Global Information Assurance Certification Paper

Building an Information Security Army
Guidelines, Best Practices with Low Overhead

Michael S. Sands
GIAC Security Essentials Certification (GSEC) Practical
Version 1.4b

Abstract

We all know that the small grocer down the street and a large Fortune 100 company have at least one thing in common, they each have some type of a security program. Whether the procedure is as simple as changing the till of the cash registers and setting the alarm prior to locking the doors at the grocery store or protecting the resources and data of the Fortune 100 company, security programs can be as simple or as complex as the needs and size of the organization warrants.

With companies still in the mode of reducing budgets and employees, the Information Security department must look for ways of improving security awareness to the entire company at lower costs. And since most IS departments have a small staff, sometimes only an officer such as an ISO, it presents an even greater challenge to audit and enforce security let alone promote security to all employees.

Table of Contents

List of Figures

Management Buy-in

While there are already a myriad of good books and articles describing how to start or develop an Information Security program, one such book is **"**Building an Information Security Awareness Program" [1] written by Mark B. Desman. The purpose here is to offer enhancements to the Information Security program. While a good awareness program is a vital key, which I will also cover, the ISO or IS staff has a greater challenge than the IT department. Many IT departments are outsourced, therefore able to stay within budget with their existing staff.

> *"One of the problems with outsourcing is ensuring the quality of work. A lot of development work is being sent offshore to India and Asia. But what controls are in place to ensure quality of service, confidentiality of information, protection of proprietary assets, [and] proper background investigations for employees working with your information? You're potentially giving the keys to the kingdom to an outsourcer, and you're relying on them to provide good security. We have to push back with our executives and advise them that the security risks might outweigh the cost savings through outsourcing."*
>
> Copyright © 2004 Computerworld Inc.
> Securing the Corporation
> http://www.computerworld.com/securitytopics/security/story/0,10801,95050,00.html

While outsourcing seems to be the way of the future what I will offer here are guidelines and best practices using existing staff for the promotion of good security within the company guidelines. This paper will offer suggestions on the creation of and successful use of an Information Security Associates program. Whatever you name your program, be it Security Associates or Security Advisors the program remains the same.

Whether working with an established Information Security Program or starting one from the ground up it is important to remember to have policies in place that will be the base foundation of your program. As this chapter title suggests, management buy-in plays an important role in the success of the program and will require upper management support including most importantly the CFO (Chief Financial Officer).

For many years Information Security has taken on a greater role within most organizations. Upper management support and adherence to Information Security and more recently, with the introduction of newer laws such as HIPAA[2] and others (Table 1 below[3]) all affecting the bottom line allows for the ammunition to eliminate office politics.

RECENT LEGISLATION	WHO IS AFFECTED?	WHAT DO THE SECURITY PROVISIONS COVER?	WHAT ARE PENALTIES?	WHEN IS IT IN EFFECT?
Sarbanes-Oxley Act of 2002	All public companies subject to US security laws	Internal controls and financial disclosures	Criminal and civil penalties	Current law
Gramm-Leach-Bliley Act of 1999	Financial institutions	Security of customer records	Criminal and civil penalties	Current law
Health Insurance Privacy and Accountability Act (HIPAA)	Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties	Final security rule takes effect in April 2005
California Database Security Breach Information Act (SB 1386)	State agencies, persons, and businesses that conduct business in the State of California	Reporting of breaches of unencrypted personal information	Civil fines and private right of action	Current law
Federal Information Security Management Act	Federal agencies	Federal information, information systems, and security programs	Loss of IT funding	Current law
Bottom Line	**Significant impact on US private sector and governments**	**Financial, customer, health, personal and government information**	**Criminal and civil penalties and private right of action**	**Most provisions are already in effect**

Table 1: Impact of Recent Information Security Legislation

Establishing Policies and Guidelines

If your company has an Internal Audit department then it most likely will handle the Corporate Governance and are the keepers of existing policies and regulations. It is very important for the ISO, CIO or individual selected to head up the Information Security department to have Internal Audit, be it an individual or department as part of the security team. Since all company policies must have executive signatures prior to implementation having them on your side will pave the way for your existing and future security policies.

Of course, as noted in the title of this paper, what about the use of guidelines? Can a guideline be used in place of a policy not yet conceived? Understanding the differences between a guideline and a policy will allow you to incorporate those that are important and should be policies now versus those

that should be followed as precautionary guidelines giving you time to implement policies.

The following information from "Your Window to Information Security Policies and Disaster Recovery[4]" provides a clear understanding when to use Guidelines and when to use Policies.

> *"An Information Security Guideline is a suggested action or recommendation to address an area of the Information Security Policy. A security guideline is not a mandatory action, and no disciplinary action should result from non-adoption. However, Information Security Guidelines are considered Best Practice and should be implemented whenever possible.*
>
> *A guideline typically uses works like "should" or "may" in the definition. Guidelines are usually written for a particular environment and are used to help guide users' actions. For example, "all successful logins **should** be logged and monitored." A guideline may apply to management, administrators, end users, or a specific group within the organization.*
>
> *Information Security Guidelines will usually supplement the Procedures Manuals with their adoption encouraged and promoted rather than enforced. "*
>
> *"A policy may be defined as 'An agreed approach in theoretical form, which has been agreed to / ratified by, a governing body, and which defines direction and degrees of freedom for action.' In other words, a policy is the stated views of the senior management (or Board of Directors) on a given subject."*

In securing the data and assets of your company it is important to determine which case you will use a policy which is enforceable and has teeth or a guideline which as stated above is just that, a guideline.

Policy and Guidelines examples

Developing a new policy or guideline does not need to be difficult. The internet and books about Information Security generally touch on the subject and may even list examples from which to work from. Once again the Internal Audit department is the key to proper policy development and guidance. Some companies such as RUSecure[5] offer evaluation and downloadable policies and information.

When writing a new policy it is important to remember your audience and keeping the legalese to the lawyers. When it comes to the title be sure to keep it simple and to the point of what the policy is for. For example you would not want to have the title of the policy say "Network Security" and include both wired and wireless types of networks. It would be far better to develop two completely and separate policies.

Listed below are sample policy listings you might find in a large organization which already has an established Information Security Program.

I have also included where these policies would have the greatest impact, understanding that all policies are corporate driven from the top down regardless of noted impact.

	Mgmt.	IT	ALL
Entrance to the Corporate Information Security Guide			X
Rules for the Workplace / Use of Work Resources			X
Rules for Managers	X		
Rules for the Operation of IT Systems, Networks, Services, and Applications		X	
Protection of Corporate Proprietary Information			X
Secure Use of E-Mail			X
Passwords			X
System/Data Access Control for IT Systems		X	
Computer Viruses			X
Data Backup		X	
Using Key Material with Encryption, Digital Signature, and Authentication			X
Emergency Concept for IT Systems		X	
Cooperation and Data Communication with Business Partners		X	
Rules for Business Partners		X	
Mobile Security			X
Secure Network Topologies		X	
Sharing LAN Infrastructure with non- (your company name) Tenants		X	
Secure Portal Access		X	
Secure Portal Application Integration		X	

Table 2: Sample policy titles

Keep in mind that policies can become outdated and should either be retired or improved upon. With technological changes, increase or decrease of the workforce or even procedural changes can affect your company policies. The general rule of thumb would be to incorporate annual reviews. Policy reviews regarding Information Security as previously mentioned would be in line with whoever handles your corporate governance, which is generally your Internal Audit department.

Additional and very informative information can be found in a Network Magazine article “Writing an Information Security Policy” in the October 2002 issue written by Avinash Kadam[6].

Gathering your troops

Most large companies are departmentalized. A large company might have supporting offices in one or more states and on a larger scale might even have offices globally. This presents a greater challenge for one ISO to cover or shall I say “Spread the word” about Information Security. While present electronic

mediums like E-Mail would take care of spreading the word, Information Security goes well beyond the word with additional challenges such as enforcement, awareness, and training that cannot be handled with just emails.

Let's say for the moment your company has an accounting department and a marketing department among many others. To simply send an email to the departments letting them know the policy of locking up their laptops at night would be only a small tip in the security iceberg. The policy is in place, the email is sent as part of the awareness campaign and so we're done, right? The problem is that social engineering being what it is means that many people are too busy with their regular tasks to give the laptop notification sent to them any thought. While this management style might work for a small office situation where everyone knows each other and the business owner is just down the hall, in a larger organization the notice might fall into the email/SPAM hole.

A better idea would be to have a one or more people in a given department be trained as a security associate, advisor or person in charge of information security for that department. This person would act as the liaison with the ISO, would be the eyes and ears of the department and responsible for the promotion of security awareness.

Undoubtedly your next question from the department manager might be "How can I get someone to add this extra work to their already busy schedule?" Or why would anyone in the department volunteer for the extra work?" For now without putting the cart before the horse we need to examine two main obstacles, the first being time and the second being cost. I want to guide you in the development of the IS program at a nominal cost.

Recruiting the staff

We have all heard the request of the Department of Homeland Security that "[7]All Americans should continue to be vigilant, take notice of their surroundings, and report suspicious items or activities to local authorities immediately". We can bring these same ideals into the workplace. Even though most employees are generally aware of security it is easy for security to be an afterthought rather than the norm. It should be easy to have department deputies, associates or advisors use their efforts to keep security at the forefront instead.

Before we begin the selection process of the Information Security associate, advisor or deputy which I'll refer to as IS Staff from here on, we must have an idea of what would be expected of them. It is important to have the responsibilities in the form of a guideline or other document which would have merit and can be referred to when new IS staff come on board. This form may look like and include the sample information as shown below.

Within their sphere of responsibility (BU/Location), the IS staff member supports the Information Security Officer (ISO), extending the latter's influence in implementing measures aimed at improving information security.

On behalf of the respective BU/Location Manager the IS staff member implements Infosec strategies, instructions and measures aimed at promoting information security goals.

1.1.1 Each IS staff member must successfully participate in the Information Security IS staff member Training Class

1.1.2 Promote Information Security within his/her organization, through the following:

- Circulating Infosec information relating to security issues within the organization and creating and maintaining IS awareness.
- Conduct (at least two/year/person) unannounced Office Workstation Reviews (in addition to the mandatory annual Reviews required by Managers).
- Showing Information Security Video Tapes (available through the IS department).
- Coordinating Information Security Reviews/Classes for members of their organization.
- Always remaining vigilant of security issues within their organization, and taking necessary steps to resolve these issues.
- Ensure compliance with implementation of security measures such as antivirus and patching processes.
- Acting as the primary contact for Information Security related questions or concerns within his/her organization.
- Reporting serious IS incidents, such as viruses, hacking, theft of information, etc.

1.1.3 Conduct Annual Information Security Audit - The Annual audit must be completed by the managers, with the IS staff member present and conducting the audit. Multiple managers may be present at the audit,

1.1.4 Dissemination of Information - disseminating information security awareness through information available on the Information Security Web Page, including, but not limited to the following:

- Security News
- Security Guidelines
- Security Instructional Notes
- Security Policies
- Information provided to ISA's via IS staff member mailings.

1.1.5 Completing Quarterly Information Security Reports to show how the ISA has promoted information security within their organization. The Report is submitted to the IS staff member manager for review and approval. If the manager feels, sufficient information has not been provided, or that the Report is inadequate, the Report will be rejected, and the Information Security Office receives the rejection. The Information Security Manager will then work with the IS staff member and the affected manager to resolve security related issues.

1.1.6 Any other responsibilities as deemed necessary by the Information Security Officer to preserve the security of the Company.

Table 3: Sample IS staff description of duties

Once the IS staff requirements are finalized it must be directed to department managers or upper management to select the IS staff. As previously mentioned it is the top down support which will make this program successful.

The cost of war on security

Before embarking up the management ladder with the idea of getting an increase to the security budget it would be more prudent to have the cost increases and reasoning down first. Of course the $64,000 question is how much it will cost to have IS staff in place? The suggestion here is to not actually hire new employees but to use existing employees. This is not a fulltime job, rather added responsibilities for an individual. While reviewing the requirements form in the previous section you will notice that much of the time the IS staff is involved with security awareness or the promotion of security.

The awareness initiative is nothing more than an extension of what the ISO/security officer is already doing, the main difference is that awareness and security auditing is done using IS staff. This limits having to send out global awareness to the entire organization which again, referring to social engineering would most likely be deleted without being read, one caveat of too much information.

As a recap let us say that you have the policies in place, and you now have an army of Information Security staff members with their marching orders. There will come a time to determine what the IS staff will get for this extra duty; be it a pay increase, a yearly bonus or just a nice coffee cup with an informative Security Awareness phrase printed on the side. This, of course, must be worked out with your IS budget and upper management. In my organization we use the annual bonus method. My reasoning behind the bonus suggestion is that many of the functions of the IS staff entail record keeping and annual security assessments and reviews. The bonus would serve as the incentive to do the extra duties asked and complete but can be held back for failure to complete assignments.

There are other considerations which I have listed below. It is important to remember that an IS staff member must have the same interest of the company in mind as the ISO.

- An IS staff member should not be a contractor.
- It is preferable to have a salaried instead of hourly employee selected as an IS staff member.
- It is advisable to have a backup IS staff member.

An example of time spent by the IS staff is shown below. Of course these are simplistic measurements which you and your organization might do

differently. The object here is to show that the extra work done by the IS staff need not be all encompassing and the selected IS staff member should be able to incorporate this time without being a burden.

HOURS ANNUALLY	TASK
80	**Two semi-annual PC audits (**should be automated for on-line input**)**
40	**Random PC audits (**should be automated for verification only**)**
4	**IS staff meetings**
8	**Annual ISA Security Audits**
16	**Security policy enforcement**
16	**Information dissemination**
4	**ISA Training**
168	

There are two or more tasks which can be automated or created on-line greatly reducing time spent.

Once the IS staff has been formalized they should introduce themselves to their respective department of coverage. A sample email might look like the following:

> I would like to officially introduce myself to all of you as your IS staff member
>
> I will be working with you and will require your assistance to comply with the corporate policy of information security awareness and to ensure compliance with them.
>
> Some of my responsibilities are getting answers to your security questions; sending you emails periodically to reinforce our awareness of information security; working with the managers for quarterly reports and also conducting Office Workstation Audits (OWA's)
>
> For those of you that do not know what an OWA is: an unannounced time is chosen when the IS staff member and manager or their designee will inspect each person's workspace to see if they are following company guidelines: some of which are (1) if a drawer or file has a lock then they should be locked, (2) not leaving confidential material out in the open; (3) keys are not accessible, (4) locking up laptops at the end of the day, they are not to be kept in their docking station. And also during the course of the day if you leave your workspace, use the control-alt-delete keys to lock your keyboard.
>
> I take my responsibilities seriously and ask for your support in making my job easier by having everyone follow the corporate guidelines.
>
> I am located on the west side of Building 1 on the third floor. If you have any questions, please stop by to see me or send me an email.
>
> (Your Signature)

Tracking the Army and their orders

In the design of the database you will have, of course, fields of information. Generally speaking these fields will be used in some form or another for lookups, searches and reporting. The old cliché of garbage in garbage out always applies to database design and careful considerations should be used. Consideration for access to the data must be done. I recommend that access be done through intranet links for ease of administration, support and overhead. A web based database or at the very least, the ability to view the data using URL's will make your life so much easier. While this could be done with web server architecture you might decide on another platform such as SQL. Any design should be flexible enough for modifications later; after reading the following sections relating to data in and data out, you should have a better idea of the platform to use.

The first and foremost important records in the database will be that of the Information Security Associates (ISA's).

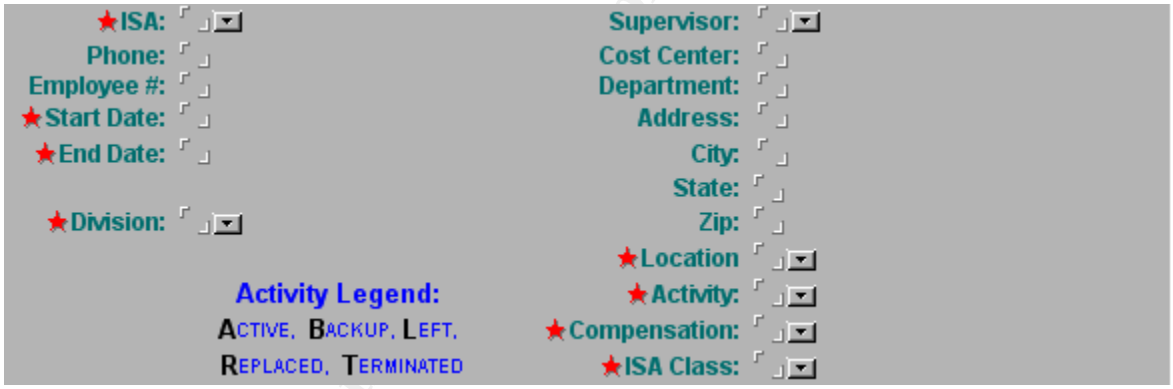


Table 4 (Sample ISA record)

The fields provided should be as follows:

ISA Field: Last Name, First Name or one field with First and Last name.

Note: It is very important that the name field or fields be connected to the local email system. The database should have the ability to do an address lookup of the name and be able to be pasted into the field(s). The field(s) should also be upgradeable in the case of a name change but permanent in the case of a terminated name. Sometimes when you have a terminated employee the mailbox is hidden for a determined amount of time. While the policy at your company may differ, you do not want the name to disappear from the record or the record to be completely deleted due to the need of maintaining permanent records for audit purposes.

As in Table 1 above, note three important requirements for the records. The first requirement is the necessary fields of information needed to keep track of the associates. The second requirement is the ability to use pop-downs within the fields making it easier to populate with correct information when updating records. The third requirement I required in the design of this database as noted previously, is the ability to pull data from the email system address books within the company. See the important notes above.

These are the fields that I have found to be very helpful which I will explain why, when and where used.

1. Address, City, State & Zip – From the obvious there may be other reasons to have these fields. One reason is that the organization may have several regional offices spread across the US or worldwide. The field's value is for keeping track of where all the associates are located which will help you when you need to find the pockets lacking security coverage.
2. Location – The location field might be a building number, cube location or some other identifiable text. Whatever works for you, but will also come in handy.
3. Activity – use the Activity field to denote whether the ISA is compensated. In the case of them being a manager or backup, they are not compensated. Also determine if this person is still an active ISA, left the company or termed. Again this will be helpful when sorting, archiving or reporting from the database. These are only suggestions but here is the legend I use.

    a. (A) - Active and is compensated
    b. (B) - Backup ISA and is not compensated
    c. (L) - ISA has left the company and is not compensated
    d. (R) - ISA has been replaced by another person in the department and is compensated using a prorated formula. (see note below)
    e. (T) – The ISA has been replaced by another person in the department and is compensated using a prorated formula. (see note below)

- **NOTE:** For a, d & e above the ISA should be compensated for work done up to the last day of time served. If you decide to compensate the ISA's with a bonus which I highly recommend, the prorating is as follows. It does not matter whether you use the fiscal year or calendar year, the basis is the same. The ISA should be compensated for the amount of time served (in months) and as a rule the starting date and ending date should be rounded up or down to the 15th of the given month to make it easier to do the calculation. So if an ISA started in August of a given year and your fiscal year (for this example) ends in September of the same year, then the ISA would be compensated for one month of service, or August 15th to September 15th. Then you would take the annual compensation amount;

divide by 12 which will give you the monthly amount. In the design of the database it is a good idea to design this field in real time and always show the compensation amount based on the Start Date in Table 1 above. This will save time and allow you to use this field in your views and reports later.

4. ISA Class – This simply put is just a yes or no to keep track of who has or has not had training yet. It makes tracking easier and you should be able to generate a report using this field.

This is the basic structure of my data requirements. Yours may be different or even expanded. The point to remember here is what data you need and what you will need for reports.

Tables, views and data – Oh My!

As with any database the queries or reports are only as good as the data in the database. The next phase in the design is the output. Unless you are using a DBMS which has an easy to use report generator then save yourself some time and plan what data to report on and how it should look. Listed below are examples of simple column reports I use and why.

1. ISA by Last Name – This view will be used by all employees and could contain columns such as phone number or extension, department name, location and other useful information. It is also a good idea to include the cubicle number or mailbox. Anything that will let the employee know who the ISA in their area is immensely helpful. Even with all these tools in place, you will find that there will be some people that when you ask, who is your ISA, their response is "I don't know".
2. ISA by Department – This view is like the previous "by Last Name" view but using the location field as the criteria. This will also come in handy letting employees know who their ISA is.
3. SA by Location – Another example of "Last Name" and is particularly handy if you have regional or satellite offices.
4. ISA Needing Training – I use this view to keep track of new ISA's that have not had training. This field is generally not referenced that often and I prefer to train ISA's when there will be more than two in attendance.

I would like to note here that having a security force of ISA's is a significant leap forward when building your Army of recruits. While a good training program will be necessary for the ISA's you should also consider extending training to all employees. An employee training program will not cover the detail or be as comprehensive as the ISA training program but still has its purpose and can only enhance the Awareness program initiative. Suggest to the ISA when they have their staff meeting within their departments that some time is devoted to talking

about information security, have handouts, show videos, questions and answer sessions, all focused on bringing security awareness to everyone.

In the past the training methods used may have been a meeting using slides and also a phone conference if they were not available to attend in person due to location. While this technology was useful in it's time, there are companies which can now offer training online. If your company does have the budget or applications development staff for internal design, these alternatives should be looked at. I have included some of these in the reference section[8].

An important addition to the database will be to include some sort of tracking system for the Office Workstation Reviews. As mentioned earlier in the functional description of the ISA, Office Workstation Reviews (OWR's) are to be done for each employee at least twice a year. To make this easier for the ISA to enter and the ISO to keep track of, the database will need the ability of input, collect and later report on the data. I will not go into design here except to keep with what I have mentioned previously. Once in awhile it may be necessary to remind the ISA's that the performing and tracking of the OWR's is an audit function and so the ease of tracking is important. As with the previous views I have listed some examples of how the database may be used to track the Office Workstation Reviews.

1. Completed OWR by Failed – The capability of reporting on a failed OWR will help the ISO to know when to follow-up and where your weak areas are. As there will be more work involved when using this view, the more work and thought used in the initial design should make it easier all around. It should also be mentioned here that the manager of the employee with the failed review should counsel them and plan for a re-review. Management involvement is a big key to the security process and awareness.
2. Completed OWR by ISA – With a count function this view can give you at-a-glance snapshots of how the ISA's are doing.
3. Completed OWR by Manager – Not to be redundant but there will be occasions where the manager will want to know how their ISA is doing. It would be a good idea if you can have one view with various sorting functions

Management Reporting

During the course of the year and as noted in the ISA functional description mentioned earlier, there will be reports due from the ISA's. The importance of these reports will vary from one company to another and will depend on if you have a compensation program in place. In the company I work for these reports are factored very heavily for compensation. In a nutshell, if the ISA completed all the duties listed in the functional description including their quarterly report and the Annual report for the managers; which I will explain below, then they would get compensated. It is a very rare case that this is not

done so you should carefully consider the ISA incentive be it a bonus, a few extra days off during the year, or others, you get the idea.

- ISA Quarterly Reporting – In the functional description noted earlier you see that there are very specific duties performed regularly by the ISA's. Any of the awareness tools that the ISA used during the quarter should be noted on their report, be it email notifications, security posters, meetings, etc. They should make note if there were any incidents or security deficiencies that need to be addressed and were corrected or need to be corrected. Everything the ISA did to promote and enforce security should be noted.

The ISA's quarterly report is like a journal, keeping track of their promoting security awareness. There may be times when the ISO requires additional information such as the number of PC's in a given area. With larger companies where the landscape changes almost daily, for example laptop users, developers and testers, the ISA should be aware of their area and can report on the changes. And there will always be personnel changes and it is important that the ISO be updated.

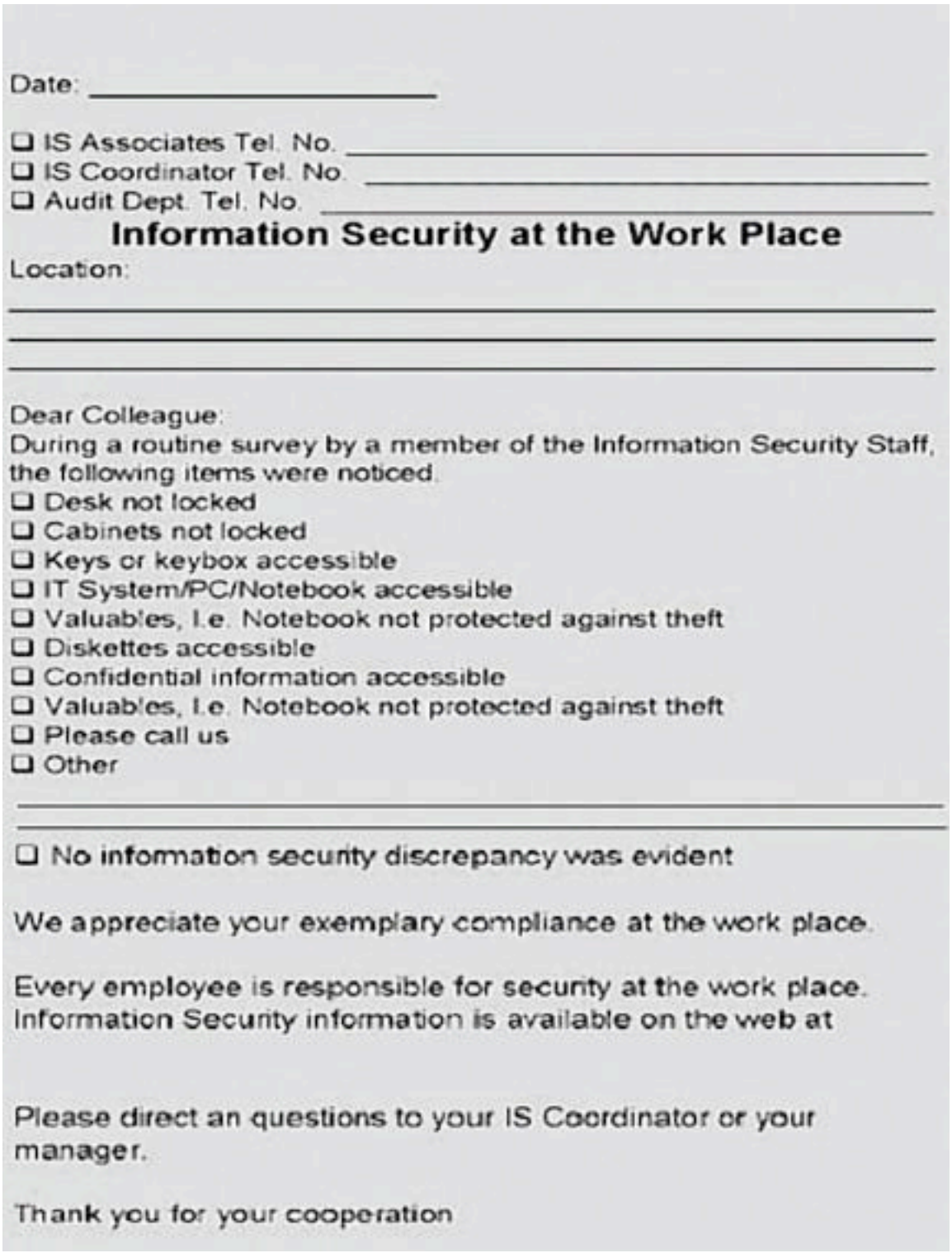
The bottom line is, if there are any questions that the ISO must report on and that information is communicated from the ISA's on their quarterly report, it makes everyone's job easier to have the quarterly report designed to include those questions that always need answers. Knowing the security health of the company is very important to the ISO/CIO and you will find that your Army of ISA's will be very helpful when compiling the information to provide company wide answers.

- Office Workstation Reviews – Again referring to the functional description; the Office Workstation Reviews is the most important awareness tool in the security toolbox. The policy used at my company requires that the ISA & manager perform these checks twice per employee per year. Your database should have a tracking mechanism to provide reports once the ISA enters these in. While the reporting on how many were done on a given time is valuable to the auditors, the real purpose of the OWR's is to instill the security requirement on the masses. This is done, not always with the "slap on the wrist" attitude but more as repetition or awareness attempt to change the social engineering.

While designing your database be sure to have the ability of tracking those that pass as well as failed reviews. This would be necessary to see at a given moment the failed OWR's so the manager can go back and pass a failed review. This should be a policy item and done within a short period of time, a timeframe of no more than 30 days. Another policy insert should include HR action after a

third failure. I am glad to say in my own experience this has never had to be done.

The form below (Figure 1 is a good example of what will be checked during the reviews. This of course is only an example and with very general security requirements. An ISA does the review, fills out the below form and leaves it at the reviewed employees workstation. I find it easy to have the form printed using post-it notes format so it can be left on the monitor of their pc. A distinctive fluorescent color so it stands out is also helpful to use. Once the employees know that they will be reviewed and you check off the "No information security discrepancy was evident" and a handwritten note of GOOD JOB, they get a sense of accomplishment that they are following the company standards. No one likes to receive a notice saying they failed.



Date: _____

❑ IS Associates Tel. No. _____
❑ IS Coordinator Tel. No. _____
❑ Audit Dept. Tel. No. _____

Information Security at the Work Place

Location:

_____
_____
_____

Dear Colleague:
During a routine survey by a member of the Information Security Staff, the following items were noticed.

❑ Desk not locked
❑ Cabinets not locked
❑ Keys or keybox accessible
❑ IT System/PC/Notebook accessible
❑ Valuables, I.e. Notebook not protected against theft
❑ Diskettes accessible
❑ Confidential information accessible
❑ Valuables, I.e. Notebook not protected against theft
❑ Please call us
❑ Other

_____
_____

❑ No information security discrepancy was evident

We appreciate your exemplary compliance at the work place.

Every employee is responsible for security at the work place. Information Security information is available on the web at

Please direct an questions to your IS Coordinator or your manager.

Thank you for your cooperation

Figure 1 (Sample OWR punch out)

Conclusion

Security auditing and awareness need not be an over taxing and expensive proposition. The cost of Information Security must be measured often and adjusted accordingly. Creating an army of deputies and having them strategically placed throughout the organization is the same as police situated in large cities. We have learned that you cannot have one police station in the center of a metropolitan area and hope to serve those on the outskirts. In the case of the police presence, they end up with satellite offices thereby serving and protecting a smaller area.

So why is the security presence in a global company any different? Let's say your company has two or more offices which the ISO must visit occasionally. Like the Internal Audit department they must go where the audit will take place so naturally there will be travel expenses. If you already had an IS staff member located in those offices then you should already have a snapshot of the health of security in that office. Of course I am not saying that the ISO will not have to travel anymore but at least the audits can be fewer.

It really is simple mathematics. How many laptops will get stolen because the general population did not know the policies about laptop security in place? Or let's say that the general population does know about the policy but a recent addition to the policy changed to make it necessary to have the laptop cable locked during the day had not been announced yet. With an IS staff member in place, the message can go further and have more impact when it is more personal and the active ISA makes their individual department aware of the change, the change can have immediate impact and you have accomplished security awareness throughout the entire company.

References

1 “Building an Information Security Awareness Program” by Mark B. Desman, Auerbach Publications.
http://www.auerbach-publications.com/home.asp

[2] HIPAA (Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 and Administrative Simplification (26 Kb)
http://dchealth.dc.gov/hipaa/hipaaoverview.shtm

[3] Table1: Impact of Recent Information Security Legislation BSA (Business Software Alliance) Information Security Governance: Toward A Framework for Action (October 2003)
http://www.bsa.org/customcf/popuphitbox.cfm?ReturnURL=/resources/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=5841

[4] Your Window to Information Security Policies and Disaster Recovery
http://www.yourwindow.to/

[5] RUSecure policies are of the highest standard - and they are fully compliant with the international security standard, ISO17799!
http://www.information-security-policies.com/index.htm

[6] Writing an Information Security Policy. by Mr. Avinash Kadam (Published Network Magazine - October 2002).
http://www.networkmagazineindia.com/200210/security2.shtml

[7] Department of Homeland Security (DHS)
http://www.dhs.gov/dhspublic/display?theme=29

[8] Inspired eLearning – all-inclusive turn-key, enterprise security awareness program trains your employees to protect your network against security breaches and keeps them security aware through ongoing awareness programs.
http://www.inspiredelearning.com/sat/

[8a] Easyi - All Easy *i* programs are fully customizable. All web-based training courses are provided with a standard edition of our own user-friendly Learning Management System (LMS) enabling you to track and administer training.
http://www.easyi.com/topics/software_is.asp

Additional resources:

Building A Security Awareness Program – Addressing the Threat From Within – By Gideon T. Rasmussen
http://www.cyberguard.com/news_room/news_newsletter_030926threatwithin.cfm