The Security Blanket

(We've got you covered!)

Volume 1, Issue 3. November 2001

In This Issue:

From the CISO
Current Activities
- Information Security Office Service Offerings

Helpful Hints
- Safe Web Browsing

Upcoming Classes and Consultations
- Lunch & Learns
- SecureIowa Conference (Keynote speaker: Tom Ridge or John Ashcroft)
- Terrorism Conference – Tentative
- Anthrax & Bioterrorism Online Tutorial

Feature Articles
- An Introduction to Public Key Infrastructure (PKI)
- Why Would Anyone Hack Me? – Prevalent Hacking Methodology

Linked Articles
Points of Contact
Links to Resources
- FBI and SANS List Top Twenty Vulnerabilities

From the CISO

Do you remember when you first heard about information security? I do. I was a 2nd Lieutenant system administrator at Wright-Patterson Air Force Base, and I was in my office being asked a bunch of questions by personnel from the Air Force Information Warfare Center (AFIWC). It was sometime in the spring of 1993. They asked questions I couldn't answer – questions I had not even considered. Little did I know at the time, but they had already broken into most of the networks on base, mine included, but not one administrator noticed the activity. I was embarrassed and felt terrible. And mad. I was mad at myself for not knowing anything about security, and mad at my management for not providing me with the knowledge to protect my systems. I had not even received the most rudimentary system administrator training and I felt as if I was thrown to the wolves. I resolved then and there to learn about security, even if I had to do it on my own. I started talking to other people about security and small groups of us began to learn about it. Then, two years later, it was time to move on. It was not a difficult decision at all to try for an assignment at AFIWC, so that's what I did. From that point on, my professional life has revolved around security full-time.

I will bet that some of you reading this feel the same way. There are also some of you who probably feel you know all there is to know about system administration and possibly even security. Hear it from me, and remember – you can never know enough. There's too much to know and understand, too much to consider, and too much to address. I learn something new almost every day – and so should you. Why am I writing this, you ask? Mainly, it's because the Information Security Office is here as a resource for you. We are continuously updating our Web site with more information on more subjects, developing more ways of getting you the information you need, and finalizing more services. If you have a question or concern, check the site or let us know. Attend the Lunch and Learns or view the PowerPoint presentations and streaming video (soon to come) on our site. Subscribe to our mailing list if you received this publication second hand. Take a look at our services and see what might be of use to you. We have developed some powerful capabilities to assess the security of our networks and protect our systems. None of this does any good if nobody takes advantage of it. If you need something we don't have, let us know and we'll see what we can do. We are here to help, and while I'm on watch we'll never embarrass anyone. This is extremely important stuff – if you don't believe that, *please* give me a call. Security is everyone's responsibility, and as we are caretakers of citizen information, it's an awesome responsibility. It should not be taken lightly.

Until next time…

Kip Peters

Return to Table of Contents

Current Activities

"I Want You – to Secure Your Networks!"

Information Security Office Service Offerings

(See http://www.iowaccess.org/government/its/rates/ for current rates.)

Security Consulting

Security consulting services are available to address general security concerns, suggest proper security implementations for current projects, or advise on other security-related topics such as physical security, business continuity, and policy development. Go to our Points of Contact for the appropriate resource person.

Vulnerability Assessments

Vulnerability assessments are an important part of an effective information risk management program and in maintaining a high quality of service. These assessments will benefit any organization that seeks to verify implemented security controls, suspects their IT infrastructure may have been compromised, desires to eliminate security weaknesses and protect their information technology infrastructure before a compromise occurs, or simply wants to establish a security baseline. Some or all of the assessments listed here may be performed, depending on the scope of the vulnerability assessment requested. Information gained from these services is kept confidential.

Network Vulnerability Assessments may include: Internal Assessment, External Assessment, Modem Sweep, Password Assessment, Physical Assessment, Corporate Security Culture Assessment. For an explanation of each of these go to: http://www.itd.state.ia.us/security/doc/va.doc. Contact Marie Hubbard for more information.

Physical Security Vulnerability Assessments

These assessments determine how physically secure locations are. They may include an evaluation of the agency's security culture, on-site property penetration, and/or on-site computer accessibility. Reports include applicable recommendations to improve physical security. Wes Hunsberger can assist you with facility-oriented physical security.

Network-Based Intrusion Detection System

ITD has implemented an enterprise intrusion detection system (IDS) composed of Cisco's Secure IDS, formerly known as the WheelGroup's NetRanger. The system currently looks at the campus backbone and is only located on the enterprise areas maintained by ITD. We have also developed our own system that we feel is much more user-friendly and capable. This capability is currently available even though we are still finalizing our service offerings. The services will more than likely include managed (installed, configured, and maintained) sensors, daily monitoring, periodic reports, timely notification, and incident response. If you want to learn more about this, please contact Marie Hubbard.

Enterprise Business Continuity

We have a certified business continuity planner on staff to develop, coordinate, and maintain the enterprise IT business continuity plan, as well as provide expertise to agencies on business continuity. If you would like to know more about this service, contact Wes Hunsberger, our resident expert.

Incident Response

In the event of a security incident, the security office is available to provide assistance in responding to the attack. Examples include network penetration and/or malicious activity, mail server exploitation, web site defacement, or possible scanning activity occurring on systems. Contact Kip Peters or Marie Hubbard for further information.

Test Lab

ITD has a test lab available for various testing purposes. Testing can be performed on new products, new machines, upgrades, patches, standard configurations, or virtually

any other purpose. If new desktops are going to be rolled out, we can configure, test, scan, and lock down a standard load in preparation for deployment. Server configurations can also be tested and made secure prior to being placed in operation. Testing can include not only automated scanning by vulnerability assessment tools, but also penetration testing. To request this capability, or get more information, contact the ITD Help Desk, 281-5703.

Awareness Briefings

Security awareness training is intended to provide average users with some knowledge of general security concerns and help them understand their security role. An on-line application is currently under development and will be available to all government-related entities within the state of Iowa. Specific awareness briefings, tailored to individual agencies, may also be provided when requested. Contact William Hubbard for more information.

UPCOMING SERVICES

On-Line Awareness Training

An on-line security awareness training application is currently under development and will be available to all government-related entities within the state of Iowa by the end of calendar year 2001.

Vulnerability Profile Database

ITD is planning to obtain the capability to identify vulnerabilities on systems based on profiles. Each profile is a single server, device, computer build, or other computer/network device. For example, a server profile will be composed of the hardware, operating system, application software, database, and other hardware/software comprising that particular system, including versions, service packs, and installed patches.

Based on the profile, specific vulnerability and countermeasure information for that one server will be available to the administrator. A capability to track the status of necessary patches, service packs, configuration changes, and other updates is included. This not only provides an opportunity to know which vulnerabilities affect which devices, but it also provides a convenient way to inventory critical nodes within the environment. Comprehensive reporting is also a feature.

This capability will be put in service some time in the fall of 2001.

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

This is the main contact point for enterprise security information and resources. It also has a companion site, the Mobile Edition, which has lots of breaking news and security articles. The mobile edition is updated every couple of days so the information is kept current.

New ITD Security Policy

A working draft of the Enterprise Security Policy will be available for review in December.

PKI Implementation

Public key infrastructure RFP's have been reviewed and are being scored. A contract is expected soon.

Return to Table of Contents

Helpful Hints

Safe Web Browsing

The Internet is rather like a jungle: vast, mysterious, full of useful resources and amazing sights, and it can be a boon for business or personal enjoyment. However, it has its pitfalls, snakes, nasty creatures that want to eat you, and dangerous places that you really want to avoid. Much like traveling in the jungle, one needs to take certain precautions when visiting the Internet.

Make sure your jeep is running well and your travel gear is in good order. That is, make sure your operating system and your web browser have current patches and fixes. If they don't, you may accidentally upload Trojan horse programs, worms, or allow personal information like credit card account numbers to be gathered by nefarious

creatures that stalk the Internet. If you use Microsoft Windows and Internet Explorer from home, for example, visit http://windowsupdate.microsoft.com/ at least once a month to stay up-to-date on fixes. Active X, JavaScript, and active scripting features have a variety of security weaknesses and exploits associated with them, so disable them if you don't need them. At work the security settings should have been set by your departmental support staff, so don't change your system or browser configuration. Think of the support staff as your local friendly native guides, they'll help you get safely to the places you want to visit. For an added safety practice (kind of like riding in an armored jeep), you can also use a free service like www.safeweb.com, which filters active x, JavaScript, and active scripting when you browse the Internet through their web page.

Keep your eyes open and watch for potential danger. A firewall can help prevent unauthorized access to your computer and inform you of suspect Internet traffic. Most state agencies have firewall protection, but for web browsing from home, a personal firewall is recommended. Free ones such as ZoneAlarm home firewall (at www.zonealarm.com), or the Tiny Personal Firewall (at www.tinysoftware.com) are available, or you can purchase products such as Symantec's Norton Personal Firewall.

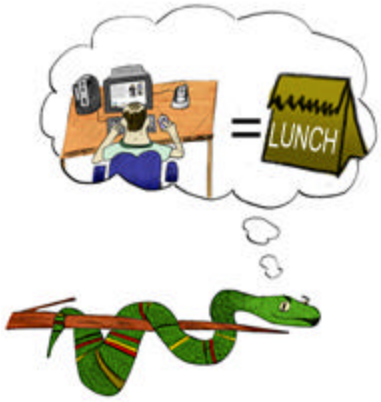
Wear protective clothing and stay inoculated. Use a virus scanner and make sure it's updated. Up to date virus protection will help tremendously in keeping nasty viruses and worms out of your system. (Especially if you access e-mail via the Internet/Intranet.)

Stay on the path. For business purposes, go to the jungle to get what you need, then go home. If your department allows web browsing and you are sightseeing and doing some exploring during a break, be prudent in where you walk. Do not go to known hacker sites, and do not visit sites that your co-workers may find offensive. There are even some sites on the Internet that can attack your system simply by your visiting them – no downloads required. Just like with quicksand, when you realize you're in it, it is usually too late.

Leave the wildlife alone. Do not download anything unless you have the authorization to do so. The Law of the Jungle states: "shareware and freeware from any source shall be installed only with management approval" (ITD Operating Security Policy). Even if you are authorized to download from the Internet, it is best not to unless absolutely necessary. If you do have authorization and do download an item, scan it for viruses before opening or running it. Documents, executables, screen savers, videos, patriotic power point slideshows, or anything else – scan it.

Say you've collected a specimen from the Internet jungle. How do you inspect it for nasty things? Well, to scan a downloaded file (in Windows using the McAfee Virus Scanner), right-click on the file and a short menu will usually appear, depending on the type of file. Select 'Scan for viruses' on the pop-up menu. The VirusScan window will appear, and the file you right-clicked on is automatically selected, so you only need to click the 'scan now' button. A second method is to go to the Windows "Start" tab, select Programs, Network Associates, and then select VirusScan. The VirusScan window will appear. You can browse through your drives and choose the file, folder, or drive you want to scan, and then click the 'scan now' button. As always, check with your departmental desktop support staff for the proper procedures for your specific operating system and Virus protection program. (Also of note, some products such as McAfee's VShield can be set up to automatically scan all downloaded files, but again this practice may vary from department to department.)

Anyone can become prey. Please be aware that there are hackers out there that don't care who you are or what you are doing, you are simply a target to them. Like a very hungry carnivore in the jungle, they will eat you if they get the chance. Be mindful that some people are even using the Sept. 11 tragedies and associated issues to lure you to their sites in order to compromise your systems or to get credit card numbers to steal your money.



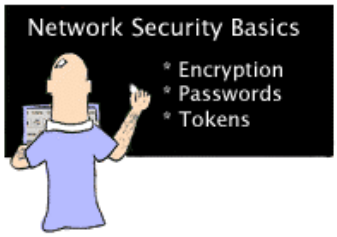
Remember that many bad things from the Internet jungle are contagious. The 1i0n worm, reputed Chinese hackers, and Russian credit card thieves are all examples of real threats. (Lions and Tigers and Bears, oh my!) If you get infected with a worm or virus, or a bad critter compromises your system, it could dramatically - and badly - affect your agency's network as well. In protecting your own system you are also protecting the state's network.

Thanks for your time, and be careful – it's a jungle out there.

William Hubbard

Return to Table of Contents

Upcoming Classes and Consultations



This section will include announcements of security training opportunities, classes, or 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. Examples of possible classes include Security Policy, How to Perform Risk Assessments, and Basic Security Training. Also included will be security-related vendor announcements for seminars. We will try to give a six-month advance notice on formal training events and opportunities.

Lunch & Learns

The Information Security Office Lunch &Learns have begun! These bi-monthly, informal get-togethers will cover a variety of security-oriented issues. No sign-ups or registration is necessary, just come on down! The current schedule is as follows:

Date and Time	Topic and Location
Nov. 27 12-1pm	Critical Infrastructure Assurance and Cyber Terrorism 1LC and 2LC, Hoover Building, B Level
Dec. 11 12-1pm	Top Security Issues for Win2000 1LC and 2LC, Hoover Building, B Level

Jan. 8 12-1pm	TBA 1LC and 2LC, Hoover Building, B Level

The Lunch & Learn location will be in the Learning Center 1 and 2, in the Hoover Building, B Level. The dates and times for the meetings will be the 2nd and 4th Tuesday of each month, from 12pm-1pm. Change of location or time will be announced via e-mail, and sent to departmental L&L security contacts. Past presentations (like **Introduction to the Information Security Office** - in .pdf and video) and an updated schedule is available at http://www.itd.state.ia.us/security/education.html#lunchnlearn. Questions regarding the Lunch & Learn program can be directed to William Hubbard.

SecureIowa Conference
December 6th and 7th, Embassy Suites on the River, Des Moines
Keynote speaker is anticipated to be Tom Ridge, President Bush's Director of Homeland Security. For more information, see: http://www.secureiowa.com.

Terrorism Conference – Tentative
January 16, 2002. STARC Armory, Camp Dodge, Johnston, Iowa.
Sponsored by the EMD
Topics may include terrorism preparedness, terrorist incidents, event exercises, and both large sessions and small breakout sessions. Contact: Thomas Baumgartner.

Anthrax & Bioterrorism Online Tutorial

"Anthrax & Bioterrorism" is a free online consumer information course available on the GeoLearning web site at http://www.geolearning.com/main/promotions/demos. The program was developed by The Patient Education Institute to help explain the causes and types of anthrax. It also reviews the symptoms, diagnosis, treatment and prevention of anthrax through vaccination and awareness of bioterrorism.

During this time of heightened alertness, we wanted to offer this practical information to the American people as a public service. Please feel free to inform others about the availability of this important information.

The Team @ GeoLearning

Editor's Note: you will need to provide your name, address, etc. to GeoLearning to be able to view the online tutorial.

Interested in SANS Conferences? See http://www.sans.org/ for details on locations, dates, and courses.

Return to Table of Contents

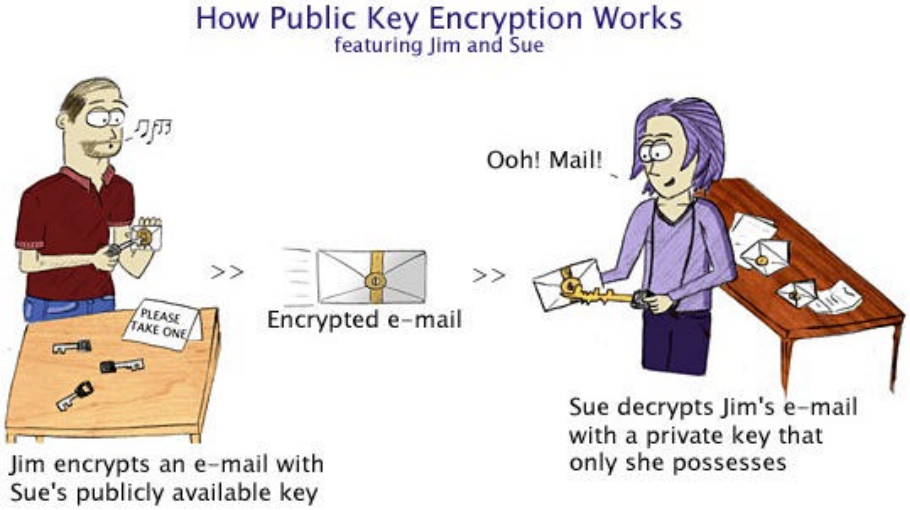
Feature Articles

An Introduction to Public Key Infrastructure (PKI)

To realize the full potential of the Internet, we need to know we can engage in electronic transactions with the same degree of trust we associate with paper-based transactions. Sealed envelopes, official stationery, written signatures, and trusted delivery services have provided confidence in traditional communications.

In today's new digital environment, a public key infrastructure (PKI) helps to ensure that sensitive electronic communications are private and protected from tampering. It provides assurances of the identities of the participants in those transactions, and prevents their later denying participation in the transaction.

The basics of PKI are fairly simple. Secret key, or traditional, cryptography ensures confidentiality by encrypting information using a secret key and an algorithm. Once encrypted, the information is secure and must be decrypted with the original key to be read. This method is computationally efficient and effective, but it has one overriding problem – the key must be shared among all communicating parties. The central problem with secret key cryptography is managing these keys and keeping them secret.



Public key cryptography solves this problem by replacing the secret key with a pair of keys, one private and one public. The private key is kept secure by an individual while the public key is published and available to interested parties, eliminating the need for the sender and receiver to share secret information. The major requirement of this system is to associate public keys with their users in a trusted manner (the concept of a certificate). With this basic structure, public key cryptosystems have two primary uses, encryption and digital signatures.

Encryption. To send an encrypted message, Jim encrypts his message with Sue's public key and sends it to Sue. When received, Sue decrypts the message with her private key, which only she has, and reads it. In this manner, anyone with access to Sue's public key can send a secret message to Sue, but only Sue can read it.

Digital signatures. To sign a message or document, Sue applies a hash function to the information, creating a unique number, or hash. She then encrypts the hash with her private key, creating her digital signature. To verify that signature, it is decrypted with Sue's public key revealing the original hash of the information. That figure is compared to a new hash taken of the information received. If the numbers do not match, the signature is fraudulent or the message, which was not encrypted, may have been altered. This provides both authentication of the message and the sender.

Public key cryptography, on its own, is not enough to re-create the conditions for traditional paper-based commerce in the electronic world. Other things are needed as well, including security policies to define the rules under which the cryptosystems operate; a means to generate, store, and manage the keys; procedures to dictate how the keys and certificates should be generated, distributed, and used; and the security of the cryptosystem itself. A PKI has many functions: it must register users, issue and revoke

certificates, store and retrieve certificates and certificate revocation lists, and update, archive, and restore keys. All of these things make up a PKI.

A PKI provides the core framework that provides the four principal security functions required of commercial transactions:

- Confidentiality – keeps information private.
- Integrity – proves that information has not been manipulated.
- Authentication – proves the identity of an individual, application, or computer.
- Non-repudiation – ensures that individuals cannot dispute having taken part in a transaction.

A PKI combined with PKI-enabled applications can enable a business or government to do many things electronically, and do them efficiently. A PKI will provide the means to enable the widespread use of digital signatures, but one of its key advantages is leveraging its capabilities across multiple applications. In this way, e-commerce and digital Government initiatives can be implemented securely and efficiently, as well as secure e-mail, Web access to both public and private information, virtual private networks, and a myriad of other applications. Today, these applications are developed and secured individually, creating a hodge-podge approach to security without adherence to common policies and procedures. Not only does this reduce the overall security postures, but it is also not cost-effective. If applications take advantage of a central PKI, then common policies, procedures, and methods are enforced. This results in an increased overall security posture, enhanced service, and monetary savings.

Kip Peters

Why Would Anyone Hack Me? – Prevalent Hacking Methodology

In my occupation as an Information Security Engineer for the Information Technology Department, I often hear questions such as "Why would anyone hack me?" or "Why would anyone want to hack the State of Iowa?" In this article I hope to briefly explain why general hackers choose the targets that they do. This paper does not try to explain the mindset of hackers, but rather their methodology in determining whom, or more precisely what computer, they *might* attack. This may help explain why someone might attack you even though you have never met him or her.

The answer to the first question really has to do with numbers. Whenever you connect to the Internet your computer gets an IP address. An IP address is much like a street address in that it tells people how to get information to you and it is unique to you alone. Many hackers have programs that just scan IP addresses looking for certain operating systems or vulnerabilities that they know how to exploit. The attacker will run these tools on a range of IP addresses. After the scans are done, the attacker will return to their computer to find a list of IP addresses of machines that may be vulnerable. Then they can choose to attack those IP addresses. At this point, your computer is purely a number to them and they do not care who you are or where you are located. They are really attacking your computer, not you.

The second question is why would a person want to hack the State of Iowa, after all, we are just Iowa. Similarly to the first question, hackers will attack State of Iowa computers simply by finding a vulnerable IP number – they may not even realize that it is a State computer. Another reason is that State websites or computers are **government** resources and some hackers take joy in knowing that they can hit anything related to the government. The fact that our homepage ends in a ".us" makes us a global target to anyone that wants to show they can hack a United States government website. Disgruntled employees or customers who are upset can also attack the State. All organizations run the risk of becoming the target of a focused attack from someone that is displeased by an action that that organization has performed.

It is important to remember that on the Internet many times we are just a number. There are times when we can be the focus of attacks for reasons that we may know of, but many times, especially with home users, we get attacked for no other reason then our IP address was scanned and our computer was vulnerable to an exploit. Ask any person out there with a firewall or anything on their computer that logs scanning activity against their computer and they can tell you that there is constant scanning on the Internet. It's a target rich environment, and unfortunately any machine, by virtue of its numeric IP address, can be a target.

Paul Schmelzel

The Information Security Office is staffed with trained security professionals, like Kip Peters and Paul Schmelzel, who are ready to serve you!

Return to Table of Contents

Linked Articles

How to Blunt the Socially Engineered Hack
Because hackers can use many small, seemingly innocuous pieces of gathered information to initiate an attack, companies are well advised to be on their guard against social engineering - exploiting people's naturally helpful natures into disclosing sensitive information. Includes tips for avoiding socially engineered hacks. (ComputerWorld, Nov. 8, 2001)

From Threats to War, Cybersecurity Enters a New Era
The Internet's greatest asset -- its open, ubiquitous nature -- is turning out to be its greatest liability. (ITToolBox, Nov. 6, 2001)

Trojan Programs Improve Attack Methods
Security watchers have warned that Trojan programs, feared for their ability to compromise a network and go unnoticed, are getting sneakier about sending data out of the network. (ITToolBox, Nov. 5, 2001)

Critics: Patriot Act puts privacy at risk
President Bush signed legislation Friday that expands the ability to tap telephones and track Internet usage in the hunt for terrorists, new powers that drew praise from law enforcement officials and concern from civil libertarians. (ZDNet, Oct. 26, 2001)

Terrorist Attacks, New XP OS Renewing Interest In Biometrics
One of the most significant changes in Microsoft's new Windows XP operating system could signal the beginning of widespread use of biometric technologies, experts said. (ComputerWorld, October 25, 2001)

Corporate Security Gets Urgent
Securing the Internet infrastructure that underpins corporate America has taken on a new urgency as the nation moves deeper into its war on terrorism. (ZDNet/Interactive Week, Oct. 23, 2001)

Identity theft more than doubling
The number of identity thefts reported by banks and other financial institutions is on the upsurge again in 2001 after more than doubling last year, according to a new report released on Monday. (ZDNet, Oct. 22, 2001)

Ridge Calls for Cooperation
Tom Ridge, the head of the newly created Office of Homeland Security, has called for government agencies to share intelligence information with each other. (Federal Computer Week, October 9, 2001)

Security Overview
Hackinthebox.org has a nice overview of security areas one should consider in their organization. It's pretty high-level but covers all the bases. It sums up 5 purposes that your security should server and lays out 5 layers within your network systems that should be protected. (Hack in the Box, October 17, 2001)

Guarding Against Cyberterrorism
With the country fully engaged in a war against terrorism, enterprise security managers nationwide are on heightened alert, scrambling to ramp up security to guard against attacks on critical electronic infrastructure. (ITtoolbox Security, October 23, 2001)

Feds Ask Business Leaders To Help Protect Infrastructure
Even as the fear of biological warfare paralyzed portions of the nation's capital, a picture of renewed cooperation between the government and industry on critical infrastructure protection was beginning to emerge. (ComputerWorld, October 22, 2001)

Experts Call for Increased Cybersecurity Funding
Speaking at a conference sponsored by the Information Technology Association of America (ITAA) and the Center for Strategic and International Studies, ITAA president

Harris Miller said that the US government needs to devote at least $10 billion to cybersecurity if the country is to be adequately protected from cyber attacks. The money would be used primarily for training, education, and upgrading critical systems. (ComputerWorld, October 18, 2001)

CERT/CC Predicts Incident Reports Will Double in 2001
The Computer Emergency Response Team Coordination Center (CERT/CC) predicts that the number of Internet attacks reported in 2001 is likely to be double that of the previous year. The dramatic increase is due in large part to a growing Internet and heightened security awareness. Automated vulnerability scans and web site defacements helped boost this year's numbers; viruses and worms are counted only once even if the attacks are massive. (ZDNet, October 15, 2001)

Review Internal Security, Say Experts
In the wake of the September 11 attacks, cybersecurity experts are encouraging businesses to reexamine their security policies with special attention paid to internal threats and physical security. No scenario is too improbable to consider. (ComputerWorld, October 15, 2001)

Return to Table of Contents

Points of Contact

Kip Peters: Chief Information Security Officer
Marie Hubbard: Chief of Security Operations
Larry Brennan: Critical Infrastructure Assurance Coordinator
Wes Hunsberger: Physical Security and Business Continuity
William Hubbard: Security Awareness
(Sir not appearing in this picture…)

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 (1 October 2001)
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.

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