Global Information Assurance Certification Paper

"I don't care what the Information Security Officer says!":
Implementing Information Security in a hostile environment.

SANS Security Essentials
GSEC - Practical Assignment, Version 1.4b, Option 1

By Douglas J. Kersten

10 December 2003

Abstract

Difficulties will always be encountered when implementing a comprehensive information security program. The problems encountered range from executive 'buy-in' to budgetary concerns to technology and training issues. So what do you do when the worst of all of these problems combine to create an environment that is openly hostile[1] to information security? How do you, as an information security professional, overcome the obstacles laid before you and succeed in implementing a security program that addresses the risks that are facing your company? This paper attempts to address these issues by combining existing techniques and processes, in unique ways, that you can follow to succeed. It also lets you know when to call it quits and move on to a place where the implementation of a good information security program is truly desired.

Introduction

There are four main issues that will effect every decision that you make when you address information security. According to Rick Doten, Director of Netsec, Inc., "...these four issues are resources, time, money and politics"[2]. Usually you will have severe problems with one of these areas in your work environment, possibly two. What do you do if you have severe problems with every one of these issues? How do you move forward with a standards based information security program when all of the components required for you to accomplish your security goals are arrayed against you? Facing this issue can be a daunting and discouraging task.

The first thing that you need to do is determine why the hostility exists. You need to do this so you can concentrate your energies and overcome the hostility. This is not as easy as it may seem. The second thing you need to do is prepare. This means that you gather the information that you need to push your plans forward. The third thing that you need to do is implement. This step can be the trickiest or easiest, depending on circumstances that you are in and the support that you can garner. The goal of the entire process is to reduce the hostility in your particular environment to such a degree that you create a self-sustaining security culture in your organization.

---

1 Merriam-Webster (hostile), hostile: **c :** openly opposed or resisting <a *hostile* critic> <*hostile* to new ideas>.

2 Doten.

Determining the core reasons for a hostile environment.

A hostile environment is usually the result of one or more of four conditions. These four conditions are politics, ego, culture and ignorance. When you are attempting to focus on the source of hostility you must always keep these four conditions in mind. Some are easier to negate then others and sometimes they play off of each other in strange and interesting ways.

Politics

Politics is defined by the Merriam-Webster Online Dictionary as, "a: the total complex of relations between people living in society, b: relations or conduct in a particular area of experience especially as seen or dealt with from a political point of view <office *politics*>"[3]. It is normal in a corporate environment for employees to align themselves to a political norm that favors their work and the need for their job to exist. In many cases people develop political allegiances to reduce the amount of work that they have to perform. In other cases allegiances are developed to further careers. In still other cases allegiances are developed to protect individuals who are perpetrating wrongdoings. Delving into the politics of an environment can be a tricky task because there can be intricate connections between different departments and individuals. The key to politics is patience and networking. Gaining trust and confidence can yield extensive dividends on this front.

Egoism

Egoism is defined by the Merriam-Webster Online Dictionary as, "a: a doctrine that individual self-interest is the actual motive of all conscious action, b: a doctrine that individual self-interest is the valid end of all actions"[4]. It is one of the worst scenarios to be in where conflicting egos are warring. This type of conflict can lead to the most illogical decisions on the part of management. Sometimes these decisions can border on the criminal and being aware of ethics and making ethical decisions should help you in this area. The easiest way to deal with an ego that is permitted by management (for reason of profits, when the person is a founder, legal requirements, etc.) is to stoke it. This can be a distasteful task and sometimes it is better to deal with ego in other ways. Possible ways to do this would be avoidance, negation by working with a bigger ego or intimidation by involving multiple supporters of your argument. Following this alternate path will require more effort and skill but could also be a more permanent solution.

[3] Merriam-Webster (politics).
[4] Merriam-Webster (egoism).

Culture

Culture is defined by the Merriam-Webster Online Dictionary as, "c: the set of shared attitudes, values, goals, and practices that characterizes a company or corporation"[5]. It is the working environment that is created at a company. This environment can be based on several things and is usually embodied in stated policies and mission statements of the company. Sometimes ego can become so overpowering as to overwhelm culture and even come to represent it. Culture can be changed but it requires managerial 'buy-in' and in a hostile environment that may be difficult to obtain. You can encourage and develop 'buy-in' by using security awareness training and other tools to allow management to feel that the required changes are of their own doing, which is always a good approach in a hostile environment.

Ignorance

Ignorance is defined by the Merriam-Webster Online Dictionary as, "the state or fact of being ignorant (ignorant is defined as 2: unaware, uninformed)"[6]. You can vanquish information security ignorance with security awareness training. In a hostile environment a formal training program can be difficult to implement. You should make every communication opportunity a training experience. You should take advantage in every meeting that you attend, putting forth a security problem and making note of the solution (which you base on your awareness training goals). After constant reinforcement eventually you will hear others voicing your ideas. Make sure that you give them credit for the idea expressed and then use their names when moving forward with the idea. This gives the idea third-party merit and brings those individuals further into the security process.

Keeping an open mind and listening will have better results then any other method when you are trying to determine the cause of a hostile environment. Even if all that you do is determine that you will never garner support from a particular direction it is still valuable information. You can spend your time wisely by working with individuals that are more likely to support information security goals and leave the unenlightened manager as a challenge that will be easier to meet once you are more established.

[5] Merriam-Webster (culture).
[6] Merriam-Webster (ignorance).

Preparing for Information Security Program Implementation

Preparing to implement an information security program requires a lot of work. The problem is that in a hostile environment it can be difficult to get the permission required to move forward with this work. The preparation required in a hostile environment is different then in a semi-supportive to supportive environment. You are required to be more inquisitive, investigative and subtle then you normally would have to be. You also have to make sure that you do not cross the line and do something that would put you in a bad moral position. You must never lie about anything that you are doing or planning when confronted directly and you must always work in the best interests of your company and profession.

Why you were hired

Even though the environment that you are in is hostile to your efforts there will be a valid reason that you were hired as an Information Security Officer or Professional. It is your job to determine that reason. Usually it has to do with auditors, a board of directors' demands or a new law, regulation or guideline.

Some of the laws or acts that could be used to justify hiring an Information Security Professional are the Graham, Leech, Bliley Act (GLBA), Sarbanes-Oxley and HIPAA. According to the FTC Privacy Initiatives website, "Under the Gramm-Leach-Bliley Act, the Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information."[7] According to the article 'Security and Sarbanes-Oxley' on SeachSecurity.com, "What the law will likely do is open a dialogue between upper-level management and their security staff on what is needed to ensure that proper and auditable security measures are in place. The executives who have to sign off on the internal controls have a lot to lose if things aren't kosher; they could face criminal penalties if a breach is detected."[8] Jonathan Bogen wrote in his white paper titled 'HIPAA Challenges for Information Security: Are You Prepared?',"The standard is a compendium of security requirements that must be satisfied. The solution will vary from provider to provider, but each provider must meet the basic requirements."[9] Clearly these laws and acts would justify hiring an Information Security Professional.

There are many examples where auditors could be the reason that you were hired. By enforcing guidelines based on legislation and regulations an auditor would be inclined to require the employment of a dedicated Information Security Professional. A good example of this type of guideline is the FFIEC Examination Handbook where it says, "Senior management should designate one or more individuals as information security officers."[10]

---

7 FTC Privacy Initiatives.
8 Hurley.
9 Bogen.
10 FFIEC.

As soon as you have determined the reason you were hired you have an in. You can use this in as leverage to justify your actions. You can subtly bring to management's attention that a policy or procedure would meet an audit requirement or fulfill the requirements of a law or regulation. Management does not necessarily have to know that you know the reason you were hired. In a hostile situation it would probably be more beneficial to you if management did not know because it could be turned around and used against you. I have actually heard management say, “I know that it would fulfill the requirements for this regulation but for what other reason should we do it?”, and then shoot down the idea. For this reason it is a good idea to keep this knowledge to yourself.

Doing your job

You should determine exactly what is expected from you in your job. Usually you will find that the work assigned to you does not accomplish much and is simple to do. By completing this work and moving past it quickly you give yourself time to work on a real security program while placating your detractors. You can also use this ‘make-work’ and transition it into real solutions to real problems.

Policies and procedures that support you

You should determine what existing policies and procedures support the objectives that you want to accomplish. Most companies have some components of an information security program in place. These components are usually the result of standard practices (for example access-control on a Windows server) but are usually implemented incorrectly and without the correct focus. By speaking directly with the system administrator or operations person you can get them to tweak their procedures enough to implement a policy that would normally require a knock-down drawn out fight. In a hostile environment something simple, like password aging, can be a big issue. Even if you have proven the need, with risk analysis, management may still refuse to mitigate or take responsibility for accepting the risk. Since management, in this case, does not truly care for information security they will usually allow a system administrator or operations person to work in any way they choose. If you can convince that person to work in the correct way you have successfully implemented policy.

Knowing your supporters

You should determine who your supporters are. You may be surprised during this process to find out that someone that you think would logically support you does not. Just because someone is not openly hostile to you does not mean that they support you. A good example of this is a case where your boss, while working with you, does not support the creation of your position or the work that you do because he or she finds it unnecessary or feels that the work is already being performed by others. This may even be the case but an Information Security Program should be focused and controlled not distributed and disorganized. Knowing that your boss feels this way should change the way that you approach him or her. Reinforcing the importance of what you are trying to accomplish should overtake the assumption that there is an automatic agreement on issues. Knowing your true supporters will allow you to know how to proceed when dealing with them to accomplish you security goals.

Information Security Policy

You should develop an 'Information Security Policy'. This may be easier then it seems. Management usually likes to "appear" to be involved and supportive of information security programs. In fact managerial involvement is required in many laws, acts and regulations. An example of this is Sarbanes-Oxley. On Searchsecurity.com writer Edward Hurley quotes Mr. Saidman,an attorney specializing in information security. Mr. Saidman says,"Yet in the law [Sarbanes-Oxley] there is a provision mandating that CEOs and CFOs attest to their companies' having proper "internal controls."[11] A good way for management to look involved is for them to approve an 'Information Security Policy'. Most times you do not have to encourage this in any way. In fact most managers will immediately see that supporting a policy will make it look like they are supporting a program, even if they are not. When you develop your 'Information Security Policy' make sure you base it off of a standard (like the Information Security Forum's, 'The Standard of Good Practice for Information Security'[12]) or, at a minimum, the policy of someone that is in the same business that you are in. This way you can justify anything contained in the policy by referring it to the third-party standard or policy. This distances you from the wording of the policy because, in a hostile environment, the hostility is usually placed towards what you have personally developed (your judgment is called into question). Using a third party as a reference you can make it look like someone else has developed the ideas while at the same time progressing towards your goal of a self-perpetuating security culture.

[11] Hurley.
[12] ISF.

According to the October 2003 ISSA Chapter Meeting presentation by Claude Brogle titled 'Enforcing Network and Security Policies', your Information Security Policy framework should be as complete as possible and the policy should be:

- Created by a cross-functional team from the IT Department, Human Resources, Legal and Business Units.
- A collaborative document that contains:
    1. *Policy Statement:* concise purpose of document that is applicable to the enterprise and industry. Should be controllable and enforceable
    2. *Scope:* Type of information covered by policy (i.e. electronic, intellectual property, etc.).
    3. *Roles and Responsibilities:* Define roles of employees, management and system administrators.
    4. *Security Practices:* Core of the policy that offers detailed security practices.[13]

You may have noticed the 'working cross-functional team', 'controllable and enforceable' and 'collaborative document' statements in the above bullet points. These are very difficult subjects to broach in a hostile environment. You should do the best you can in this case and use the supporters that you discovered in the prior recommendation. The Information Security Policy does not have to be perfect, but it does have to exist. It is going to be your "constitution" and the base that you use to grow your program. You should also try to get management to approve the Information Security Policy (ultimately this will be a requirement). Putting the policy before management can also be used to determine if politics, egoism, culture or ignorance (or a combination) is at the core of the hostility. If the management immediately approves your policy without discussion or argument then ignorance is probably a factor.

You should be thorough in your preparation and realize that it is going to take time. Working subtly, quietly and efficiently will allow you to place the foundation of your information security program into place without facing the hostility face on. It should always be in the forefront of your mind that the hostility is, more often then not, caused by a lack of understanding. This lack of understanding could be on the part of the political structure, the egos involved, the culture itself or just plain ignorance. Enlightenment is your goal and for some this may never happen. If it does not happen with any, or just a minority, of the involved parties then it may be time for you to seriously think about whether you want to spend time fighting a losing battle.

[13] Brogle, p. 5.

Implementing the Information Security Program

Driving Change

Once you have finished your preparation you should begin to move forward with the implementation of your program. At this point you should know who your supporters are and have possibly educated some of you prior detractors sufficiently enough so that you can depend on them in some situations. You should begin to drive change by picking your battles. You want to pick battles that will have the biggest effect (mitigate some of the biggest risks) while costing a minimum amount in terms of dollars, time and political capital. Remember this is a hostile environment and you are having problems with resources, time, money and politics. You should use every tool in your arsenal (supporters, laws and regulations, third-parties, your information security policy, prior successes, etc) to move forward. Your goal is to build momentum and kick-start the creation of a self-sustaining security environment in your organization.

The Three E's

You should begin to encourage compliance with the Information Security Policy. You can do this by implementing the following cycle put forth by Claude Brogle in his presentation 'Enforcing Network and Security Policies':

Educate
- Create a security awareness program.
- Educates the end-user on what is right and wrong.

Engage
- Engage InfoSec/IT/NetOps as well as HR to create and maintain a policy driven secure environment.

Enforce
- Enforcement should be done proactively, real-time and post-event
- Written procedures and points of escalation are well-defined and utilized when necessary.[14]

Since you are working in a hostile environment it will probably be impossible to set up formalized training. Instead use the tools that you have access to: email, phone and your voice to train employees and management. E-mail a weekly security tip that you take straight out of the security policy. Use virus alerts to inform users not to open emailed files that they don't expect to receive or from someone that they do not know. Talk to employees on the phone and face-to-face about security issues. These are not necessarily the fastest or easiest ways to train but they are effective and raise awareness.

[14] Brogle, p. 7.

Engaging IT, Network Operations and Human Resources usually should not be a problem since they have many of the same goals that you do. IT and network operations usually understand that by implementing security policy their jobs actually become more interesting and easier. IT and NetOps find it more interesting because they can work on new technologies and easier because the responsibility for security gets moved outward, to the business owners and users. Human Resources should already be doing what is required by information security, namely background checks, distributing policy information, ensuring that users who are terminated or transferred have access quickly removed, etc. If you initially get resistance from these departments by the time you are ready to implement your program they are usually on board, or soon thereafter. Since they are not profit centers they are more likely to see the relationship between increasing information security to their own job security.

Enforcement will be the most difficult of the three E's. Remember that enforcement does not always mean punishment. Many times just pointing out to a user that they are doing something incorrectly will cause them to change their actions. There will always be a few who chose to ignore policy. For these few you slowly escalate enforcement actions. It is a good idea to follow the following process:

1. E-mail the user with your concerns.
2. Speak to the user directly.
3. E-mail the user and their manager.
4. Speak with the user's manager.

You should never threaten the user or manager at any point in time. Treat the opportunity as a training matter and be fair and clear in you concerns. Following this process will build respect for you and your methods with the manager and, hopefully, the user. They will understand that you are trying to help instead of trying to punish and will be more willing to work with you in the future. You may not get the results that you hope for even after this careful, cultivating process. If you are totally ignored by all concerned then document what has happened, send copies to all concerned parties and file the documents away. Doing this you make sure that management is aware of the risk that it is taking and they can't deny that they did not know the risk existed if something goes wrong. You should be aware of the formal disciplinary actions available at your company and if the violation is extreme it is in your best interest to initiate the disciplinary process on your own, even if it causes some of your carefully cultivated relationships to go sour.

Working with the difficult

The prior section covers some techniques for working with difficult users. Working with difficult managers requires a little more finesse. Getting a manager to participate in the security process is essential. If you have ten managers on board and the eleventh refuses then the eleventh manager is your weakest link. If the situation is so bad that the manager refuses to participate in any way then you should treat that manager and his people as an untrusted entity. This means that you develop policies and procedures that isolate the particular department as much as possible from your main network. You basically treat that department as if it is a public network, like the Internet, and act accordingly. Of course this requires that you have built up to support necessary to accomplish the task. If you have not then your only recourse is to document the risk, distribute the document and file the document until such time as you have built up the necessary support to manage the risk correctly. Other techniques include meeting with the manager, with supporting managers in attendance, and taking as much time as necessary to instill understanding. Usually Compliance, Audit and Systems are good at expressing the logic behind information security policies and procedures. There are times that you will be asked to compromise. If the manager is willing to take responsibility for the risk involved then you should compromise but make sure the agreement is clearly documented. If you feel that the risk is to great make sure that you make this clear and make sure that the manager's superiors understand the risk that he or she is taking on.

Enterprise Risk Management

It is important that your Information Security Program is based on the management of risk. According to searchCIO.com, "Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings. Enterprise risk management expands the process to include not just risks associated with accidental losses, but also financial, strategic, operational, and other risks."[15] I have used this definition of risk management because it includes what most definitions do not, the recognition that the organization's capital and earnings are what allows the organization to exist and should be center of your security efforts. Information Security does not only deal with the technical aspects of a business. It also deals with financial, strategic and operational areas of the business. If you only focus on the technical aspects you are sure to be attacked from a non-technical direction. Competent hackers tend to attack at the point of least resistance and do not limit themselves to one avenue of attack. You should prepare in the same way.

[15] SearchCIO.com.

In a hostile environment it is even more important that you base your actions on the management of risk. Business owners can understand this method since most business decisions are not made until after all of the risks have been analyzed. If you present your arguments in terms of risk and use clear and understandable metrics to back up your recommendations it will be that much harder for a difficult manager to work against you. The worst that can happen is that the risk is not addressed in any way, either by mitigating it or accepting it. If this occurs then you are in a good position, but your company may not be, since you have documented that you have made management aware of the risk and it was their decision not to act.

You may have noticed in the last paragraph the term 'accepting risk' was mentioned. It is not necessary to mitigate every risk. In fact mitigation of some risks may be too expensive in terms of time, money, effort or complexity. In these cases knowledgeable management will not attempt to mitigate the risk but instead will accept the risk. Accepting risk means that management must clearly understand the risk and formally declare that they accept it. It is your duty to create that understanding and present the consequences. It is management's duty to agree on a way to mitigate the risk or to accept the risk. It is best practice to have both parties document that the outcome is acceptable. If management fails in it's duty then it is up to you to at least document what has occurred. If the risk is great you may wish to ensure that the risk is mitigated in some way. This is the difference between a hostile and non-hostile environment. In a non-hostile environment you would never take it on yourself to mitigate a risk without the acceptance of management. Being placed in a position where, for reasons of due diligence, you are forced to mitigate risk in an unapproved way you may run astray of ethics issues. You should think long and hard before you go down this path.

The Endless Cycle

The Information Security Process is what I define as 'The Endless Cycle'. Information Security, by virtue of the Information Security Process, is an ongoing venture and validates the need for a strong Information Security Program. The Information Security Process is paraphrased here from the FFIEC IT Examination Handbook:

> The [Information] Security Process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify, measure, manage and control the risks to system and data availability, integrity and confidentiality, and ensure accountability for system actions. The process includes five areas that serve as a framework for the Information Security program.
>
> - Information Security Strategy [based on the Information Security Policy].
> - Information Security Risk Assessment [used to tune the Security Strategy].
> - Security Controls Implementation [based on the Risk Assessment].
> - Security Testing [testing the Security Controls and the validity of the Risk Assessment].
> - Monitoring and Updating [Reviewing and monitoring the whole process].[16]

Information Security, conducted in a good way, is a never-ending process. New threats and vulnerabilities are constantly being created and discovered causing the constant need to address new risks. When implementing your Information Security Program you should work towards making this a self-sustaining cycle. A self-sustaining security culture will continue to function on its own, without your guidance. Even in a hostile environment this requirement does not change. In fact, it may be even more important that you promote this. Open hostility tends to tear down security, which is why you must carefully plan to ensure stability. In terms of risk you could say that the hostile environment falls under the headings of a threat and a vulnerability. You can mitigate the effects of such a risk by following 'The Endless Cycle' and constantly reviewing the deteriorating effects of a hostile environment and then implementing change to counter it.

[16] FFIEC.

Facing Ethics Issues

You hear about ethics a lot in the news lately. Whether it is Enron, Tyco or Martha Stewart ethics has become a big issue. One of the core character traits of a person in the information security profession should be the placement of a high value on ethical conduct. Many information security groups and associations recognize this requirement by requiring you to agree to a 'Code of Ethics'. Some notable groups that promote a 'Code of Ethics' are SANS/GIAC[17] and the ISSA (Information Systems Security Association)[18].

Hostile environments are sure to put you in a place of ethical dilemma and you should be prepared to handle the situation correctly. Violating ethical principle should be avoided at all costs since it can put you and the people around you into uncomfortable situations, in the least severe cases, and in trouble with the law in the most severe.

Defining Ethics

Ethics is defined by the Merriam-Webster Online Dictionary as, "the discipline dealing with what is good and bad and with moral duty and obligation."[19] The ISSA Code of Ethics spells out clearly what ethics means in the terms of an Information Security Professional. Their code states the following:

> I have in the past and will in the future:
>
> - Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
> - Promote generally accepted information security current best practices and standards;
> - Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
> - Discharge professional responsibilities with diligence and honesty;
> - Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association; and
> - Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.[20]

---

17 SANS/GIAC.
18 ISSA.
19 Merriam-Webster (ethics).
20 ISSA.

It is your professional duty to conduct yourself in an ethical manner and by doing so you keep yourself on a moral high ground, thereby improving your ability to function in a hostile environment.

The gray areas of Ethics

There is a gray area in ethics that you need to be aware of. Some situations require you to make a decision based on an argument that looks like it could be justified ethically in more then one way. What do you do in a situation like this? The Small Business Administration (SBA) give the following guidance:

> According to Kenneth Blanchard and Norman Vincent Peale, authors of **The Power of Ethical Management**, there are three questions you should ask yourself whenever you are faced with an ethical dilemma.
>
> - **Is it legal?** In other words, will you be violating any criminal laws, civil laws or company policies by engaging in this activity?
>
> - **Is it balanced?** Is it fair to all parties concerned both in the short-term as well as the long-term? Is this a win-win situation for those directly as well as indirectly involved?
>
> - **Is it right?** Most of us know the difference between right and wrong, but when push comes to shove, how does this decision make you feel about yourself? Are you proud of yourself for making this decision? Would you like others to know you made the decision you did?
> Most of the time, when dealing with "gray decisions", just one of these questions is not enough. But by taking the time to reflect on all three, you will often times find that the answer becomes very clear. [21]

[21] SBA.

When Nothing Works

You may come to a place where you have tried everything in your power to implement a good information security program and nothing works. You may have followed every technique and process listed in this paper but find that you have accomplished nothing. You may find that management does not support you and that any work that you do accomplish is dismantled and you are constantly put in a position where you have to start over. In this case you are limited to "putting it on the line" and "knowing when to quit".

Putting it on the line

If you find yourself in a position where nothing works you may have to "put it on the line". By this I mean that you must put your concerns forward in a forceful way. You must walk into the office of the CEO, President or GM and present your concerns to him or her and then wait for an answer. If the answer is not a satisfactory one then you must explain why it not and wait for an answer again. You should only use this method when nothing else works because there is a risk that your career with the company may end. Usually only one of three things will be the outcome of this situation:

1. You will gain newfound respect and have a supporter in a high place.
2. Nothing.
3. You will lose your job.

The final outcome will make it clear to you what you should do next.

Knowing when to quit

It should be obvious at this point when you should quit. If you have done everything that you can and still have no support then you should move on. If you have been asked to violate an ethical principle or a 'law of the land' then you should quit. If you want to be a figurehead of course you can stay but then you are not really an Information Security Officer or Professional you are a figurehead and need to be aware of that. Putting yourself into the position of a figurehead means when the auditors or the law come to the door you are a culpable as the people they are coming to see. In fact, you may be the person that they are coming to see. In the best case you are working for a company that has placed itself in a position that lacks security but by doing so the company's existence and, by extension, your job may be forfeit.

Conclusion

Hopefully you will never be in a situation like the one discussed here. While the task may be daunting and discouraging the feeling of accomplishment that comes from implementing a self-sustaining security culture is worth the effort. The effort itself may take years to manifest itself into success so it is vital that you can see the path that you should be following. You should now have some of the tools and insight that you will need to approach the problems involved and succeed. In the end remember that the four issues of Rick Doten, "resources, time, money and politics"[22], are what is truly driving your information security environment and addressing these issues will move you a long way towards accomplishing your information security goals.

[22] Doten.

References

Merriam-Webster (hostile). “Merriam-Webster Dictionary.”
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=hostile
(08 December 2003). hostile: **c :** openly opposed or resisting <a *hostile* critic> <*hostile* to new ideas>

Doten, Rick. “Ten Components to a Wireless Security Policy.” – Presentation by the director of Netsec, Inc. given at the ISSA-NY Chapter Meeting, 11/19/2003.

Merriam-Webster (politics). “Merriam-Webster Dictionary.”
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=politics
(December 2003).

Merriam-Webster (egoism). “Merriam-Webster Dictionary.”
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=egoism
(December 2003).

Merriam-Webster (culture). “Merriam-Webster Dictionary.”
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=culture
(08 December 2003).

Merriam-Webster (ignorance). “Merriam-Webster Dictionary.”
URL: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=ignorance
(08 December 2003).

FTC Privacy Initiatives. “The Gramm-Leach-Bliley Act: The Safeguards Rule.” Privacy Issues. URL: http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html
(08 December 2003).

Hurley, Edward. “Security and Sarbanes-Oxley.” 25 September 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html
(08 December 2003).

Bogen, Jonathan. “HIPAA Challenges for Information Security: Are You Prepared?” 2001.
URL: http://www.healthcio.com/hipaa%20security%20update.htm
(08 December 2003).

FFIEC. “Security Process.” FFIEC IT Examination Handbook. URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/01_security_process.htm
(8 December 2003).

ISF. “The Standard of Good Practice for Information Security.” March 2003.
URL:
http://www.securityforum.org/ReportsLibrary2003/categories/summary/sum030301.htm
(08 December 2003).

Brogle, Claude. “Enforcing Network and Security Policies.” 14 October 2003.
URL: http://www.nymissa.org/documents/ISSA-_enforcing_network_and_security_poli.pdf
(08 December 2003).

SearchCIO.com. “Enterprise Risk Management.” SearchCIO.com Definitions.
November 7 2003. URL:
http://searchcio.techtarget.com/sDefinition/0,,sid19_gci508983,00.html
(08 December 2003).

SANS/GIAC. “GIAC Code of Ethics.”
URL: http://www.giac.org/COE.php
(08 December 2003).

ISSA. “ISSA Code of Ethics.”
URL: http://www.issa.org/codeofethics.html
(08 December 2003).

Merriam-Webster (ethics). “Merriam-Webster Dictionary.”
URL: http://www.webster.com/cgi-bin/dictionary?book=Dictionary&va=ethics
(08 December 2003).

SBA. “Business Ethics.” Growing and Managing Your Business.
URL: http://www.sba.gov/managing/leadership/ethics.html
(08 December 2003).