Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Creating an IT Security Awareness Program for Senior Management

This paper will present an approach to creating and deploying a security awareness program with senior management as the intended audience. This paper is intended as a guideline to creating a successful security awareness program for your organization. A successful program for senior management is the key to the security program for the entire organization and therefore needs to be carefully and concisely constructed. Creating the program requires numerous resources, a clear understanding of security within the organiz...

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

Creating an IT Security Awareness Program for Senior Management

Version 1.4b

By Robert Nellis, CISSP

March 24, 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

This paper will present an approach to creating and deploying a security awareness program with senior management as the intended audience. This paper is intended as a guideline to creating a successful security awareness program for your organization. A successful program for senior management is the key to the security program for the entire organization and therefore needs to be carefully and concisely constructed. Creating the program requires numerous resources, a clear understanding of security within the organization and an understanding of the position of senior management on IT security. This paper will outline the steps necessary to identify the current level of senior management's IT security knowledge. Once the knowledge level is identified the steps to develop the content of the awareness program based on this knowledge will be discussed. The paper will provide recommendations on data gathering, risk analysis, resource requirements and how to correlate the information to the impact that is has on the organization. Options for presenting the program to senior management and ongoing communication recommendations will also be discussed.

Introduction

Creating and implementing an effective program to educate senior management will be the cornerstone for the Security Awareness program for the entire organization. Without the support and acceptance of senior management, the security awareness program for the organization is in serious jeopardy. Employees will follow by example and look to management for guidance and direction. Executives who do not clearly understand the importance and impact of a solid security awareness program for the organization are doing a serious injustice to not only the employees of the organization, but the shareholders as well. Providing senior management the tools and knowledge needed to understand the threats facing the organization is the goal of the Senior Management Awareness program. Information presented to senior management must be carefully collected and organized providing a clear correlation between the threats and the potential impact on the business. The creation of a successful security awareness program is no easy task to undertake. Many people have attempted this monstrous effort fail due to the miscommunication of information presented to senior management. Security Awareness must be communicated and accepted as a normal job function, not something employees have to attend once a year as mandated by management. This paper will cover the steps required to put together a successful security awareness program targeting senior management as the audience.

Getting Started

Taking Your Personal Inventory

The first step on the path to creating an effective security awareness program is to identify your own key strengths and weaknesses. By taking your own personal inventory and understanding the level of knowledge you posses in both security and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

developing presentations, you can quickly identify the key areas necessary for the program that require additional resources and knowledge. Building a successful program is like building a house. No one person possesses all of the skills to construct the foundation, framework, electrical, plumbing and finish work to efficiently build a house from the ground up. A security awareness program will require the expertise of many individuals to develop and implement. Communication of accurate security and business related information is essential to ensure that the program not only achieves its goal, but also to ensure that the program has a future. Poor planning and misinformation will can result in a less that successful program and may damage your reputation as well. If this is your first attempt at creating an awareness program, consider taking a course offered by one of the many security organizations to establish a solid understanding of the task at hand. There are also books available on creating security awareness. The Internet is another valuable resource for information as well as examples of security awareness programs. Take the time to research and gain a solid understanding of the mechanics of a successful security awareness program before proceeding. Once you are comfortable with the mechanics of the program and have a general understanding of the type of program that best fits your organization, you can then begin to establish the team necessary to develop an effective program.

Getting the Team Together

The first step in the creation of the security awareness program will be identifying as many resources within the organization with the information necessary to construct the program. Creating an effective program will require a large amount of research, analysis and documentation to identify the appropriate content for the presentation. By creating a team to put together, the program will be easier to accomplish and include a broader view of security. At a minimum the team should consist of representatives from the following organizations:

Human Resources – Can provide current polices, standards and examples of investigations and policy violations.
Legal – Can provide information regarding legal issues, regulatory or statutory requirements and interpretation of current laws regarding IT security.
Internal Audit – Can provide current security issues, audit reports and insight on how to present the information to senior management effectively.
Business Continuity Manager – Can provide information regarding risk assessments, examples of incidents, how they were handled and the impact on the business.
Finance and Accounting – To provide information relating security issues to financial impact on the business.
Information Technology Manager(s) – Can provide information on system and application security.
Public Relations - Can provide information on the impact of incidents on the public image and reputation of the organization.
Training and Development – Can assist in creating the formal training program for the organization. They may also be willing to conduct the training sessions as well.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Interviews

A key step to any successful presentation is to understand the intended audience and their current knowledge level on the subject to be presented. One approach to gaining this understanding is to conduct interviews with senior management. The interviews will identify their current knowledge level on security and provide a starting point for the construction of the executive security awareness program. The interviews can also serve as a dry run of the presentation to determine how to effectively present the information in a manner that is acceptable to senior management. This will also be an excellent opportunity to get them thinking about the current status of IT Security within the organization. One key factor to keep in mind is the availability of senior management. The interview process should take between 30 minutes and 1 hour. Be flexible when scheduling the interviews to make this as convenient as possible for senior management. If senior management is unavailable an alternative is to schedule the interviews with their direct reports or other members of management. The goal is to develop an understanding of the topics that senior management is concerned with in security and to level set their understanding on the areas of IT security that impact the organization on a daily basis.

Preparing for the Interviews

Select at least three key members of senior management within the organization to be interviewed and author an email to them outlining your intentions and inquire on their availability for the interviews. If they are unavailable for personal interviews, suggest a phone interview and try to keep less than 30 minutes. Preparation is vital to ensure that you get the answers needed to develop the program and clearly understand the content needed. Below are sample questions as a starting point:

1. What does Information Technology Security mean to you?
2. What is your understanding of IT Security and it's role within the organization?
3. What key concerns does senior management have in regards to IT security?
4. What level of security knowledge or training do you possess?
5. What type(s) of security training benefit senior management?
6. How are security incidents and issues communicated to senior management?
7. How effective is the incident response team?
8. How would you rate the level of security awareness within the organization?
9. What suggestions do you have to increase the level of awareness?
10. What are some of the current security issues facing the organization?
11. How effective are the security policies currently in place?
12. What suggestions do you have to improve the security awareness within the organization?

To get a better understanding of the questions that you need to compile, you may want to survey your IT staff to get their viewpoint of security awareness within the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

organization. They will not only provide a realistic viewpoint on the situation, but also may you with provide real life issues that they deal with on a daily basis.

Once you have compiled all of the questions identified for the interview and prior to scheduling the interviews, you will want to review and rehearse the script for the actual interviews. Ask a manager or supervisor who is familiar with the members of management selected to assist in rehearsing the interview. Remember that senior managements time is very valuable and you want to present a polished and professional image if you are to obtain their support in promoting the security awareness program.

After completing the interviews with the individuals selected, you will need to compile their responses to identify the common areas of deficiency or topics of interest. One approach is to create a matrix as show below:

	Executive 1	Executive 2	Executive 3	Executive 4
Question1				

This matrix can be created prior to the interviews and used to record the responses during the interviews. In either case the table is an effective way to compare the results of the interviews and identify the common areas to be addressed in the awareness program.

Organizational Assessment

The next step to building the security awareness program is assessing the level of security awareness within the organization. This step will attempt to identify the strengths and weaknesses that currently exist. This step will be the most time consuming and also the most enlightening or frightening. During this phase you will be reading through policies, procedures, audit reports, risk assessments and conducting interviews with may different individuals within the organization. Keep a notebook handy to record notes and information that could present itself at any time for future reference. Water cooler discussions can provide you with a real world picture of the security awareness knowledge and compliance. Remember that as information travels up the organization, each level will interpret to the best of their ability and convey the information as they presume to have understood it. Accurate communication to senior management will provide the credibility needed to gain their attention and support.

Policies and Standards

Policies and Standards for the organization may be spread throughout may different groups and geographical locations. Your goal will be to identify where they reside, how they are maintained, communicated and enforced. Enforcement is the key to effective policies and standards. If they are not being enforced adequately, this must be a key point identified within the executive security awareness program. A good

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

starting point for gathering policy and standard information is the human resource department. They are normally responsible for approving and communicating policies and standards to employees. They can also provide information regarding the enforcement and effectiveness of policies and standards within the organization.

Risk Assessments

Formal risk assessments will provide information needed to identify key topics to be included in the presentation to senior management. The department responsible for business continuity and disaster recovery may be able to provide reports of risk assessments performed. If there are no formal risk assessments available, you may need to perform an informal risk assessment on one or two of the key business processes or systems to obtain information to be included in the program. Chapter 15 – Risk Management in Information Security Management Handbook 4th Edition[1] is an excellent resource for information on conducting the risk assessments. There are also numerous resources on the Internet available to assist in this effort.

Penetration Test Reports

Penetration/Vulnerability test reports if available will provide additional keys areas to be addressed in the awareness program. Utilizing information obtained from risk assessments and comparing the results of the penetration test reports, you can identify two or three key issues to present in the awareness program. When preparing the results obtained for the program, ensure that the information presented is not too technical and clearly identifies the potential impact on the business.

System or Application Audits

Audit reports can be an excellent source of information for the awareness program. Not only do they identify key issues within the organization to be addressed, but they are also in a format that is familiar to senior management. These reports can server as a template for the awareness program and provide vocabulary that is targeted towards senior management. Both internal and external auditors can assist in obtaining and understanding the reports.

Financial Impact

Financial impact of security related issues and awareness should be underlying theme for the program. After all, the organization is in business to make money. Annualized Loss Expectancy (ALE), Annualized Rate of Occurrence (ARO), Exposure Factor (EF) and Single Loss Expectancy (SLE) are key terms used to calculate risk and financial impact[2] that need to be clearly understood and represented within the program. The Finance and Accounting department along with risk management can assist in developing content to address this subject. The accuracy and relevance of the information presented on financial impact will be one of the most critical success factors

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of the awareness program for senior management. Security compromises can affect not only the bottom line, but often will affect the stock price as well. Investors today may question the stability of an organization that is the victim of comprise, especially if the compromise could have been avoided and the organization failed to implement basic security controls. Dedicate the time and resources needed to ensure that the information is presented accurately and depicts issues currently impacting the business. Avoid discussing potential risks or depicting that the organization's future is in jeopardy due to the current state of security. "Avoid the temptation to be an alarmist." Chicken Little speeches also referred to as FUD (Fear, Uncertainty, and Doubt)[3] may work initially, but in time this approach will loose its impact and result in tarnishing the creditability of the program.

Regulatory and Legal Requirements

Regulations and laws dealing with computer and information security impact every organization today. Whether they are regulations targeted at specific industries (HIPAA for Health Care, GLB for Financial Institutions) or laws defining illegal practices, all organizations today are impacted in some manner. A clear understanding of the laws and regulations that impact your organization will assist in selling the entire security program to senior management. As the dependency and availability of information systems and digital increases, we are seeing an increase in the controls mandated by government agencies to protect digital information. Educating senior management on the new and updated and laws and regulations today can be a full time job and should not be the intent of the security awareness program. You will however want to include an overview of the current regulatory or legal issues impacting the security program. It is important to understand and include regulations in the awareness program to ensure that senior management clearly understands the impact they have on the organization and on security. Obtain the assistance of your legal department to identify and document these issues accurately. You may also want to utilize this information if you are experiencing difficulties obtaining the support of senior management for the security awareness program. If there are laws or regulations mandating certain levels of security and awareness, you can use this to help promote the program.

Corporate Image and Reputation

Public image and reputation are extremely important in the success of any organization in existence today. Many computers related incidents go unreported due to the impact they may have on the reputation and image of the organization. The incidents that are reported often get extensive media coverage. Microsoft, Ebay, Amazon.com and Playboy are just a few examples of organizations that have had security breaches publicized. These organizations incurred losses not only from the incidents themselves, but also had there reputations damaged. We continue to hear of more and more of organizations that loose valuable organization and customer information as a result of a security incident. There are also many others that we do not hear about because of the impact that bad publicity would have on the organization. Many consumers are cautious of doing business over the Internet as a result of this

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

publicity. This is why it is important to understand how image and reputation will affect the organization and to relate this information as it pertains to the security awareness program. If your organization has a public relations department, they can assist in obtaining information on how negative publicity affects the organization. The marketing department is another source of information and can assist in relating how it affects sales, stock prices or customer retention.

Putting It All Together

The goal of any awareness program is to educate the intended audience on their role within the security program. A good awareness program will not only educate on the importance of effective security polices and practices of the organization, but also teach the three basic elements of security, confidentiality, integrity and availability. By understanding how each of these elements impact the business and how employees affect the levels of each, management can begin to understand the impact it will have on the success of the business. They will also have a better understanding of their role that they will play in the security program.

To achieve the goal of effectively educating senior management on security and its impact of the business, you will need to review all of the information obtained from the resources outlined above and identify no more that three key areas to be addressed. Reducing the vast amounts of data obtained or finding that there is very little data available to create the presentation can seem like an impossible task. In either case an effective program can be designed with a little hard work and imagination. Keep in mind that the intended audience is senior management and that the presentation should be between thirty minutes to no more than one hour. It must clearly and concisely communicate the essential elements of security that senior management will require to effectively make decisions regarding the security of the organization. So where do you start?

Identify the Format to be used

Based on the information obtained in the interviews and the availability of senior management, the communication format of the program needs to be identified. There are different options available based on time, frequency, and preference of management. One or more of these options can be utilized to effectively conduct the awareness training with minimal impact on senior managements busy schedule.

If availability of senior management is an issue you may want to create a newsletter that is no more than one page as an initial implementation of the awareness program. This is a great way to start a communication method with senior management with very little impact on their busy schedule. The newsletter can be published at regular intervals to provide current up to date information on issues and the status of security within the organization.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Monthly statistics or metric reports can also be an option if senior management prefers this type of communication. These reports can be difficult to prepare if the information required is not currently being tracked. You will need to gather the requirements of senior management for the content and the format of the reports. Once the requirements are gathered, the methods and procedures to obtain the data will need to be developed. Developing the procedures to gather the data may require coordination with several different departments to complete. Clearly communicate to everyone involved the object and the requirements as defined by senior management.

A short presentation at senior management staff meetings is another option. Keep this presentation to no more that fifteen minutes. The content of this presentation should cover the current issues or incidents that need to be addressed by senior management. Additional information regarding security metrics can also be included if time permits. Allow enough time in the presentation for any questions that may be asked. Detailed information on the subjects discussed may be provided in handouts to clearly communicate the information. Preparation and accuracy are important for this type of presentation.

Formal security awareness training session is the most preferable option, as it will provide a structured training environment targeting only the subject of security awareness. This will require a commitment by senior management for attendance. If the organization has Training and Development department, ascertain their assistance in developing the program. The length of the presentation should be between thirty minutes to no more than one-hour. A recommendation for the content and structure of this program is outlined below. Utilize all of the resources available to develop and present the program.

Outside training is an additional option if you are having difficulties preparing an effective presentation. There are many security organizations that provide specialized training programs for senior management. This may be a better approach if you are having difficulties in selling an awareness program. Management may be much more receptive to the ideas and information presented by someone outside of the organization who does not appear to have any personal agenda. This may also be a good approach if you are new to the organization and have not yet established a solid reputation with senior management.

Formal Security Awareness Training Program for Senior Management

Getting Their Attention

Start the presentation with an introduction that will get their attention and start their minds thinking about the topic of security. One approach is to start off with collage of news articles depicting security incidents that received a good amount of publicity in the media. You may want to put a little twist on this by replacing the actual organization name with your organization's name to really get their attention. Explain that an effective security program for the organization will reduce the risk of the headlines becoming a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

reality. You may also want to start out with actual issues or incidents that have impacted your organization both in a negative and positive nature. Remember that you do not want to give the impression that the state of security is hopeless, but imply that with the proper training and awareness, the appropriate level of security for the organization can be achieved. Keeping a positive theme throughout the presentation will be better received than a negative one.

Current Status of Security Within the Organization

Now that you have their attention, begin by outlining the current status of security and security awareness within the organization. Utilize the information obtained from the audit reports, penetration test reports and reported security incidents to summarize the current situation. This information should include issues that are identified as severe on previous years audit reports that still need to be addressed, summary of penetration assessment results, the number of reported security incidents, investigations and a report on the number of policy violations investigated.
You may also want to include metrics from the various security organizations on virus and worm activity, hacker activity, vulnerabilities and exploits that may impact the organization. Provide if available, the cost incurred as a result of the incidents as well. Take the time to calculate as accurate as possible the cost including, direct financial loss, productivity lost, investigative costs and recovery costs. Do not try to calculate intangible costs associated with the incident. Keep in mind that you need to provide accurate information that management can comprehend.

Security Polices and Procedures

The security policy statement for the organization is another very important issue to be addressed in the awareness program. Without a policy statement, the employees of the organization will have their own perception of what security is and what the organization's position on security is. If the organization has a weak policy statement, provide recommendations on how to improve it. You can also provide examples of well-constructed policy statements that are available on the Internet. If the policy statement is effective, communicate this as well. Again you will want to cite examples on the positive impact that security and security policy has on the organization.

Security standards, policies and procedures should be addressed as well, as the work to further clarify the organization's position on security. Reviewing the standards and procedures in detail is not necessary as senior management is usually who approved them in the first place. The enforcement of established security standards, policies and procedures should be discussed as well. You will need to communicate that without effective enforcement at all levels of the organization, the policies, standards and procedures are nothing more that recommendations that most likely will not be taken seriously. You may also want to provide examples of how enforcement may prevent previous incidents from reoccurring.

Organizational Security Awareness Program

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The weakest link in the security chain for the organization is its employees. After all, computers don't make mistakes, people do. Human error, misinformed users, understaffed IT departments result in many of the security incidents within a corporation.

The CSI "2002 Computer Crime and Security Survey" shows the following statistics[4]:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty percent detected system penetration from the outside.
- Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- Eighty-five percent detected computer viruses.

Many of the issues identified above can be avoided or reduced through education and training of employees on their roles and responsibilities as it relates to security. The cost of an awareness program for an organization is far less that the cost to recover from security incidents. You will need to provide the estimated costs of developing and deploying a security awareness program for the organization in comparison to the cost of a security incident that has or may happen. This may be difficult to calculate if your organization is fortunate enough to not have experienced a security related incident and loss.

An additional benefit that a security awareness program provides is an extension of the security organization. When employees are properly educated on their role in security and accept their responsibility, they do become the first line of defense in the security of the organization.

Discussion of Risk

As a result of the research performed in preparing for the executive awareness program, you should have been able to identify between three to five risks that currently exist within the organization. Briefly identify each of these risks and the potential impact they could have on the business. Discuss the incurred or potential financial loss associated with the risk and the cost if applicable, to eliminate or reduce the risk to an acceptable level. This subject can generate a great deal of discussion as it brings to light the issues that have the potential to directly affect the profits of the organization. Keep the discussion on track and do not try to resolve or promise a resolution within a certain time frame for the risk. You will however want to correlate the risk to the appropriate policy, awareness topic or business process with potential to eliminate or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

reduce the risk. Remember that the goal is to educate senior management and obtain their backing for a security program for the entire organization.

An additional subject to address when taking about risk is the impact that an incident could have on the reputation and public image of the organization. Based on the information obtained from the Public Relations and Marketing departments discuss how negative publicity has impacted the stock price or sales in the past. Compare this to the risks identified and ask management to give their thoughts on the impact that the risks may have on the organization. Additional information on how security related incidents incurred by other organizations within your specific industry has impacted their reputation and public image. Try to identify incidents that could have been mitigated through an effective security awareness program. Provide accurate details as to the incident, the impact on reputation, what the revenue loss was, and the cost to mitigate the risk if available. Conclude the discussion of risk with the point that mitigating risk to an acceptable level is the objective of risk management. The complete elimination of risk may not be attainable or practical due to the nature of the risk or the cost associated with elimination could be greater that the actual cost if the risk was to occur.

Information Law and Regulations

With the assistance of your legal department you will want to identify three to five key computer laws or regulations currently impacting the organization. The services or products that the organization provides will dictate compliance to the applicable laws or regulations. The Heath Insurance Portability and Accountability Act (HIPAA) and the Gramm Leach Bliley Act (GLB) are two of the most recent pieces of legislation that impact how health care providers and financial institutions secure and protect information. Both of these acts have specific guidelines on how data is collected, stored, transmitted and released. Although these acts were intended to govern specific industries, any organization that handles this type of data may be required to comply. Senior management will need to be briefed on any relevant laws or regulations that impact the level of security and information protection that is mandated. This is the type of information needs to be identified, the explicit requirements defined and communicated to senior management on a regular basis. Solicit senior managements recommendations for communicating legal and regulatory information as it pertains to the security of the organization to them. Keep in mind that the purpose of the awareness program is to educate them on security related issues and information as it pertains to the organization.

Ongoing Communication

The last subject to include in the awareness program is future communications. Security awareness training is not a “get it and forget it” program. A successful program will require two-way communication on a regular basis. One recommendation is to conduct annual awareness training and follow up with monthly or quarterly newsletters.

Creating a newsletter is an efficient way to communicate the current status of security within the organization if constructed properly. Survey the intended audience to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

determine the style and content that is most beneficial and appealing to them. Including the intended audience in the development of the newsletter and soliciting their input will increase the likelihood of success. You may even want to ask one or two individuals to write an article for the newsletter. The more interaction that the intended audience has and the relevance to not only their job, but also their personal security as well will further promote the message and fuel the ongoing success of the awareness program.

Another approach to suggest to senior management is a security awareness day for the organization. Use your imagination and creativity to develop the activities for the security awareness day. Make the activities enjoyable for both the employees as well as senior management. Encourage senior management to actively participate in the activities. This will not only show the organization senior management's support for the awareness program, but also allow senior management to learn first hand what security issues the employees encounter on a daily basis. This will also allow senior management to listen to the employee's suggestions on how to improve security awareness within the organization. The more active role that senior management plays in the security awareness program, the greater the chance of on-going success of the security program for the organization has.

Conclusion

Educating senior management on IT Security and the impact that it has on the business will no doubt be the most difficult step in creating an effective security awareness program for the organization. Allocate the time and resources necessary to create a well-polished training program for them. Provide clear, accurate and well-researched information in a format that targets senior managements role and responsibilities in the security of the organization. Provide the appropriate level of technical detail required to clearly explain the security topics at a management level. Utilize the information obtained in the interviews, as a baseline for the level of technical knowledge senior managements possesses. Remember that without the backing of senior management the security program will have very little chance of success. That is why it is critical to the success of the organizations security program to effectively educate senior management on the role that they need to play within the security program. Their support will be required not only for financial backing, but also for promoting and enforcing the security program within the organization. Senior management must clearly understand the impact that the security program will have on the business and recognize the value of such a program. Avoid references to any potential threats that do not have direct impact on the business. The best approach is to provide real issues that currently impact the business without projecting the image that the current situation is a train wreck waiting to happen. Clearly explain the issues and provide a brief synopsis of the requirements to mitigate the risk if applicable. If the requirements to mitigate the risk are not available, communicate this risk only if it needs to be addressed immediately and needs senior managements attention. A successful education program will result in senior management's ability to make effective decisions that impact the security of the organization. The program should provide them with a clear understand the risks that currently face the organization, and provide the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

necessary information required to establish the acceptable amount of risk to ensure the success of the business.

© SANS Institute 2003, Author retains full rights

Works Cited

[1] Ozier, Will Information Security Management Handbook 4th Ed. Tipton, Harold F. and Krause, Micki. Ed. Boca Raton: Auerbach Publications, 2000

[2] Harris, Shon All In One CISSP Certification Exam Guide . New York: McGraw-Hill / Osborne, 2002

3 Holtzman, David H. "Is the Sky Really Falling." *CSO* December 2002: 26

4 Computer Security Institute. ""2002 Computer Crime and Security Survey" April 7, 2002 URL: http://www.gocsi.com/press/20020407.html

© SANS Institute 2003, Author retains full rights

References

Computer Security Institute. “2002 Computer Crime and Security Survey”. 7 Apr 2002. URL: http://www.gocsi.com/press/20020407.html

Cutter, Ken. “Hitting the Bull’s Eye”. Aug 2000. URL: http://www.infosecuritymag.com/articles/august00/columns5_logoff.shtml

Desman, Mark B. Building an Information Security Awareness Program. Boca Raton: Auerbach, 2002.

Dow, Anna. “The Executives Role in Network Security”. Sep/Oct 2000. URL: http://business.cisco.com/prod/tree.taf%3Fasset_id=49850&public_view=true&kbns=1.html

Fogerty, Karen, and Watson, Susan, eds. “New Study from CIO and Darwin magazines reveals: American executives leave room for improvement in their personal security practices”. 7 Feb 2002 URL: http://www.cio.com/info/releases/020702_release.html

Harris, Shon. All In One CISSP Certification Exam Guide. New York: McGraw-Hill/Osborne, 2002.

Hollander, Yona. “Six top security issues for executives”. 30 Dec 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,77132,00.html

Holtzman, David H. “Is the Sky Really Falling”. CSO December 2002: 26

Hurley, Edward. “Crossing the divide: Upper-level managements role in IT security”. 13 Feb 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci880395,00.html

Levine, Lawrence. “Putting Management to the Security Test”. SC Magazine September 2002:82

Richards, Donald R., et al. Information Security Management Handbook 4th Edition. Eds. Tipton, Harold F., and Micki Krause. Boca Raton: Auerbach, 2000.

Rudolph CISSP, K. et al. Computer Security Handbook 4th Edition Eds. Bosworth, Seymour, Kahay, Ph.D., M. F.. 2001. URL: http://www.nativeintelligence.com/awareness/chap29-1.asp

Symantec. “Top Management’s Perspective on Security”. Jan 2001. URL: http://enterprisesecurity.symantec.com/PDF/097100405_TopMgtPerspec_wp.pdf?EID=0

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced