
# The Security Blanket

Issue 8, April/May 2002

In fair weather or foul,
we'll keep you covered.


**In This Issue:**



## From the CISO

There are a lot of questions being asked right now about how much the federal government knew before the events of September 11th occurred. I get the feeling there isn't a whole lot of confidence in government right now - we can't maintain a budget, we can't accurately forecast revenues, we can't maintain services, and we can't protect American citizens. A lot of frustrated people are beginning to make a lot of waves, and it seems as though you can never do enough. It doesn't matter that the threat is so widespread and unpredictable that it is virtually impossible to counter it, and it doesn't matter that untold numbers of possible events have been thwarted - it only matters that one got through.

As we move ahead with the charter projects, and as we continue to progress with our security program, it is important to realize that we have a responsibility to do what we can to protect the information placed in our trust. We will never be able to do everything we want to do, as there will never be enough time or money to address it all. Therefore, we must make good decisions, prioritize well, and manage risk effectively with what we have. To do this, we all must be involved in the effort. The Security Office can't do it all; it must provide guidance and policy, and provide support as much as possible, but every state employee has a role to play in protecting state information and information systems. If you don't understand your role, either check out the Enterprise Security Policy or ask me. I can be reached via e-mail at Kip.Peters@itd.state.ia.us or via phone at 725-0362.

Kip Peters

Return to Table of Contents

## Current Activities

### Security Certifications

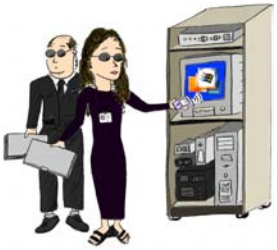
Seven members of the Information Security Office have recently received GIAC GSEC certifications from the SANS Institute. Marie Hubbard, John Maxwell, Larry Brennan, Jared McLaren, Paul Schmelzel, Amy Wilmeth, and Bill Hubbard have all successfully completed the GIAC program. Congratulations to all!
http://www.giac.org/

ISO personnel are involved with many projects. We are currently assisting with the five charter projects envisioned by Governor Vilsack, which are designed to provide better governmental services to the citizens of Iowa while decreasing the costs associated with those services. ISO personnel also support various security efforts within ITD and in other departments, and our Security Awareness efforts continue. Check out the latest Security Policies, Procedures, and Guidelines at our website, too!

### Information Security Office Service Offerings

Service rates are now available for ISO Services.
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

**Information Security Officer Distribution List**

The Information Security Office also has a distribution list with which we can easily send out security announcements, security events, and other mailings to security contacts. Some of these 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.

## UPCOMING SERVICES

**Security Awareness Training**

The new Security Awareness Tutorial is in its final stages of editing. It will be made available to all State of Iowa Enterprise agencies free of charge (a fee will be required from Non-Enterprise agencies) and will be ready for use by the end of June 2002. This Tutorial will likely become part of the annual security awareness training available to all Enterprise IT employees.

Topics covered in the Security Awareness Tutorial include training on Confidential Information, User Accounts and Passwords, Workstation Security, Malware (Viruses, Trojans, and Worms), Laptops, and Modems. The training course will be available on CD as well as online. Contact William Hubbard for more information.

## 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, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's your resource for Enterprise and ITD Security Information.

**ITD Guidelines and Procedures**

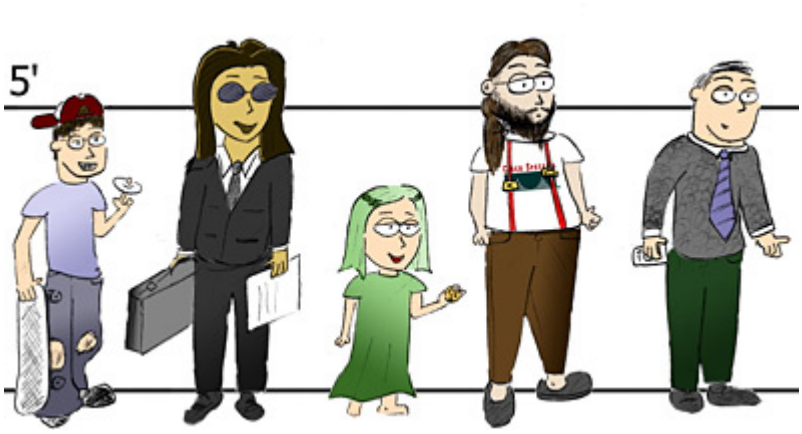
Go here to see new ITD ISO Guidelines and Procedures for Workstations and Servers, Tips on Malicious Code, and non-IT general security issues.

Return to Table of Contents

## Helpful Hints

### Spot the Hacker

Can you spot the hacker in the picture below? Most of us would probably pick the grungy teen-ager, but in actuality ANY of these people could be a hacker. Can you spot the system administrator? Yeah, the suspendered Unix guy fits the image, but similarly to the hacker question, any of these people could have some of the skills necessary to be a system admin. (O.k., maybe not the little girl, but you never know…)




No matter what you want to call them, hackers, crackers, intruders, or criminals, they can use a variety of social engineering tactics to obtain access to computer systems. They can exploit the helpful attitude of people working at help desks, peer over shoulders to gather PINs and passwords, sift through trash, impersonate network administrators online, or even pretend to be trusted support personnel to gain access to computers and accounts.

How do we defend against this type of behavior? First, it is important to be aware that it happens, and that anyone can be a target of social engineering. See an unknown person trying to get inside the department's locking door? Check their badge or other identification. Ask why they are there, and escort them to where they are going. (Or call the Capitol Police, if warranted.) Is someone asking for a password over the phone? Be cautious and verify who they are – and try calling them back on their office phone. As a general rule, however, do not give out confidential information (like passwords, PINs, or access numbers) over the phone, or even via unencrypted e-mail (especially over the Internet).

Be mindful of proper procedures, and be wary of unknown or unverified persons. The most difficult aspect of keeping a secure environment is always using good judgment in uncertain circumstances.

William Hubbard

Return to Table of Contents

## Upcoming Classes and Consultations


This section includes announcements of security training opportunities, classes, and conferences that are available to State of Iowa employees. Some events will be geared toward all employees, while others may be more appropriate for server administrators or web administrators. Also included are security-related links to vendor announcements for seminars.

The Information Security Office's Lunch &Learn Program continues… These monthly, informal get-togethers 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 |
|---|---|
| June 4<br>12:00pm-1:00pm | Iowa Enterprise Security Policy, Part 3<br>Grimes Bldg., South Conference Room |
| June 18<br>12:00pm-1:00pm | Iowa Enterprise Security Policy, Part 4<br>Grimes Bldg., South 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. SANS also offers online security courses.
In the next few months there are large SANS GIAC Certification and Training programs in Boston, London, Washington, Denver, New York, Los Angeles, and Toronto and smaller programs in Phoenix, Minneapolis, Portland, Colorado Springs, Chicago, and Detroit. Details and registration information: http://www.sans.org/

**Microsoft**: (Vendor Announcements)

MSDN Webcasts

Are you looking for training resources and don't have the budget or time to travel? Then the MSDN Webcasts can be your training solution. Attend a MSDN Webcast to learn about Visual Studio.NET, .NET Framework, XML Web Services, and hot to develop applications for Windows XP.

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. Online seating is limited to the first 1000 registrants, so please register early. Looking forward to seeing everyone at our online events!
Recorded sessions can be found here.

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 Vendors**:

e-Security Conference & Expo

Date: May 29-30, 2002, Location: Vienna, VA

The e-Security Conference provides the perfect forum to do just that. Here you will find security issues, tools, trends and techniques discussed in a business context, at a management level. You'll be able to meet, learn, see what's new, and network with your peers. We will deliver the information you need to ensure your organization is not only properly protected but also prepared to take advantage of the business opportunities a sound security strategy can present.

GARTNER INFORMATION SECURITY 2002

Date: June 10-13, 2002, Location: Las Vegas, NV

The need for 24x7 "anytime, anywhere" data availability has created a requirement for storage systems that are virtually organic, capable of replication and self-healing. What now sounds fantastic will soon become commonplace. Gartner PlanetStorage 2002 Conference June 10-13, 2002, Las Vegas, NV is the only conference that offers you a complete view of storage markets and technologies from both end-user and vendor perspectives.

Return to Table of Contents

## Feature Articles

### Home PC System Updates and Basic Security Checks

Keeping your home PC up-to-date and checking for intrusions is a great way to keep your machine healthy and your personal information private. There are a couple of easy ways to do this, and they are free. The process to keep your machine current can be done in very little time, should be done at least once a week, and is the minimum that should be done for a system. Also, performing the checks suggested below can help detect an intruder and keep your system safe.

The best way to keep your system current is to keep the operating system up-to-date. And the easiest way to do that is to visit the vendor's Web site. Microsoft has a Windows update site that will check your machine for patches that are tailored for your system. The site can be reached at http://windowsupdate.microsoft.com/default.htm.


They will also break the patches into critical, recommended, and popular picks categories. From there you can click on ones you want and have them automatically downloaded and installed on your system. It is a good idea to visit this site at least once a week. A word of warning is that you may have to reboot after installing one, so make sure you are prepared to do that if necessary. Redhat Linux also has an "Update Agent" program that can be found under "System" in the program listing in Gnome or can be called from a command prompt by typing *up2date*. You have to register with Redhat, but you can register one machine for free. This will check with Redhat for updated programs and will allow you to choose which ones to download and install on your system. For other operating systems, check with your vendor.

After your system is patched, there a few programs you can run to look for unauthorized activity on your system. One command that a user can run, whether they are using Linux, Windows, etc., is the *netstat* command. At the command prompt, type *netstat –a | more*. This will show you all of the connections that your machine has and will show you ports that are listening on your machine. The *more* part makes the screen scroll one at a time so you can view them all. It is a good idea to become familiar with the output from this command because it will help you look for odd ports or odd connections. Looking at this screen can help show you if you have a backdoor on your machine or if you are connected to an intruder at the moment. One sign of a backdoor would be a port listening that you are not sure why. For example, if the telnet port (tcp 23) is listening when you are not running a telnet service. Or if port numbers 12345 and 12346 are open then it is a sign that the backdoor program NetBus may be running on your system. You may see some higher port numbers (2000 range) connected to IP addresses and these are usually connections to web sites, but you can always check them out. The Web is a great place to search for what runs on a port. One site that has a searchable database is http://www.portsdb.org/.

A favorite trick of hackers is to replace system programs with there own hacked programs. One example is to replace the netstat program with their own version that will not reveal their connection to your machine. This is when it is a good idea to get an outside program and keep it on a floppy disk to ensure it has not been replaced. Two good programs for supplementing netstat are Inzider and fport. Inzider can be found at

http://ntsecurity.nu/toolbox/inzider/ and fport can be found at http://www.foundstone.com/knowledge/proddesc/fport.html. Fport is run from a command prompt, and inzider is run by double-clicking the inzider icon. Both programs report open ports and the files that opened them. This is a great way to track down open ports on your machine. Unix/Linux users can utilize the program called lsof, which stands for LiSt Open Files. Open files will include open Internet connections that services are listening on - they will be denoted in parentheses. For more information about lsof visit http://www.cert.org/security-improvement/implementations/i042.05.html or search for it on the Internet.

The next place to check is in your log files. For this to work, logging must first be turned on. You should make sure to log successful and failed logins to your machine because this is a good way to check for someone brute forcing your password. When you have logging set up, you have to check the logs regularly for them to be effective. Make sure to look for entries with odd times when you weren't working on the machine and for large gaps in time because this could mean that someone edited your logs. Hackers love to delete themselves from your logs if they get in.

If you are running Microsoft Windows, there are a couple of other places to look. The startup folder is a good place to look for odd programs. These programs are run when the system boots up. The other place to look is in the registry. Checking the registry is for advanced users only and the registry should be backed up before any changes are ever made. One mistake here can cause your whole system to malfunction. Listed below are some places to check in the registry.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx

If you find anything that looks odd to you, make sure you fully check it out before doing any system changes. You can always search the Internet for any information about the key, value, or data.

This process is in no way a complete check of your system and cannot guarantee that you have not been compromised. These are just some minimal things that a typical user can do to check their system for intrusions and malicious programs. For further reading, a separate paper, "Home PC Security", contains more detailed information about securing your PC and is located at: http://www.state.ia.us/government/its/security/doc/sb_october01.htm#Feature_Articles. (It is the second feature article down the list.)

Paul Schmelzel

Lessons Learned with Susie is an ongoing 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.

**Lessons Learned with Susie**

What an exciting week we've had! For once it wasn't me that caused the security breach! It all started on Tuesday. These are the details the security team was able to piece together from the incident.


About midmorning a man was going around the office looking at computer cables and writing things down in a notebook. An employee asked him what he was doing and he replied that his name was Tim and he was to take stock of the entire computer inventory of the company. Thinking Tim was part of the company computer operations team, the employee let the man continue without further questioning.

Pleased with the response he received, Tim decided to try something else. He found another employee working at his computer with no one else around. Tim explained he was new to the company and his first assignment was to take inventory of all the computers. This employee asked to see Tim's identification card. He responded that he had just started the day before and had not yet received his identification card. This seemed like a plausible answer to this employee since it took him a couple of days to get an identification card also.

The employee asked what information was needed for the inventory. Tim replied that he would need each employee's name and logon user name along with some numbers off of the computer itself. The employee provided the information and Tim wrote down the numbers from the computer in his notebook and went on his way.

Next, Tim found two young female employees working near each other in another part of the building. He told them he was taking inventory and asked for the same information again. One of the employees said she didn't know if they were supposed to give out that information. Tim explained that he just needed to verify who was using what company equipment for the company records. He asked if he should come back later with his supervisor to get the information. Not wanting to inconvenience someone in management, the two employees gave Tim the information he asked for.

The next day everyone in the department was required to attend one of two previously scheduled training sessions either in the morning or in the afternoon. We arrived to find

that the computer security team was conducting the training. The topic of the training session was social engineering and what we as employees could do to protect the company's computer systems. They told us that social engineering could be someone coming in or calling us on the phone and asking for information such as user names and passwords or company network information, things that only someone within the company should know.

At that point some people started talking about what had happened the previous day with the unknown man named Tim asking for usernames. The security team had been unaware of this incident and started to investigate right away. The lead security team member let us know how to contact the security team to report such cases as this one. We were told we should report any suspicious people in the building, or any requests for sensitive or confidential information via phone or email no matter how small or insignificant it may seem. It's always better to report something that turns out to be a false alarm, than not reporting something that turns into a major security breach that could have been avoided.

Someone could pose as a new employee or assume the identity of an employee in a management position in order to coerce someone into giving them information. There are any number of possible scenarios someone could use, so it's best not to give information to anyone you do not know or to anyone that does not need to know that confidential information. Always ask questions, and never assume anything about the person. Always ask to see identification for someone you do not know, and verify the story the person is telling you. These guidelines will help you protect the company's computer systems and information.

After the training session, the employees I mentioned earlier were able to relay the appropriate information about the mysterious man, known only as Tim, who had been in the building the previous day. The information was enough for the security team to track down this mysterious man as he entered the building on the surveillance cameras located at the main entrance. The physical security surveillance team was alerted to keep a look out for him, should he come back. If he does come back, everyone in our department will be prepared. He or anyone else won't be getting any more information from us, and we know to contact the security team right away if any unknown person should ask for computer network information in the future.

Amy Wilmeth

---

(Editor's note: The following linked article is a nice introduction to information security. It discusses several security topics and ten good elements of information security programs.)

**The ABC's of Security**

From CIO Online Magazine and SANS NewsBites

This article offers a primer of information security advice, answering questions about firewalls, outsourcing, insurance, and reporting security incidents. It also lists ten important elements of good information security, which includes identifying risks,

developing and implementing a security policy, and hiring an independent third party to conduct a security audit. (February 21, 2002, CIO Online)
http://www.cio.com/security/edit/security_abc.html

Return to Table of Contents

**Linked Articles**

Always On, Always Vulnerable: Securing Broadband Connections
Individuals with broadband connections at home lack the security resources of a company with an IT department, but they need to protect their machines from attacks nonetheless. Broadband users should install a firewall and remove unnecessary services and components from all their devices before putting them on line. Finally, users need to make sure that their on-line behavior emphasizes security. (Security Focus, March 26, 2002) [Security Focus Editor's Note (Grefer): Broadband users are urged to employ hardware based solutions, like the LinkSys, NetGear or DLink DSL/Cable-Routers, which typically include NAT and limited firewall capabilities. Using personal firewall software like ZoneAlarm, Tiny, BlackIce, McAfee Personal Firewall or Norton Internet Security will provide an additional layer of defense.]

Threats to Come
Stephen Northcutt, principal incident handler for The SANS Institute, warns that within six months an SNMP worm will be on the loose. Northcutt has been analyzing attack patterns and noticing several SNMP vulnerability disclosures and believes that attackers will soon release a worm into the wild. Security experts have seen a very sophisticated set of worms in the last year that involved worms, viruses, and hacking all in one. This should act as a motivation for administrators to patch their systems before another one comes along that now acts on SNMP. (eWeek, March 25, 2002)

A Tangled World Wide Web of Security Issues
The World Wide Web (WWW) was initially intended as a means to share distributed information amongst individuals. Now the WWW has become the preferred environment for a multitude of e-services: e-commerce, e-banking, e-voting, e-government, etc. Security for these applications is an important enabler. This article gives a thorough overview of the different security issues regarding the WWW, and provides insight in the current state-of-the-art and evolution of the proposed and deployed solutions. (ITToolBox, March 25, 2002)

Order From Chaos
When a server at Georgia Tech was hacked, its IT people had no battle plan. But over several days, they took action a step at a time, yielding a lesson for any organization facing a similar problem. (ComputerWorld, March 25, 2002)

CERT Warns of Social Engineering IM/IRC Attacks
CERT/CC has released an advisory warning that people using instant messaging (IM) and Internet Relay Chat (IRC) have been tricked into downloading malicious software that could be used to glean personal data, take remote control of an infected computer or to

take part in a distributed denial of service attack (DDoS). (ComputerWorld, March 20, 2002)

Mueller Mulling Dividing NIPC
FBI Director Robert Mueller is apparently considering splitting the National Infrastructure Protection Center (NIPC) and placing parts of it among different agency divisions. Senator Charles Grassley (R-Iowa) sent Mueller a letter enumerating the reasons the decision would prove detrimental to information sharing. (ComputerWorld, March 21, 2002)

Understanding Cross-Site Scripting
For a few years now, a security vulnerability called "cross-site scripting" has been receiving widespread attention. This problem is particularly insidious because it arises from a simple and very common oversight. Tens of thousands of server-side programs have this problem, and no programming language or development tool is exempt. (Web Review, January 21, 2002)

Nigeria Launches Web Site To Target E-mail Scams
A Nigerian government Web site targets e-mail fraud scams that have been sweeping the world. (ComputerWorld, March 26, 2002)

Supplemental Budget Request Includes IT Security Items
The White House submitted a supplemental budget request for fiscal 2002 requests asking form more than $36 million IT security programs for homeland security. That number includes $2.5 million for the GSA to establish the Internet Vulnerability Management Office. (Federal Computer Week, March 25, 2002)

FBI survey finds computer attacks up
Most large corporations and government agencies have been attacked by computer hackers, but they frequently do not inform authorities of the breaches, an FBI survey finds. (April 8, 2002, USA Today)

More Government, Military Databases Left Exposed
For the third time in less than a month, internal databases owned by U.S. government agencies have been found exposed to anyone with a Web browser. (April 05, 2002, Newsbytes via COMTEX)

Outflanking The Cyberterrorist Threat
Cyberterrorism may not be an immediate threat, but it would be foolish to ignore the fact that we face an enemy that will adapt to attack our vulnerabilities. Read what Bill Crowell, formerly of the NSA, and another expert have to say about the threat of cyberterrorism and what we can do to thwart it. (April 8, 2002, ComputerWorld)

Hidden Programs on Free Software Could Pose Problems
Programs piggy-backing on free software can take actions ranging from sending users ads to gathering surfing habits to changing Internet settings. Some can make computers crash. They could eventually be used by hackers to take more malicious action. (April 14, 2002, CNN.com/SciTech) [SANS Editor's (Paller) Note: This article points out risks in legitimate free programs. An even more dangerous related risk is posed by the screen

savers, fake pictures and music, and bogus security patch alerts created as malicious software. Unsuspecting users receive spam instant messages or spam email or visit web sites telling them to take advantage of a free download. When they execute the downloaded program, their systems are immediately infected.]

Florida Bank Suffers Online Security Breach
A large commercial bank in Florida said Wednesday that "an Internet hacker" penetrated the security of its systems earlier this month and made off with a file containing 3,600 online-banking customer names and addresses. (April 18, 2002, Newsbytes)

Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row
The Computer Security Institute (CSI) announced today the results of its seventh annual "Computer Crime and Security Survey." (April 7, 2002, CSI)

Scam Artists Use Brute Force to Find Valid Credit Cards
Several groups of credit card scam artists are using brute force to run credit card numbers through Authorize.Net, "a payment gateway system" that requires no password, only a login name. Every transaction is charged a fee, regardless of the credit card number's validity. (April 23, 2002, MSNBC) (Editor's note: Authorize.Net has since taken steps to validate all authorization requests.)

GAO Undercover Agents Gain Access to Federal Buildings
Undercover investigators from the General Accounting Office (GAO) were able to gain access to and move freely about through four federal buildings in Atlanta. They were also able to obtain building passes and after hours access codes, and made copies of the credentials on computers. (April 29, 2002, MSNBC)

Military Academy Cyber Defense Exercise
Military academy students participated in a cyber defense exercise. Six groups of students were pitted against professional military teams comprised of National Security Agency (NSA) employees and soldiers from the U.S. Air Force's 92nd Information Warfare Aggressor Squadron and the Army's Land Information Warfare Activity. For some students, this competition inspired a passion for hands on cyber security. (April 26, 2002, ZDNet)

FBI to Establish Three New Regional Cyber Forensic Labs
The FBI plans to set up three new cyber forensics laboratories in Kansas City, Chicago and San Francisco; the FBI has already established labs in Dallas and San Diego. Half of all cases the FBI opens now involve computers. (April 26, 2002, Silicon Valley News)

Movement afoot to beef up industrial cybersecurity
Federal officials and experts from the private sector have started the long-awaited process of studying the IT security requirements of the nation's industrial-control systems, which link critical systems in the electric, oil and natural gas industries. (April 26, 2002, ComputerWorld)

Ashcroft Wants Harsher Penalties for Identity Thieves

Attorney General John Ashcroft wants increased penalties for identity thieves. There are an estimated 500,000 - 700,000 cases of identity theft every year. (May 3, 2002, Washington Post)

War on Cybercrime--We're Losing
The nightmare for Ecount, an online gift certificate service, began last year when a hacker broke in to the company's system and stole personal information belonging to its customers. (May 14, 2002, ZDNet News)

How do you deal with Internet Fraud?
This paper covers fraud that uses Internet technology as an integral part of the fraud and fraud that is already taking place by other means where the Internet is merely another method of delivery. By ArticSoft (May 13, 2002, ITToolBox)

Personal Data Available On Line
The Internet has proven to be a virtual bazaar for identity thieves; law enforcement web sites publish names, birth dates, social security numbers and even pictures and driver's license numbers of prison inmates and wanted criminals. Court documents available on line can contain much of the same data; bankruptcy cases can even include bank account information. Though some states are passing laws requiring that such sensitive data be edited out of public documents, much will remain to be picked over by data miners. (May 12, 2002, MSNBC)

NSA Adds Universities to its Academic Excellence Program
The US National Security Agency has renewed seven universities (including ISU) and designated an additional thirteen universities as Centers of Academic Excellence in Information Assurance Education for academic years 2002 through 2005. The aim of the program is to help protect national critical infrastructure systems through promoting Information Assurance in higher education and producing knowledgeable and capable IT professionals. (March 8, 2002)
See also: http://www.nsa.gov/isso/programs/coeiae/index.htm

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: Chief, Security Operations

Vulnerability Assessments, Intrusion Detection, Incident Response, Test Lab
515-281-4905

Larry Brennan: Critical Infrastructure Assurance Coordinator
515-725-0365

Wes Hunsberger: Certified Business Continuity Planner
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*