Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

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

# Recovering Security in Program Management

Many project management training courses include sound advice about incorporating security early in design and development. After project launch, good intentions can fall by the wayside as victims of schedule and cost pressure. Later in the project lifecycle, demands for certification and accreditation force project managers to recover security. This paper works through some of the challenges to rebuilding a reasonable security profile in an ongoing project and should be of interest to the person called in to fix secur...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

# Recovering Security

*GIAC (GSLC) Gold Certification*

Author: W. H. Thomas, thomaswh@va.metrocast.net
Advisor: Marc Westbrock

Accepted: 10 August 2012

Abstract

Many project management training courses include sound advice about incorporating security early in design and development. After project launch, good intentions can fall by the wayside as victims of schedule and cost pressure. Later in the project lifecycle, demands for certification and accreditation force project managers to recover security. This paper works through some of the challenges to rebuilding a reasonable security profile in an ongoing project and should be of interest to the person called in to fix security after the damage has occurred.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

# 1. Introduction

Few Information Security (InfoSec) professionals[1] get the opportunity to build a program from the ground up. Whether brought in to maintain, enhance, or fix an existing environment, most inherit a security situation not of their own making. Often, the situation exists in the context of a specific project that requires external recognition or validation of the security posture of the resulting product.

Characterizing the rebuilding of an InfoSec posture as a project has several advantages. Creating and packaging the InfoSec project proposal will require cooperation and consultation with other people in the organization. These interactions can be opportunities to gain allies in other departments and to learn more about other disciplines that affect the InfoSec goals. Presenting the project can be a general education opportunity to a broader audience within the organization. Within a well-defined InfoSec project, behavior modification efforts or new policies become more palatable as tasks leading to the accomplishment of larger project goals.

For the InfoSec professional coming into a new job or a new work assignment, the first order of business is to assess the situation. Careful listening and thorough reading, especially at the beginning, set the stage for defining an InfoSec plan that can execute as an independent project or as a viable sub-project within a larger project. With an understanding of the environment, people, and goals, the InfoSec challenges can be addressed methodically and dispassionately.

Modern InfoSec is often viewed as risk management (Stoneburner, Goguen, & Feringa, 2002). As a participant in the overall risk management for the organization, an InfoSec professional should be objective and risk neutral (Pettigrew & Ryan, 2012).

[1] Throughout this paper, the term Information Security (InfoSec) professional is used generically to refer to that person tasked with making or implementing the organization's security policy for information technology (e.g., Chief Information Officer, Information Assurance Officer, Information Security Manager, etc.)



© 2012 The SANS Institute Author retains full rights.

# 2. Recovering Security

## 2.1. Getting Started

If building or rebuilding a good InfoSec profile in an ongoing project is the job to be done, then determining the scope of the effort is an important first step. The answers to a series of common questions (Biafore, 2010) will help to define the boundaries and initiate the remediation. There are many ways to begin.

### 2.1.1. Defining Questions

***Where are we now?*** The answer to this question is intended to identify erroneous assumptions. The project journey begins here and ends with the accomplishment of some goal. If the InfoSec professional is not clear about the current state of affairs, then the map to the goal will be in error. Assumptions at the beginning of the project have a way of turning into expensive liabilities later, so only trust what can be proven and plan everything else as a task to be scheduled and executed.

***What do we want to accomplish?*** The goal of the project is important for many reasons. A clearly stated goal acts as a litmus test for determining whether an activity should be part of the project or not. A well-defined goal describes the end of the project. A measureable goal is not subjective. A goal should also be positive, specific, attainable, and challenging.

***How are we going to do it?*** Answering this question is where the InfoSec professional as project manager can bring all that training and experience to bear. Knowing the starting and ending points are important, but choosing the path to get from one end to the other requires an understanding of the solution space.

***Why are we going to do it?*** There should be no ambiguity in the response to this question. A clear and succinct answer should relate to the larger project goals and the organization's vision. It has to make sense to motivate cooperation.

***When will the project begin?*** Every project should have a definite beginning and end (Project Management Institute, 2008). Rebuilding InfoSec may be an immediate start or it may make sense to time the kickoff with the next iteration of a planning cycle of the



© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

larger project. In either case, a strong start will help the team and organization reach the InfoSec project goals.

***When will the project end?*** Again, every project should have a definite beginning and end (Project Management Institute, 2008). This question might seem strange in the InfoSec context because the intent is to build up security and that job never ends. The answer to this question is mainly one of perspective. A seemingly unending barrage of demands for behavior adjustment (longer passwords, unattended smart cards, password protected screensavers, etc.) often simply antagonizes the user community. If a clearly defined project goal (e.g., HIPAA certification) is scheduled to be accomplished by a given date (e.g., contract award), then the behavioral modifications can be pursued as tasks in reaching a recognized goal that is meaningful to the organization (e.g., increased business). The fact that certain of these desired behaviors may live beyond the project end date is a welcome side benefit.

***Who are the stakeholders?*** For the InfoSec professional, this question is closely related to risk management. The same people who are responsible for identifying, assessing, or accepting risk on behalf of the organization are stakeholders in InfoSec.

***Who will work on the project?*** In one sense, the caliber of the people assigned can be a reflection of management's commitment to the project. A more positive view realizes that the InfoSec professional can be an agent for change (improvement). When people understand the importance of a job and feel important to that task, they will show up to work, both literally and figuratively (Deming, Out of the Crisis, 1994).

***How much will it cost?*** This can be a misleading question. In some cases, it can be evidence of a very short-sighted view that focuses on the bottom line. Particularly in the InfoSec realm, the most important figures are unknowable. In a similar vein, a cost-to-benefit analysis is an incorrect argument because neither the true cost (of either success or failure) nor the true benefit can be calculated (Deming, Out of the Crisis, 1994). With this understanding, a simple response tallying the known costs (e.g., licensing costs of network monitoring tools) may be the only answer available.

***What constitutes good enough and how will we measure that?*** A clearly defined project goal can help to answer these questions because they should be asked when



© 2012 The SANS Institute Author retains full rights.

defining the goal. For projects that set out to achieve a certification or pass an external inspection, the answers are obvious. The questions become important when there are subjective degrees of accomplishment. For example, a bank will obviously want to protect the cash and other valuables that it holds. The layered security may include cameras, security guards, time-locked vaults, and many other deterrent measures. What constitutes adequate security depends on the location of the bank, the time of day, and many other factors.

***Should we be doing this project?*** This is a fair question that deserves an answer from all of the stakeholders. The InfoSec professional is one member of a team responsible for identifying and managing risk. The collective answer reflects the organizational level of importance and commitment.

### 2.1.2. Listen and Learn

As most of us learned in kindergarten, we each have two ears and one mouth to be used in the same proportion. Especially at the beginning of a new job, listening is the critical skill required for understanding the task at hand.

People, as information consumers and technology users, constitute a huge part of what InfoSec is all about (Bratus, Masone, & Smith, 2008). Listening with empathy helps to define the relationships with colleagues and bosses. Listening well and responding appropriately reflects professionalism and gives one considerable control over various situations (Thompson & Jenkins, 1993). Since so much of InfoSec depends on the behavior of users, the ability to gain cooperation from other people is an important part of the job.

Careful listening often points to other concerns that must be researched. Existing practices and processes, whether formally documented or not, grew in a constrained environment of policy, regulation, and personality. This environment is constantly changing as new laws are enacted, amended, or repealed; policies are updated or rescinded; and people change jobs or retire. To dispel the legends and folklore that tend to accumulate, listen for the references and ask questions to uncover sources. To determine whether the existing practices and processes are current, the InfoSec professional must survey and understand the current environment.



© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

In addition, the InfoSec landscape is changing at least as fast as the technology that drives the information infrastructure. Given the wide variety of operating systems, hardware, protocols, and associated certifications, it is difficult to imagine one person being able to master everything. Fortunately, omniscience is not required for many InfoSec positions.

Trust in well-trained intuition. Training helps to develop intuition. Without knowing everything about a particular aspect of InfoSec, training helps the practitioner to sense when things aren't quite right and these moments of intuition should not be ignored. The smallest discrepancies can lead to huge discoveries. In one case, a minor accounting error was the first evidence of large-scale computer espionage (Stoll, 1989). Stories like these remind us to pay attention to log reviews.

Abnormality in process is also cause for concern. A classic example from the fiction of Tom Clancy demonstrates how circumventing a procedure allowed a spy to dispose of incriminating evidence (Clancy, 1988). When the InfoSec professional finds behavior that does not conform with established procedures, then either the procedure is out of date and needs to be revised or something deeper needs to be investigated.

Whether questioning an anomaly in a log review or a variation in procedure, the InfoSec professional must constantly seek to understand why. The answer to this question will inform the subsequent judgment of whether or not this event contributes to or detracts from the organization's InfoSec goals.

Of the many ways that a project can flounder, many of the remediation plans include listening. Listening for information, listening to build relationships, and listening to maintain awareness of project progress are all necessary skills (Management Concepts, 2009).

## 2.2. Challenges

***Who has what authority?*** In some organizations, the InfoSec component is clearly subordinate to the business unit. The final decision to take action in response to an incident lies with the business unit leader who must weigh the risk of continuing operation against the liability associated with potential compromise (SANS, 2008b). In



© 2012 The SANS Institute Author retains full rights.

other organizations, notably in the federal government, the InfoSec contingent controls the information technology infrastructure absolutely. Equipment can be taken out of service or removed for remediation with little or no regard for the user or the current work. The InfoSec professional must be aware of the boundaries of authority.

***InfoSec is too expensive.*** "Expensive" is a relative term and begs the question "In comparison to what?" An automobile is certainly more expensive than a bicycle, but the vast majority of employees own and use a car. An individual's opinion of expense is commonly driven by the additional time that it takes to accomplish a task once certain InfoSec measures are put in place. Frustrations about longer boot times for computers, slower performance from fully encrypted hard drives, or lack of machine portability now that port security has been enabled on all of the switches sometimes manifest as complaints of expense. The business office can sometimes balk at the price tag on the latest network monitoring equipment.

Answering these concerns requires empathy from the InfoSec professional. Listening to the surface complaint and then asking a probing question or two should identify the real issue that should be addressed. By identifying something of high value to that individual and then showing how InfoSec protects it sometimes helps. For many businesses, the integrity, confidentiality, and availability of proprietary data or intellectual property is more than sufficient motivation.

***Just do the minimum (i.e., due diligence).*** This can actually be a good challenge. Projects typically do not get blank checks for unlimited resources and direct challenges like this can serve to keep extravagance in check. On the other hand, this statement may reflect a fundamental lack of support for the InfoSec vision or the InfoSec project at hand. The InfoSec professional must clearly understand what message is being sent. Ask for clarification; it's important.

***I'm a chemist, not a computer geek.*** This challenge can be a reflection of frustration that users feel when overwhelmed with InfoSec policy or process. Password policy, for example, continues to generate complaints. Requirements for longer passwords that are different than the previous 24 passwords and must be changed every 90 days without being written down seem onerous and unproductive (Schaffer, 2011).



© 2012 The SANS Institute Author retains full rights.

This voice of frustration can be taken as yet another opportunity both to educate and to learn. It is unreasonable to expect every user to have or build the proficiency required of a system administrator. Most users tend to treat their computers as appliances and the network as a bottomless well of information. Listening through the gripes and complaints allows the InfoSec professional and staff to learn where they may have assumed too much from the users they support.

Addressing valid concerns where possible and educating people in the process goes a long way to making end users happier and more compliant. For example, one response to the problem of tracking and changing multiple complex passwords is to identify and advocate an approved password keeping program to help users manage passwords and the task of frequent password changes.

***But it's not a production system; it's only for development.*** This complaint assumes that InfoSec can be bolted on after the development is complete. The common practice of scanning for vulnerabilities before and after patching emerged, in part, from the recognition that action taken to correct one problem can introduce new problems. It is not uncommon for development efforts to be immediately adopted as production products with InfoSec becoming an afterthought. Since many InfoSec problems can be directly attributed to poor programming, adopting good security habits and techniques in the design and development stages reinforces the InfoSec posture.

***InfoSec hurts productivity.*** This sentiment is often heard in the same context as the previous statement, but exhibits the same narrowness of perspective from a different point of view. Where the earlier complaint at least acknowledges the need for security in a production system, the view that InfoSec hurts productivity completely discounts the value of any security at all. Like quality, security cannot be tested in after the fact. Security must be designed into an information system or network from the beginning and recognized as a necessary part of the end product (Yee, 2004).

***InfoSec limits personal creativity.*** Often, this is a disguise for a complaint about not having the coolest or latest stuff.

Whatever the condition of the current program, the first step is to determine where the program is, because that is where any corrective action must begin. For the InfoSec



© 2012 The SANS Institute Author retains full rights.

professional, this will require a great deal of reading and interaction with other people in the organization.

## 2.3. Documentation

Royce pointed to the high cost of recovery in a software development project gone awry as a motivation for doing proper design and documentation early (Royce, 1970). This oft-cited paper has contributed to arguments for doing many things as early in a project as possible. Safety, requirements analysis, testing, and security, among others, are recognized as parts of a project that must be dealt with in the earliest stages and tended throughout the product lifecycle. Security, in particular, cannot easily be bolted on to a complex system after the system is built (Yee, 2004).

Preparing an InfoSec remediation project requires clearly stated goals with well-defined tasks based on real requirements. Get the references. With the furious pace of change in the information technology landscape, security references and associated standards are constantly evolving. Working from a known and defensible position with supporting documentation makes a proposal stronger.

### 2.3.1. Regulations

The tag line on the e-mail read "The objective of IT Security isn't to make life difficult, it's to comply with the law." This statement is unsettling for several reasons.

The first part of the statement carries a tone of either apology (i.e., "I'm sorry for making your life difficult…") or sarcasm (i.e., "My objective isn't to make your life difficult, but I am going to…"). Neither leaves the reader with the feeling that anything good is about to happen. While some in the InfoSec industry are viewed as obstructionist, this is not a good reason to reinforce the image (Adams, 2007). For objective risk assessment, the InfoSec professional should remember that the task at hand is neither personal nor emotional. Working from facts, the resulting security decisions are then supportable.

The second part of the statement makes people nervous. The implication is that the reader must conform to every dictate of the InfoSec establishment or, somehow, be in violation of some law. By extension, this asks the reader to acknowledge the authority of



© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

the InfoSec practitioner to correctly interpret the applicable laws. The resulting feeling of unease makes the reader want to ask, "Who died and made you General Counsel?"

The laws and regulations at every level of government introduce constraints that define, in part, the environment in which information systems live and InfoSec professionals work. The patchwork nature of the legal landscape is complex and disjointed (Gaff, Smedinghoff, & Sor, 2012). For the InfoSec professional, the law represents a minimum level of effort. Laws written in response to particular situations or events can be overly narrow or broad when applied to a specific set of circumstances.

For example, the loss of data for 26 million veterans by the Veterans Administration sparked tremendous outrage (Yen, 2006). Privacy is one of the foundations on which the Constitution of the United States is built (U.S. Const. amend. IV), so it makes sense to have laws surrounding the information associated with an individual (HIPAA Privacy Rule, 2002). As the concepts and techniques for handling personally identifiable information evolved in response to this event, modern law enforcement must now deal with the question of whether facial imagery from surveillance cameras must be given the same level of protection as a name, an address, or a social security number. Similar examples exist for financial systems, medical records, and intellectual property.

Laws define necessary requirements, but are often insufficient to define the optimal security posture that a company may need to protect its information. The InfoSec professional and all stakeholders need good legal counsel to properly understand the associated risk.

### 2.3.2. Policy and Procedures

Policy answers the basic questions of who, what, when, where, and why; procedures explain how (SANS, 2008a). A plan explains how the organization will maneuver through the constraints of policy and law to attain a stated goal.

There are a few things to look for here. Organizational policy that is established in response to a regulation should reference that regulation and be periodically reviewed to ensure continued compliance as regulations change. Here is where the InfoSec



© 2012 The SANS Institute Author retains full rights.

professional needs to team with General Counsel or the designated Compliance Official. Policy that supports best practices should also be referenced and reviewed as the industry landscape changes.

Policy without cause leaves a bad smell. When circumstances arise that challenge a policy, the trace back to law or best practice (showing due diligence) helps employees understand and support the policy. "Because those are the rules," is not a useful or satisfying response (Thompson & Jenkins, 1993).

### 2.3.3. Best Practices

InfoSec, by nature, is still very defensive. As technology advances in both power and scope of connectivity, the "bad guys" are hard at work. From the attacking perspective, the increase in complexity of operating systems, applications, and hardware creates new vectors to exploit. A wide variety of tools are freely available on the Internet, so that it no longer requires the resources of a nation-state to successfully mount an attack. Together with a federal acquisition philosophy to buy commercial solutions for information systems and security, it should come as no surprise that the commercial sector is maturing the best practices of information security far more rapidly that the government (Ghosh & McGraw, 2012).

The real power of defense lives in the community. It is natural for individual organizations to focus on defending their own assets (e.g., computers, networks, intellectual property, etc.), and such vigilance also enhances the security of the larger community (Malamud, 1992). Beyond the passive benefits to the community, the sharing of information related to vulnerabilities, indicators, and attacks represents another level of good citizenship and should be encouraged.

The InfoSec professional contributing to the management of the risk profile of the organization must know what to protect. Defense-in-depth seeks to prevent as many attacks as possible through defense strategies centered on the data to be protected. Detection is the key. To this end daily contact with the systems and networks builds familiarity that establishes the normal in order to recognize the abnormal.



© 2012 The SANS Institute Author retains full rights.

### 2.3.4. Processes

One of many pointed statements attributed to Dr. Deming reads, "If you can't describe what you are doing as a process, you don't know what you're doing." (Deming, n.d.)

The bulk of modern InfoSec work lends itself nicely to Deming's view of statistical process control. At the deck plate level, almost everything that the InfoSec organization does is repetitive and definable as a process. From indoctrinating new employees, to setting up new computers, to scanning and patching networks, to reviewing logs, to configuring firewalls, the tasks are repetitive and the processes that are used to accomplish them should be documented for many reasons.

Documented processes are more likely to be accomplished.

Documented processes can be monitored for statistical control.

Documented processes can be changed in a controllable way.

Documented processes are key components to successful audits and inspections.

Documented processes allow a normal to be defined so that the abnormal can be recognized.

Documented processes are where lessons learned can be recorded to provide positive feedback into the system (i.e., How will we ensure this -- some error or other bad thing -- doesn't happen again?)

One advantage of building or rebuilding a security program in the context of a project is that the creation of new processes or the improvement of existing processes is tied directly to a goal that is important to the organization. Creating new tasks (processes) without the larger goal can seem arbitrary and will probably meet resistance.

## 2.4. Vision

There are at least three visions to which the InfoSec professional should be sensitive: organization, supervisor, and personal.

First, understand the organization's vision. Learn what the company or agency leaders are saying about the next year, the next five years, and the next fifty years. Is the



© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

organization aggressive to the point of recklessness (e.g., Enron) or stable with a strong emphasis on integrity (e.g., General Electric)? This larger organizational vision influences the supporting policies that help to define the vision for information security.

Next, understand the boss's vision. As the first, and possibly the most important advocate for an InfoSec project, the actions of an immediate supervisor have a significant influence on both project and career success. The InfoSec project manager needs to know if the boss's vision is in line with the larger organizational vision or not. Will this supervisor embrace change or whine? The answer to this question and many like it will shape the proposal and execution of a project to remediate security.

Finally, understand the personal vision. Ideally, any differences between the InfoSec professional's personal vision and the organization's vision were discussed and considered as part of the hiring process. In some cases, the InfoSec professional was appointed to the task and real differences may exist in the underlying vision or philosophy. If this is the case, then the project is unlikely to succeed until these differences are reconciled.

## 2.5. Introducing Change

### 2.5.1. Through Education

Deming noted that young new executives in Japanese companies are expected to learn the jobs throughout the company (Deming, Out of the Crisis, 1994). This gives the future leader an awareness of the complexity of the organization when making decisions. In this context, we might reasonably ask what qualifies an InfoSec professional for the job. In many organizations, the IT security posture is dictated by one group and implemented by another. Should the CIO know how to configure a firewall? Are a handful of courses adequate to properly set policy?

While modern executives are aware of InfoSec to some degree, the levels of understanding vary widely. To address this lack of uniformity in a background audience, the InfoSec professional must be prepared to explain and educate other members of the staff. Fortunately, or unfortunately, depending on the point of view, there is a rich body of accumulated experience describing the aftermath of failed InfoSec.

W H Thomas, thomaswh@va.metrocast.net

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

It is a fact that there are enemies out there (Liang & Xiangsui, 2002). Every network and every machine on the network is subject to attack (Whitaker, Evans, & Voth, 2009). Each connection to the larger network is a potential pivot point that could put the entire network in danger. This realization can generate paralyzing fear resulting in decisions to harden systems to the point of uselessness. Scare tactics can be counterproductive to the InfoSec professional.

While each organization must acknowledge the existence of a wide variety of threats, each also has work to do in order to remain profitable and effective. Education, training, and diligence in staying abreast of current trends and techniques allow the InfoSec professional to add perspective and reasoning to the assessment of risk. The InfoSec project proposal should include an honest assessment of education and training among all stakeholders, including bosses, peers, developers, and users. What does each team member have and what does each still need?

### 2.5.2. Change as a Project

Big change is best handled as a project.

For example, suppose that a medical office is seeking HIPAA certification for a new records management system. A project is defined by a start date, an end date, and a product, defined by requirements (Biafore, 2010). In this example, the installation of the new system could mark the start date and the end date could be the date of system certification. The main product is the certification, but many other useful "products" accumulate during the execution of the project.

The certification criteria provide the initial set of requirements. As other requirements are identified, the project documentation is formally updated. Configuration management is controlling change to requirements and, thereby, controlling change to the product. Within the boundaries of a project, many recurring tasks, defined by processes, may need to be documented and scheduled. Daily log reviews, system audits, and regular backups are examples of tasks that will directly contribute to the realization of the certification. Done well, these processes continue beyond the project end date. The legacy of such a project is an improved InfoSec posture.



© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

### 2.5.3. Scoping the Project

Just as a topic sentence focuses a paragraph and a limiting sentence anchors a report (Santmyers, 1968), the project goal defines and guides the InfoSec change that the project is intended to accomplish. It is important to write down this goal. A clear and unambiguous project goal serves to limit scope creep and to provide a litmus test of sorts when deciding whether to invest time or resources into any particular activity. With the written project goal before every member of the project team, each can ask if a proposed action is helping to realize that goal or not. Writing down the goal makes us more likely to realize that goal (Matthews).

With a clear goal in mind, the task of gathering and refining requirements becomes easier. While all of the usual characteristics of good requirements (clear, consistent, atomic, verifiable, etc.) certainly apply, an InfoSec project must also specify to whom the requirement applies. For example, system logging and auditing requirements apply to all users, but additional logging for the use of elevated privileges would apply to those with the broader credentials.

### 2.5.4. Charter or Letter of Authority

Many project management references advocate writing out a charter or letter of authority (Project Management Institute, 2008). The project's name and purpose; the project manager's name, duties, and authority; and the organizational commitment to the project are among the desirable elements of a charter (Biafore, 2010). The project charter is a functional instrument that announces the organization's intent and its champion.

The project charter is usually distributed to a wide audience within the organization and among the project stakeholders. Referring to research by Yorks and Whitsett in *Scenarios of Change*, Bender identifies a rough categorization of personality types ranging from "Innovators" to "Boiled Frogs" (Bender, 1997). The latter are those people most resistant to change and potentially the most dangerous to the InfoSec project. These are the voices, sometimes highly respected, that label new programs, processes, or procedures as fads that can be outlived. Thompson identifies these types as Wimps and warns that they bear watching for the damage they can do (Thompson & Jenkins, 1993).



© 2012 The SANS Institute Author retains full rights.

To avoid making the project and the InfoSec professional leading it into a target for the Boiled Frogs, the charter should be professional and convey serious intent and commitment. Flashy starts with catchy names and buzzwords invite the Boiled Frogs to resist. If the organization is serious about creating an enduring InfoSec environment that manages risk, then that support must be communicated effectively to give detractors reason to pause before attacking.

© 2012 SANS Institute, Author retains full rights.

W H Thomas, thomaswh@va.metrocast.net

© 2012 The SANS Institute Author retains full rights.

## 3. Conclusion

Rebuilding an effective InfoSec profile into an existing project is a project itself. By treating it as such and bringing the incredible variety of management tools and techniques to bear, the InfoSec professional can assess the current state, define the desired state, and map a sure path through the jungle of policy and regulation.

The InfoSec job is primarily about people. Machines tend to do what they are told to do, unlike people. Effective communication and motivation are necessary to implement the changes required to move people from where they are to where they need to be (Thompson & Jenkins, 1993).

The InfoSec professional has an important voice at the table when discussing risk. Accurately assessing and effectively mitigating InfoSec risk requires patience, persistence, and practice. The information technology landscape is constantly changing and requires the InfoSec professional to work hard to stay current.

While a specific goal helps to focus the InfoSec project effort and resources, the long-term benefits that accrue to the organization make great returns for the investment. From heightened user awareness against social engineering to the identification and elimination of unnecessary network services, the InfoSec professional can introduce or reinforce processes that reduce organizational risk and add value to the delivered product.

W H Thomas, thomaswh@va.metrocast.net

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

## 4. References

Adams, S. (2007). *Dilbert.* Retrieved from http://dilbert.com/strips/comic/2007-11-16/

Bender, S. A. (1997). *Managing Projects Well.* Woburn, MA: Butterworth-Heinemann.

Biafore, B. (2010). *Microsoft Project 2010: The Missing Manual.* Sebastopol, CA: O'Reilly.

Bratus, S., Masone, C., & Smith, S. W. (2008, May - June). Why Do Street-Smart People Do Stupid Things Online? *Security & Privacy, 6*(3), 71-74. doi:10.1109/MSP.2008.79

Clancy, T. (1988). *The Cardinal of the Kremlin.* New York, NY: G. P. Putnam's Sons.

Deming, W. E. (1994). *Out of the Crisis.* Cambridge, MA: MIT.

Deming, W. E. (n.d.). Retrieved from ttp://thinkexist.com/quotation/if_you_can-t_describe_what_you_are_doing_as_a/12330.html

Gaff, B. M., Smedinghoff, T. J., & Sor, S. (2012, March). Privacy and Data Security. *Computer, 45*(3), 8 - 10. doi:10.1109/MC.2012.102

Ghosh, A., & McGraw, G. (2012, January - February). Lost Decade or Golden Era: Computer Security since 9/11. *Security & Privacy, 10*(1), 6 - 10. doi:10.1109/MSP.2012.12

HIPAA Privacy Rule. (2002). 45 C.F.R. § 164.

Liang, Q., & Xiangsui, W. (2002). *Unrestricted Warfare: China's Master Plan to Destroy America.* Panama City, Panama: Pan American.

Malamud, C. (1992). *Stacks: Interoperability in Today's Computer Networks.* Englewood Cliffs, NJ: Prentice-Hall.

Management Concepts. (2009). *The 77 Deadly Sins of Project Management.* Vienna, VA: Management Concepts.

Matthews, G. (n.d.). Goals Research Summary. Retrieved July 03, 2012, from http://www.dominican.edu/academics/ahss/psych/faculty/fulltime/gailmatthews/researchsummary2.pdf

W H Thomas, thomaswh@va.metrocast.net

© 2012 SANS Institute, Author retains full rights.

Pettigrew, J. A., & Ryan, J. J. (2012, January - February). Making Successful Security Decisions: A Qualitative Evaluation. *Security & Privacy, 10*(1), 60 - 68. doi:10.1109/MSP.2011.128

Project Management Institute. (2008). *A Guide to the Project Management Body of Knowledge* (4th ed.). Newtown Square, PA: PMI.

Royce, W. W. (1970). Managing the Development of Large Software Systems: Concepts and Techniques. *Proceedings of IEEE WESCON* (pp. 1 - 9). Los Angeles: IEEE.

SANS. (2008a). *401.2 Defense-In-Depth.* The SANS Institute.

SANS. (2008b). *504.1 Incident Handling Step-by-Step and Computer Crime Investigation.* The SANS Institute.

Santmyers, S. S. (1968). *Practical Report Writing.* Scranton, PA: Haddon Craftsmen.

Schaffer, K. (2011, December). Are Password Requirements too Difficult? *Computer, 44*(12), 90-92. doi:10.1109/MC.2011.357

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York, NY: Doubleday.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* (Special Publication 800-30). Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Thompson, G. J., & Jenkins, J. B. (1993). *Verbal Judo: The Gentle Art of Persuasion.* New York, NY: William Morrow.

U.S. Const. amend. IV. (n.d.).

Whitaker, A., Evans, K., & Voth, J. B. (2009). *Chained Exploits: Advanced Hacking Attacks from Start to Finish.* Upper Saddle River, NJ: Addison-Wesley.

Yee, K.-P. (2004, September - October). Aligning Security & Usability. *Security & Privacy, 2*(5), 48-55. doi:10.1109/MSP.2004.64

Yen, H. (2006, May 23). Thieves Steal Personal Data of 26.5M Vets. *The Washington Post*. Retrieved from: http://www.washingtonpost.com

W H Thomas, thomaswh@va.metrocast.net

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Last Updated: June 19th, 2013

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Melbourne 2013** | **Melbourne, AU** | **Sep 02, 2013 - Sep 07, 2013** | **Live Event** |
| **SANS Capital City 2013** | **Washington, DCUS** | **Sep 03, 2013 - Sep 08, 2013** | **Live Event** |
| **Network Security 2013** | **Las Vegas, NVUS** | **Sep 14, 2013 - Sep 23, 2013** | **Live Event** |
| **SANS Canberra 2013** | **OnlineAU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |