The Security Blanket

Issue 9, June/July 2002

The State of Iowa information systems can only be secure if each one of us acts in a security conscious manner – we each must play our part.

Have a Great 4th of July!

In This Issue:

From the CISO

With Independence Day this week, I thought it would be a good idea to identify two items that in many ways exemplify America and our way of life. They are reminders that our freedom is not free and that we should look at the 4th not only as a day off, but also as a celebration of the United States of America. While some look at Veteran's Day as a time to observe and honor our military heroes, I think now is also an appropriate time.

The first item is the speech General Douglas MacArthur delivered at West Point upon his acceptance of the Thayer Award. It concentrates on the West Point motto, "Duty, Honor, Country," and how those words build basic character. Rather than put it here, you can read it at http://www.west-point.org/class/usma1989/macarthuracceptance.html. The second item is the military Code of Conduct, which I have provided below. Find some time tomorrow to go somewhere alone and read these words – they are reminders of those who have suffered, those who have made the ultimate sacrifice, and those who remain who stand ready to protect our great nation.

The Code of Conduct

Article I

I am an American fighting in the forces which guard my country and our way of life. I am prepared to give my life in their defense.

Article II

I will never surrender of my own free will. If in command, I will never surrender the members of my command while they still have the means to resist.

Article III

If I am captured, I will continue to resist by all means available. I will make every effort of escape and aid others to escape. I will neither parole nor special favors from the enemy.

Article IV

If I become a prisoner of war, I will keep faith with my fellow prisoners. I will give no information or take part in any action which might be harmful to my comrades. If I am senior, I will take command. If not, I will obey the lawful orders of those appointed over me and will back them up in every way.

Article V

When questioned, should I become a prisoner of war, I am required to give name, rank, service number and date of birth. I will evade answering further questions to the utmost of my ability. I will make no oral or written statements disloyal to my country and its allies or harmful to their cause.

Article VI

I will never forget that I am an American, fighting for freedom, responsible for my actions, and dedicated to the principles which made my country free. I will trust in my God and in the United States of America.

Kip Peters

Return to Table of Contents

Current Activities

Charter projects, Security Policies, Awareness Projects, Crisis Management, Vulnerability Assessments – all have seen a great deal of activity. Check out our website to see the latest and greatest, or just to refresh yourself on current guidelines or policies!

Information Security Office Service Offerings

Would you like to have a vulnerability assessment performed on your systems? Do you need help with an incident? Are you looking for security services? Check out the ISO Service Offerings!

Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates. (Security Services are listed in the last quarter of the web page.)

- Security Consulting
- Vulnerability Assessments
- Physical Security Vulnerability Assessments
- Network-Based Intrusion Detection System
- Enterprise Business Continuity
- Incident Response
- Test Lab
- Awareness Briefings
- Enterprise IT Business Continuity

Charter Project Transition

The ISO is currently working with other sections and departments to assist with the Charter Projects envisioned by Governor Vilsack. Want to know the latest on Charter Project Security Issues, Security Planning, and Security Status? Send your questions or concerns to Marie Hubbard.

Information Security Officer Distribution List

The Information Security Office has a distribution list with which we can easily send out security mailings to security contacts. Mailings include the Security Blanket, Security Quickies, Lunch & Learns, Security Alerts, daily news and virus reports, security events, or other announcements. Some contacts also disseminate the ISO mailings to their departmental personnel. If you are interested in being included in this distribution list, drop a note to William Hubbard.

Security Awareness Tutorial

The new Security Awareness Tutorial (SAT) is complete and ready to use! Topics covered in the Security Awareness Tutorial include training on Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. The training course is available online and on CD-ROM, and will take up to 90 minutes to complete. It is divided into separate lessons, so you can complete the lessons at different times if needed.

All ITD staff will be using the SAT for annual security awareness training. (Details forthcoming in a departmental message.) Because the Information Security Office has Enterprise-wide responsibilities, the SAT is also available to State of Iowa Enterprise agencies at no charge. In addition, the SAT will be available to non-Enterprise agencies and non-State of Iowa organizations as well, for a licensing fee. Contact William Hubbard for more information.

UPCOMING SERVICES

Certification and Accreditation Process

Security was a primary concern of nearly everyone who participated in the Charter Advisory council meetings. In order to ensure that all data and network components are appropriately secured, we will be instituting a customized version of the Department of Defense's Information Technology Security Certification and Accreditation Process. The ITD Information Security Office is currently developing this process. It will contain all key elements used by the DoD, but be tailored specifically for the Iowa Networks and streamlined wherever possible. The working draft name of this document will be the Iowa Certification and Accreditation Process (ICAP)

The purpose of a Certification and Accreditation process is to assure that all systems are fully documented, securely configured and that full life cycle plans are in place. The use of C&A processes assures that standardized methods are used in the development, security configuration and ongoing management of all networked systems, which greatly improves the overall security of a network and the ease of ongoing system management in large network environments.

Certification and Accreditation will eventually be required for all information systems on State of Iowa networks, and should be incorporated in the development, continued

maintenance and reconfiguration or upgrading of these systems. It will also be required for systems that are developed by outside contractors, which should improve State employees' ability to support those systems after the contractor leaves.

In the case of the Charter projects, it would not be appropriate for ITD to assume control of systems without having full knowledge of their current condition, operating needs and life cycle plans. If this documentation were to be delayed until after the charters are implemented we would be risking the chance that valuable knowledge regarding systems would be lost.

I hope to provide further details on this process in each upcoming issue of the Security Blanket. The next issue should include a detailed explanation of the first of the four phases of a C&A process, the Definition phase. If you have any questions, comments or suggestions, please contact Marie Hubbard at Marie.Hubbard@itd.state.ia.us.

Risk Assessment

A standard risk assessment methodology will be developed for use in Iowa state government. Training will be provided on how to best utilize the methodology, and staff assistance will be available for agency assessments.

OTHER ACTIVITIES

Enterprise Security Website
Have you been here? From this site you have access to a plethora of security information: Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's your resource for Enterprise and ITD Security Information.

New Section: **Educational Extras**
We've added some extra educational material and resources for other departments to use in their Security Awareness efforts. Newly added are Security Screen Savers and a link to the Stay Safe Online effort. (Be sure to get permission from your department before installing the screen savers!)

ITD Guidelines and Procedures
Go here to see new ITD ISO Guidelines and Procedures for Workstations and Servers, Tips on Malicious Code, and non-IT General Security issues:

Configuring a Windows 2000 Desktop	Preparing a Windows 2000 Server for Production
Windows IIS 5.0 Guide	IP Security Policies
Apache 2.0 for Windows NT/2000 Secure Installation Guideline	Enterprise Messaging System Protection Measures
Virus Detection and Prevention Tips	Virus Response Procedures
Travel Security Guidelines	Letter and Package Handling

Return to Table of Contents

Helpful Hints

Help for the Home User: Stay Safe Online

As both home Internet connectivity and online malicious activity have increased, there has been increasing concern regarding home computer security on the part of consumers, businesses, and government agencies. Cyber crime, identity theft, Distributed Denial of Service (DDOS) attacks, illegal copying or sharing of copyrighted material, National Security, the proliferation of viruses and worms – all of these things might impact the home computer. A national effort has arisen to help educate home users to the risk involved with home computers, especially those systems that are connected to the Internet, and to help home users find the tools they need to help keep their systems safe.

One of the largest efforts is Stay Safe Online, sponsored by a variety of organizations. To quote from their site:

> "This web site is designed to give you the information needed to secure your home or small business computer. You'll find tips on how to safeguard your system, a self-guided cyber security test, educational materials, and other Internet resources, as well as valuable information from our sponsor organizations."

Stay Safe Online is a good source of information for home computer security, especially for those who have not dealt with home computer security previously. I encourage you to use it to help you keep your home systems and your personal information more secure.

William Hubbard

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about…
Information Sharing!
Security Training!
Conferences!
Programs!
Security Vendor Announcements!

The Information Security Office's Lunch &Learn Program continues… These informal meetings cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. Change of location or time will be announced via e-mail, and sent to departmental Information Security Officer contacts. The past presentations (lots of them - in .pdf, .ppt, and/or video) and an updated schedule are available at the Lunch & Learn site.

Date and Time	Topic and Location
July 18 12:00pm-1:00pm	Iowa Enterprise Security Policy, Part 4 Grimes Bldg., North Conference Room

Questions regarding the Lunch & Learn program (or the Information Security Officers contact list) can be directed to William Hubbard.

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing information.

Security Vendors

SANS Offerings:
Each month SANS offers at least one training conference in a major U.S. city. In the next few months there are SANS GIAC Certification and Training programs in Detroit, St. Louis, Denver, Omaha and many other places. SANS also offers online security courses for those who are unable to travel much, but still wish to participate. Details and registration information: http://www.sans.org/

SANS also offers a free First Wednesday Webcast series. This series is dedicated to sharing information on current security issues. The latest one on Wednesday, July 3rd at 1pm EDT (1700 UTC) is: 10 Steps Towards Solaris Security presented by Hal Pomeranz, Deer Run Associates. (It can also be viewed at a later time.) For registration information go to: http://sans.digisle.tv/audiocast_070302/brief.htm

Microsoft: (Vendor Announcements)

MSDN Webcasts

The MSDN Webcasts team holds 90 minutes of deep, how to technical webcasts presented by knowledgeable Microsoft software design engineers, developer evangelists, and a host of others. This free event is held live, and it's interactive. Customers can see code and application demos online, and ask the presenter technical questions, or listen to their peers ask questions. Recorded sessions can be found here.

Microsoft Online Training

In an effort to meet the demands for training and certification on Microsoft products and platforms, Microsoft Government is sponsoring Online Training for selected courses for a limited time. These courses will be provided on a first come first served basis. Government employees can register for training at a reduced cost, as we have arranged for the Microsoft discount to be extended to our government customers. To register, Government technical professionals need to go to the web site: http://www.msgovernmenttraining.com/offer/

Other Events:

Black Hat Briefings and Trainings

Date: July 29-August 1, 2002

Location: Las Vegas, NV

Founded in 1996, the Black Hat Briefings has earned the respect of the most influential computer security people on the planet. Spanning two days with four tracks of speaking, you will meet with the cutting edge minds in computer security.

Network Security Conference 2002

Date: August 12-14, 2002

Location: Las Vegas, NV

The Network Security Conference grew out of the need to offer highly technical competencies in information security to ISACA members. ISACA has a growing number of information security professionals in its ranks. IT audit professionals are required to perform more information security reviews and audits. The Network Security Conference offers information security topics with the IT auditor in focus. The North America event is held annually in August and attracts upwards of 200 international delegates. Each session is a half-day workshop allowing the presenters to cover the subject matter in great depth and detail.

Return to Table of Contents

Feature Articles

Biometrics – Not Yet Ready to Solo

While long a staple of television and movies, and in fact deployed in some business and government installations, recent tests have shown that most current biometric devices are not accurate enough to be used as a sole security lock. Indeed, these tests have revealed some interesting limits to current biometric implementations. (And the grisly method of cutting up an authorized person to gain unauthorized access is not needed at all!)

Fingerprint readers have been fooled by ‘gummy’ gelatin molded with a copy of an authorized fingerprint. In another test researchers found if they cupped their hands around the sensor and blew gently, the oils and residues from the last fingerprint left on the device would be read, and if that person was authorized access would be granted.

Facial scanners are not doing much better. One system was fooled when researchers used a photo of an authorized person with the pupils cut out. The researcher's own eye movement behind the mask was enough to convince the sensor that the picture was the person. Another sensor was fooled when researchers held up a laptop that was playing a video loop of an authorized person.

Voice recognition may be farther along, but anyone who has tried to use a speech recognition program knows how hard it can be to 'train' it to individual speech patterns. In addition, voice authorization will require trade-offs between locking you out when you have the sniffles and allowing so much latitude for an acceptable response that you, James Earl Jones, and Kathleen Turner all pass its authentication parameters.

The single major problem with all current biometric scanners is accommodating typical human day-to-day inconsistencies – changes in sensor or body or air temperatures, health changes, nicks and cuts to the fingers, even bad hair days can trouble the biometric sensor. Systems can be 'de-tuned' to make them more tolerant of these changes, but that may defeat the system's ability to distinguish one person from another similar person.

While the biometric industry will improve its products, it is important to realize that biometrics will always work best when used in conjunction with other tools. The old rule that the best security checks are 'something you have, something you know, and something you are' still applies.

If as the technology matures, for example, your fingerprint initiates a prompt for your password, then requires you swipe your pass card, then requires a retinal scan, that's security in depth and is harder to defeat than just scanning or just using a password. This is a more beneficial and realistic use for biometrics than replacing current working security procedures.

It is likely that biometrics will never be the final answer for secure authentication, but will become an important layer in a defense in depth security strategy.

John Maxwell

Lessons Learned with Susie is a fictional account of an employee learning, sometimes the hard way, about security awareness. The situations Susie finds herself in are quite common, and she, like all of us, finds new ways of practicing good security. (Editor's note: This will be the last installment of this series, and my thanks go to Amy for her time and efforts.)

Lessons Learned with Susie

I was so excited this week! My boss chose me to work on a big, new project in our department. He said he didn't have time to discuss it with me at the moment, but he gave me a CD and said I would need this software on my workstation for the project. He said I

could start becoming familiar with the program now, so I could easily navigate through it once the project began next week.

I eagerly returned to my workstation and popped the CD into the CD-ROM drive to see what this new software was. The CD was unmarked, so I had no idea what to expect. I heard the CD spinning and soon an install wizard came up on my screen to help me install the software.

I clicked next and entered the appropriate information when prompted. A minute later, the files were being copied to my hard drive. When the wizard was finished installing the files, I was prompted to restart my computer to finish the installation. I clicked the appropriate box and my machine began to shutdown and reboot. I thought that was pretty simple, so I hoped that everything would work right.

After my machine had rebooted, I logged in again with my username and password like normal. I went through the start menu and found the new application I had installed and clicked on it. I waited, but nothing happened. Thinking maybe I didn't click on the right spot, I found it again in the start menu and clicked on it again. Still nothing happened. I tried opening some other programs. Most of them seemed to work fine, but a couple didn't come up like they normally had before. I began to worry that I had somehow gotten another virus on my machine. I remembered the time I had opened the email attachment and gotten the Goner virus and sent it out to a bunch of fellow employees in the company by accident. That was definitely not good.

But I hadn't opened any email attachments lately. I try not to open them at all, unless I know exactly what they are and whom they are from. I decided to call the help desk and see if they knew what could be causing me problems this time. The guy that answered the help desk line said he would send Mark over to look at my computer within the hour. He told me not to restart or try to fix anything until someone got there to take a look at it.

Half an hour later Mark showed up to look at my machine. He tried opening the programs I was having trouble with and some other ones, getting the same results that I had gotten. He said something was definitely not right with my computer. He asked what I was doing before it started acting like this. I told him I had just installed some software my boss had given to me on a CD and restarted my machine.

He informed me that I wasn't supposed to install software on my machine. It turns out we are supposed to call the helpdesk and have them send someone to install any software on our desktops if it has been approved. Mark said I had probably either loaded a virus or Trojan program on my computer, or the program I loaded was not compatible with the current software installed on my PC - hopefully the latter. He uninstalled the software I had loaded and restarted my computer. When I logged in again, everything was back to normal and working properly again! He checked to see if I had any unusual processes running on my machine, but he couldn't find any. He checked a few other things and

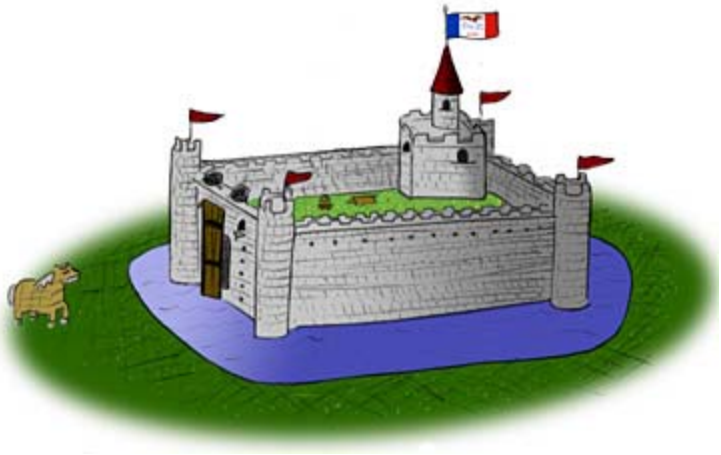
was satisfied it wasn't a virus or Trojan program. Lucky for me it just looked like a software compatibility issue!

Mark was very nice and said he would look into the compatibility issue and see if he could find a way for me to use the software on my desktop. Now I know that loading software on my computer, no matter what the source, can cause major problems for me, and possibly others. Problems could come from a virus or Trojan, or even simply be caused by a compatibility issue. I will make sure to get authorization first, or call to have someone else install software on my computer next time. Then, I won't have any problems!

Amy Wilmeth

Defense in Depth: Our Place In It

The concept of defense in depth has been around in military terms for quite some time. It involves multiple layers of defense, often overlapping or supporting each other. With a generic medieval castle, for example, you have an open field surrounding a ditch, which surrounds a crenellated wall and towers, which encircles an inner court, and finally at the center is located the keep, or donjon. Gates, archery slots, heavy doors, and other devices protect access points into the castle and are designed to stop or delay intruders. If intruders do breach one line of defense, there are other layers of defense to protect those living in the castle.



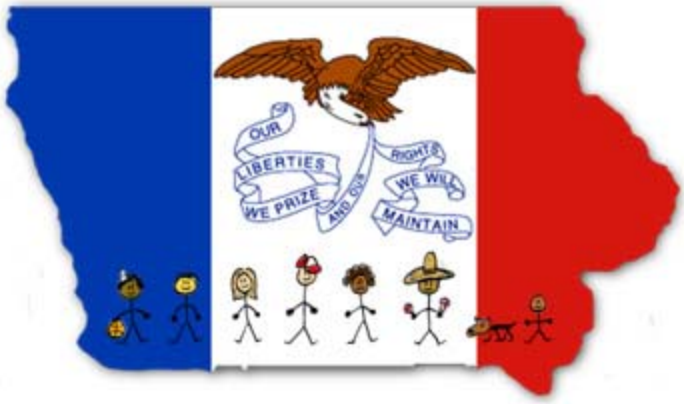
This concept of defense in depth is also very applicable to computer networks, like the State of Iowa network. We have separate defensive mechanism to guard various access points (Internet, e-mail, applications, etc.) to protect the network and the information stored in it. If one line of defense fails, then an intruder must go through other layers of defense to get to the center. Much like peeling through the layers of an onion, for instance. The layers of defense can both stop or delay an attacker. If he is delayed, then he may simply give up and go away, or at the very least it will take more time to reach his goal. If he is delayed, there is a greater chance for discovering the intrusion or attempted intrusion.

Firewalls, access control lists, passwords, crypto cards, routers, anti-virus software, separated subnets, and the like all are part of the defense-in-depth strategy. All have their

place in the schema. However, one other defensive element is so important that it must also be noted: **You**.

Every individual, via his or her awareness level and behavior, influences how secure the State network is. Each user helps keep the network safe by using good passwords, protecting passwords, locking workstations, backing up data, using anti-virus software, reporting questionable activities, and otherwise acting in a security conscious manner.

Not only that, but **every** user must act in a security conscious manner in order for everyone else (and the network) to stay safe. If one of the citizens of the aforementioned castle inadvertently let an intruder in, would not everyone in the castle be in jeopardy? Similarly, if one of us, through error or misjudgment, allows a hacker or intruder into our network, everyone else's data, profile, or confidential information might be at risk, not to mention the State network in and of itself. Each State information technology employee must learn basic information technology security awareness to reduce the potential (and thus risk) of an intrusion. Only together can we mitigate that threat.



William Hubbard

Return to Table of Contents

Linked Articles

Education

Personal Privacy for Personal Computer Users
Personal computers have provided fertile ground for data collection about individuals. In this short paper, ordinary, non-technical users can get a sense of the fundamental issues that face all of us as we try to strike a balance between efficient commerce and our concerns about personal privacy. (June 3, 2002, ITToolBox/Pest Patrol)

Secure Coding
SecurityFocus has published a good article on secure coding. The article covers the areas to watch when doing application development and the different points of attack that can be used by a hacker. Building 100% bug-free code isn't possible, but researching areas mentioned in this article can definitely help strengthen your application security. (June 20, 2002, SecurityFocus)

Buffer Overflows – What are They and What Can I Do About Them?
What are buffer overflows and why are they still a significant source of program vulnerabilities when the problem is well understood and the solutions well known? And what can Joe and Jane User do to prevent intruders from exploiting their computer systems? This article discusses those topics. (ITToolbox, May 28, 2002)

Fighting back against PC invaders
Activist programmers are fighting back against intrusive ads, software that tracks online behavior, and other mechanisms that quietly co-opt computers for marketing and other business purposes. (June 25, 2002, ZDNet) (Includes links to many privacy and firewall products, page 4).

Consumer Reports: Anti-Virus Software and Firewalls
Consumer Reports tested firewalls and anti-virus software. This article describes why the software/hardware is necessary and how it works. Linked articles offers advice on keeping yourself safe from common virus/worm ruses, keeping your data safe, and what to do if your computers have been infected or hacked. (June 2002, Consumer Reports)

Security Manager's Journal: The Naked Truth About Porn Surfers
They know the policy. They know about monitoring. But some employees still surf Web porn at work—and get fired. What are they thinking? (June 24, 2002, ComputerWorld)

Homeland Security

Cyber-Attacks by Al Qaeda Feared
Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say. (Six pages) (June 27, 2002, Washington Post) Single-page link.

They Want You for a Safer Infrastructure
Security: Q&A with National Cybersecurity Czar Richard Clarke and Howard Schmidt are coordinating a volunteer effort to try to protect the nation's critical infrastructure. Can they convince corporate America to play along? (June 15, 2002, CIO Magazine)

Homeland Security Department Would Serve as Central Data Clearinghouse
If it works as envisioned, the Homeland Security Department will be the center of a torrent of intelligence data. At least eight major agencies and numerous smaller ones will funnel information to the Homeland Security Department, which will serve as a "central clearinghouse to collect and analyze" data related to terrorism, according to the Bush administration. (June 10, 2002, Federal Computer Week)

Computer Group's Security Role Grows
Phyllis Schneck doesn't wear a badge or carry a gun, but she plays a key role in protecting America from terrorists. (InfraGard) (June 27, 2002, ITToolBox)

IT pros: Cyberraid to hit U.S. agencies
It's only a matter of time before a major attack is launched on government computer systems, say IT professionals in a new survey. So how do they rate U.S. tech security? (June 25, 2002, ZDNet)

Cyber Security Plan Contemplates U.S. Data Retention Law
Internet service providers may be forced into wholesale spying on their customers as part of the White House's strategy for securing cyberspace. (June 18, 2002, SecurityFocus)

State CIOs aid White House in Homeland Security Plan
State chief information officers are coalescing to help the White House Office of Homeland Security with technology-related components of the national homeland security strategy. (May 24, 2002, GovExec)

Senate panel OKs security standards
The Senate Commerce Committee has approved a bill that would create a set of "best practices" for computer security for federal departments and agencies, among other things. (May 21, 2002, C/Net News)

Pro-Islamic Hacker Groups Joining Forces Globally
There is evidence that shows Pro-Islamic hacker groups are joining forces. Each group is carrying out digital attacks under a common banner and has pooled their expertise to broadcast political views. The three main groups are Unix Security Guards, World's Fantabulous Defacers, and Anti-India Crew. Both USG and AIC have become very active in carrying out 111 attacks between them in May. The main sites being attacked belong to universities and educational institutions, businesses, hotels and retailers. (June 18, 2002, Content Wire)

Bush Cybersecurity Strategy To Be A Living Document
Howard Schmidt, vice chairman of the president's Critical Infrastructure Protection Board, attended the fourth and final White House-sponsored "town hall meeting" on cybersecurity in Atlanta before the release in September of the next version of the National Strategy to Secure Cyberspace. (June 19, 2002, ComputerWorld)

Cyber Crime

Secret Service warns of Afghanistan e-mail scam
The U.S. Secret Service warns there is a new e-mail scam circulating around the Web to join the already famous Nigerian government official scam. May 24, 2002, ComputerWorld

Six Arrested Over 'Nigerian e-mail' Fraud
Six people were arrested in South Africa over the weekend on suspicion of being involved in the infamous "Nigerian" e-mail and letter fraud. May 21, 2002, ZDNet

In FBI shift, cybercrime is a priority
The director of the FBI announced Wednesday that a major reorganization of the agency would include a new focus on cybercrime and technology. Protecting the United States against "cyber-based attacks and high-technology crimes" is one of the FBI's top 10 priorities, Director Robert Mueller said at a news conference detailing a major reorganization of the agency. CNET News May 29, 2002

FBI Wants To Know Who Took 13,000 Credit Reports
Someone posing as a Ford Motor Credit employee obtained credit reports on 13,000 people across the U.S, reports that included addresses, account numbers and Social Security numbers. (May 17, 2002, ComputerWorld)

CA State Personnel Database Security Breach
Hackers breached security at California's state personnel database and were able to see names, social security numbers and payroll information about all 265,000 state workers. The intrusion took place on April 5, though it was not detected until May 7. (May 25, 2002 SFGate)

School hackers may face Secret Service
Students at universities in four states may have been monitored by "spyware" placed on computers by online criminals to capture passwords and credit card numbers, a public safety officer at one of the schools involved said Thursday. (June 21, 2002, ZDNet)

Woman Charged With Breaking Into Company's E-mail System
Massachusetts Attorney General Tom Reilly has filed charges against a Middleton, Mass., woman, accusing her of hacking into her former boss's computer system and forwarding confidential e-mails to former co-workers. (June 13, 2002, ComputerWorld)

Court Says Iowa PC Users Can Seek Damages From Microsoft
If the class-action lawsuit is ultimately successful, Iowa users of Windows 98 could get refunds of about $40 each. (June 14, 2002, ComputerWorld)

Feds, DirecTV Move on Canadian Hacking Case
Federal investigators arrested a few individuals responsible for satellite TV hacking. Three US citizens and a Canadian citizen were illegally designing, manufacturing, and distributing DirecTV access cards across North America. This group has been creating and selling illegal access cards since 1996 and has likely made millions on the deal. Jun2 25, 2002, Sky Report)

Web Site Exposes Credit Card Fraud
An anti-fraud education group that tipped federal authorities to a major Internet credit card scheme has opened a Web site that will let Americans check to see if their card numbers are in the hands of thieves. (June 26, 2002, CNN/Sci-Tech)

FBI to valley: Tell us about attacks
Businesses have remained tight-lipped when it comes to reporting cyber attacks or other breaches of their security for fear that the bad publicity would also bombard their bottom lines. But the FBI has begun offering them anonymity and critical information in exchange for their much-needed cooperation in battling hackers and other terrorists. (July 1, 2002, MSNBC)

News

Wireless attacks: Wave a white flag?
The major Internet backbone networks for the Pacific Northwest converge at a single location: the Westin building in Seattle, a 32-story structure that houses dozens of major

and minor Internet service providers. It is also home to more than 50 wireless networks, most of which apparently have no security. (July 1, 2002, ZDNet)

Mitnick Testifies Against Sprint in Vice Hack Case
The ex-hacker details his past control of Las Vegas' telecom network, and raids his old storage locker to produce the evidence. (June 24, 2002, Security Focus)

Microsoft, States Sum Up Case For Judge
Microsoft and the non-settling states who are still fighting the antitrust battle against the software giant filed court papers summing up their ideas for resolving the case. (June 10, 2002, ComputerWorld)

Simile D Spawns New Virus Age
The discovery of the first cross-platform metamorphic virus will challenge business assumptions about the security of Linux, according to experts. (June 12, 2002 VNUNet.com)

Tactical Database and Web Page Used in War
American commanders at Bagram airbase in Afghanistan and in the United States are using the Tactical Web Page and underlying database to communicate and make military decisions. The site is used to transmit field information and orders, and is protected with intrusion detection systems and firewalls. (May 30, 2002, SANS/CNN)

Security alerts: jumping the gun?
A security company faced criticism Monday after it released critical security information without giving the open-source community adequate time to respond. So how much time is enough? (June 19, 2002, ZDNet)

Government Uses Open Source Products Despite Microsoft's Protests
Though Microsoft has been pressuring the Pentagon to use its products, a study conducted by Mitre Corp. for the Department of Defense says that open source software is often more secure than proprietary products. Microsoft has also complained about the government's funding of research to secure open source software. (May 23, 2002, Washington Post)

DoD Smart Cards
The Air Force is using smart cards for entry at more than 100 Air Force bases and for computer access. The Department of Defense (DoD) plans to issue 4 million smart cards to enlisted forces and their families by the end of next year. The cards will contain photographs, digital certificates and encryption keys. (May 21, 2002, Government Computer News)

Corporate Layoffs Create Security Havoc For IT Pros
Big corporate layoffs are creating a nightmare of security risks as IT workers scramble to close down network connections and plug up dangerous holes as employees are walked out the door. (July 2, 2002, EarthWeb)

Return to Table of Contents

Points of Contact

Kip Peters: Chief Information Security Officer (CISO), Enterprise Security Consulting, Enterprise Security, Policy, Standards, Overall Security Issues
515-725-0362

Marie Hubbard: Charter Projects: Transition Security Issues, Security Planning, Status
515-725-0385

Paul Schmelzel: Security Operations: Vulnerability Assessments, Intrusion Detection, Incident Response, Test Lab
515-725-0410

Larry Brennan: Critical Infrastructure Assurance Coordinator, Iowa Crisis Action Team
515-725-0365

Wes Hunsberger: Business Continuity, Physical Security
515-725-0361

William Hubbard: Security Awareness
515-725-0452

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/
The awesome Enterprise Security website. You can find tons of state or ITD security information here. Policies, procedures, guidelines, educational resources, lists of services, useful links, and more!

http://www.cert.org/nav/index.html
Homepage for CERT (Computer Emergency Response Team)

http://www.sans.org/newlook/home.htm
SANS (System Administration, Networking, and Security)

FBI and SANS List Top Twenty Vulnerabilities and Free Scanner
Security leaders from 30 organizations, led by the FBI's NIPC and the SANS Institute published a list of the top twenty Internet security vulnerabilities along with instructions on how to fix them.

Iowa Homeland Security

This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more.

Homeland Defense Journal

This is the federal Homeland Defense journal homepage.

Return to Table of Contents

If you have questions or comments relating to this newsletter, or if there is a topic you would like to see an article on, please contact William Hubbard.
Cool artwork provided by Sam Wong.

The ISO Code:

Integrity…Service…Excellence