implement teleworking.[2] The law requires all Executive Agencies to establish policies under which employees may participate in telework to the maximum extent possible, without adversely effecting employee performance. Twenty-five percent of the eligible workforce was offered telework in FY01, with an increase of twenty-five percent each year thereafter. In other words, currently all eligible employees of the Federal

1 Lillycrop, p. 2
2 United States, p. 8

Government are offered telework. The Department of Defense (DoD) Telework Policy gives the following purposes for promoting telework:[3]

a. "promote DoD as an employer of choice;
b. improve the recruitment and retention of high-quality employees through enhancements to employees' quality of life;
c. enhance the Department's efforts to employ and accommodate people with disabilities, including employees who have temporary or continuing health problems, or who might otherwise have to retire on disability;
d. reduce traffic congestion and decrease energy consumption and pollution emissions;
e. reduce office space, parking facilities, and transportation costs, including costs associated with payment of the transit subsidy; and
f. complement Continuity of Operations Program (COOP) plans."

JD Edwards has one more good reason to encourage telework. They believe their teleworkers are 20 to 25% more productive than the employees in the office are. American Express teleworkers produce 43% more business. Add to that International Telecommunications Company BT's reduced property costs. BT has 7500 employees without a desk with an estimated savings of $290 million since 1992.[4] All told, both employers and employees have substantial reasons to telework. So, what does all this mean to the network manager?

### *Risks of Remote Access*

Network managers spent years perfecting their network security architecture. Firewalls, intrusion detection, anti-virus, operating system patches, and auditing practices are all well defined and operational. As a result, most organization networks are well protected from the wild, wild Internet. Remote access requirements add an entirely new dimension to security architecture. Now the well-defined organization network boundary has holes created by the need to give teleworkers access to the network from anywhere in the world. The network and organization information risk exposure from all angles.

To illustrate the magnitude of the problem, a computer system using a cable modem left on 24 hours a day for 10 days using a firewall set at the highest security setting. The log recorded 86 intrusion attempts. Even though most were judged to be false alarms, potentially serious attempts occurred at a rate of over three a day.[5] These probes were hacker's attempting to fingerprint the system to identify vulnerabilities they could later exploit.

**Authentication.** In most systems, internally or externally, the password is the chosen method of authentication and the first line of network defense. Weak

3 United States, p.1-2
4 Lillycrop p.2-3
5 Kuhn p.17

passwords, poor password protection, weak password-based authentication schemes and the prevalence of password cracking programs combine to make all passwords crackable. Some just take longer than others. Since most dial-up modems set behind the firewall, users have full access to the network once they authenticate to the server.[6] With a breached password system, the hacker can have full access to the network within minutes.

**Malicious Content.** "U.K.-based Sophos LPC said 70% of the 3,000 IT systems administrators it polled were updating remote office and telecommuter anti-virus signature files once a week or less. More than half of those people said they only update on a monthly basis. "[7] On the other hand, Sophos reports that 66% of office-based systems are updated daily.[8] Due to unpredictable network access and variable line speed, teleworkers are often left behind.[9] Large system patches and anti-virus updates can take hours to push over a dial-up connection. Thus system administrators often wait to push updates until the system is brought back into the office or the update is left to the user altogether. As a result, remote systems often are not current on patches and updates. And, what about home systems? Since many teleworkers use their personal computers, the organization patching process does not reach to their machines leaving those machines all that more vulnerable unless the teleworkers is conscientious about anti-virus and operating system updates.

**Confidentiality.** In the office, the risk of sensitive information being compromised is minimized just by the mere fact of being in the office. At the office, physical access is controlled with only personnel with the "need to know" typically in the area. Data on the hard drive may be stored in the clear with minimal risk of its compromise. Similarly, there is little risk of someone looking over your shoulder and seeing organization secrets. Remote systems have none of these protections. Plain text stored on the system can be compromised when the laptop is lost or stolen. For home teleworkers, family members have access to the data. This coupled with the increased risk of malicious infections puts organization data at even greater risk. The friendly fellow sitting next to remote users on the airplane or standing behind them at the airport also has access to organization sensitive information. In addition, some transmissions are in the clear exposing organizational data to the wilds of the Internet.

**Firewalls.** Firewalls are essential components of all computer networks. SANS goes so far to call them the "primary intrusion detection sensor on planet earth."[10] I cannot imagine a network with out a firewall. Not all firewalls are "locked down" but even the most liberal firewall policies provide a level of protection to the network. Both the CERT Coordination Center and the National Institute of Standards and Technology (NIST) recommend all home systems

---

6 Cole p. 400
7 Hurley
8 Hurley
9 Lillycrop p.3
10 Cole p. 673

have a firewall.[11] [12] However, in my experience the majority of remote systems do not. Few home users, including some Information Technology professionals this author knows, consider a firewall necessary until they purchase broadband. In 2000, only 15% of some 300-security professionals surveyed used firewalls to protect remote systems.[13] Some corporations do not field firewalls on remote devices due to the expense and difficulty in managing them. Although some good personal firewalls are free to home users there is a cost to businesses. In addition to the cost of the software itself, there is the cost of managing the software. As a result of these factors, many home and organization remote systems are unprotected. In addition, some architectures for remote access connect the remote user behind the firewall. In those instances, the remote user is left unprotected and the organization network is unprotected from the remote user. If the remote system is infected it can easily infect the organization network. This is especially true if the remote access server is behind the organizations firewall. Without firewalls on the remote systems, the system is wide open to attackers.

**Dial-up vs. Broadband.** Many people consider Broadband connections more dangerous than dial-up. In fact, both access modes experience the same threats. Whenever a computer is connected to the network, it is at risk. Period. The real difference is in the always-on feature of broadband. Dial-up users tend to spend less time connected to the network while broadband users may leave their systems on for 10-14 hours a day.[14] That difference makes it much easier for a hacker to penetrate an unprotected broadband system than a dial-up – he has much more time to find a vulnerability and exploit it. Consequently, the protection measures discussed in this paper apply to both dial-up and broadband systems. They are just more critical for broadband systems.

### *Remote Access Security Architecture*

All this leads to the conclusion that an organization needs a defined security architecture addressing the unique and not so unique risks of doing business remotely.

**Identify Critical Information.** The first step in developing a new security architecture is to identify the levels of information it must protect. All information is not created equal. Each organization has information that is critical to the future survivability of the organization. DoD classifies such information as Top Secret while corporations sometimes call it Trade Secrets. The compromise of this type of information can cost lives in the case of DoD or the loss of millions of dollars for a business. Other information, while important, is not as critical to the organization. Some information must be protected in accordance with legislation or other governmental regulation. Examples include Privacy Act data, banking,

11 United States, p.10
12 CERT Coordination Center
13 Radcliff
14 Kuhn p. 17

investment data, and Health Insurance Portability and Accountability Act (HIPAA) information. Still other information is sensitive and requires some level of protection but its release does little damage to the organization. Disaster Recovery and Business Continuity Step-by-Step lays out a model for classifying information.[15] Once the various classification levels are determined and information is labeled the organization must decide what information, if any, will be accessible to remote users. The security architecture can then be developed to protect all the information appropriately while minimizing costs. Somewhere in the middle of this process, the organization will most likely have to make a conscious trade-off between protection of the information, remote access and cost. Two words in the last sentence are important: conscious and organization. It is important that the organization (not IT) make a conscious decision to assume any risk not mitigated by the security architecture.

**Personal System Challenges.** Ideally, the organization prohibits personally owned systems from accessing the network. They are a red herring. Even the most secure systems introduce risk and complexity to the organizational network. The multitude of operating systems and personal applications increase the probability of interoperability issues with organizational applications. That combined with the high probability that the home user engages in risky network behavior is enough to give a security manager fits. Very often, other family members that share the system may regularly download applications and other content from Internet sites that would normally be prohibited or restricted on the organizational network. As a personally owned system, the organization cannot control their configuration or operating habits. For this reason, the DoD Telework policy requires the use of government furnished equipment for all regular and recurring telework requiring access to sensitive information (including Privacy Act). Employees working on an ad-hoc basis may use personal systems provided they delete and verify in writing all DoD from the hard drive. Personal systems are not authorized to access DoD systems or networks remotely.[16] Special provisions for personal systems are discussed below.

**Strong Authentication.** A number of problems are typically associated with passwords. Some common problems include: weak passwords (null, guessable or default); improper password storage by the application or user (write it down) and sniffable passwords where the applications sends passwords in the clear.[17] Even strong passwords are crackable.[18] Despite these problems, passwords are by far the most prevalent of authentication systems.

If passwords are used, the network manager must take steps to mitigate inherent risks. First, users must be educated on how to create strong passwords and proper control of their password. Deploy a password enforcement application, such as Password Policy Enforcer (PPE), which allows the

15 SANS Institute p.20
16 United States p.4
17 Mortenson
18 Cole p. 423

administrator to technically enforce the organization's password policy. Regularly run, with permission of course, password crackers against your system. The author's organization uses PPE as the standard and requires monthly use of a password cracker like L0phtCrack or Jack the Ripper. Users with poor passwords are locked out of their system until the password is changed. Disable services (Telnet, FTP, r-Commands) that transmit passwords in the clear.[19] Passwords are suitable on the internal network and may be sufficient for a remote user who requires minimal remote access. However, they fail to provide sufficient protection for critical data on the remote network.

Strong or two-factor authentication is preferable to passwords. Where passwords only require something you know, strong authentications requires something you know (password or PIN) and something you have (authenticator). Thus, it provides an additional layer of security. Strong authentications can take several forms. One-time passwords are perhaps the most common. One of the most popular implementations of one-time passwords is RSA Security's SecurID with over 10 million users.[20] SecurID users carry a hardware token (key fob, card on PINPad) or maintain a software token. A PIN is used in combination with a pseudo random value created by the device.[21] The result is a new password every 60 seconds.[22] With one-time passwords, weak passwords and other compromised passwords are no longer an issue. Applications using passwords transmitted in the clear should use one-time passwords.

Smart Cards and USB tokens are additional strong authentication techniques that are gaining popularity. Smart cards are one of the strongest forms of authentication but suffers from a labor and cost intensive implementation since all systems need card readers and all users need a smart card cut. USB tokens are similar to smart cards without the disadvantages. Since virtually all systems today have USB ports, hardware requirements are nonexistent. They are also more durable than smart cards.[23]

Biometric systems are gaining in popularity especially with the high-tech crowd but still not widely used. Although these systems are one-factor authentication (something you have), they are still strong because of the physical characteristic used. Common systems use fingerprints, retinal scans, voice recognition and facial characteristics.[24] These systems tend to be more expensive than other options and can be slow which complicates user acceptance.

**Anti-virus and Patch Management.** Perhaps the most important factor effecting network security is anti-virus and patch management. Since most malicious content and known hacker techniques exploit known vulnerabilities, properly patched systems prevent virtually all intrusions. Thus, it becomes

19 Cole p. 1479
20 RSA
21 Mortenson
22 RSA
23 Kawumura p.5
24 Mortenson

critical to keep remote systems patched at the same level (or better) than those on the office network. Network managers must develop and implement a process to ensure timely patches occur.

Duplicating the process on the internal network is one possible option. Chances are patches are automatically pushed and installed upon log-in. Remote users could easily use the same system. With this method, the network manager can keep all systems equally secure. Patches can be tested prior to implementation ensuring interoperability with organization applications. On the downside, the size of many patches and anti-virus updates will cripple bandwidth challenged users. Many users will terminate the connection before the patch is installed thinking the system has locked up or unable to wait any longer. Keeping pushes as small as possible (don't bundle multiple patches together) will help. If most organizational users access the network via broadband, this approach may be tolerable.

Another possibility would require the user to keep the system patched. Train users to check vendor web sites regularly for updates and download the latest updates. Of course, bandwidth challenged users may also find this approach unacceptable. Additionally, some updates may adversely affect applications running on the remote system and users may be unable to resolve the conflict on their own. An obvious shortcoming of this approach is the requirement to trust the user to stay on top of things.

Administrators could require the remote system to return to the office regularly for updates. This approach is painful for the user but doable if the remote system is a laptop or other mobile device and the user is home based in the area. This system is particularly effective for remote systems that are also the users' primary system while in the office since these systems automatically update when they log onto the network. Other users must make a trip to the help desk for their updates. A variation of this approach would have the network manager provide each user a disk with the latest updates on it. With the disk and specific instructions, the user could update the system at a remote location. Naturally, this system would be difficult to manage in an organization with a large number of users.

Sophos offers a technical solution for remote user anti-virus updates. Their Remote Update Tool extends the functionality of the Sophos Enterprise Manager for Sophos anti-virus software and virus identity files. Users still have to dial into a server (manually or automatically) for their updates. However, the big difference is in the size of the downloaded files. Virus identity update files are typically 1 or 2KB and even the monthly update is usually below 200KB.[25] At that size, even bandwidth challenged users can keep their anti-virus current.

Users using their personally owned systems to access the organization network require a different approach. The organization must make it easy for the home user to stay current. One approach used by DoD is an Enterprise-wide

[25] Lillycrop p. 6-7

anti-virus license. The license authorizes DoD employees to load the software on their home systems and includes updates. This coupled with initial and recurring training and awareness raises the level of security of these systems. Training should also include the use of Windows Update. Detailed procedures will ensure the user can duplicate the process at home. Encourage the user to make regular calendar appointments for any manual updates required. The network could also periodically send out emails reminding users to complete the necessary updates especially during virus outbreaks. These systems still might not be as secure/current as the organizational network but they are closer.

One final comment on anti-virus and software patch management, this author believes that once the organizational remote update policy is in place it must be enforced. If the network detects a system is not current, refuse user access. The danger to the overall organization network is too great to allow one unprotected user access. Recommend the network check for current patches and software updates each time the user logs on. If the system is slightly outdated, notify the user to remind him of the proper procedures and the consequences of inaction. If the system is too far out of date, deny access. How far is too far will depend on the individual organization and the criticality of their systems.

**Confidentiality.** Loss of confidentiality can occur from two vectors with remote users. First, large amounts of data are stored on the hard drive of the remote system. If this system is lost or stolen, all that data is compromised. A password protected system can slow them down but can easily be bypassed. Encryption can protect the sensitive data on the hard drive. If only some of the data is sensitive, file encryption can be used to protect the system. Windows 2000 and Windows XP both use a routine called Encrypted File System (EFS) to encrypt files. They enable the user to create an encrypted folder(s). This would allow the user to store files in this folder without individually encrypting each file. EFS is perhaps the simplest method to encrypting files. If the data requires a higher degree of protection, Pretty Good Privacy (PGP) or Information Security Corporations SecretAgent are good choices. PGP is not as simple as EFS but provides greater protection while still being somewhat user friendly. Although a little expensive SecretAgent is FIPS 140-1 compliant making it an excellent choice for more sensitive data and governmental applications (http://www.infoseccorp.com/products/secretagent/contents.htm).

If the requirement is to encrypt the entire hard drive an application such as SecureStar's DriveCrypt (http://www.securstar.com/products_drivecrypt.php)[26] or PC Guardian's Encryption Plus Hard Disk [27] (http://www.pcguardiantechnologies.com/Encryption_Plus_Hard_Disk/index.html) offer a high degree of protection. Both use the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES). DriveCrypt can

[26] DriveCrypt 4.0
[27] Encryption for Your Companies Valuable Data

also use Blowfish and Triple DES among others. PC Guardian has a package that has met Common Criteria at Evaluation Assurance Level 1.

To secure the data during transmission a Virtual Private Network (VPN) is most commonly used. VPNs are a common alternative to an organization creating its own private network using dedicated leased lines – typically too expensive and only provides security between fixed sites. A VPN uses encryption to protect traffic on the Internet. VPNs can provide (depending on the individual application) connectionless integrity, data origin authentication, confidentiality, traffic analysis protection and access protection. Some implementations will require software on the client others like Secure Socket Layter (SSL) do not. For a complete discussion on VPNs, consult Chapter 7 of NIST Special Publication 800-46.[28]

Here again personal systems complicate efforts to maintain a secure system. Typically, an organization would not load VPN client software or any other application for that matter on a personal PC. If personal systems are used the organization may have to use a SSL based VPN.

**Firewalls.** As discussed earlier, firewalls are an essential component of any security architecture. The trick for a Network Manager is to field and maintain them. Ideally, personal PCs are not allowed access to the network and all systems that do connect to the network include a centrally managed firewall. These are typically software-based systems deployed at endpoints throughout the enterprise – not just for remote users. With this mode of operation, the security manager maintains a consistent set of security policies across the network. The organization maintains complete control over the Ports and Protocols allowed on their network. Cisco Security Agent, Sygate Centrally Managed Personal Firewall and Zone Labs Integrity are just a few examples of centrally managed firewalls. An obvious downside to this approach is the cost of maintaining hundreds or thousands of firewalls. Yes, many even most of the settings are standard. However, if in a large organization, even 10% of these firewalls require deviations from the standard they become expensive to maintain. The question the organization must answer is it more expensive not to control your security policy.

An alternative to centrally managed firewalls is stand-alone firewalls. In this case, a separate firewall is installed on each remote system. These "personal" firewalls filter packets going to and from the system. Jeff Sengstack provides this definition of personal firewalls in his article "Make Your PC Hacker Proof". "The perfect personal firewall would be inexpensive and easy to install and use, would offer clearly explained configuration options, would hide all ports to make your PC invisible to scans, would protect your system from all attacks, would track all potential and actual threats, would immediately alert you to serious attacks, and would ensure nothing unauthorized entered or left your PC."[29] There are a number of good firewalls out there. Many are free to the personal

[28] United States p. 58
[29] Sengstack p.4

user. The NIST Publication Security for Telecommuting and Broadband Communications contains an excellent discussion on the various features to look for in a firewall.[30] It in combination with the reviews from the Home PC Firewall Guide[31] and other Internet reviews will enable the user or organizational manager to select an appropriate firewall.

These stand-alone firewalls offer multiple challenges to the security manager. First, they must be installed and configured on the numerous remote systems. This task alone is a nightmare unless the firewall is easily pushed to remote desktops. Once installation is complete the security manager loses all control. Since the firewall is controlled at the desktop and most remote users have administrator rights on their machines, the user now has full control of the system. The user can turn off the firewall or open up Ports if he perceives it is preventing him from downloading the new application he wants. Here again user education is essential. If stand-alone firewalls are part of the security architecture, it is critical to have a trained user. They must understand the purpose of the firewall and the risks they take (and pass on to the organization) any time they adjust the firewall settings. Organizational policy should include provisions for disciplinary actions if the firewall is tampered with. If any actions are required of the user, they must be provided detailed procedures.

If any users are allowed to user their personal systems, the organization should strongly encourage the use of a personal firewall. These users also need training to raise their awareness on the threats and vulnerabilities their home systems are exposed to and how to mitigate that risk. By raising their awareness level, the organization will be encouraging them to take the necessary actions that will protect their personal system and the organization. Perhaps the training could go so far as to be personal firewall specific to help the user learn to manage a specific firewall system. DoD has purchased an enterprise license for personal firewalls that covers employee home systems. This is one additional way to encourage their use.

**Policy Enforcers.** Throughout this discussion, a recurring theme occurs. How to enforce the security policies of the organization? Managed solutions enable the organization to outsource endpoint security. They typically combine a VPN and firewall with enforced security. During the log-on process the system checks to see if the latest software and policy code is on the machine, if it is not the updates are loaded. Only then is the machine connected to the organizations network. AT&T and IPass offer managed solutions. Offerings such as these provide reliable and scaleable security but may not be cost effective for small organizations. They also require the organization to give network access to an outside organization.

The alternative is to manage the system in-house. Cisco Security Agent provides a multitude of services to include: distributed firewalls, intrusion prevention, malicious mobile code protection and operating system integrity

[30] United States p. 21
[31] Personal Firewall Reviews

assurance. The interesting aspect of this product is its claim to base decisions on behaviors versus signature matching. In this way, it purports to protect against Zero Day attacks.[32] Zone Labs Integrity combines their firewall technology with central management to provide "transparent" policy enforcement.[33] What these and other systems all have in common is the ability to detect systems who don't meet policy and quarantine them from the network until the policy issue has been resolved (latest anti-virus update loaded). InfoExpress CyberGatekeeper only enforces policy. It gives the manager the additional flexibility to select a firewall and VPN product. It also has the capability to set different policies for different situations. For instance, someone coming in from a trusted network would not require a firewall policy. [34]

What all these products have in common is the requirement to control the end device, which as we have discussed earlier may not be feasible. However, if all the systems are organizationally owned and the bandwidth is available this is an excellent way to take back control of your network and still meet user needs.

**Multiple Architectures.** This practical has discussed a number of issues to take into consideration when building a secure telecommuting architecture. Because of the work done to identify critical information, the organization now has a good idea what the critical information is and where it resides. From there determinations can be made on designing a security architecture. In reality, there most likely will not be one architecture but many. For some less sensitive data, SSL may provide sufficient protection and access. Some email and database applications may fall into this category. For an extra layer of protection, strong authentication could be used. If the data is a little more sensitive, but the job still requires remote access, then a stronger architecture must be put into place. Here access to the internal network will be granted at least partially. The connection will be protected by VPN, firewall and strong authentication. Some file or hard drive encryption should be considered. Access to the organization's most sensitive data needs the highest level of protection. At this level, telework must only occur on organization systems. The data should be protected with a strong encryption algorithm while stored on the system. A VPN-firewall combination will protect the system while on the network with strong authentication ensuring identities are not stolen or spoofed. If possible, an endpoint security system should be used. In all cases, a organization owned system should be used. At no time should organization data be stored on a personal system. In all cases, the systems must be current on anti-virus and operating system patches.

***Summary.***

Access to the internal network from outside the network boundary must be avoided as much as possible. These connections always weaken the security

[32] Cisco
[33] Enterprise Solutions
[34] DeMaria

posture of the network. Loss of confidentiality becomes a very real concern. The remote system is exposed to enumerable probes and malicious content. Of course, telework is here to stay which means remote access is here and will continue to grow. Large numbers of teleworkers combined with the threats on the Internet exposes the remote systems and the internal network to increased risk - most likely unacceptable risk. The only way to maintain the level of security on the internal network is to significantly step up protection measures on the remote access network. Patch management, strong authentication, firewalls, file/disk encryption and policy enforcement software all play a vital role in the new security architecture. Finally, the organization must come to terms with personally owned systems. If their use on the internal network can not be avoided then strong processes must be implemented to mitigate the risks they bring.

## References


CERT Coordination Center. "Home Network Security". Carnegie Melon Software Engineering Institute. http://www.cert.org/tech_tips/home_networks.html#IV-A-3 (24 Jan 04)

"Cisco Security Agent". Cisco Systems. http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html (27 Jan 04)

Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS security Essentials with CISSP CBK Version 2.1. Vols 1 and 2. SANS Press. 2003

DeMaria, Michael J. "InfoExpress CyberGatekeeper Ensures Remote Users Comply With Security Policies". May 13, 2002. NetworkComputing. http://www.networkcomputing.com/1310/1310sp3.html (22 Jan 04)

"DriveCrypt 4.0 – 1344Bit Hard Disk Encryption". SecureStar. http://www.securstar.com/products_drivecrypt.php (27 Jan 04)

"Encryption for Your Company's Valuable Data". PC Guardian. http://www.pcguardian.com/computer_security/g_ephd.html (27 Jan 04)

"Enterprise Solutions". Zone Labs. http://www.zonelabs.com/store/content/company/corpsales/endpointSecurity.jsp (27 Jan 04)

Hurley, Edward. "Survey Remote offices, workers get short end of security stick". 2 May 2003 SearchSecurity.com. http://searchsecurity.techtarget.com/originalContent/0%2C289142%2Csid14_gci897087%2C00.html (23 Jan 04)

Kawumura, Cynthia. "Remote access for Healthcare – HIPAA and Beyond." Rainbow Technologies. http://www.rainbow.com/insights/white.asp

Kuhn, Richard D., Miles C. Tracy, Sheila E. Frankel. Security for Telecommuting & Broadband Communications. National Institute of Standards & Technology. Special Publication 800-46. August 2002. http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf (23 Jan 04)

Lillycrop, Mark. "Remote User Security: Your IT's Archilles Heel?." Arcati Research Bulletin. August 1, 2003. http://www.sophos.com/wp/?wp=wp14&l=bp3 or http://www.bitpipe.com/detail/RES/1061479889_313.html (24 Jan 04)

Maslowski-Yerges, Al. "Securing the Enterprise from the dangers of remote access: Analysis of new options available for Personal Firewall management in comparison with other established and emerging remote access solutions".

GSEC Practical. 2002. http://www.sans.org/rr/papers/index.php?id=316 (27 Jan 04)

Mortenson, Jason. "Password Protection Is This the Best We Can Do?" GSEC Practical. August 2001. < http://www.sans.org/rr/papers/index.php?id=114>

"Personal Firewall Reviews". January 24, 2004. Home PC Firewall Guide. < http://www.firewallguide.com/software.htm> (26 Jan 04)

Radcliff, Deborah. "Feature: Firewalls Reach Out". NetworkWorldFusion. March 26, 2001. < http://www.nwfusion.com/net.worker/news/2001/0326firewalls.html>

"RSA SecurID: Tokens." RSA Security. http://www.rsasecurity.com/products/securid/tokens.html (24 Jan 04)

SANS Institute. Disaster Recovery and Business Continuity Step-by-Step Version 2.0. Ed. Mark T. Edmead. SANS Press, 2002

Sengstack, Jeff. "Make Your PC Hacker-Proof". September 2000. PC World. http://www.pcworld.com/howto/article/0,aid,17759,pg,1,00.asp (26 Jan 04)

United States. Department of Defense. DoD Telework Policy. http://www.cpms.osd.mil/fas/benefits/pdf/telework/telework_policy.pdf

Last Updated: October 19th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS vLive - SEC401: Security Essentials Bootcamp Style | SEC401 - 201710, | Oct 23, 2017 - Nov 29, 2017 | vLive |
| San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | vLive |
| SANS Seattle 2017 | Seattle, WA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS San Diego 2017 | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Gulf Region 2017 | Dubai, United Arab Emirates | Nov 04, 2017 - Nov 16, 2017 | Live Event |
| Community SANS Colorado Springs SEC401~ | Colorado Springs, CO | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| SANS Miami 2017 | Miami, FL | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| Community SANS Vancouver SEC401^ | Vancouver, BC | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| SANS Sydney 2017 | Sydney, Australia | Nov 13, 2017 - Nov 25, 2017 | Live Event |
| SANS Paris November 2017 | Paris, France | Nov 13, 2017 - Nov 18, 2017 | Live Event |
| Community SANS St. Louis SEC401 | St Louis, MO | Nov 27, 2017 - Dec 02, 2017 | Community SANS |
| 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 San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| SANS Khobar 2017 | Khobar, Saudi Arabia | Dec 02, 2017 - Dec 07, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Dec 04, 2017 - Dec 09, 2017 | Community SANS |
| 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 |
| SANS vLive - SEC401: Security Essentials Bootcamp Style | SEC401 - 201712, | Dec 11, 2017 - Jan 24, 2018 | vLive |
| SANS Bangalore 2017 | Bangalore, India | Dec 11, 2017 - Dec 16, 2017 | Live Event |
| 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 |
| Community SANS Hawaii SEC401 | Honolulu, HI | Jan 08, 2018 - Jan 13, 2018 | Community SANS |
| SANS Security East 2018 | New Orleans, LA | Jan 08, 2018 - Jan 13, 2018 | Live Event |
| 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 |
| Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style | Las Vegas, NV | Jan 28, 2018 - Feb 02, 2018 | vLive |
| SANS Las Vegas 2018 | Las Vegas, NV | Jan 28, 2018 - Feb 02, 2018 | Live Event |