The Security Blanket

(We've got you covered!)

Issue 7, March 2002

In This Issue:

From the CISO

From the CISO...

Our security Web site is something we have spent a lot of time on and we try to keep it as up-to-date as possible. As the security program moves ahead, we will be populating it with more and more information as it is gathered or developed. On this site, you can find all sorts of security-related information, including alerts, policies and procedures, updates on our current activities, videos of our Lunch & Learn programs, general security publications and information, links to other sites and information, archives of the Blanket and Security Quickies, and points of contact. There is even an option to synchronize current security news and information on PDA's. Our goal is to make this site a valued security resource for state personnel - a first-stop shop, if you will. We have tried to make the site informative and interesting while bringing in a hint of humor to reduce the tedium, and we are fast on our way and hope to make it even better.

We are currently undertaking a revision of the site in an effort to make it more user friendly. If a visitor finds it difficult to locate the information they require, it is not beneficial and they likely will not return. If you are a frequent visitor to our site and have any recommendations, please contact Bill Hubbard and provide some feedback. If you are not a frequent visitor, or have not visited the site before, please check it out. Security is everyone's responsibility in some shape or form, and there is information available that applies to everyone from department directors to system administrators. Check us out!

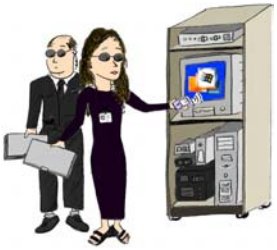
Kip Peters

Return to Table of Contents

Current Activities

ISO personnel are currently 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 to grow.

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**

UPCOMING SERVICES

On-Line Awareness Training
(The new Security Awareness Tutorial is in its final stages of editing!)
Vulnerability Profile Database (early 2002)
Risk Assessment

OTHER ACTIVITIES

Enterprise Security Website
Have you been here? From this you have access to a plethora of security information: Security Awareness Resources, Operational Services, Procedures, Recommended Reading, and Mobile News. It's the place to be for Security!

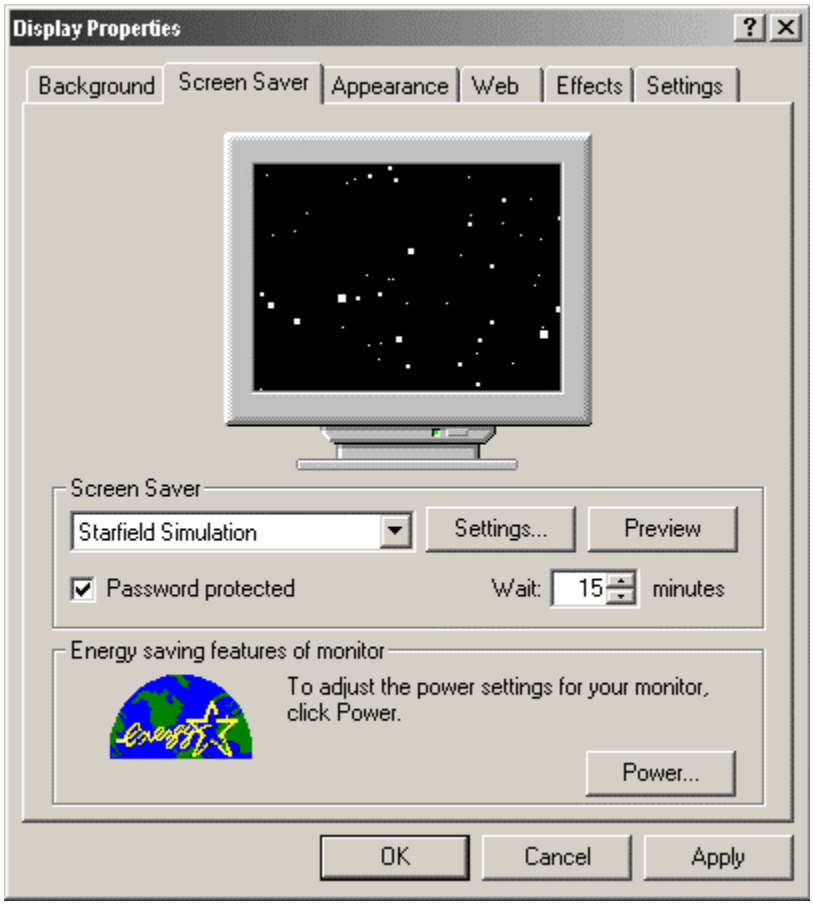
Return to Table of Contents

Helpful Hints

Locking a Windows Workstation

Locking your workstation when you leave it is a simple and effective way of improving workplace information security. The "three finger salute", as some call it, should be second nature to us all. To lock a Windows workstation, simply press the <CTRL><ALT><DEL> keys simultaneously, then either hit the <ENTER> key or click the 'Lock Computer' button in the onscreen window. Those few seconds of following security procedure can save many hours of headaches and embarrassment that come with a compromised system. (As long as your system is Windows NT/W2K/XP, that is. The password protection on older Windows systems – Win9x and Me – can be easily bypassed.)

One other procedure that is quite important is to configure your workstation to automatically lock after a short period of inactivity. If you wander off to get a printout, visit the restroom, or get tied up in a conversation this configuration will lock your workstation for you. Very kind, don't you think?



You can configure automatic locking through the Display Properties window, and there's a very easy way to get to there. Simply right click on an empty area on your desktop screen, and Viola! (Another way to get there is to click the Windows 'Start' button, then go to 'Settings', and click on 'Control Panel'. Click on the 'Display' icon and you get to the same place – the Display Properties window.) Now choose the Screen Saver tab. This will bring up the Screen Saver options window. Make sure the Password Protected box is checked. Then go to the Minutes box, and make sure that 15 minutes (at most) is selected. As an added bonus, you also have a variety of cool screen saver pictures to select from. When you have configured the

screen saver settings, click the 'Apply' button to enable the protection. Then click 'OK' and you're all set.

Some network domains (like the Iowa Domain) automatically configure all workstations within their domain with this locking configuration. As long as the Password Protected box is checked and the time selected is 15 minutes or less, the setting is fine - and meets the ITD Operating Security Policy as a bonus! (XP systems have had some problems with this – contact your departmental desktop support for assistance.)

Remember, the password for the screen saver is the same password you use to Login to your system in the first place. The only really different thing is the few seconds it takes to lock the workstation, and those few seconds can really count.

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 roughly bi-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. Questions regarding the Lunch & Learn program 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

SANS Twin Cities 2002
SANS invites you to attend a conference on May 6-11 in Minneapolis, Minnesota for SANS Security Essentials Bootcamp. This track is a beginner level course that prepares you for the next level of computer and information security. At this conference this track will be Bootcamp style, which means they will have special evening sessions during the conference with hands-on exercises led by a qualified SANS instructor. These special night sessions help you to get the most out of your time at the conference by giving you a chance to put into practice the skills you learn during the day!

SANS Great Lakes 2002
This conference will be taking place June 16-21, 2002 in Chicago, IL. At this conference we will feature SANS Security Essentials, courseware designed to teach the basics from risk assessment and policy to firewalls and operating systems.
SANS Great Lakes 2002 will also offer advanced training for those that already know the basics of how to protect their systems and information - Track 2: Firewalls, Perimeter Protection and VPNs; and Track 3 Intrusion Detection In-Depth.

Techno-Security 2002
April 7-10, 2002, Myrtle Beach, SC - Wyndham Myrtle Beach Resort
The 4th Annual International Techno-Security Conference will be presented this year by Enterasys Networks and will be held in conjunction with the Internet Security Alliance Conference. This one-of-a-kind conference is intended for corporations, government and law enforcement decision makers and technical enthusiast in the fields of Information & Network Security, Operational and Physical Security, Auditing, Cyber-Crime and its prevention.

Return to Table of Contents

Feature Articles

Defense-in-Depth: The ITD Exchange Mail System

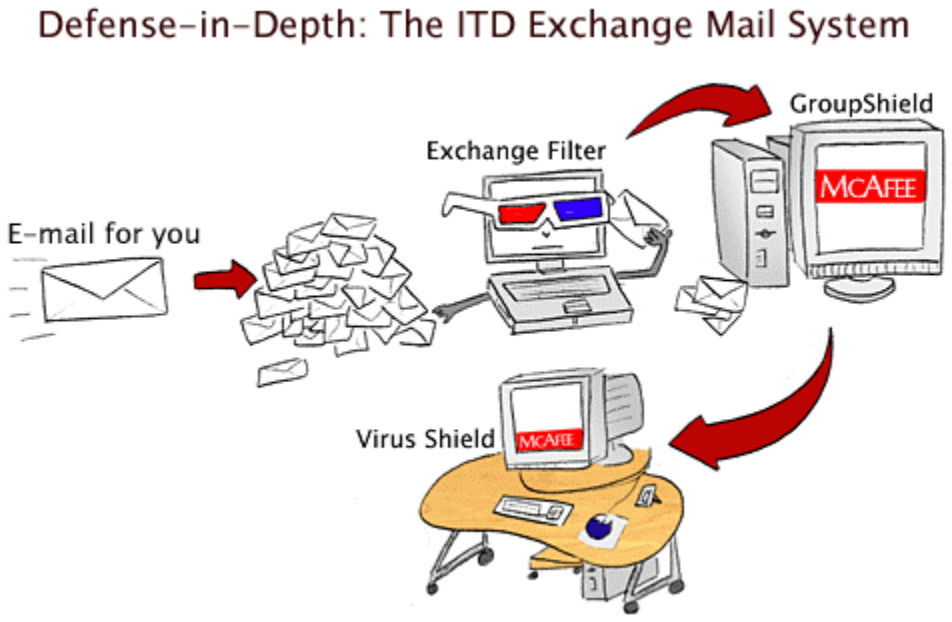
With the popularity of email increasing, businesses that once used this tool as a reliable means to communicate with their staff are now facing new challenges in keeping their networks secure, employees safe, and business protected. Most people are aware that email is a common method of transmitting viruses between systems, but this is only one of the risks facing email administrators today.

Since computer virus outbreaks are becoming newsworthy, it would be surprising to find many computer users that are not at least vaguely familiar with this term. The reality is however, that many people do not take adequate measures to protect themselves from email-born viruses. Customers of the ITD Exchange mail service are protected on multiple lines of defense against virus outbreaks.

The first line of defense against viruses is provided by an email-filtering application. All SMTP traffic entering ITD's Exchange Server is scanned for matches against a database of rules. These rules can examine almost every aspect of the message. For example, any message that contains a subject line that matches "ILOVEYOU" would be blocked because it matches a known virus pattern of the Loveletter virus. In another example, any message that contains an attachment that is of an executable nature would be blocked because of the high risk of virus infiltration. In even more extreme cases rules can be written to block by sender or domain. The filtering application in some cases is used to examine the message body for key phrases such as: "I am in a harry, I promise you will love it!" that are associated with known viruses, in this example the Goner Virus. By using this application to examine all messages coming into the Exchange system, ITD is able to stop most known viruses before they ever arrive at our mail servers.

The second line of defense for email-borne viruses occurs on the Exchange Servers themselves. ITD uses the McAfee GroupShield product for its anti-virus software. As is common with traditional anti-virus software, this application is updated by way of virus definitions that are downloaded from McAfee. ITD automatically looks for new definitions throughout the day, and our servers are configured to download any new definitions automatically. This level of protection examines every message that reaches the mail server – not just the ones inbound from the Internet. That way if a virus were to be introduced internally the anti-virus software would isolate it before it could spread to other people.

Customer desktops represent the third line of defense in the war against viruses. ITD supported desktops are configured with an installation of McAfee Virus Shield that is configured to scan incoming files. These desktops also download automatically any new virus definitions as part of the ITD configuration. It is extremely important that end-users not disable this software because it represents the final line of defense against computer viruses.



By combining multiple lines of protection from email-borne viruses, ITD is attempting to prevent the introduction and spread of these attacks on State systems. While the efforts made at the server level requires a degree of monitoring and support, end-users can do their part by practicing good procedures. Start by not tampering with or disabling any anti-virus applications that have been installed on your computer. Be cautious of email messages from unknown senders – especially ones that contain attachments or links to websites. If you are concerned about a particular message either delete it, or contact your support person. When virus attacks do occur, take the time to read any advisories distributed by the ISO or your administrators to make sure that you know what to look for and how to react.

Another recent development is the use of email to solicit individuals for money or personal information. Lately there seems to be a large increase in this type of activity, and the risks can be high! Remember to never share personal information over email. Most of today's email conversations are not encrypted and even if you know the person on the other end, you cannot be sure that your information is not being intercepted. Information such as credit card numbers and social security numbers does not belong in email! Be even more cautious when you receive unsolicited requests in email. Recently there have been scams that appear to be from the Internal Revenue Service and messages promising large sums of money from a foreign dignitary who is in trouble. These are not legitimate, and people that succumb to the fear of an IRS audit or to the allure of free money may be sharing very personal information with people that do not have your best intentions at heart.

The final type of message being addressed by ITD technology today is SPAM or unsolicited email. These messages range from sales on printer ink to invitations to join adult chat rooms. Because we do not want to censor the content of email, this type of message is the hardest to combat. ITD does subscribe to a service that identifies servers that are known SPAM senders. When we receive mail from those servers it is rejected, but no service can be completely accurate, and this "junk mail" is still going to find its way into our mail systems. The best recommendation to minimize your receipt of unwanted mail is to guard your email address. When you sign up for newsletters or use your address on web sites, you run the risk that your address will be sold to mass-mailers. If you do receive unwanted mail, try to unsubscribe if the sender gives you the option. If the mailings continue, you may want to visit with your support staff about creating rules to automatically delete the unwanted mail.

As the attackers we fight become more and more ingenious, so will our measures to combat them. Already newer versions of Outlook are starting to block attachments that contain suspect code, and network devices are becoming available to do even more extensive scanning of the traffic coming into our networks. Just remember, that all of this effort is designed to protect you and the enterprise you work for.

Kevin Miller

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

Another month has past, so I've now been working here for two whole months! The other day I received a message reminding me that it is time to change my password. According to company policy, we are required to change our passwords every 60 days. So I found the spot to change my password and successfully changed it to my cat's name: Fluffy. That would be easy for me to remember!

This morning I received another message concerning my password. The message said we are to use strong passwords and protect them. My current password did not meet these standards and was easily cracked with the company's password auditing tools. I was to change my password immediately to comply with these specifications.

So what constitutes a strong password and how am I supposed to protect it? I decided to look around on the web for strong password and protection practices. I've heard that www.google.com is a good search engine to use for these technical things, so that's where I started.

I found a lot of useful information, but some of the suggestions were stronger than others. For example, one source suggested that the password lengths be at least six characters long, while another source suggested at least eight. I decided that I should find out what the requirements are for my company, so I don't get into trouble … again.

I was able to locate the security policy on our company web site without too much trouble. The section on passwords is very specific. There are a lot of requirements in the policy that I didn't know about. Not only requirements for the password itself, but also for protecting the password. Here are the major password requirements I discovered:

- A minimum of 8 alphanumeric characters with at least one special character
- Upper and lower case letters
- Not written down or recorded on-line in any form
- Not shared with anybody
- Not words, or combinations of words, found in dictionaries, spelling lists, or other lists of words, even if combined with other alphanumeric and special characters
- Not a user ID in any form
- Not information easily obtained about the user

I guess using my cat's name, Fluffy, violated quite a few of those requirements right off the bat. It was not 8 characters long, didn't have a special character, was a word in the dictionary and was information easily obtained about me. No wonder they want me to change it right away. What could I use that would be long enough and meet all the other requirements and that I would be able to remember without writing down?

I did see something about using a pass phrase if you have trouble remembering passwords. You just pick a phrase that you can remember and use the first letter of each word in the phrase. I can do that! I just have to make sure there is a mix of numbers, capital and lower case letters, and special characters. Then, if it's long enough, it should meet all the password requirements.

I could use something about Fluffy for my pass phrase. Then it would be easy for me to remember, but still a strong password that would be difficult to crack! I could use the phrase "I need to feed Fluffy at 6pm!" That would translate to "IntfF@6pm!" for my password. It includes 10 characters with a mix of capital and lowercase letters, 2 special characters and a number! I can remember that phrase without writing it down, so I can protect my password too! I won't be getting in trouble for not having a strong password anymore!

Amy Wilmeth

Return to Table of Contents

Linked Articles

Microsoft hammers Windows security kit
The Baseline Security Advisor will scan Windows computers for unpatched programs, weak passwords, and vulnerabilities in the operating system.

Fingerprints mark tighter IBM security
IBM is brushing up its computer security system to further protect its customers' data.

CIO Cyberthreat Response & Reporting Guidelines
CIO Magazine worked with a group of industry experts and law enforcement officials to create the first set of security reporting guidelines sanctioned by both the Secret Service and the FBI. This groundbreaking PDF includes phone numbers of federal and local law enforcement agencies and a reporting form that you can use at your organization. Other resources on Incident Response, Helpful Agencies, and other topics are available at: http://www.cio.com/research/security/response.html

The ROI of Security: You Wanted Numbers, We Got Numbers
Finally, a real return on security spending. For years CIOs have had to use scare tactics and other soft arguments to justify an investment in security. Now, for the first time, they may be able to get numbers they need to show a measurable ROI.

Cyberattack Could Provoke Military Attack
White House technology adviser Richard Clarke said that a cyberattack launched by foreign countries or terrorist groups could prompt a retaliatory military attack from the US. Clarke also indicated he believes that many critical infrastructure systems have already been broken into. (14 February 2002, USAToday)

Info on Web Sites Could Pose Security Risk
Corporate websites contain floor plans and back-up facility locations, telecommunications sites include locations of routers and major network nodes, and DOE websites provide sensitive information about plutonium storage and nuclear reactor locations. Richard Clarke says there is evidence that al-Qaeda used the Internet to gather information about US facilities, and that other groups may be doing the same thing. (11 & 13 February 2002, ComputerWorld)

Application Security "In Grim State"
A security research company reports that most e-business applications have serious security flaws. 17 February 2002, VNUNet

Anonymous Surfing Technology has Holes
Two researchers published a paper describing flaws in SafeWeb's anonymous surfing technology that could allow web sites to gather visitors' Internet addresses and other surfing habit information by using JavaScript. SafeWeb says it will fix the problems. (12 & 14 February 2002, Wired)
http://www.wired.com/news/politics/0,1283,50371,00.html
http://www.wired.com/news/business/0,1367,50424,00.html

Online Fraud Detection Takes Diligence
By all accounts, the online business-to-consumer market is growing at a healthy pace, but along with the increase in revenue comes a rise in the number of fraudulent transactions. (Network Computing)

Microsoft Freeware Checks For Windows Security Holes
The company's new Baseline Security Analyzer allows networked administrators to check whether their NT 4.0, Windows 2000 or XP desktops and servers are properly patched and configured. ComputerWorld

Microsoft Program Tracks User's Habits
Microsoft's new version of its popular Media Player software creates a list of the digital songs and movies each computer user has played - a potential treasure-trove for marketing companies, lawyers, even snooping spouses. (Feb. 21, 2002, ITToolBox)

Security Manager's Journal: The Strange Case Of The Phantom Intruder
Someone has been accessing a sales staffer's computer at night, leaving a trail of Web site addresses. Security tools identify a potential internal perpetrator, but it's human detective work that finally closes the case. (ComputerWorld, Feb. 25, 2002)

Energy Firms Move To Thwart Cyberattacks
Looking at information sharing as critical to securing the nation's oil and gas infrastructure, energy industry giants have banded together to form an information-sharing and analysis center. (ComputerWorld, Feb.25, 2002)

Pointed Questions
A hacker's recent infiltration of Comcast's Web site offers us all this lesson: Don't be sloppy with the administration of your Web servers and in securing the data that resides on them. (ComputerWorld, Feb. 25, 2002)

Official: Terrorists Used Internet To Get Info On Potential Targets
There is growing evidence from Afghanistan that al-Qaeda was going online to gather information about U.S. critical infrastructure, the head of the White House Office of Cyberdefenses told a Senate hearing. (ComputerWorld, Feb. 25, 2002)

Network Admin Who Destroyed Network Gets 41 Months Of Jail Time
Timothy Lloyd was sent to prison for nearly 3 and a half years and ordered to pay 2 million US dollars in restitution for planting a time bomb that destroyed the manufacturing software developed by his employer. (4 March 2002, NWFusion)

Federal CIOs Rate Security Higher Than E-Gov
According to a survey, defending federal systems against Cyberterrorism has passed the quest for electronic government as the highest priority for federal CIOs. (27 Feb. 2002)

Malicious Code Infection Soars
Despite increased spending, the rate of malicious code infection continues to climb. A staggering 1.2 million incidents took place over a period of just 20 months, according to a new study. (ITToolBox, March 5, 2002)

Online Fraud Loss 19 Times Offline's – Gartner
More than 5 percent of online consumers last year were victims of credit card fraud, a crime that accounted for more than $1 out of every $100 spent on Internet sales, according to a report published today. (ITToolBox, March 4, 2002)

Alarmed: Information security is the stinky office fridge. Everyone knows it's a big problem, but nobody thinks that it's their problem. (March 4, 2002, CIO Insider)

Air Force CIO Wants Better Security In Microsoft Products
Air Force CIO John Gilligan says the Air Force will stop using Microsoft software if the company doesn't improve its products' security; Gilligan says the Air Force will do business with the companies that offer the best solutions. *[Editor's (Schultz - SANS) Note: This is an extremely significant development. A large customer is standing up to vendors and saying "We will not buy your products any more if you don't give us better security." Vendors say they do not provide better security in their products because customers do not demand it. Now Gilligan is demanding it. If others like Gilligan follow suit, vendors will for the first time feel genuine pressure to develop better, more secure software.]* 11 March 2002, SANS Newsbites

Cyberspace Terrorism
We are now on the verge of an era of super worms that are malicious in nature, not platform-dependent, using new methods of exploit, and difficult to detect, defend and eliminate. How ready are you? March 13, 2002, ITToolBox

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 (7 general, 6 Windows NT/2000, and 6 UNIX/Linux), 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.

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