
The Security Journal

"Common Sense Security for Common Businesses"

Volume 4 - Summer 2003 Edition

What you can't see can hurt you...
The Dangers of Steganography
by Chet Hosmer & Christopher Hyde

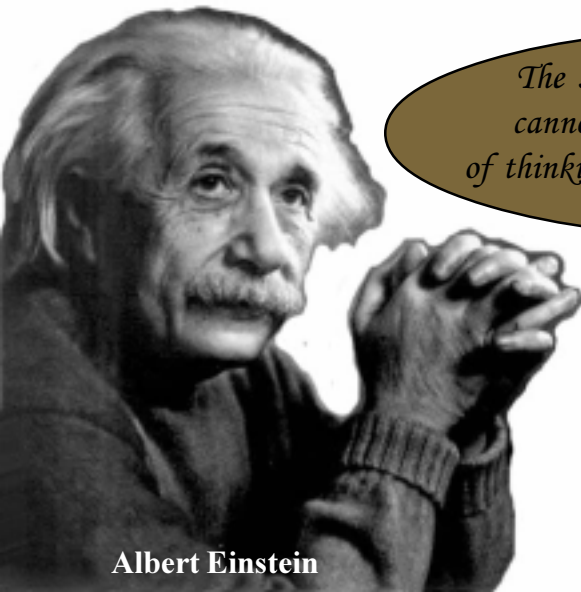
Simplicity is the Key
by Russ Rogers

Incident Response - Part II
by Greg Miles

Privacy Issues
by Ed Fuller

Using the IAM to Request an IATO
by Ted Dykstra

A Note on Asset Management
by Travis Hartman



*The significant problems we have
cannot be solved at the same level
of thinking with which we created them.*

Albert Einstein





Security Horizon

Security Horizon, Inc.
5265 N. Academy Blvd.
Suite 1400
Colorado Springs, CO
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers
Contributing Authors:

Russ Rogers, Security Horizon
Greg Miles, Security Horizon
Ed Fuller, Security Horizon
Ted Dykstra, Security Horizon
Chet Hosmer, Wetstone Tech.
Christopher Hyde, Wetstone Tech.
Travis Hartman, CompuCom

The Security Journal is always on the lookout for quality writers for this publication. If you're interested in submitting an article for inclusion in an upcoming edition of The Security Journal, please contact Russ Rogers at journal@securityhorizon.com.

For more information on Security Horizon, please visit our web site or send us an email at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is based out of Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents:

Notes From the Editor

By Russ Rogers.....p.2

What you can't see can hurt you: The Dangers of Stegonography

By Chet Hosmer &
Christopher Hydep.4

Simplicity is the Key

By Russ Rogers.....p.7

NSA IAM Course Schedule

.....p.8

Incident Response - Part II

By Greg Miles.....p.9

Privacy Issues

By Ed Fuller.....p.13

Using the IAM to Request an IATO

By Ted Dykstra.....p.15

A Note on Asset Management

By Travis Hartman.....p.17

All content used by permission or
Copyright 2000-2003,
Security Horizon, Inc.

Notes From the Editor

Dear Friends,

The Spring of 2003 has brought a wind of change that is making a marked difference all around the country. Rain continues to pelt the formerly drought ridden Southwest areas of Colorado, Wyoming, and New Mexico, bringing new growth. The stock markets are beginning to show signs of change from the frustratingly slow economy we've been living with for the last 2 years to one of growth and progress.

In keeping with the spirit of this change, this issue is dedicated to changing the mental focus of businesses and security professionals around the country. As Albert Einstein so eloquently stated many years ago:

“The significant problems we have cannot be solved at the same level of thinking with which we created them.”

The world of technology has continued to grow, unabated for decades with no real deep thought on security. The creation of so many open systems, worldwide, has created business opportunities beyond belief, but it has also created security concerns beyond belief.

The same technology that allows businesses to operate on a global basis also leaves them vulnerable to attack and the theft of proprietary information. In order to plug these holes, we need to start thinking differently about

the problems we have created for ourselves. Continuing the patch security vulnerabilities and perform triage on broken networks will not resolve the inherent issues with the systems we've built.

It's time to start looking at our networks from a new perspective. What parts of our architecture and design have caused our networks to be vulnerable to attack?

Why are our current software engineering techniques allowing our customers to be compromised?

Are there smarter ways to do business over the Internet without sacrificing the privacy of our customers?

Can we honestly continue to ignore the blatant exposure that exists simply because the security measures to mitigate those risks cause our business some inconvenience?

For instance, how complex is your network? How many administrators do you need? How many security professionals does it take to secure? Is it really truly secure, or is it simply patched against known problems?

Do you know what Steganography is? If so, have you performed checks on your public web site to see if you're being used for covert communication?

Have you considered Asset Management to help track and manage your network?

As with all other things in life, continued effort towards a single goal will eventually lead to success. The industry needs to make security a focus, a core goal. My grandfather had an old saying, "Persistence is Omnipotent."



Black Hat Federal 2003 Call for Papers

Join the ranks of the most elite minds
in information and computer security

Call for Papers are currently being accepted for the upcoming
Black Hat Federal 2003 Briefings. For more information and to submit,
please go to www.blackhat.com



Black Hat[®]
Briefings & Training Federal

September 29-October 2, 2003 • Sheraton Premiere Tysons Corner, VA

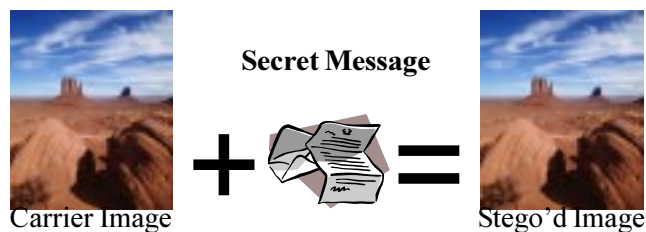
What you can't see can hurt you... The Dangers of Steganography

By: Chet Hosmer &
Christopher Hyde

Steganography is a word originating with the Greeks meaning 'covered writing.' Its use can be traced back at least 2,500 years, when Demaratus smuggled a secret message under the cover of wax in order to warn Sparta of an impending attack on Greece¹. Other examples used throughout history include invisible ink, null-ciphers, and microdots.

Steganography Today

In modern times, digital images, audio files and streaming video have become carriers for hidden information, while our networks are the high-speed delivery channels. Unfortunately, modern delivery channels continue to be guarded by unsuspecting sentries, in the form of firewalls and sensors that are unable to detect messages hidden inside of digital images and audio files.



Why use an ancient method to hide data? Surely modern cryptography provides a more proven method for keeping information private. The distinction between steganography and encryption is the answer. Encryption is used to keep the contents of information private or confidential and only those holding the proper keys can extract the secret contents. The sole purpose for the use of steganography, on the other hand, is to hide the fact that a secret message even exists. The military calls this 'covert communication,' and the path for this communication is called a 'covert channel.'

To illustrate an example of steganography, the following figure shows two images whose differences are undetectable to the naked eye. The original 680 KB image on the left appears identical to the image on the right. The image

on the right, however, contains a secret message in Microsoft® Word format that is 88KB in size, or about 13% of the original cover image.



Original



Original + Secret Message

During the last decade, technology for digitally manipulating image, video, and audio data has advanced tremendously, resulting in the rapid development of information hiding in binary data files. The sophistication of the steganography programs has also evolved from simple homemade solutions to commercial grade offerings.

The proliferation of steganography software is widespread. During a recent research effort, WetStone Technologies examined over 100 programs that hide messages in image files, audio video files, and in text documents. Many of these programs are freely downloadable from the Internet, while some charge a nominal fee of between \$49 and \$89. Our research indicates that over one million copies of steganography software have been downloaded or purchased over the Internet during the last 24 months.

Methodologies

There are many techniques for hiding secret messages in images. The common denominator among them is that they combine a carrier file with a secret message to produce a new binary file containing a hidden message. The process hides the data in such a way that the changes are indiscernible to the human eye or ear. The methodologies vary widely from simple least significant bit (LSB) modification to sophisticated JPEG and MP3 algorithm modifications.

In LSB substitution, modifications are made to

least significant bits of the cover file's individual pixels or sounds, thereby encoding hidden data. Generally, these changes make imperceptible modifications. In more sophisticated methodologies, such as hiding in JPEG's and MP3's, the actual compression algorithms are modified in a way that data can be hidden during the encoding process. Other methodologies of digital steganography exist including word substitution, file appending, covert channels, and file source modification.

Dangers of Steganography

The increase in availability, sophistication, and popularity of steganography programs increases the potential opportunities for industrial espionage, trade secret theft, cyber weapon exchange, and criminal coordination and communication. There is a growing concern in law enforcement and private investigations that steganography is an unknown, and until now, an undetected component in various criminal activities.

The explosion of Internet traffic provides the perfect environment for data hiding via steganography. With the vast amount of potential cover files that are posted, e-mailed, and viewed on web pages every day, it is impossible to manually scan even a fraction of them. Tremendous potential exists for a significant amount of illicit traffic to go undetected by law enforcement. Furthermore, as the bandwidth of the Internet increases to afford easier transmission of large files such a real time video, there will be an increased risk that illegal communications will go undetected.

What is the threat, then, to our corporate infrastructures from this new form of invisible ink? The answer comes in three basic areas:

First, the use of steganography provides the ability to smuggle sensitive information out of an organization. This can be accomplished by hiding the information via steganographic techniques inside an innocuous attachment to an email message.

Second, the use of steganography allows

someone to hide criminal or unethical information on corporate resources. A quick scan of a departing user's desktop might reveal digital photos from the company picnic, family outings, or a collection of clipart used for building slide presentations. These all will appear completely harmless and innocuous, when in fact they contain hidden information.

Finally, steganography allows for the use of corporate resources to communicate criminal or terrorist information. Most companies are extremely diligent about the content of their corporate web sites and public-facing information. However, every image on that corporate web site is a potential carrier of hidden information. Many of these images float around the organization and originate from many sources, providing the opportunity for insertion of secret or covert content. Furthermore, web sites that allow public postings of information (i.e., auction, dating and real estate sites) offer outsiders a way to use the Internet to communicate virtually anything without detection.

Since the terrorist attacks of 9/11, it has come to light that steganography was probably used as an element of communication during the planning of the operation. According to reports in USA Today, Wired News, and on CNN, Al-Qaeda was interested in steganography and its uses¹. Given the probability of the continued use of steganography as a method of covert communication, there is an urgent need to develop semi-automated and automated methods of detecting, investigating and recovering hidden data from stego'd files.

Steganalysis and Forensic Investigation

As steganography becomes more prevalent in the criminal world in both the traditional and the new and growing world of cyber crime, inspecting digital files to discover or detect steganography takes on increased importance. The emerging discipline of steganography investigation, or steganalysis, is a specialized subset of digital forensics, which should be practiced hand-in-hand with other investigative activities.

“Since the terrorist attacks of 9/11, it has come to light that steganography was probably used as an element of communication during the planning of the operation.”

Steganalysis is the science of detecting, destroying, extracting, and modifying data embedded in steganographic files. The detection and extraction of steganography is the focus of investigators and is a complicated process that requires a holistic approach to investigations.

There are two different forms a steganography investigation can take. The first is a “stake-out” style investigation of a live web site where files are downloaded and examined on a regular basis to determine if there is suspicious content. The second type of investigation involves the postmortem analysis of a hard drive or other storage media for suspected files. In either investigation there are various steps which should be taken, and that work simultaneously with a traditional forensic investigation.

The first phase of an investigation is suspicion. Is the suspect computer savvy? Does the computer contain encryption or steganography programs? Is there an unusually high number of potential cover files present? Does the suspect communicate in way that does not make logical sense or convey unexpected information?

The next phase is identification. During this phase the investigator tries to identify specific items such as installed programs or program remnants, web histories, and specific image or audio files which contain suspicious “finger-prints” of steganography.

The third phase combines examination, detection, and analysis of suspect material. The analyst performs a detailed examination and analysis of suspicious content using automated, semi-automated, and manual means to determine the probability of individual files containing steganographic content. Due to the complexity

and nature of data hiding, this process cannot be fully automated at present and requires personnel who are specifically trained to detect the subtle signs left by steganography.

The fourth and final phase is recovery. In files where steganography is probable, the investigator may attempt to recover the hidden information. This may be done by using information gathered earlier in the investigation such as probable software used and potential passwords recovered from the system.

Conclusion

Steganalysis of data hidden in computer files is a relatively new field of study. More research needs to be done before there will be a reliable amount of data regarding different investigative techniques. Steganography will continue to be a problem for law enforcement as more users realize the value of hiding certain data. Unless reliable and automated detection methods are developed to compliment traditional investigative techniques, law enforcement will continue to be at a disadvantage to computer savvy criminals.

Chet Hosmer is a co-founder, and the President and CEO of WetStone Technologies, Inc. His specialty areas include secure time, intrusion detection and response, and cyber forensics. If you'd like to contact Mr. Hosmer, you may reach him at chet@wetstonetech.com.

Christopher Hyde is a Digital Forensic Analyst with WetStone Technologies, Inc. He has been researching steganography and digital forensics since 1999. If you'd like to contact Mr. Hyde, you may reach him at chris@wetstonetech.com.

WetStone Technologies, Inc.: www.wetstonetech.com

Resources:

Steganography Tool Archive: www.stegoarchive.com
Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Neil Johnson, et al.

¹ Kahn, *The Codebreakers*, 1967, page 81

² <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm>

<http://www.wired.com/news/politics/0,1283,41658,00.html>

<http://www.cnn.com/2001/US/09/20/inv.terrorist.search/>

Security was never a huge concern for organizations that were implementing high tech networks and information systems 10 years ago. The goal was always on open systems and interoperability. In the last 5-7 years, however, security has become an increasingly important component of the process. But due to the methodologies (or lack thereof) used during the creation of these information systems, organizations inadvertently introduced complexity into the environment.

Part of the challenge is that security professionals were never involved in the creation of these systems. In fact, at the time, most organizations weren't thinking about security. It was still a relative unknown. But contrary to popular belief, 'security' is not a distinct and separate process that operates totally isolated from the rest of the organization. Instead, security should be ingrained within the culture of the organization and used to guide mission operations. Unfortunately, a lot of information systems are created, maintained and enhanced in an "ad hoc" fashion, which introduces a surprising level of complexity.

“Complex and Chaotic systems are more difficult to secure...”

Complex and chaotic information systems are more difficult to secure and maintain than simple systems. When every server is configured differently (also known as the snowflake effect) the security process becomes infinitely more difficult and each server becomes an individual case study in information security. Standardizing base configurations and processes across the organization, however, removes complexity, simplifies the security process, eases the maintenance process, and creates the opportunity for optimum information security within the organization. Everyone

knows how things are supposed to be because the configurations or processes are documented and enforced.



The International Standards Organization (ISO) is a great example of this process. The ISO 9000 series of certifications attempt to organize the processes and procedures within an organization so that each one is documented and repeatable. If Joe Bob gets hit by a train tomorrow morning, Sally Lynn can easily pick up the process from where Joe left off before the accident. This is because the process is documented and known.



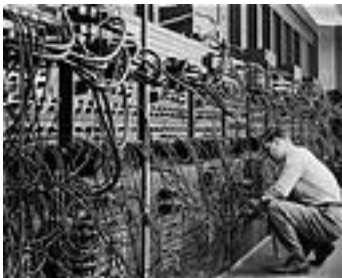
Repeatable processes create standards and simplicity, which enhances the ability of the organization to provide better security for their critical information assets. The ISO process, in and of itself, is not terribly painful and difficult. The difficulty and pain experienced are derived from the evolution of the organization from a state of complexity and chaos to a state of simplicity and standardization.

The creation and standardization of repeatable processes, procedures, and configurations within any organization also helps eliminate the confusion and misunderstanding that many employees have concerning their roles and responsibilities. Employees can be more at ease with their own efforts within the organiza-

Simplicity is the Key

organization when these things are defined, stable, and secure versus dynamic, undefined, and complex.

Once a state of standardization is reached, the organization needs a mechanism in place to handle required changes to the systems and/or processes. Change is required for the evolution of any organization, but it should also be strictly controlled and monitored in order to avoid slipping back into a state of complexity. Each change should be authorized, documented and mapped directly back to a legitimate business process. Changes that can not be justified based on legitimate business processes or needs should not be implemented, as they introduce additional complexity into the system.



The past days of ad hoc networking need to be resolved. In order to increase the security of our information assets we need to simplify our configurations and standardize our processes. Communicating with the rest of the world is no longer a huge challenge, but instead we face the need to protect the one critical component that differentiates us from our competitors; our information.

Russ Rogers, CISSP, CISM is the President of Security Horizon and a regular contributor to The Security Journal.

if you'd like to contact Russ, he can be reached at the following email address:

russ@securityhorizon.com
www.securityhorizon.com
719-488-4500



Schedule of Courses

7/13-7/14, 2003	New York, NY
7/21-7/22, 2003	Washington DC
7/28-7/29, 2003	Las Vegas, NV
	BlackHat
8/8-8/9, 2003	Omaha, NE
8/18-8/19, 2003	San Antonio, TX
9/12-9/13, 2003	Raleigh, NC
9/18-9/19, 2003	New Orleans, LA
9/29-9/30, 2003	Washington DC
	BlackHat Federal

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting INFOSEC assessments of U.S. Government information systems. The course teaches NSA's INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

Find out about how you can get our high quality IAM training at **your** company!


Don't be fooled by other low prices!

IAM training so good that even our competitors attend **our training.**

To register for one of these courses or to get further information on the IAM methodology, please contact us at:

Security Horizon, Inc.
(719) 488-4500
info@securityhorizon.com
<http://www.securityhorizon.com>





Discovering the Hidden

Steganography Investigator Training Course

- ✓ Uncover vital evidence in your investigations
- ✓ Learn critical digital investigation skills and techniques
- ✓ Learn the latest hidden communication methods used by criminals and terrorists
- ✓ Understand steganalysis and the benefits its use provides

Presented by

**WetStone Technologies, Inc.
and
Security Horizon, Inc.**

Next Course – Black Hat 2003
July 28 – 29, 2003



www.wetstonetech.com

Last issue we took a look at the critical step of being prepared for a computer security incident. This article is the second of a six part series in Incident Response (IR). IR professionals have adopted a basic core set of activities that encompass the IR discipline which includes IR preparation, identification, containment, eradication, recovery, and follow-up. Professional organizations that provide advice in the IR arena include but are not limited to the Carnegie Mellon Software Engineering Institute CERT® Coordination Center (www.cert.org), the SANS Institute (www.sans.org), and the Forum for Incident Response Security Teams (FIRST) (www.first.org). This article focuses on IR Identification.

Identification of a computer security incident is one of the most critical and difficult elements of the IR activity. This is due to the fact that without the proper detection tools, logging, and security awareness, most incidents will go unnoticed for a long period of time. By the time it is discovered a great deal of damage can be done to the system or network. Also of concern is the amount of damage done to an organization's business or mission because of lost time, stolen data, damaged data, or bad press.



The primary goal of the identification process is to determine if a problem really exists, what systems does it affect, what users does it affect, and what is the impact to the organization. And it may be difficult to determine because there are not always clear signs of an incident. You may experience a slow system, missing data, or other problems. In order to identify whether something is an incident, it is useful to have intrusion detection tools, virus scanning tools, audit logs, etc.

Without investigation by a subject matter expert many incidents can be incorrectly labeled as user error, hardware failure, or software misconfiguration. Technicians and system administrators need to learn to investigate problems fully and pass to the appropriate security personnel. Education is extremely important to assure investigations are conducted in the appropriate manner to preserve the integrity of the evidence and find the real cause of an incident.

There are certain indications or “symptoms” of an incident that deserve special attention:

- System crashes
- New user accounts or high activity on a previously low usage account.
- New files (possibly with strange file names)
- Accounting discrepancies (in a UNIX system you might notice the shrinking of an accounting file called `/usr/admin/lastlog`, something that should make you very suspicious that there may be an intruder).
- Changes in file lengths or dates
- Unexplained web page changes (defacement)
- Attempts to write to system
- Data modification or deletion
- Denial of service
- Unexplained, poor system performance
- Anomalies (strange unexplained/abnormal events)
- Suspicious probes (there are numerous unsuccessful login attempts from another node).
- Suspicious browsing
- Inability of a user to log in due to unexplained account modifications

Incident identification involves more than just identifying the type of incident. It also involves identifying the scope of the incident. The scope of the incident will identify how far reaching the incident may be. Does the incident affect one system or all? Is it applicable to one operating system or all? Investigation of the reach of the incident is going to be critical in the containment

and recovery process.

Classifying an incident is one of the last critical steps of the identification process. The following is a list of possible classifications of incidents. This list is by no means comprehensive, but provides solid examples from which to build your tailored set of classifications to meet your IT process needs.

Incident Type Classifications:

1. **Unauthorized Privileged (root) Access** — Access gained to a system and the use of root privileges without authorization. without authorization.source.
2. **Unauthorized Limited (user) Access** — Access gained to a system and the use of user privileges without authorization.source.
3. **Unauthorized Unsuccessful Attempted Access** — Repeated attempts to gain access as root or user on the same host, service, or system with a certain number of connections from the same source.
4. **Unauthorized Probe** — Any attempt to gather information about an Automated Information System (AIS) or its users on-line by scanning a site and accessing ports through operating system vulnerabilities.)
5. **Poor Security Practices** — Bad passwords, direct privileged logins, etc., which are collected from network monitor systems.
6. **Denial Of Service (DOS) information attacks** — Any action that preempts or degrades performance of a system or network affecting the mission, business, or function of an organization.
7. **Malicious Logic** — Self-replicating software that is viral in nature; is disseminated by attaching to or mimicking authorized computer system files; or acts as a trojan horse, worm, malicious scripting, or a logic bomb. Usually hidden and

and some have the potential to Replicate. Effects can range from simple monitoring of system/network traffic to complicated automated backdoor with full system rights.

8. **Hardware/Software Failure** — Non-malicious failure of HW or SW assets
9. **Infrastructure Failure** — Non-malicious failure of supporting infrastructure to include power failure, natural disasters, forced evacuation, service provider failure to deliver services, etc.

Other classifications that should be considered based on your organizations security and system use policy include:

Unauthorized Utilization of Services – This can include game play, relaying mail without approval, creating dial-up access, use organizational equipment for personal gain, and personal servers on the network.

Espionage – This includes information stealing or manipulation, email monitoring, computer theft, data copying, and trojan/tunneling.



“Classifying an incident is one of the last critical steps of the identification process.”

Along with the incident identification and classification process, the incident needs to be labeled with an incident severity level that will help to identify the suspected impact of the incident on the business operation and help to establish the priority that will be associated with its resolution. The severity levels should be closely linked to your organizations disaster recovery plan.



Incident Severity Levels:

1. Severity Level 1: Incident could have long-term effects on business or incident affects critical systems.
2. Severity Level 2: Incursion on non-critical system; detection of precursor to a focused attack; believed threat of an imminent attack.
3. Severity Level 3: Threat of a future attack; detection of reconnaissance.
4. Severity Level 4: Unsubstantiated rumor of security incident

You must realize that this process may take as short as a few minutes to as long as weeks to complete the identification process. Ideally, the identification process is completed quickly, and the CIRT can then work out a plan for the containment of the incident, and begin the recovery process.

With most incidents, you will not have the luxury of an indefinite timeframe to identify the incident and start the remainder of the IR procedures. The primary focus will be "just get it working, NOW!". With this in mind, treat every incident

as a criminal investigation, preserving evidence wherever possible. It is highly recommend that you conduct a **bit for bit image of the affected system(s) for analysis. If you have the luxury of being able swap out hard drives to preserve original evidence, that is highly desired. Keep in mind, without this "best evidence", the ability to prosecute an incident will be highly unlikely.**

Recommended Reading: Incident Response: Investigating Computer Crime, Mandia & Prosis published by McGraw-Hill.

Preparation and Prevention are still your best defense against information security threats.

Next edition we will be discussing Incident Response Part 3: Containment.

Dr. Greg Miles, CISSP, CISM is a Vice President at Security Horizon and regular contributor to The Security Journal.

If you'd like to contact Dr. Miles, you may reach him at the following:

greg@securityhorizon.com,
www.securityhorizon.com
719-488-4500.

Personal privacy and concern for what information is being publicly exposed is growing. Companies are beginning to assign a new position, Privacy Officer. The job is not to configure systems or do direct information security. The job of the Privacy Officer is to ensure the organization is meeting the new legislative privacy requirements. Unfortunately, some appear to be intimidated by security professionals. This is a bad thing. With the aggressive growth of regulations to protect privacy, people responsible for privacy have to talk to the security folks. As privacy practices continue to grow and mature they will become directly and irrevocably tied to the security practices of the organization.

In the mid to late nineties the information security profession matured considerably. Security people are now better at explaining things. Maturity has also brought about better understanding of the roles within security: management, operations, and technology. You don't have to be able to write firewall filter rules to know what a firewall does and when one is needed. You don't have to be able to code encryption algorithms in C++ to make purchasing decisions about encryption products.

The simplest way to avoid being intimidated by something is to learn more about it. How much you need to know about security? If your job is providing privacy protection for your organization, or you are concerned with your own personal privacy, you should learn enough about information security to ask the questions that need to be asked, and to evaluate the answers. Consider what happens when you are creating a privacy statement for the company web site.



You may want to use language like this: "To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect online." (This is from our own web privacy statement.) But how do you confirm that this is actually the case?



A good first step is to ask whoever is in charge of information security: "Do we have appropriate physical, electronic, and managerial procedures to protect customer Personally Identifiable Information (PII)?" You probably will need to explain that PII is personally identifiable information, because this acronym is not yet part of the standard security language. If the response is "No" then there is work that both sides have to do before that privacy statement can go up. But what if the answer you get is "Yes"? Can you rely on this statement? The answer to that question depends on your assessment of the person or persons making the statement. How long have they been in charge of organization's information security? Do they strike you as competent? How seriously did they take your question? Do they have any security-specific credentials, such as CISSP?

The last question is not meant to imply that only a CISSP is entitled to assess security. However, it is important to note that the FTC's settlement with Microsoft over privacy and security issues related to Microsoft Passport, the FTC specifically identifies CISSP. The settlement requires Microsoft to provide a biannual report to be "prepared by a Certified

Information System Security Professional (CISSP) or by a person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission”.



Bear in mind that, while best practices in privacy are still evolving, security best practices are well established. This is why the government’s delaying over the final draft of the HIPAA Security Rule makes no sense. That rule will be a statement of how to provide the “reasonable safeguards” for protected health information mandated in the Privacy Rule; the standards for that statement already exist in today’s security best practices.

“As the person responsible for privacy, you need to validate the statements from the people in charge of security.”

As the person responsible for privacy, you need to validate the statements from the people in charge of security. Ask for copies of recent security audits, internal and external. Ask if there has been a penetration test of the web site in the last six months. If so, what were the results? If issues were identified, have they been resolved? Who did the test? Was it a reputable, independent, outside, trusted authority? Assessments by your ISP, Web hosting company, or hardware vendor are not really independent, and although tests by internal

security staff can be very helpful, they are not, in terms of due diligence, as valuable as an external test.

The growing interest in privacy posture by federal and state regulators, coupled with the lack of leeway with respect to security standards, means that privacy people need to talk to security people, not only to make sure that security standards are being met, but to make security professionals aware of the new rules of the game. The idea that exposure of customer PII is inherently bad because it violates privacy promises is a relatively new one, and some security professionals are only now realizing that there is a new player in security, the customer.



Ed Fuller, CISSP, GSEC is the Vice President of Training and Education at Security Horizon and regular contributor to The Security Journal.

If you’d like to contact Mr. Fuller, you may reach him at the following:

*ed@securityhorizon.com,
www.securityhorizon.com
719-488-4500.*

L E W A N

Technical Services

Becoming your trusted partner in *Anything* IT.



It's rarely a slam-dunk launching the right information technologies. Successful technology innovation takes business insight - *pure people power*. New installations and system upgrades require technical experience and know how. That's why people call Lewan.

Innovation, problem solving, accountability.

That's the Lewan way.

IT consulting *services*

For more information visit www.lewan.com

Since 1986, Lewan has helped thousands of customers meet their businesses objectives through *leading-edge technical consulting services*. Our Consulting Services Team has multidisciplinary expertise to solve your *local and wide area network* challenges.

Lewan's resume includes success with some of the region's most respected large corporations. And we've helped transform hundreds of small and mid-size companies as they embrace enabling technologies.





In our INFOSEC Assessment Methodology (IAM) classes, we discuss how well the IAM process wraps around multiple different service offerings and requirements. In this article I'd like to share an example of how I have used the IAM as a framework for generating an IATO submittal. Whether you're looking to begin the certification and accreditation process for a National Critical Infrastructure System (NCIS), Military Healthcare System (MHS), or National Security Information Systems (NSIS), etc., the IAM is quite flexible. DITSCAP, NIST 800, or other standard set aside, a proper IATO request process can be accomplished efficiently.

Starting off, before you even plan the on-site Pre-Assessment visit, the guiding documentation for IATO/C&A must be reviewed and understood. You can usually find a considerable amount of information regarding governing requirements at your customer's website. One reason for this is that the "Information Criticality" product, which is a main component of this phase, may already have been started for you. Certain organizations already have the High / Medium / Low attributes defined, as well as the Critical Information Types. This greatly increases the speed and efficiency with which you can build your matrix (as well as verifying it is done to form), and is required by some standards. With a large portion of the site visit completed more rapidly than usual, time can now be spent on a major requirement for an IATO, the System Description.

The System Description can vary by process, but the mission of the system is an excellent place to start. Over the course of the on-site visit, you should be able to compose a brief description of the functions, hardware, software, type, etc., of the system being appraised. This goes a long way in assisting you with the first

step in the deliverable, as well as affording you a much better understanding of the level of effort that may be required to complete the task. Throughout the process this description will continue to be fleshed out until you have a major component of your IATO request completed.



Now onto the meatier part of the process, beginning documentation review! For me, very little in this life is more difficult than just starting the request for documentation and the mapping of legislation to standards, to guidelines, to policies, to processes, etc. Don't forget to verify that you have the latest version of any guidance documents or templates; they tend to change rather often. Just as in a standard INFOSEC Assessment, in the Pre-Assessment Phase you begin your documentation review to determine the level of compliance based on policies and procedures. Always mapping to your overall requirements, you can begin getting a feel for components that may be lacking or need modifications.

Moving to the On-Site Phase, you will now begin to validate assumptions made about the system's current readiness for an IATO. Following your guidelines, you will be performing interviews based on items such as NIST 800-26 and the DITSCAP Compliance Checklist. An IATO will also require other documentation, for example proper completion of the Asset Valuation Guide (AVG) for Department of Interior (DOI) systems. A Department of Defense IATO also requires an IATO Report (risk assessment). Both of these documents can be found in template form. Again, this is why

understanding the specific system's certification and accreditation environment is so vital in the beginning. Being prepared as you enter each phase is critical for the success of the project.

“Don't forget to verify that you have the latest version of any guidance documents or templates...”

An IATO also requires some form of a Technical Vulnerability Assessment. In some instances a third party scanning tool may suffice, or the use of host based C2 compliance scripts. Independent of whatever guidance you must follow, findings will need to be analyzed and shared with the system managers. Here is one place I deviate slightly from a typical assessment; I incorporate an informal “mid-briefing” to discuss the findings immediately. We then jump directly into the vulnerability mitigation processes. I may be as involved as a lead engineer, or as little as an observer depending on the system and the environment. Once it is believed mitigation has been achieved for at minimum all high vulnerabilities, I then perform a second TVA and formally document the results as part of the planned deliverable and perform my normal out-briefing. Remember, I'm not there to just find holes and recommend solutions. The deliverable in this case is an IATO request, which will be denied immediately if any high vulnerabilities exist, and in most cases if any medium vulnerabilities exist.

Moving forward after a successful on-site visit, we enter the typical Post-Assessment Phase. Much like any other assessment, this phase includes final documentation review, TVA analysis, and recommendations. Differing from the typical assessment, I conduct the recommendations portion with involvement from the organization. A required component for granting of an IATO is a mitigation plan. Known in some areas as a work-off plan or a Plan of

Action and Milestones (POA&M), this document must contain solutions to findings that can and will be addressed. The document must contain target completion dates, current status, responsible parties, etc. Obviously, the planned mitigation activities must be achievable by the system managers, or C&A advancement beyond the IATO is not likely.

In most instances, the deliverable includes creation of required IATO documents such as the Security Design Document (SDD), System Security Authorization Agreement (SSAA), or System Security Plan (SSP). Most entities have pre-defined templates in existence for use in the Certification and Accreditation process, which should include documents such as these. Most of the information gathered up to this point (such as the system descriptions!) can be plugged into the templates and readied for distribution. The final report is then formatted as a request for IATO, including attachments and appendices displaying your assessment efforts and future system direction.

Ted Dykstra, CISSP, CCNP is a security consultant at Security Horizon and regular contributor to The Security Journal.

If you'd like to contact Mr. Dykstra, you may reach him at the following:

ted@securityhorizon.com,
www.securityhorizon.com
719-488-4500.

The Security industry is often filled with righteous indignation whenever a new vulnerability is discovered. “You were using that operating system – of course it has problems!” is a refrain heard on a regular basis. While it is easy to look at things in hindsight and see where the problems occurred it is a challenge to take a broad look across an environment, accurately identifying trouble areas and ranking their importance to the organization. Security professionals must move from technology disablers to technology enablers. Reactive security controls are received poorly when compared to proactive planning and design efforts by the security team.

“...many Asset Management systems are not up to acceptable security levels.”

One area that is emerging with great impact to the Security community is Asset Management. Imagine a person walking into the Security area with a tool that would accurately identify every system within a 60,000 node environment that was vulnerable to the latest vulnerability and provide the results within 5 minutes, without utilizing any network bandwidth. If the security group wanted, patches could be applied to every vulnerable system within 30 minutes. Asset Management systems provide considerable power and benefit to the corporate environment, but their usefulness is often overlooked by Security practitioners.



The above scenario isn't fictional. It occurred at a large global company when the SQL Slammer worm appeared. While the asset management systems are bringing a broad range of abilities to identify system information, restrict programs from running on certain systems, identify vulnerabilities, and distribute patches the internal workings of many Asset Management systems are not up to acceptable security levels. Spoofing workstations, poisoning asset databases, and pushing out arbitrary patches are all vulnerabilities that CompuCom's researchers have identified in various Asset Management products. Properly deploying the Asset Management tools and integrating them into the security architecture provides stronger capabilities than either discipline used alone.



Take a look around your corporate environment. See what tools other people have and what they use them for. Don't restrict yourself to the security hammer that was the only tool in your bag.

Travis Hartman, CISSP, IAM is the Director of Enterprise Security for CompuCom, Inc.

If you'd like to contact Mr. Hartman, you may reach him by emailing:

travis.hartman@compucom.com,
www.compucom.com

