GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Training Users in Security Awareness

David Rosenthal
SANS GSEC Practical Assignment version 1.4b
Option 1 – Research on Topics in Information Security
July 31, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Training Users in Security Awareness

ABSTRACT

This paper is about how to create an Information Security User Awareness Training Program. It is important to train users to understand information security and to follow security policies that are in place to protect data from theft, loss, or damage. Teaching users about security creates another level of defense for an organization. The following pages detail the steps for developing and producing a training program to prepare users to be part of an overall information security system.

The first steps of creating this program include establishing the need for training, getting sponsorship and resources to support the development of the program, identifying the audience, choosing the presentation medium, and determining the sources of content.

The next steps include creating the content. The content includes basic security principles, your company's security plan, and practical tips for users to remember and apply to their daily jobs, and examples that illustrate how security awareness is used to protect companies from data loss or theft.

The final steps of creating a user awareness program include producing the program using the available resources to plug the content into the chosen medium.

Following these steps to create an Information Security User Awareness Training Program will enhance the security of an organization by helping users understand its security policies, preparing users to make the right decisions about security, and empowering them to protect their organization by using security principles. If an organization trains its personnel to be aware of information security, these users become part of the organization's security system.

© SANS Institute 2003, Author retains full rights.

INTRODUCTION

This may come as a surprise, but according to Sharon Gaudin in her article, "Social Engineering: The Human Side of Hacking," not all hackers use their computer skills or malicious programming to hack their way into corporate systems to steal hostnames, logins, passwords or sensitive information.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

"Sometimes all they have to do is call up and ask."[1] The article discusses how intruders gain access to internal resources either passively by overhearing business discussions at public places or digging through trash cans for confidential documents; or interactively by calling a company using name, title, and phone number information commonly available on company websites, or by dressing up as a maintenance or delivery worker pretending to have legitimate need for access. It is much easier to gain access through people than it is to hack through systems and devices. Training people to recognize threats makes an organization more secure.

No matter how much you spend to secure your company's data, security comes down to human awareness and preparing employees to make informed decisions. In the above discussion on social engineering, a hacker expects his target to be helpful and give up a password after some convincing role-play. Social engineering hacking is a prominent topic when discussing security awareness because it is uniquely dependent on human interaction, but it is not the only vulnerability that users have under their control. Your presentation must include other vulnerabilities within your organization. With guidelines and guidance, you can prepare your users to keep your information secure from social engineering and other threats. Your guideline is the corporate security policy. All organizations should have a security policy that documents how to protect the business by keeping information confidential and private while maintaining availability and integrity. You'll provide the guidance by teaching employees the features of the security policy and how to apply its rules. This gives employees the tools they need to make the right decisions in support of information security.

THE NEED FOR USER AWARENESS TRAINING

You have corporate security policies. Your network is protected with redundant firewalls, circuits, and infrastructure, you backup your data regularly and store your media offsite, and you have precise access controls. What do all of these systems and devices have in common? People need passwords to access them. The password and the person holding that password then become part of your security system. In a recent study, 90% of office workers were fooled into giving their passwords to strangers in a train station.[2] Equipped with these passwords, any intruder can blow right past login prompts to access sensitive data. Do your employees know how to follow your security policy, identify risks, and keep your information secure? You should take the opportunity to provide training to help employees do their part in security. In March of 2000, the FBI's director of Cybercrime reported before the Senate Subcommittee for the Technology, Terrorism, and Government Information:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

> It is important to remember that often "cyber crimes" are facilitated by old fashioned guile, such as calling employees and tricking them into giving up passwords. Good cyber security practices must therefore address personnel security and "social engineering" in addition to instituting electronic security measures.[3]

The FBI points out that breaching security can be as simple as asking for a password, so it is important that your employees recognize this as a threat, and know what to do. Providing security awareness training enables your employees to become another line of defense in your security plan, so that they don't simply give out passwords to whoever asks for them.

Users have control over many common vulnerabilities besides password handling. Providing security awareness training can prepare them to recognize these potential problems. These problems include physical vulnerabilities, such as allowing unauthorized people to enter restricted areas where they could possibly damage or steal equipment or documents, or view sensitive information on screens, on printouts, or in trash cans. These include natural vulnerabilities, such as knowing what to do in the event of a natural disaster or destruction of facilities. There are also hardware and software vulnerabilities, like installing unauthorized software, allowing malicious code from emails or web pages to enter the organization, configuring, installing, or turning equipment on or off inappropriately.

In a recent survey of IT professionals, CompTIA determined that, "Where agencies and companies have looked primarily to technology for network safety, in over 63 percent of identified security breaches, human error looks to be a major, underlying factor."[4] This highlights the need to adequately train users in security principles, as well as how to manage their equipment safely. With the amount of control users have over the safety of their organizations' information, it is very important that they understand how to make the right decisions to keep the information secure.

GETTING STARTED

Teaching security awareness is a major undertaking. Before you start this project, you'll need to get sponsorship to help you with the resources you need. Unless you plan to complete the project on your own time, with your own equipment, you'll need a sponsor to help you obtain resources. A sponsor can be a business manager, a technology manager, or a corporate executive, depending on the organizational structure of your company and its level of commitment to information security. The sponsor can also ensure that your

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

finished project is actually put to use if security awareness and certification are not yet a corporate or audit requirement. In order to obtain sponsorship, first agree upon the general goals for the training, then define the scope and resource requirements of your project, and determine its timelines.
Information Security Awareness Training can address many different organizational needs. You will have to determine the overall goals for your security training before you can do anything else. Security training will help employees appreciate the value of the information that they can access as well as the systems and facilities that they use to perform their job. With training, your employees can recognize risks to data, systems and property, and be prepared to prevent or report incidents. The training can provide familiarity with the security policy and give employees the tools that they need to apply the documented practices to their own tasks. After receiving this training, the employees will be more informed about security principles and the reasons behind security policies, thereby reducing false alerts and preventing some calls to the helpdesk. The goals of the training should be based on the role the employee is expected to have in the organization's overall security program. Discuss these expectations with the project's sponsor and decide upon the organizational needs you will fulfill by providing this training.

Once you have agreed upon the goals, begin planning the actual project. Create a project scope with the help of your sponsor. This will include items such as:

- Identifying the audience
- Estimating the required size and length of the finished presentation
- Deciding on the media and format of your presentation
- Choosing what topics will be covered and how much detail will be presented
- Mandating whether employees are required to complete the training program and whether it will include testing
- Determining whether periodic re-certification is necessary

It is important to establish the scope so that you know how much time and effort you'll need to put into completing the project, and so that you'll have a means to determine if your program meets your sponsor's requirements.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

You will need resources to complete your project. Resources include items such as:

- Company equipment including telephones, computers, printers and copiers
- Media and materials
- Information security specialists
- Application developers
- Graphic artists
- Programmers
- Outside vendors

External consultants and vendor services can be used for developing content, producing the finished presentation, or both. Don't forget to include your own time as well, because developing this training program will require time that you would be spending on other projects. All of these resources cost money, so you'll have to be very clear about budget constraints when setting your scope.

Identifying the audience is the most important part of creating a security awareness presentation. Your audience can be newly-hired employees, contractors or vendors, or it can be part of a cross-training program to prepare employees for new responsibilities, or it can be a part of an annual security review process. If you have enough time and resources, you can customize content for several different audiences based on their level of access. Depending on your organization, technicians, technical support personnel, systems administrators, business managers, and production staff may need to see different presentations based on their job responsibilities. It is important that the information presented is consistent, but employees with different roles have different privilege levels and see different risks. Be especially mindful of employees who are on the perimeter of your organization, such as telephone operators, security guards, administrative assistants, and front desk attendants; they monitor and control physical access to your facilities or answer telephone calls from the outside, so they are most likely to be exposed to social engineering intrusion attempts. If you need to address these specialized needs, you could create a core presentation to cover general security principles and your security policies, then individual modules that are developed for the specific audiences. You and your sponsor will need to agree on the types of audiences, whether you need multiple presentations and how you will tailor your presentations to suit their needs.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Once you have decided on your audience, you will need to determine how to present your material. Whatever media you select, it is most important to keep your presentation creative, entertaining, and memorable. Include cartoons or tables to provide visual impact; we tend to gain meaning from pictures. Develop your presentation so that your audience learns your security policy, understands how to apply it, and is certain to remember it.

Keep your overall goals in mind as you develop your content. Your presentation should be created to address your organization's need to make users aware of security principles and the corporate security policy. These principles and policies will form the basic content of your presentation. Most organizations have a security policy to protect it from theft or loss of information. If you do not have a corporate security policy, this is the time you should look into getting one. A security policy is created either by the organization, or with assistance from external consultants, to form a set of rules and procedures to keep the organization's assets, especially its information assets, safe from loss, theft, or damage. The policy includes a description of the roles and responsibilities of personnel and equipment in protecting data, including data handling, distribution, transmission, and disposal. To view some sample corporate security policies, go to the SANS Institute Security Policy Project website at http://www.sans.org/resources/policies/ .[5] These policies are to be used as guidelines when developing your own security plan. Your plan must fit your organization, the type of information and facilities you have, and what roles your employees have in security.

Add depth to the presentation by teaching how to identify risks and showing examples of recent information security incidents. Teach how to apply good practices to everyday tasks and explain your security planning process. Encourage employees to ask questions whenever they encounter questionable activity, such as unknown people within secured areas, or inappropriate requests for information. Also, provide a useful summary or take-away like this one at the end of the National Institutes of Health security awareness program: http://irm.cit.nih.gov/security/takehome.html .[6] It is helpful for users to have some easy-to-use materials so that they can refer to them if they see questionable activity or if they need to react to an incident such as intrusion, theft, or damage to information. The take-away includes highlights of security principles, your security policy, examples of common threats and procedures for reporting and responding to incidents. If your organization is large, it is possible that someone has already developed some security training, and they may have materials that you can use to create content. Any materials that you already have can be of help. Security awareness training program cannot take the place of a complete corporate security policy, but it can provide your organization with another level of security by preparing users how to guard against vulnerabilities, how to recognize threats, or what to do in the event of damage, loss, or theft of information.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If your corporate security policy requires that all employees document their understanding of the plan, then your security training should include a process to certify the audience. It is important for organizations to have security policies, and it is just as important to ensure that those policies are applied. It is also good practice to periodically remind employees of the security policies so that they continue to apply them in their everyday jobs, and it is necessary to inform your organization whenever your security policies change. Sometimes annual or quarterly certifications are required either because of the emergence of new technology, potential exposure, newly discovered threats, or regulatory requirements. Perhaps your organization has an audit requirement, or your sponsor has enough authority to enforce a security certification requirement. Your project can include a method for recording and retaining these certifications.

Now that you're ready to pound the keyboard to create your presentation, you have to determine how long it will take to finish it. The required scope and available resources will determine your timeline, based on the quality of the finished product. If your sponsor has given you a deadline for the completion of your project, then it is very important to determine your timeline. If you cannot complete the project in time based on the scope of the training, the resources you have available to you, and the quality that is expected, then you'll have to renegotiate these elements with your sponsor.

Create a rough outline of your project based on the information you've gathered so far, and discuss these findings with your sponsor. With his assent, show your plan to representatives of your audience. Make sure to understand their needs and expectations. Get agreement on all aspects of the scope and timeline, gain approval for your plan, and you have yourself a project.

CREATING THE CONTENT

Now that the scope and timeline are established and accepted, it is time to focus on content. For an effective presentation, make it real and relevant. Provide an overview of generally accepted security principles, discuss risk, and show how your security policy can be used to apply those principles to control risk.

SANS teaches the Three Bedrock Principles of information security as:

- Confidentiality
- Integrity
- Availability.[7]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Confidentiality means protecting the information from unauthorized access, ensuring that only those who have the right and the need to the information can use it. Integrity means protecting the information from damage, ensuring that information is not changed inadvertently by a corrupt process, during storage, or during transmission. Availability means protecting access to the information so that those who have legitimate access to the information can get to it when and where they need to. Confidentiality, Integrity, and Availability are fundamental principles of information security, and all security training should include these principles.

Some organizations might have additional fundamental principles that are critical and must be observed. Industries such as banking and healthcare also add Privacy as a fundamental principle. It may seem that Confidentiality and Privacy are the same thing, but they are actually very different issues. To clarify, Eric Bergeron summarized in "The Difference Between Security and Privacy" that whereas information belongs to the organization, it is about a person, and therefore privacy specifies the ability to determine how the information about that person is used. Security protects the data and assures privacy.[8] The healthcare industry is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[9] where privacy is the main focus. It summarizes, "A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[10] This means that while the information needs to have confidentiality, integrity, and availability, the organization is responsible to ensure that the information is used to the benefit of the patient. Financial institutions are subject to privacy, information gathering, and information sharing restrictions under the Gramm-Leach-Bliley Act:

> Protecting the privacy of consumer information held by "financial institutions" is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some – but not all – sharing of their information.[11]

The Federal Trade Commission recognizes that privacy is a primary responsibility of financial institutions, so it is important to include privacy as a fundamental security principle if you are creating security training for an organization that requires information privacy. If your industry has other critical security-related fundamentals, such as accountability, veracity, economy, or safety, be sure to include information about these issues.

Illustrate the security-related principles by describing steps that employees can take to apply them. This will create a more effective presentation. For example,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The National Infrastructure Protection Center published "Seven Simple Computer Security Tips for Small Business and Home Computer Users:"

- Use strong passwords. Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts.

- Make regular backups of critical data. Backups must be made at least once each day. Larger organizations should perform a full backup weekly and incremental backups every day. At least once a month the backup media should be verified.

- Use virus protection software. That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically.

- Use a firewall as a gatekeeper between your computer and the Internet. Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections but they are also valuable for those who still dial in.

- Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.

- Do not open e-mail attachments from strangers, regardless of how enticing the Subject Line or attachment may be. Be suspicious of any unexpected e-mail attachment from someone you do know because it may have been sent without that person's knowledge from an infected machine.

- Regularly download security patches from your software vendors.[12]

Other tips can be tailored for your organization. For example, if your employees travel with laptops, it is important for them to be mindful of their surroundings when viewing sensitive information on the laptop screen in a public place. If you have a high rate of laptop theft or loss, teach your employees how to lock up their machines when they aren't using them. If your facilities receive visitors, make sure employees know how to recognize people who do not have a legitimate reason to be there. Illustrate an example of a natural disaster that threatens data or equipment, and describe what to do to protect the information, or to report the incident. These tips show how systems administrators and end users can do their part to guard their information. Be sure to emphasize similar security tips that are relevant to the contents of your security plan, as well as the principles of Confidentiality, Integrity, and Availability. Include other fundamentals that may be requirements within your organization or its industry.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Your presentation should also explain different risks to data. In Computer Security Basics, Deborah Russell and G.T. Gangemi Sr. summarize seven major vulnerabilities that threaten data:

- Physical – your buildings and computer rooms are vulnerable. Intruders can break into your computer facilities just as they can break into your home. Once in, they can sabotage and vandalize your computer, and they can steal diskettes, disk packs, tape reels, and printout…

- Natural – computers are very vulnerable to natural disasters and to environmental threats. Disasters such as fire, flood, earthquakes, lightning, and power loss can wreck your computer and destroy your data. Dust, humidity, and uneven temperature conditions can also do damage.

- Hardware and software – certain kinds of hardware failures can compromise the security of an entire computer system. For example, many systems provide hardware protection by structuring memory into privileged and nonprivileged areas. If memory protection features fail, they wreak havoc with your system, and they open security holes…

- Media – disk packs, tape reels, and printouts can be stolen, or can be damaged by such mundane perils as dust and ballpoint pens…

- Emanation – all electronic equipment emits electrical and electromagnetic radiation. Electronic eavesdroppers can intercept the signals emanating from computer systems and networks, and they can decipher them…

- Communications – if your computer is attached to a network, or even if it can be accessed by telephone, you greatly increase the risk that someone will be able to penetrate your system…

- Human – the people who administer and use your computer system represent the greatest vulnerability of all. The security of your entire system is often in the hands of a system administrator…. Ordinary computer users… can also be bribed or coerced into giving away passwords, opening doors, or otherwise jeopardizing security in your system.[13]

These are examples of general risks that can form a part of your presentation. Be sure to describe the vulnerabilities as they apply to your environment, and temper these vulnerabilities with how likely they are to actually occur. For example, it is not likely that most organizations need to be concerned with intruders sniffing around your office to pick up the electromagnetic emanations coming off of your screen or wiring, so you probably won't need to discuss TEMPEST systems,[14] however it is quite possible that a natural disaster or power outage can occur that interrupts business and jeopardizes availability, so you can

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

selectively emphasize the vulnerabilities that are most likely. It is also important to spell out what to do in case any of these vulnerabilities are threatened. For example, do your users know what do you do if your data center is hit by lightning, and it knocks out power? Your presentation can include basic incident response and reporting instructions. Describe how these vulnerabilities demonstrate a risk to your equipment and information. SANS points out that the level of risk is a function of vulnerabilities and the actual threat to these vulnerabilities.[15]

Include examples by adding current events in order to illustrate how security policies were successful in fending off attacks. Other examples can be used to demonstrate the damage attacks caused that could have been prevented. There are several outstanding sources of current events relating to information security, including the Internet Storm Center,[16] CERT ® Advisories,[17] Hack in the Box,[18] and even the technology sections of general news websites. Search the sites for articles relating to your company, your industry, or other companies within your industry. It is also helpful to subscribe to the news alerts that these sites provide. When illustrating examples, make them meaningful by describing the incident, specifying the vulnerability, and explaining how your security policy could have prevented or mitigated the attack.

Be sure to include incident reporting. Whether or not your organization has a formal process for it, employees should always report damage, loss, intrusions, or attempted intrusions. Specify what types of incidents are reported, and who receives these reports. If there is no formal process, employees should be instructed to report incidents to their management.

Pull it all together. Demonstrate to your employees that they have tools available to keep your network secure. These tools include general security principles, your security policy, tips on how to apply your policies, understanding and recognizing risks, and incident reporting.

CREATE THE PRESENTATION

You have your content, now create the show. You can produce a typed document or slideshow presentation with popular office software products, or use prepackaged security training from vendors such as Security Awareness Incorporated.[19] You could go all out and prepare a multimedia presentation such as the charming Sydney, the Sr. Lab Rat that the National Institutes of Health uses to teach its employees the fundamentals of information security[20] in a course developed by Global Learning Systems.[21] There are several vendors available to help you produce web-based learning systems, like web application developers Presidia[22] and Docent.[23] If you use a vendor for producing the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

finished product, determine your selection criteria first. Since there are so many resources available, and they differ by their level of experience and expertise, their cost, style, and available services, you should choose the one that fits your needs and your budget. You might already have a business relationship with one of these vendors. Decide whether you will select a vendor to produce your presentation, or you do it yourself.

Decide on the presentation medium. Look around your organization and determine the best way to present your training program. The media can be anything from printed workbooks to slide shows, films, or web-based presentations. You can also include informational posters and handouts as reminders of the training. This choice will also depend on your scope, available talent, resources, and budget.

CERTIFICATION

If your organization requires you to document that all employees understand the security policies and agree to follow them, then you should include some type of certification in your training program. This certification can simply indicate that they have read the material or attended the training. To test how well they understand the security principles and company policies presented in the training program, include quizzes throughout the program, and/or a comprehensive test at the conclusion. Passing results can be stored with personnel records, or with corporate security for audit purposes. In addition, most web-based learning systems will record the learning sessions and test results.

For further development, several Information Security Industry Certifications are available. Many are listed in the Computer Security Resource Center Professional Development web pages, http://csrc.nist.gov/ATE/prof_development.html [24] If you are pursuing a career in information security, an industry certification demonstrates your level of understanding in the topic. Organizations that provide certifications are also tremendous resources for training and research in the security field.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CONCLUSION

Organizations of all sizes, with all levels of information sensitivity and all varieties of information security technology are at risk of jeopardizing the confidentiality, integrity, availability, and privacy of their data to all sorts of threats, either by intruders, hardware failure, natural disasters, or simple human error. Teaching your employees how to handle company resources and respond to threats goes a long way to protecting your information. After all, whether or not they realize it, your employees each must decide to keep your information secure. Security awareness training can help your employees make the right decisions.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES

[1] Gaudin, Sharon "Social Engineering: The Human Side of Hacking," May 10, 2002
URL http://www.cioupdate.com/reports/article.php/1040881

[2] Hurley, Edward "Study: Employees willing to share passwords with strangers," SearchSecurity.com, April 24, 2003
URL
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci895483,00.html

[3] Freeh, Louis J. "Statement for the Record Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information." March 28, 2000.
URL http://www.fbi.gov/congress/congress00/cyber032800.htm

[4] McCarthy, Brian in "CompTIA Survey Reveals Human Error Most Likely Cause of IT Security Breaches," The Computing Technology Industry Association, March 18, 2003
URL http://www.comptia.org/pressroom/get_news_item.asp?id=207

[5] SANS Institute "Security Policy Project," 2002-2003
URL http://www.sans.org/resources/policies/

[6] National Institutes of Health, "Computer Security Awareness," April 23, 2003
URL http://irtsectraining.nih.gov

[7] SANS Institute SANS Security Essentials II: Network Security Overview, 2002 p 1-5

[8] Bergeron, Eric "The Difference Between Security and Privacy," Zero-Knowledge Systems Inc, December 7-8, 2000
URL http://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html

[9] United States Department of Health and Human Services, "Medical Privacy - National Standards to Protect the Privacy of Personal Health Information," Office for Civil Rights – HIPAA, May 29, 2003
URL http://www.hhs.gov/ocr/hipaa/

[10] United States Department of Health and Human Services, "Summary of the HIPAA Privacy Rule," May, 2003
URL http://www.hhs.gov/ocr/privacysummary.pdf

[11] Federal Trade Commission, "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

URL http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

[12] National Infrastructure Protection Center, "Seven Simple Computer Security Tips for Small Business and Home Computer Users"
URL http://www.nipc.gov/publications/nipcpub/computertips.htm

[13] Russell, Deborah and Gangemi, G.T. Sr, Computer Security Basics, Cambridge: O'Reilly & Associates, Inc, July, 1992. 12 – 13

[14] Information Assurance Directorate, "TEMPEST Endorsement Program," National Security Agency – June 25, 2001
URL http://www.nsa.gov/isso/bao/tep.htm

[15] SANS Institute SANS Security Essentials II: Network Security Overview, 2002 p 1-11

[16] Internet Storm Center
URL http://isc.incidents.org/

[17] CERT ® Coordination Center Advisories
URL http://www.cert.org/advisories/

[18] Hack in the Box
URL http://www.hackinthebox.org

[19] Security Awareness, Incorporated, "Security Awareness, Training, and Reference Tool," 2000-2003
URL http://www.securityawareness.com/start.htm

[20] National Institutes of Health, "Computer Security Awareness," April 23, 2003
URL http://irtsectraining.nih.gov

[21] Global Learning Systems
URL http://www.globallearningsystems.com

[22] Presidia web application development
URL http://www.presidia.com/webapplication.html

[23] Docent Learning Content Management Systems
URL http://www.docent.com/products/data6_lcms.html

[24] Information Technology Laboratory – Computer Security Division, Computer Security Resource Center (CSRC), "Professional Development," National Institute of Standards and Technology, May 21, 2003
URL http://csrc.nist.gov/ATE/prof_development.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.