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 Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Steve Montgomery
SANS Security Leadership
GLSC Practical Assignment, Version 1.0
August 11, 2003

# RIGHTSIZING INFORMATION SECURITY PRACTICES – A PRACTICAL GUIDE FOR THE SMALL ORGANIZATION

© SANS Institute 2003, Author retains full rights.

## *Abstract*

I've been in the technology industry for over 25 years, filling roles from junior developer to I.T. Manager in companies both large and small. I've watched as computers have evolved from huge mainframes with rooms full of peripherals to desktop appliances found not only on every employee's desk but typically in most homes as well. But perhaps no facet of computer technology has changed as much as information security. Twenty years ago information security did not receive much attention. Policies and procedures to protect networks and data were not widely implemented, and only the largest of corporations gave information security much attention. But in today's corporate technology world information security is no longer an option. All sizes of organizations, even home users, must consider the security of their computers, networks and data.

Large corporations can typically justify a significant investment in security programs, intrusion detection systems, vulnerability assessment and monitoring systems, and the staff and consultants to provide the know-how where necessary, to protect their corporate technology. But small companies rely as much, and with limited staff sizes sometimes even more, on their technology and information than the large corporation. How then does a small company with a limited budget implement an adequate information security program?

## *Management Perspective*

Information security is not a simple topic. It is dynamic, multi-faceted issue that must receive almost constant attention in order to be effective. New vulnerabilities surface almost daily. Internet and business to business connectivity requirements move faster than a speeding bullet. It is challenging for a small company with limited financial resources to maintain an adequate security posture.

Implementing an effective information security program is as much a management issue as it is a technical matter. There are resources aplenty from which one can gain an understanding of the issues that should be considered when trying to protect threats to systems and information. And there are no end

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

to “security experts” (e.g. security consultants both large and small) who can help implement the hardware, software, policies, procedures, etc. that are necessary. But without management support and direction, the best technicians and resources will be ineffective.

### *Gain Management Support and Assign Responsibility*

So how does someone in charge of information security implement effective, affordable safeguards in the small organization?

First, you must gain support from company management to commit some resources, both financial and human, to the task. The first mistake organizations make in developing an information security program is not dedicating sufficient resources to the task. From the SANS Institute “The 7 Top Management Errors that lead to Computer Security Vulnerabilities”, the primary reason vulnerabilities persist in an organization is because management tends to “Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.”

Senior managers and department managers must be made to understand that while I.T. can provide the leadership toward securing information, the entire corporation must have an interest. Without the aid and interest of management, even something as simple as implementing a good password policy will be doomed to failure.

In each small organization there is a director’s group or steering committee. Arrange to make a presentation to them. You will need to gain their support for at least four initiatives:

1. The need for increased security awareness throughout the organization.
2. The need to assign responsibility for information security to someone within the organization. The amount of staff time required will depend on the size and needs of your organization, but it would not necessarily need to be a full time position.
3. The need to commit some financial resources to information security. There may be some hardware and software to be purchased, and possibly some training.
4. You will need management support for the implementation of some fundamental security policies.

If you are a Healthcare organization, you can cite the requirements of HIPAA as one reason to formalize your information security program. If you are a financial institution, the Gramm-Leach Blileg act presents compliance issues. But in any case you must be prepared to indicate to management why an improved information security program is important.

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

Often system and network reliability alone can provide sufficient justification. A survey conducted by CIO Magazine indicated corporate estimates for the cost of downtime range anywhere from $1000 to $50000 per hour. A simple virus infection could easily cripple your companies' computers for a day or longer. Using even the conservative estimate of $1000 per hour of downtime, you can justify enough money to implement all the security infrastructure your small company will require.

### *Assess Risks*

Do you really have to perform risk assessments? Yes, but unless you are subject to some strict auditing or reviews, they may not need to be overly formal. You do need to evaluate your organization's vulnerabilities however, in order to understand where improved security is necessary.

At the very least you should consider;

1. Risk of virus infection – this is almost a given in today's Internet-enabled world. If you receive Internet email or allow CDs or diskettes be brought into the organization, then you are vulnerable to viruses. Protect yourself with a good antivirus package installed on all PCs and servers, and keep it updated.
2. Risk of intrusion from the Internet or business to business connections – If you connect to the Internet or other businesses, then you must consider your risk of intrusion. And don't fall into the trap of thinking that high profile corporate giants like Microsoft are the only targets. Trojans and backdoor viruses are scanning the Internet constantly for a place to lodge themselves from which they might propagate further or initiate a distributed denial of service attack. A firewall, antivirus software, and good testing and monitoring procedures are imperative for adequate protection.
3. Risk of access to critical or confidential information – If you have multiple levels of responsibility in your organization, and what organization doesn't, then you have a vulnerability of someone accessing information they shouldn't. Whether that leads to embezzlement, disclosing private healthcare information, or simply learning about the boss's bonus plan, it is a problem. You must implement good account management practices with strong passwords that must be changed regularly, and limit access to critical or confidential data to only those employees that need it.

You should document your findings and proposed solutions, even if informally. The documentation can be used to demonstrate progress to management and as a source of information to other I.T. staff. Additionally it should be reviewed and updated at least annually.

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

***Write a Security Policy***

I know, I know, nobody really likes to develop formal policies. But it is important to supplement your risk assessment with a document that defines how you intend to implement security on your network. There are plenty of sample policies available that you can use as a starting point, so again, this does have to be an overly time consuming or expensive task.

How will the security policy be used? For one, it is your personal roadmap to implementing your security plan, your checklist so to speak. It is also your primary tool for communicating your information security plan to affected I.T. staff, management, and other employees within the organization. It should be communicated just like HR and personnel policies, e.g. posted on your company Intranet, handed out to new staff, and covered in corporate information security training.

What should be addressed in the security policy? You should cover all the points found in your risk assessment and any other issues pertinent to the implementation of information security within your organizations. At the very least, a good security policy would cover:

1. Appropriate Use – a legal statement for all employees, indicating that computers and information are for business use only, that the organization has the right to monitor all usage, etc.
2. Password and account management – how are accounts created, deleted, and how are passwords constructed and managed?
3. Logon - when and to what systems are logons required?
4. Access to information – how is access to confidential or critical information requested and managed?
5. Viruses and other forms of malicious code – how do you plan to protect against them?
6. Portable Computer Security – how will you protect portable computers that often leave your secure network environment?
7. Physical Security – what systems must be physically secured and how will that occur?
8. Fax Policy – if your organization does much faxing, particularly of sensitive or important information, how will that information be secured?
9. Auditing – what system and security logs will be reviewed, by whom, and how often?
10. Backing up and restoring data – how will you do it, how often, who is responsible, how is the backup media protected?
11. Remote Access – how will remote or traveling staff access your network? How will software vendors access your network for troubleshooting and repair?
12. Communications security – what precautions will you take for dedicated or dialup connections to other businesses, the Internet, etc.?

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

13. Security Response Procedures – what will you do if there is a detected security incident, who is notified, how is the incident handled?
14. Responsibilities and Consequences – who is responsible for enforcing the policy, who maintains the policy and how often, what are the consequences if employees do not adhere to the policy?

For more information on developing a security policy, refer to "Proven Practices for Managing the Security Function", a security policy primer available on the SANS website.

### *Educate*

In order for your information security program to be effective, you must educate management, I.T. staff, and users. You will need help from all three to enforce your security policy, so you better make sure they know what it means.

Remember that management group you convinced to provide resources for an information security program? If you haven't been keeping them informed of your progress, now would be an excellent time to re-involve them. Give them an executive briefing of your risk assessment results. Show them your security policy. And give them training on their responsibilities as managers and directors. As managers, will they be required to submit a form for new user accounts or for someone on their staff to have access to the payroll or personnel data? Train them on why this is important and how to fill out the forms and submit the request.

Do you have a help desk or I.T. person that will receive calls when users forget their password? Don't just train them on how to help the user change the password, but take time to go over the security policy in detail so they know the proper way to enforce the password policy.

And don't forget the user. If you don't want them to give the financial system password to the janitor so he can check the nightly batch job, then spend some time helping them understand how and why that is prohibited by the security policy. Have each user read the security policy and point out topics that are most important for the user to understand. Conduct a training session for all staff or put the information in a PowerPoint presentation on your Intranet and require each user to view it.

Once you've developed your "curriculum" and delivery method it will be easy for you to supplement the training with any new topics and repeat it at least annually.

### *Implement and Test*

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

Most of your time and effort will undoubtedly be spent here. I will touch on a few of the more critical elements of what you could be faced with and how you can make it affordable.

Firewall – Unless you have some elaborate protection requirements, you can implement an acceptable firewall solution for as little as $100. Even Cisco, who arguably provides the most configurable firewall appliances, has a small office firewall that is highly manageable for under $500. Look for something that provides Network Address Translation for your internal clients and has some logging capability. If you run your own web and email services you will need some flexibility in configuring the firewall to allow specific services to specific addresses. Many firewall appliances (including Cisco) are diskless and cannot maintain a log file. You can use a piece of freeware called the Kiwi Syslog Daemon by Kiwi Enterprises on a Windows PC on your network to capture the logs from devices that cannot keep their own.

Account and password management – You should implement strong passwords on your network (e.g. a combination of numbers, upper/lowercase letters, and special characters), require users to change their passwords regularly, and limit the reuse of passwords. You should also log failed logon attempts and lock out accounts after a series of logon failures. You may also want to log failed file access attempts, but beware of the processing overhead this puts on a server. If you are a small shop then chances are you are also a Microsoft Windows shop. All of these features are available in the Windows domain architecture and require no additional expense. Test your password strength by using LC4 by L0PHTCrack. Available in a 15 day free trial version, or for a $350 license at www.atstake.com/research/lc, LC4 is widely considered the best Windows password cracking utility available.

Anti-virus software – anti-virus products abound, but you will always be safe looking at Symantec, McAfee, TrendMicro, or Computer Associates. This may be your single largest expense because it should be implemented on every workstation and server. Be sure to get something that will automatically retrieve and distribute signature file updates at least daily. If this is done at night, be sure to instruct users to leave PCs powered on so the distribution will be successful. Decide how you will deal with notebooks that may not be on the network all the time.

Check logs – someone must be responsible for checking the security and antivirus logs on your servers, firewalls, and other perimeter devices. How else will you know if someone is trying to guess the Administrator account and break into payroll? Check them daily. It really doesn't take that long unless there is an incident requiring research and resolution, in which case it is time well spent. Check your antivirus logs too, to ensure signature files are being retrieved and updated on *all* clients as planned.

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

Patch workstations and servers – subscribe to security alerts from SANS. Review them and decide which patches are necessary for your workstations and servers and apply them. Keep a log of the patches you apply, to which machines, and why. That way if you have to rebuild a machine, or need to build a new machine you'll know which patches should be applied.

Test your vulnerabilities – use NmapWin from www.nmapwin.org (free) and Nessus from www.nessus.org (also free) to assess your network vulnerabilities. Use NmapWin to scan machines on your network for open ports. Use Nessus to probe those open ports and determine if they are in fact vulnerable to known attacks. Run these tools from your PC at home and scan your corporate network to see what is exposed and attackable. Do this on at least a quarterly basis or after any significant change to your perimeter security. Nessus runs on any POSIX system such as FreeBSD, GNU/Linux, NetBSD or Solaris, so you may need a little Unix experience or help from someone who has Unix background.

### *Applicability*

How much time have you spent implementing your security program? As it turns out, not that much.

| | |
|---|---|
| Gaining management support | 1 day to prepare and make a presentation to management. |
| Assessing risks | 1 day, assuming you are already familiar with your corporate network. |
| Developing a security policy | 3 days to research topics, evaluate other security policies, draft a policy and have it approved by management. |
| Education | 3 days to prepare materials and train managers, IT staff, and users. |
| Implementation | your mileage may vary depending on how sophisticated your implementation has to be, but this will be the most time consuming task. If you have to install anti-virus software on all PCs and servers, set logging on your firewall, enable strong passwords on your NT domain, etc. it may take as much as a few months to get everything in your security policy implemented and working. But on an ongoing basis, monitoring and managing |

© SANS Institute 2003, Author retains full rights.

your security should take only minutes a day on average.

And how much has this cost in hardware and software?

| | |
|---|---|
| Small firewall | $500 |
| Antivirus software | $1300 for 25 users, including an email agent |
| Logging tools | $0 |
| Monitoring tools | $0 |
| Password enforcement | $0 |
| Password testing tools | $350 |
| Vulnerability testing tools | $0 |

The bottom line?

Having effective and reliable security practices: Priceless (but affordable).

**References**


SANS Institute, "The 7 Top Management Errors that lead to Computer Security Vulnerabilities". 08 September 2003. http://www.sans.org/resources/errors.php.

CIO Magazine website. "Cost Of Downtime". 08 September 2003. http://www.cio.com/archive/061500/tl_downtime.html.

Guel, Michelle. "Proven Practices For Managing the Security Function". 2001. 08 September 2003. http://www.sans.org/resources/policies/Policy_Primer.pdf.


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