fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

News and Views

Issue Four of FISSEA Year 2005-6 March 2006

IN THIS ISSUE

Letter from the FISSEA Executive Board Chair

Dear FISSEA,
Chief Seattle once said "Man did not weave the web of life, he is merely a strand in it." We, as practitioners of computer/information security Awareness/Training/Education are but enablers on the learning continuum. Our part of this spider web is to provide the strand which enables students to find, interpret, and understand concepts thru realities… from technology changes on the horizon to the latest malware scourge to affect users. As Christa McAuliffe stated, "I touch the future, I teach." She is teaching us still. Years back, FISSEA picked up this quotation and presented it as our organizational mantra. During the shuttle mission, Christa was scheduled to teach two lessons from space. In a pre-flight interview, surrounded by 1,300 switches and dials in the cockpit, Christa said "That's our new frontier out there, and it's everybody's business to know about space." Just 73 seconds after lift-off on 28JAN1986, the space shuttle Challenger exploded, killing all seven astronauts aboard. It is difficult for me to believe that the tragic incident occurred 20-years ago, however her message continues to speak to us, today. Here in FISSEA, we deal in cyberspace and our Awareness/ Training/Education mission helps pave a secure path to the future. In the same way that Christa taught children, we do what we do to aid other's understanding and improve their abilities to successfully do their daily work.

In composing these newsletter articles, I am affected by what is currently happening in the world and often things going on around me. Perhaps you saw the recent news article which reported that an Escambia County, Florida, teacher "allowed kids to skip his class if they paid him $1 a day… They say he may have racked up more than $1,000 over three months." The Principal was quoted as saying "He had a very good rapport with the kids." Following his resignation, she added "It's just sad. Our troubled young kids – he could reach them. Now he's gone." It begs the question, should he be rewarded for reaching the students or reprimanded for reaching into the students' wallets? No, I know that's not the point. But, the article's Principal was also quoted with "The basketball team had lost every game for five years… This year (while under this teacher's coaching), we only lost two games, and they were only by two points." Me thinks this Principal has no principles, Folks.

Practitioners must have principles (get the segue?) by which to perform and be measured. Our principles are based on Rules of Behavior, NIST and other stated guidance, findings from Inspectors General audits, Best Practices, and the states of art in both technology and security. To be ahead of the game, we must have management's blessing as well as buy-in from all involved. Be the organization large or small, the concepts are the same. But we must each assume responsibility for this important arena made up of Awareness/Training/Education. And in so doing, we will all work together toward common goals. If we consider Inspectors General, Information Technologists, and Management to all be just fish in the cyber sea… little fish may not stand up well to predators but when all are swimming tightly in their school they can appear as a single much larger and formidable creature and confuse a potential attacker.

In the analogy, if the attacker was let's say named FISMA, by having all the fish in a school, following required guidance, and working toward the same mutually beneficial goal, their actions might be good enough to improve their lot while protecting the public trust reposed in them and their organization. William Wordsworth wrote "Come forth into the light of things. Let Nature be your teacher." And so, we approach our 19th annual FISSEA Conference as little fish… seeking to join our peers in school… and take home the learned practices to improve work and evaluation as well as security from whence we came.

Hope to see you on 20-21MAR2006,

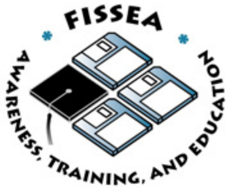
Louis

P.S.
FISSEA is proud to announce that two of its major contributors have achieved the status of "Professor, US Military Academy." COL Curt Carver (FISSEA Exec Board Member and Conference Program Co-Chair) and COL Dan Ragsdale (past FISSEA Exec Board Member and Educator of the Year) have been selected by this institution of higher learning. Dan will be the Vice Dean for Education, duties which he will assume upon return from overseas duty. Curt has been named Vice Dean for Resources which he will begin in April, 2006. Please join me in congratulating these West Point friends and supporters of FISSEA.

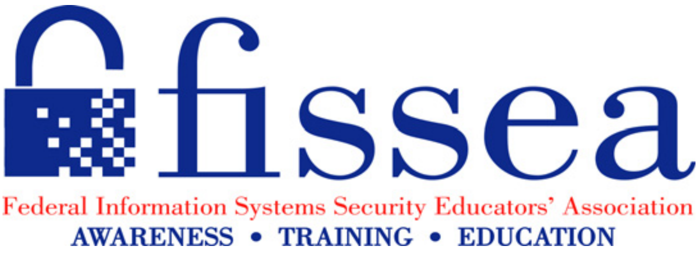
FISSEA LOGO

In case you hadn't noticed FISSEA has a new logo. David Kurtz and Jose (Joe) Matias from the Bureau of the Public Debt submitted the winning entry to our logo competition following our 2005 conference.

Our old logo has served us well for many years but its design has been overtaken by technology. We no longer actively use 5 ¼ or 3 ½ floppy diskettes as storages devices. The image showed a mortar board made up of four computer disks surrounded by the words FISSEA Awareness, Training, and Education, see below.



The new FISSEA logo is shown below. This uses a digitized (as in high tech information systems) lock (as in computer security) that mimics a similar arc when placed next to the lower-case "fi" in fissea.


fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Though the new logo spells "fissea" in lower case we still want "FISSEA" to be utmost in your mind.

Congratulations to our logo contest winners. If you wish to meet them, come to our Conference!

4th FISSEA WORKSHOP SUMMARY

"Best Practices for Executive-Level Training: A Panel Discussion"

By: Susan Hansche, CISSP-ISSEP
Program Manager, Nortel Government Solutions for the U.S. Department of State, Information Assurance Training Program

On October 12th, over 35 FISSEA members attended the 4th FISSEA Workshop (offered free to FISSEA members) on "Best Practices for Executive-Level Training: A Panel Discussion." The U.S. Department of State Information Assurance (IA) Training Group sponsored the panel discussion at the Diplomatic Security Training Center in Dunn Loring, Virginia. It was a morning full of activities (including a fire-alarm drill) and discussions on the best practices for how to design and develop training for the executive role as part of an agency's role-based IA training program. We were pleased to have four panelists who brought unique perspectives on what their organizations consider to be the best practices for executive training. In this overview, I will highlight the key points of the panelist presentations and then provide a summary of additional items that were discussed during the question and answer period.

The four panelists in order of appearance were:

- Patricia Harris, Course Manager/Senior Instructor at the U.S. Department of State, under contract from Nortel Government Solutions
- Joshua Feldman, IT Security Engineer/Trainer at the Defense Information Systems Agency.
- Jim Litchko, President of Litchko Associates
- Gil Duvall, Professor of Systems Management at the National Defense University

Each of the panelists was given 10-15 minutes to discuss best practices for providing IA training for the executive-level role. The next section provides an overview of their key points.

<u>Patricia Harris – "Department of State IA for Executives Seminar"</u>

- Provides an instructor-led 2-1/2 hour training course.
- Two primary objectives of the training:
  - Stress the importance of having executive support for IA initiatives
  - Explain the seriousness of the threats and vulnerabilities
- Threat demonstrations can make a big impact – something as simple as showing a password cracking tool such as LoPht Crack can really catch their attention. Executives will need to enter in their own password and can judge how long it will take for the tool to decode their password.
- As the leaders of the organization, they can create a climate and set the tone for IA; thus, they can be conduits for a change to create a culture where IA is of importance.
- Bring up the recent score cards or OIG reports to show the serious nature of compliance with IA initiatives.
- Discuss the risk management approach and their role in accepting risk for the organization.
- Discuss the IA team that is in place and how the executives can provide support to those employees.
- Discuss the role that executives have in handling incidents – are they setting a good example as the leader.
- Have them create an action list of items they need to do bring about a culture change that values IA

<u>Joshua Feldman "Training and Certifying Executives Across the DoD"</u>

- Due to the Department of Defense (DoD) decentralized approach to building and acquiring information systems, there are many systems and each system has a Designated Approving Authority (DAA)
- Currently, an executive with significant security responsibilities would also be the DAA. The DAA is defined as having budgetary

responsibilities for either development or operations of a system or both.

- There are approximately 12,000 to 15,000 DAA (executives) that need IA training.
- The most feasible solution was to use distance learning products.
- DoD policy states "If you are a DAA, you must take the DISA DAA Computer Based Training (CBT)."
- There are several DISA CBTs and many have been converted to Web-Based Training (WBTs) – their website is: www.iase.disa.mil. DISA offers their CBT and WBT courses free to government agencies.
- One of their challenges is to track who has taken the training. A new initiative, the "IA Learning Center" is in pilot phase and will be able to help resolve the tracking issue. The "IA Learning Center" is based on a Learning Management System (LMS) that will not only provide the courses, but will also track student registration and completion.
- DISA has found that training material that is has been approved and blessed by senior management is the most efficient.
- The training team must work in conjunction with the policy team; otherwise training will lag 6-12 months behind new policy initiatives. Instructional design can begin while the policy is being written and can be released when the policy becomes final.

Jim Litchko – "Best Practices for Executives"

- Trainers need to understand the executive's mission or business. In order to be effective, it is necessary to tie in the importance of IA with the importance of the organization's mission or the mission that a particular executive is responsible for.
- It is necessary to know the executive's goal and to meet the executive's goal and not your own goal.
- Other than a formal training course, you might have 5-7 minutes to talk to an executive about an IA issue. During this time frame you have to be able to get your point across, which is to explain the problem AND also provide a solution.
- An outline that might be helpful for this 5-7 minutes is:
    - o Know your audience – be prepared for what they will want to know (i.e., how much will your recommended solution cost)
    - o Explain the purpose of the meeting – this should take no more than two sentences.
    - o Explain the problem and it how it relates to the mission or business.
    - o Explain the options available.
    - o Express your recommendation.
    - o Then wait for questions and be prepared to answer the tough questions.
- Be respectful of their time. They have many important problems to resolve; IA is not the only problem.
- Take into account the budgetary process and timing. Do not recommend solutions that cost money after the budget has been determined.

Gil Duvall "IA Teaching Laboratories"

- National Defense University (NDU) has four colleges, one of which is the Information Resource Management College (IRMC). NDU has two masters degree programs.
- IRMC has several information system security, CIO, IT Acquisition, and Organizational Transformation certificate programs in additional to elective courses for the National War College (NWC) and the Industrial College for the Armed Forces (ICAF).
- The College is also approved by the Committee on National Security Systems (CNSS) to award the Information Systems Security Professionals Certificate (CNSSI No. 4011) and the Senior System Managers Certificate (CNSSI No. 4012), and the Chief Information Security Officer (CISO) Certificate.
- A key component of their educational offerings is various simulations and lab exercises. These include:
    - o Cyber Protect Simulation – this is a network attack simulation and is a DISA CBT product
    - o Attack and Defend Hacker Challenge – this is a series of red team/blue team attack and defend scenarios
    - o Sniffer, Firewall, and Intrusion Detection labs
    - o Authentication and Biometric Labs – this lab provides the opportunity to use voice, fingerprint, and iris recognition equipment

and explore the pluses and minuses for each type of system
  - Cryptographic labs – hands-on opportunity to use PKI in various situations
  - Steganagrophy labs – shows how easily messages can be encoded and decoded
  - Wireless network labs – includes using tools to conduct war dialing and war chalking
  - Digital Forensics labs– a new lab that explores the searching and seizing of computer equipment and explores the chain of custody and other legal issues involved
  - SCADA labs – show how the SCADA network is designed and the vulnerabilities that can be exploited
- In order to accommodate the executive, they have identified a schedule or profile for executives that takes either 60 or 90 minutes (depending on 1 or 2 labs):
  - Introduction to the topic – 10 minutes
  - Mini-lessons – approximately 15-20 minutes
  - Biometric lab – 25 minutes
  - Wireless lab – 25 minutes
- Their labs are built to be mobile, so they can bring the lab exercises to the executives.
- They also conduct various threat demos such as password cracking and Trojan horse (malicious code) infections such as NetBus and Sub7.

In order to make sure all panelists had an opportunity to present their material, the questions were held to the end of the presentations. At this time, the following items were generated as additional best practices for executive IA training:

- In order to get the executive to understand the importance of IA initiatives, take advantage of the FISMA reporting schedule, either the quarterly requirement or the year-end roll-up in September.
- Having a diverse group of students together provides the best results. It provides an opportunity for participants to hear what others in the organization are doing and also avoid group-think. It can also keep the focus on the mission of the organization and not on the technical mission.
- Checklists can be helpful – it provides an easy way for executives to look at what needs to be done, who is responsible, and how they can provide support to those employees.
- Executives need to know the standards and policies.
- Allow the executives an opportunity to express their knowledge as well.
- Timelines for training, such as "executives need formal training every two years" are good, but training should be centered on new risk perspectives or changes to the risk tolerance level. Thus, training must also have a just in time feature so that new material can be injected as needed.
- Need to have an on-going focus so that the message is reinforced.
- Combine training with policy changes.
- Training is also an agent for change; especially attitude change that will create an environment that will support IA.
- "Good teaching is still good teaching" -- bring out your best and also allow them to learn from each other.

I would like to add one final comment about FISSEA's workshop on role-based IA training for executives -- a two-hour workshop is just not enough time! Again, a special thank you to the panelists and all those that attended, there were so many interesting observations, discussions, and comments. If you would like to contribute additional ideas or suggestions about how to best provide IA training to the executive role, please feel free to send comments to the FISSEA list serve or directly to me susan.hansche@nortelgov.com.

{FISSEA would like to thank the US Department of State Information Assurance Training Group for sponsoring this panel discussion at their Diplomatic Security Training Center. Attendees agreed that the session was quite worthwhile and held in comfortable surroundings. Thanks for the tasty treats, as well, and a Special FISSEA Thank You to Susan for coordinating the panel. Louis N.}

Conduct vs. Security

By Joe Fields and James Hackley

Pearl Software

Employee conduct is the foundation for the success or failure of any enterprise. Efficient government agencies are defined by their ability to promote a culture of excellence within the workforce while eliminating distractions and unnecessary risk from the workplace. Network managers within these agencies are expected to limit misconduct within their networks while managing an increasingly mobile workforce and continuously evolving network environment. Now, regulatory mandates such as FISMA, HIPPA and Sarbanes Oxley require agencies to implement extensive information security programs. Failure to comply with these regulations may not only result in hefty fines & penalties but also an increased risk to National Security.

Network managers have always known that the misuse and abuse of network resources by employees is a significant source of risk and lost productivity within government agencies. Careless or negligent conduct by employees reduces resource availability, compromises security policies and exposes vulnerabilities in the electronic communications (e-communication) systems of these agencies. Now, these managers are being asked to fortify systems that are being accessed by employees, virtual employees, business partners, contractors and outsourcing service providers, just to name a few.

Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) have developed comprehensive systems security to manage the increasing risk posed by employee conduct. With proper changes, and the use of new monitoring technology that consistently enforces these policies down to the user level, government C-level officers and network managers can effectively manage the risk of employee conduct and systems abuse.

Comprehensive Policy Management & Enforcement

The solution or tools agencies rely upon must deliver real-time management of all e-communications (email, encoded attachments, IM, Internet, FTP, etc.) on every workstation regardless of its physical location or type of internet connection used. This solution must also provide flexible configuration and control over employee usage policy that is consistent with their HR and information security policies.

Legacy monitoring solutions, attempted to address the issue of usage control by routing all e-communication traffic through security appliances within their networks. This approach forced network managers into trade-offs to either increase information security or improve network performance. Often, these single-threaded security appliances created bottlenecks and increased latency. They also often required network managers to re-engineer their architecture to overcome the complex integration and compatibility issues resulting from distributing these appliances throughout their network.

A greater concern for most security officers, however, is that a strategy based exclusively upon specialized appliances cannot eliminate circumvention when a user's communications pass across foreign networks or through external devices such as modems. Because of these limitations, many network managers are adopting a new approach to independent workstation management.

The fundamental driver behind their new approach is the emergence of monitoring technologies that balance both centralized user administration & records archival and real-time traffic analysis & control across existing network resources. This approach utilizes a centralized administration platform to bond user/group usage controls onto the Windows communication architecture of the workstations or Terminal servers themselves. It delivers several significant advantages because it not only increases visibility into an employee communication patterns, but also extends management onto mobile devices.

Unlike the bottlenecks and latency associated with a specialized appliance or proxy server-centric approach, the independent architecture of these emerging monitoring technologies often improves IT performance by ensuring legitimate bandwidth utilization throughout the workforce. Another tremendous advantage of these new technologies is that they monitor, filter and control the full content of e-communications down to the user level, providing agencies with the ability to quickly reconstruct comprehensive forensic quality data for any monitored user.

The evolution of these new monitoring technologies is being fueled by government agencies' demand for comprehensive risk management solutions that capture and control the e-communications activities of their workstations regardless of their location or type of connectivity. Increasingly constrained IT budgets have created additional pressure for these solutions to also provide a lower total cost of ownership, delivering increased automation and an economical means of installation and compatibility within existing network hardware, middleware and firewalls. The emerging suite of e-communication monitoring, filtering and control solutions address these needs, delivering a straightforward and cost-effective approach to managing risk within the workplace.

For additional information about emerging monitoring technologies or questions about Pearl Software, please contact the corporate headquarters at (800) 732-7596 or email information@pearlsw.com.

The Perfect Dead Drop

By James E. Wingate, CISSP/CISM
www.BackboneSecurity.com

Dead drops, or physical locations for the clandestine exchange of intelligence information, are a standard part of the field agent's trade craft and have been portrayed in countless movies as predetermined hiding places for the deposit and distribution of classified or sensitive information and other illicit goods such as drugs, stolen property, or money extorted by kidnappers in exchange for the safe return of someone who has been abducted.

The vastness of cyber space provides the perfect place to establish digital dead drops for conducting covert communications. Whether a hidden message is a clear and present danger such as those of terrorists planning another attack or is something much more mundane such as Bob from Accounting having a clandestine affair with Sally in Human Relations, anyone can obtain easy to use tools freely available on the Internet to establish covert channels for communicating anything to anyone at any time and at any place on the Internet.

Steganography, or the art of *covered writing*, has been used throughout the ages to conceal messages between senders and receivers from being viewed by others. The Digital Age has provided fertile ground for the evolution of steganography from the physical world to the virtual world of cyber space.

The Internet provides a practically infinite number of places where those who wish to communicate covertly can establish virtual dead drops. Imagine the billions and possibly trillions of files on web sites or floating around the Internet as attachments to e-mail each and every day. Coupled with that, consider the large number of freely available digital steganography applications that are easy to find and simple to install and use.

The combination results in a *Perfect Storm* scenario for covert channel communications that represents an extraordinary challenge for law enforcement, intelligence community, and private sector computer forensic examiners.

I've just finished reading the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2004[1] and remain very concerned about the acquisition of classified, sensitive, and proprietary information by foreign entities, both government and private. To me, it's a no-brainer that foreign operatives are using digital steganography applications to conduct both economic and industrial espionage against the US. It is equally likely that domestic entities are using these applications to conduct industrial espionage against both domestic and foreign competitors.

In addition to these national and homeland security concerns, digital steganography provides an excellent means for criminals to conceal illegal

[1] www.ncix.gov

activity in cyber space. For example, digital steganography provides a convenient, easy to use, and difficult to detect means for distributing child pornography, arranging drug deals, and any other type of illegal activity that you can think of.

It is also important to understand that not only can web sites on the Internet be used as dead drops for information in one digital file hidden inside another digital file, but individuals can also use digital steganography applications to communicate directly with each other via email and hide their secret communication in text, image, video, or audio files attached to the e-mail—with little concern for their secret communication being detected.

Ultimately, whether the hidden information is in a file on a web site or in a file on an individual's computer, an application had to be installed on a computer, or possibly two or more computers, to hide the information. Discovering the application used to hide information just might be the key to unlocking the hidden message or otherwise extracting it from the carrier file.

Digital steganalysis, or the detection of digital steganography applications and extraction of hidden information, is a very young and evolving extension of traditional digital forensics that is relatively unknown by the vast majority of digital forensics practitioners in the field. A June 2002 assessment by the Institute for Security Technology Studies (ISTS) at Dartmouth College[2] included steganography as one of the emerging technologies requiring research and development and stated that "Steganography also represents immediate and long-term challenges for law enforcement."

The Steganography Analysis and Research Center (SARC) was established within Backbone Security with the objective of becoming the clearinghouse for digital steganography applications called for in the ISTS assessment. Beyond establishing a comprehensive hash set of files that can be associated with a particular steganography application, a major objective of the SARC is to encourage practitioners to extend their digital forensics examinations or investigations to include steganalysis.

Our philosophy in the SARC is that if an artifact (i.e., file or Windows Registry key or value), or several artifacts, associated with a steganography application is found to exist on seized storage media, then there is a very high probability the associated steganography application was used to hide something. The examiner's task then becomes one of trying to find where the information may have been hidden and then trying to figure out what was hidden by extracting the embedded file containing the hidden message from the carrier file.

The "traditional" *blind detection* approach to steganalysis may give an indication that information may be hidden in a particular file and may provide some clues to the application that may have been used, that approach is not without its limitations. Accordingly, the SARC is approaching steganalysis from a different perspective that we refer to as the *analytical detection* approach to steganalysis. The analytical approach attempts to determine which application may have been used to hide information. Then, knowing enough about how that application embeds information, it may be possible to extract the hidden information. One of the techniques used to determine how a particular application embeds information is to hide a known message in a reference image known to not contain any hidden information and then do a side-by-side comparison of the reference image with the carrier image with a hex editor. Taking that approach has led to the development of hex byte patterns, or signatures, unique to particular applications. An examiner can search all the files on suspect media for the presence of any of the signatures. When found, techniques and procedures developed in the SARC can be employed to extract the hidden information. A major potential show stopper is encountered if the message was encrypted with a strong encryption algorithm, such as 3DES or AES, prior to being embedded in the carrier file.

As my good friend, Russ Rogers, wrote in Part 2 of his series on Covert Channels, our ability to detect the use of digital steganography

[2] http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf

applications is lagging years behind the technology being used to create the applications.[3]

We must put forth whatever effort is required to catch up. We can't just simply admire the problem, wring our hands, and say "Oh my, that's too difficult to do."

Ultimately, digital steganography and the Internet combine to be the perfect dead drop for clandestine communications. This represents an extremely high threat to our Homeland Security, Critical Infrastructure Protection, and the continuing battle against cyber crime—a threat that is not widely perceived or appreciated.

Accordingly, we must face the threat and challenge posed by use of digital steganography head-on. We must adopt a "full-court press" mentality and approach to develop the tactics, techniques, and procedures along with the automated tools needed to both detect the use of digital steganography and extract the information hidden with those applications.

A Fruitful First FISSEA

By David Kurtz
Bureau of the Public Debt

I attended my first FISSEA Conference last year, and did not leave empty-handed. One of the many interesting presentations I attended was "The West Point Carronade" by Aaron Ferguson. It detailed an information awareness exercise conducted at the U.S. Military Academy. Suspicious e-mails were sent to the entire student body to see if they would fall for them. It was a very pro-active (some might go as far as to say "sneaky") approach to user education.

We decided to try our own version of this exercise on the more than 1800 employees of the U.S. Treasury Department's Bureau of the Public Debt. The increasing number of "phishing" e-mails that contain embedded links became our focus (most of our employees have been conditioned to not open unexpected e-mail attachments, but some don't understand the new dangers of merely clicking on a link). Each year, we try to do something special for Computer Security Day, so this special project was set for November 30.

Specialists within Public Debt's Office of Information Technology (with the knowledge and support of management officials) created an e-mail that was sent from an external Internet service provider (ISP) to all employees. It contained a number of "red flags" designed to raise suspicions, such as misspelled words, a spoofed commercial address, two variations in the spelling of the same name, etc. This fake phishing e-mail was sent to all Public Debt employees, but the recipients were designated as "user@bpf.trea.go," an obviously incorrect and suspicious address (one would normally expect to see "bpd.treas.gov").

An embedded hyperlink was included that, if clicked, led to a special webpage created for this exercise on our internal network. This webpage exclaimed "Happy Computer Security Day!" and went on to educate the reader as to why they should not have clicked on the link. In addition, the webpage suggested further remedial education through several on-line options.

There was no effort made to trace the individuals who landed on the webpage—it was not intended to be the grounds for any discipline. Based on a simple count of visits to this particular page, only about 6% of Public Debt's workforce viewed it that day. There was quite a "buzz" created by this pro-active approach to user education. The next day, an explanation of the exercise was sent to all employees, and everyone was encouraged to view the special webpage. We were pleased with the overall success. As a result of this exercise, Public Debt employees are more attuned to the dangers of clicking on embedded hyperlinks within e-mails.

I never would have tried such an exercise (nor could I have sold it to upper management) had I not attended the FISSEA Conference last year. It was a fruitful experience—because there were

[3] http://www.securityhorizon.com/journal/spring2005.pdf, *Covert Channels: Part 2*

many other ideas that I took home with me as well. I am looking forward to attending the 2006 FISSEA Conference. Hope to see you there!

The FISSEA Annual Conference

What it means to me…

By Gretchen Ann Morris, CISSP

I once wrote a poem that started like this…

I need a place where I belong
To be a part of things
A group of friends to do things with
Relax, create, or dream

Now before you skip to the next article, because this one is too philosophical or emotional, follow along with me for a little bit.

The first conference I attended was in March of 2001. I went with my new co-worker (Bob Solomon). He had attended the conference for a few years already and was looking forward to going. He had invited our whole team to go and encouraged us that we would learn new things, get new ideas, meet others who do what we do, and become better at what we do by attending. I went with him and had high hopes; I was not disappointed.

When I had attended other conferences that were related to the work I had done in the past; I learned some things that were helpful. But, I had never found the sense of camaraderie, teamwork, or kinship that I remembered from when I was in the service as I did when I went to my first FISSEA conference. I met vendors who wanted to help, contractors who were striving to find answers and support their agencies, and civil servants who wanted to find ways to work smarter and get quality work done with limited resources.

I learned:

- how others were implementing recent laws and regulations
- what types of awareness, training, and education efforts were happening
- that there was such a thing as chocolate-covered espresso beans
- that security can be fun
- what others were doing to support their agencies

Bob also taught me to share. We went to learn from everyone else, we also went to share with everyone what we were doing. This is truly one of my most favorite aspects of the conferences.

I have gone to the FISSEA conference every year since that first visit. It has never been disappointing. It has never been boring. I learn something new every year, I get new ideas and I've shared our ideas with others. I've met new friends and fellow Information System Security educators who desire, as much as I do, to do what is best with the resources we are given to make our Agencies more secure through our awareness, training, and education efforts. We have to travel from Cleveland, OH, but my whole team will be there this year because we find it to be worth every penny! We hope to see you there!

Gretchen Ann Morris, CISSP
RSIS / NASA IT Security Awareness and Training Center
FISSEA Executive Board Member

Strengthening the Federal Cyber Corps:

The Federal Cyber Service: Scholarship for Service (SFS) Program

By Dr. Diana L. Burley
National Science Foundation

The Federal Cyber Service: Scholarship for Service (SFS) program, offered by the National Science Foundation (NSF) and co-sponsored by the Department of Homeland Security (DHS), seeks to increase the number of qualified students entering the fields of information assurance (IA) and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields. The SFS program was established as the result of a January 2000 Presidential Executive Order that defined the

National Plan for Information Systems Protection, and is a component of the Federal Cyber Service Training and Education Initiatives.

The SFS program vision is to enhance the security of the federal critical information infrastructure by providing funds to colleges and universities for capacity building and scholarships in IA. In order to qualify for NSF funding, an institution must first be designated as a Center of Academic Excellence in Information Assurance Education (CAEIAE) by the National Security Agency (NSA) and DHS, and must then be selected through a highly competitive NSF proposal review process.

Institutions use capacity building dollars to support faculty, institutional, and partnership development. Since the program inception in FY 2001, NSF has distributed $13,793,131 to more than 70 institutions for course development, laboratory improvement, and faculty training. Further, capacity building funds often are used by CAEIAEs to broaden participation in IA through partnerships with Historically Black Colleges and Universities, Community Colleges, and other underrepresented institutions.

Scholarship awards provide funding to institutions to support students in the final two years of undergraduate or graduate education in IA. To date, NSF has distributed $71,619,223 in scholarship funds to 26 institutions. Scholars receive up to two years of scholarship support that includes tuition, stipend, room and board, and fees. Upon graduation, scholarship recipients agree to work for a Federal agency for a period equal to the length of their scholarship period. Since the first scholarship recipients entered the program in 2001, NSF has supported approximately 715 SFS scholars with more than 375 of them now working in the Federal cyber workforce.

In January, the SFS program held its Annual Symposium and Job Fair in Washington, DC and hosted more than 400 scholarship recipients, university faculty, agency representatives, and invited guests to the 3-day event. The agenda featured sessions on career opportunities in the Federal cyber-security workforce, industry certifications, and a briefing on the DHS Cyber-exercise, “Cyber Storm.” The job fair welcomed over 35 Federal agencies and more than 100 students left the job fair with conditional job offers for full-time employment. These future members of the Federal cyber corps, along with the hundreds of other students around the country who benefit from advanced curriculum and state-of-the-art security laboratories provided through capacity building funds, will make a significant impact toward enhancing the security of the federal critical information infrastructure.

For more information on the SFS program, contact:

Dr. Diana L. Burley, SFS Program Director
PH: 703-292-8669, Email: dburley@nsf.gov
SFS program website: http://www.sfs.opm.gov

The Human Side of Section 508

By Trevor J Osgood and Russ Mumford

Introduction

We all need to be cognizant of our responsibilities to make our web sites and software accessible to all users. We've all heard of Section 508 and a lot of us are probably scared of it. It’s impossible to read or interpret not only for the layperson but also for the majority of decision makers. In this series of 4 articles, we'll put a human face on Section 508 and return the dialogue to good, old-fashioned common sense. Section 508 isn't a construction manual; it's a set of abstract standards with some (obsolete) examples. By the time we're done, you'll know the basic terminology, the concepts they represent and you'll be a more informed decision maker.

A Brief Perspective on Website Accessibility.

Let's look at this from a historical perspective. Initially, web designers tended to be young, bright-eyed go-getters. Lacking many precedents for the new medium of the Internet, they designed web sites that looked good to them. The result was frequently something that was "intuitive" for a 20-something who spends all his spare time playing video games. For many of "the rest of us", understanding and using these web sites presented a challenge. It also quickly became apparent that they were impossible for a great many persons with common disabilities.

The Downfall of Inaccessible Web Sites and Software.

This is a lamentable condition. Being able to interact with the world and to obtain basic services online should be a high priority. We can deliver many services more economically and immediately online which are less costly for the public to obtain and can be delivered to remote areas 24x7x365. And when we talk about economy, we're talking about public citizens, not just institutional budgets.

We can all see what a great thing wheelchair access to our public buildings is for the wheelchair-bound. Now imagine the time and expense saved for that person if they can obtain the same services and never have to leave the house.

How Many People Are Affected With Disabilities?

These examples can be misleading. Most of the disabilities we encounter that make it difficult to use the web aren't as extreme as immobility. A lot of them are age-related issues that most of us will face in our lifetimes. It's commonly held that 20% of the population is affected with a disability of some sort. The figure remains relatively static from year to year. In itself, this represents a large portion of our population. If we look at percentages of disabled persons in various age groups, we get a better idea of how many persons in our specific audience are affected with disabilities.

Age Group	Percent with Disability
All Ages	19.7%
Under 15 years	7.8%
15 to 24 years	10.7%
25 to 44 years	13.4%
45 to 54 years	22.6%
55 to 64 years	35.7%
65 years and over	54.5%

U.S. Census Bureau: Americans with Disabilities
http://www.census.gov/hhes/www/disable/sipp/disab97/ds97t1.html

Clearly, if we're communicating to groups of adults, we can estimate that between 1/4 and 1/2 of our audience is challenged by inaccessible websites. Alas, the older we get, the more difficulties we may have.

The Range Of Disabilities Affecting Web and Software Users.

Despite the broad range of disabilities affecting website accessibility, we can categorize them into four basic groups: Cognitive/behavioral, Visual, Mobility and Auditory.

- Cognitive/behavioral disability includes extreme disability such as autism, but also more common disabilities such as dyslexia, a language-based learning disability (about 15-20% of us have them) or Attention Deficit Disorder (4-6% of population) http://www.interdys.org/servlet/compose?section_id=5&page_id=95 -How%20common%20are%20language-based%20le http://www.add.org/articles/factsheet.html.

I also have to note, with some chagrin that about 60% of our population reads at a 6th-grade-or-below comprehension level. Clearly, part of accessibility involves neither speaking nor writing over people's heads.
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=1999470

- Visual disabilities include folks who require glasses, color-blind (a surprising 6% of the population), partially blind persons, or blind people.

http://www.stlukeseye.com/Conditions/ColorBlindness.asp

- Mobility challenges can include partial to full paralysis, fine-motor coordination challenges and disease-related challenges such as the palsy that accompanies Parkinson's disease.
- Auditory dysfunction such as deafness or common age-related hearing loss can affect the online experience particularly with multimedia presentations.

What We've Learned.

Fortunately, we've made great progress in developing web technologies that are accessible to persons with these broad spectra of disabilities. What we've learned has also allowed us to create standardized approaches to information presentation so that's it's easier for the rest of us to work with and understand. These technologies are lighter-weight than previous web development techniques, so they offer greater accessibility to persons with slow, dial-up Internet connections, a key accessibility metric. The new approach is called Standards-Based Web Development but the principles exactly parallel any software development project.

And Some Good News.

Not only is the information we see and interact with on the web evolving, the browsers that most of us use to access it are getting better and we as Internet users are getting better at using them. What this means to you is that a good deal of what is written in Section 508 is obsolete, has been shown to be "a bad idea" or simply doesn't present itself as a problem all that often these days.

For the length of this series on Section 508, Greenidea, Inc. and dataSpheric will be moderating an online discussion where we hope to answer some of your more specific questions. Please drop by ask your questions and add your viewpoint. The address for the forum is:

http://www.dataSpheric.com/services/508/forum/

Trevor J Osgood, trevor@dataSpheric.com
Russ Mumford, Mumford@greenidea.com

FISSEA's 19th Annual Conference will provide you with Training Wheels for a Cyber-Secure Future

FISSEA Executive Board 2005-2006

Louis Numkin, CISM, Board Chair**
louis.numkin@irs.gov
COL Curt Carver, Jr., Conference Co-Director**
curtis.carver@usma.edu
Barbara Cuffie, CISSP, Assistant Chair**
4312@yahoo.com
Thomas Foss*
tomfoss@usa.net
Susan Hansche, CISSP-ISSEP**
susan.hansche@nortelgov.com
James Litchko**
jim@litchko.com
Gretchen Ann Morris, CISSP*
gretchen.a.morris@grc.nasa.gov
K Rudolph, CISSP**
kaie@nativeintelligence.com
Jeffrey Seeman*
jaseema@nsa.gov
Mary Ann Strawn, Publicity*
mast@loc.gov
LTC Will Suchan, CISSP, Conference Co-Director*
will.suchan@us.army.mil

NIST Contacts (Not Elected):
Mark Wilson, CISSP, NIST Liaison
mark.wilson@nist.gov
Peggy Himes, Executive Assistant to Board
peggy.himes@nist.gov

* Term ends March 2006
** Term ends March 2007

FISSEA List Serve:

The NIST Computer Security Division is hosting the FISSEA membership e-mail list in support of FISSEA and the federal IT security community. The list is not moderated; any FISSEA member subscribed to the list can post a message directly to the list. This list will allow us to converse with other IT security professionals who have an interest in awareness, training, and education issues. Any issue related to federal IT security awareness, training, and education is fair game. It can be used to ask for help from the many veteran FISSEA members who have experience designing, developing, implementing, and maintaining awareness and training programs. Please refer to the FISSEA website for complete rules and guidance. To summarize the rules:

- No spam nor advertising unless it is for free training/workshops
- Respond to the sender rather than "reply to all"
- Avoid "me too" replies
- Do not send attachments

To post a message to the entire list, send it to fissea@nist.gov
If you want to be added or deleted send a message to fisseamembership@nist.gov

FISSEA

Federal Information Systems Security Educators' Association

Building better Computer Security through Awareness, Training, and Education

TRAINIA

This column's name is a contraction of the words "Training" and "Trivia." It includes information on upcoming conferences, book reviews, and even humor. The purpose is to provide readers with places to go and things to use in pursuing and/or providing Computer Security awareness, training, and education. However, FISSEA does not warrant nor determine the value of any inclusions. Readers are encouraged to do their own checking before utilizing any of this data. If readers have items to submit to this column, please forward them to Nan Poulios at nan.poulios@walshcollege.edu and Louis Numkin louis.numkin@irs.gov.

****

Are you a FISSEA Fuddy Duddy? If you were part of FISSEA in its early days, please contact our Exec Board Chair, Louis.Numkin@irs.gov

****

ISACA March/April offerings:
23-4MAR2006 8:00 a.m. to 4:30 p.m. - ISACA Introduction to IT Auditing - at the Inter-American Development Bank, 1300 New York Avenue, N.W., Washington DC 20577 - 14 CPE credits - more info at: http://www.isaca-washdc.org/content/events/seminar-Mar2006.htm

28MAR2006 9:30 a.m. to 1:30 p.m. - ISACA National Capital Area Chapter's March Monthly Meeting - An Introduction to Web Application Security - at the Holiday Inn Capitol, 550 C Street, SW, Washington, DC. - 3 CPE credits - more info at: http://www.isaca-washdc.org/content/events/monthly-Mar2006.htm

11-2APR2006 8:00 a.m. to 4:30 p.m. - ISACA Special Seminar - Sarbanes-Oxley for IT Auditors: How To Do It and How To Audit It - at George Mason University, Arlington Campus - 14 CPE credits, $500/person - more info at: http://www.isaca-washdc.org/content/events/seminar-Apr2006.htm

****

March 28, 2006 FREE SANS Webcasts
WhatWorks in Log Management: "Caring for Logs with Northwestern Memorial Hospital" Tuesday, March 28 at 1:00 PM EST (1800 UTC/GMT) Featuring: Alan Paller & Asad Syed https://www.sans.org/webcasts/show.php?webcastid=90685
Sponsored by LogLogic

****

April 25-27, 2006 GOVSEC, U.S. LAW and READY. America's premier homeland security event. Washington Convention Center, Washington D.C. Government rate $195, Industry rate $895. Registration url www.govsecinfo.com.
April 25, 2006 FISSEA Workshop: What's new in Security Awareness, Training, and Education" during the GovSec conference. Professionals from the commercial and government sectors will share their experiences on how to effectively increase employee, executive and public awareness through awareness, training and education. This workshop will present various successful techniques and technologies that can be used to motivate groups and individuals to prepare for potential attacks on their computers and communities. This workshop will be interactive to ensure that ideas are shared from the panelist and the audience to provide solutions for diverse situations. Attendees will learn when to use posters, presenters, promotions, PR, etc.; what are the technology advances, like interactive, automated, web-based awareness; improved training and education strategies; and sources for maintaining awareness. Presenting during this workshop, will be Barbara Cuffie, CISSP, former Principal Security Officer, SSA, Louis Numkin, CISM, IT Security Officer, IRS, Susan Hansche, CISSP-ISSEP, IA Training Program Manager, Department of State/Nortel Government Solutions, and Jim Litchko, Senior Security Consultant, Litchko & Associates, Inc. This is a free seminar for everyone interested in improving their security awareness, training and educational programs. Registration for the free FISSEA workshop is on a walk-in basis.

****

April 26, 2006 NIST FISMA Implementation Project Phase II: Workshop on Credentialing Program for Security Assessment Service Providers. 9:00a.m. 4:00p.m. National Institute of Standards and Technology, 100 Bureau Drive, Red Auditorium, Gaithersburg MD 20899. NIST is holding a public workshop to discuss Phase II of the FISMA Implementation Project and proposed requirements for credentialing organizations to conduct information security assessments of federal information systems, including those information systems operated by contractors on behalf of the federal government.

Workshop topics: Overview of the FISMA Implementation Project, Overview of Key Documents Produced in Phase I of the Project, Strategy and Vision for Phase II of the Project, Prospective Models for Credentialing of Security Assessment Organizations; and Proposed Requirements for Service Providers and Oversight Bodies. Concurrent breakout sessions will be held in the afternoon of prospective credentialing organizations/authorities, service providers, and consumers of security assessment services to discuss workshop topics. Attendees can comment on the material presented and/or provide their own inputs/ideas on the proposed credentialing program.

The registration fee is $20 per person and includes coffee breaks, lunch, and workshop materials. Pre-registration is required and must be done by April 19. Cancellations and/or substitutions must be requested, in writing, by April 19, and no refunds will be made after this date. Due to increased security, no on-site registrations will be accepted and all attendees must be pre registered. Electronic registration: https://rproxy.nist.gov/CRS

See the FISMA Implementation website < http://csrc.nist.gov/sec-cert> for additional workshop information including directions. Technical contact Arnold Johnson, Arnold.johnson@nist.gov or Pat Toth, patricia.toth@nist.gov. Administrative contact Peggy Himes, peggy.himes@nist.gov

****

5th FREE FISSEA WORKSHOP COMING IN MAY
The First Step in Developing a Role-Based Training Program: Identifying Who Has Significant Information Security Responsibilities. FISMA states the Chief Information Officer is responsible for ''…training and overseeing personnel with significant responsibilities for information security … (H. R. 2458—52 (3) D). One of the first steps in designing a role-based training program is to "identify your audience" – for this you will need to identify who within your organization has significant

responsibilities for information security. Please join us for an interactive discussion and sharing of ideas, thoughts, and experiences in how to answer this question. *(Details will be announced through the FISSEA list serve.)*

****

May 7-11, 2006 ISACA will host its North America Computer Audit, Control and Security Conference at the Royal Pacific Resort at Universal Orlando in Orlando, Florida. Attendees can earn up to 44 CPE hours. More info at www.isaca.org/nacacs

****

June 12-14, 2006 CSI NetSec 06 will be held at The Phoenician Resort in Scottsdale, AZ. It focuses on the *practice* of information security—speakers understanding is from real-world experience and practitioner point of view. 13 Tracks with 90+ sessions. Interested, check out: **http://www.csinetsec.com/**

****

June 19-20, 2006. AFCEA TechNet International "TechNet International 2006 will provide a unique opportunity for U.S. Combatant Commanders, Homeland Security/Homeland Defense activities, and traditional international coalitions to explore emerging information sharing and interoperability solutions." - Gen James L. Jones, USMC, Commander, U.S. European Command. For a current list of exhibitors, go to: http://expo.jspargo.com/tni06/exhibitors.asp. A detailed agenda, a listing of speakers, fees, general information and hotel reservations, go to http://www.afcea.org/events/technetinternational. https://reg.jspargo.com/technet06/reg/

****

During our conference, be sure to ask MaryAnn Strawn from the Library of Congress about the "Smencils" (scented pencils made from recycled newspapers) that are available in the Jefferson Building. Flavors include: bubble gum, cherry, root beer, peppermint, cinnamon, cookie dough, chocolate milk, and hazelnut latte (the latter three have not received good reviews in the Washington Post), and the cost is $1.50 each.

****

Computers, PDAs, and IM aside, it appears that people are getting back to the fine art of *writing*. Remember, writing used to be what we did with pen/pencil and paper before technology took us down a different course. Of course, we could write on our computer journal but we will have lost some of the beauty and flair that existed when your hand held a Papermate and you jotted thoughts in your Moleskine. These little black notebooks which are similar to those used by Papa Hemingway are making a comeback even alongside or in place of the high tech newbies. It's a low tech solution to a high tech problem. If you really can't separate your hands from the computer, Moleskines can double as mousepads (get it, paper pad to mousepad!). These retro devices are making a statement for you, the user: "I don't need no stinkin' keyboard to write a column for FISSEA News&Views!"

****

MAC users … immune, no more. A threat level which is low but since Apple users' security chromosomes have been lulled to sleep since no real virus threats have been seen in years, this one might inspire copycats to challenge MACs. Reported on 17FEB2006, it travels via IM (actually iChat) and targets Apple's Mac OS X operating system. Its lure is for those who might like to see a picture of the next generation Apple OS. Infection occurs when users download "latestpics.tgz" and install it on their computer. It then sends itself to everyone on the user's "buddy list." Even Granny Smith in Fuji should keep a Red Delicious eye out for this one!

****

Makau Corporation's catalog is available. Though not limited to security courses, their curriculum appears to be oriented toward various certifications and professional development. Contact them on (877)752-5329 or at www.makaucorp.com

****

If you have employees who are working on MCSE certification, TestOut is offering ten Certification Suites for free if the MCSE 2003 Suite is purchased for $1,995. If interested, go to www.testout.com/start or call (800)877-4889.

****

Tidbits for Awareness presentations:

* It was reported in the Washington Post on 29JAN2006, that “18% of Washington area households said someone in the household owned a PDA, or personal digital assistant, last year, according to a survey by Scarborough Research. That’s an increase of 35 percent over the previous year.”

* Privacy Times is a subscription-only newsletter, but its Web site, www.privacytimes.com, offers news and information on privacy issues such as identity theft and homeland security.

* If you are looking for interesting facts with which to pepper your Awareness presentations, check out the three following books: “A Book of Curiosities” by Roberta Kramer; “Who Knew” by David Hoffman; and “Why” by Eric Laithwaite.

****

nCircle has many informative webinars available at: http://www.ncircle.com/index.php?s=news_webinar2 One recent session dealt with **Internal Security Compliance and Best Practices** wherein they show how to measure, manage and improve your internal security posture, as well as streamline your compliance processes. It demonstrates via an outline the most effective compliance strategies like base-lining and trending, as well as best practices for reducing inherent security risks. This particular webinar is at: http://www.ncircle.com/webinarreg/compliance_recorded.html A second offering was **How Much Security is Enough Security?** Creating the delicate balance of "just enough" security is difficult since what is considered enough security today may be too much/not enough security tomorrow. To provide an organization framework to review the current security state versus business objectives and determine the right level of IT security, check out http://www.ncircle.com/index.php?s=registration_registernew&src=enough