The Security Blanket

(We've got you covered!)

Volume 1, Issue 2. October 2001

In This Issue:

From the CISO

The events of September 11th have made a profound impact upon society and attitudes, not only in this county, but in other countries as well. There will undoubtedly be more changes to come. One of the

realities since those events is a renewed emphasis on all things security. The things some of us have been talking about for quite some time are now being recognized as important. Many of us have started sentences with, "I hope it doesn't take a catastrophic event…" - it appears that it did. That is most unfortunate, and quite a costly lesson. I'm sure it brings no comfort to the thousands directly affected by this tragedy. Nothing can bring us back to September 10th, and nothing can make the hurt go away.

In thinking about this, I'm reminded of a quote I read in a newspaper. It was probably The New York Times, but I don't remember. I don't remember who said it, either. But I remember the quote. It was something very close to, "It appears that those who have been speaking about and arguing for security weren't just trying to boost their budgets." I'm actually appalled that someone actually thought it was strictly a budgetary issue. No, we aren't trying to boost our budgets or create job security, we are trying to raise awareness and make security a priority. What many of us already knew the entire world now knows – it's a new world, and new priorities are required. What you are going to see is an expansion of the attention currently directed towards terrorism and physical security to other things, such as critical infrastructures. It has already begun, certainly at the national level, but also within state government in Iowa. If you really want to take a look at some of the serious issues this country is facing, take a look at a paper I wrote a few months ago. It's not perfect and probably has some grammatical errors, but the research and conclusions are sound. To reach it, follow the Independent Research link at http://www.public.iastate.edu/~ciso.

One of the things we have all noticed is a higher display of patriotism than we have seen in this country in a long time. I live on a cul-de-sac, and since I've lived there only one other neighbor has ever displayed an American flag. You'll find a flag waving every day at our house, just as it has every day since we moved in. Now, most of our neighbors display a flag of some sort. It's a nice change and I hope it continues. I also hope they start to show the National Anthem being played at sporting events on TV again. NASCAR telecasts have always done this quite a bit, but it has lagged a lot in other sports in recent years. I remember watching baseball with my father; the Anthem was always something we looked forward to. I suppose I get my patriotism from him. He has always worn t-shirts about love of country, and was never shy about talking about it. Others now share this same sentiment. I hope they always will.

Kip Peters

Return to Table of Contents

Current Activities

ISO Offers Intrusion Detection Service

- Have you ever wondered if hackers are lurking through your systems?
- Did you know that an unprotected PC would likely be spotted by a hacker the first day it is online?
- Do you know that money spent on proactive prevention outweighs the cost of system cleanup?

Hackers are prevalent on the Internet and sift through thousands of computers daily looking for a place to break in. Though many hackers use sophisticated software tools, there are effective ways to inspect your network and stop them before they stop you. The Information Security Office is willing to provide you with an affordable solution to detect hacker intrusions and keep your information secure.

The Information Security Office has a product available that will make you aware of dangerous hacker activity and strange traffic on your network. We offer an Intrusion Detection System (*IDS*) package that is affordable and rivals the quality of any "top of the line" multi-thousand dollar system for just a fraction of the price.

Our system is based on the open source IDS called "Snort". Members of the Internet security community created Snort as an effective alternative to expensive commercial IDS's. We have utilized this excellent software and created a manageable system that gives us the ability to proactively analyze your network for a multitude of attacks, like Nimda and Code Red. Our service provides constant software updates, remote system administration, and data analysis that would take hours of weekly staff-time to do on your own. With our IDS solution, we can offer you instant alerts upon hacker attacks as well as weekly or monthly reports that include analysis of your network traffic.

The Information Security Office wants to help you protect your network without putting a pinch on your budget. Now is the best time to take a proactive approach in protecting your Information Systems. Our affordable IDS solution will keep an eye on your network - 24/7 - when you can't be there to watch it. If you want to take a proactive approach to network security with our Intrusion Detection System, please contact Marie Hubbard at 291-4905.

Jared McLaren

Security service offerings are being finalized and will be published in a few weeks.

Enterprise Security Website

This is the main contact point for enterprise security information and resources. The current Enterprise Security Policy can be accessed here, too! 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.

Enterprise Intrusion Detection System

The ITD Security Operations Team monitors a great deal of network traffic with their IDS. This system has not only alerted us to network attacks or security issues, it can also help alert us to what systems may have been compromised during attacks. If you want to learn more about this, please contact Marie Hubbard, the Security Operations Team Coordinator.

Security Consultation

Members of the ISO have a plethora of security information we can discuss with or advise you on. Security Policy and Procedures, Network Security, Information Assurance, Biometrics, and a host of

other issues are all part of our field of expertise – and if we don't know we'll help you find a resource that does! Go to our Points of Contact for the appropriate resource person.

Test Lab

The Information Technology Department has a test lab available for agency use. Testing can be performed on new products, new machines, upgrades, patches, standard configurations, or virtually any other purpose. If you are going to roll out new desktops, they can configure, test, and scan a standard load in preparation for deployment. To request this capability, or get more information, contact the ITD Help Desk, 281-5703.

In Development:
Security Awareness Online Training
Vulnerability Profiling Service
New and Improved Enterprise Security Policy

Return to Table of Contents

Helpful Hints - Workstation Security

Every person is responsible for keeping his or her workstation secure. An unlocked, unattended workstation is a serious security risk. When a user leaves his or her workstation unlocked, **anyone** can use it and assume the user's identity, gaining access to any applications or files the authorized user has access to. Users should lock their workstation whenever they leave it, even if they will only be gone for a few minutes.

Also, password protection should be enabled in the workstation configuration so that the protection will be invoked after a short period of inactivity (15 minutes is recommended). Ask your support staff for assistance if you don't know how to lock your workstation or set the screensaver settings. There is truly no faster way to get unauthorized access to systems than by simply walking up to someone's unlocked workstation: point and click, and they're in.

Going to a meeting? Lock your workstation. Going to get some coffee? Lock your workstation. Going to the restroom? Lock your workstation. It's very easy to get sidetracked and stay away from your desk longer than you anticipate, so its best just to keep your workstation secure whenever you leave it.

Return to Table of Contents

Upcoming Classes and Consultations

- Security training opportunities and classes
- Conferences
- Security-related vendor announcements

Lunch & Learns

The Information Security Office is beginning ongoing 'lunch-and-learn' sessions in November. Our idea is to have a bi-monthly, informal get-together during a lunch hour to go over a variety of security-oriented issues. These sessions will be on new Security Policies and Procedures, Operating System security, Intrusion Detection, Viruses, and a host of other issues. The current schedule is as follows:

Date and Time	Topic and Location
Nov. 13 12:30-1:30pm	Introduction to the Information Security Office Grimes South Conference Room, 1st Floor
Nov. 27 12-1pm	Critical Infrastructure Assurance and Cyber Terrorism 1LC and 2LC, Hoover Bldg.
Dec. 11 12-1pm	Top Security Issues for Win2000 1LC and 2LC, Hoover Bldg.

Change of location or time will be announced via e-mail and an updated schedule will be on the Enterprise Security Website.
Questions regarding the Lunch & Learn program can be directed to William Hubbard.

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.

Iowa Technology Showcase
October 24 - 25, 2001, 10:00 am - 4:00 pm Daily
ITEC's Iowa's Technology Showcase is Iowa's premier government and education focused IT event because we deliver the companies, people, technology and relationships that you need to evaluate the constant changes in the IT industry.

SANS Network Security 2001
Date: October 15 - 22, 2001
Location: San Diego, California
SANS Network Security 2001 is by far the largest conference on network security and the people who have given presentations at previous SANS Network Security

conferences have gone on to lead the security programs at organizations around the world. It offers a multi-track technical conference focusing on proven solutions for the challenges facing UNIX and NT security professionals. Hot topics include: Intrusion Detection, Network and System Forensics, Vulnerability Assessment, Firewall Architectures and Product Selection and more. (8 tracks),

Other SANS Network Security Conferences:
**Great Lakes SANS (3 tracks), Chicago, IL, Nov. 5-10
**Three Rivers SANS (1 track), Pittsburgh, PA, Nov. 15-20
**North Pacific SANS (1 track), Vancouver, BC, Nov. 15-20
**SANS Cyber Defense Initiative (6 tracks), Wash. DC, Nov. 27 - Dec. 3
**SANS Cyber Defense Initiative (3 tracks), San Fran. CA, Dec. 16-22
**Plus new, on-line, security training programs
See www.sans.org for details.

CSI 28th Annual Computer Security Conference and Exhibition
Date: October 28-31, 2001
Location: Washington, D.C.
Venue: Marriott Wardman Park
Setting the industry standard for 28 years, this event is the largest and most comprehensive in the industry. The program features over 130 sessions focusing on Internet/intranet/extranet security, VPNs, PKI/cryptography, NT security, WWW, network intrusions and Counter measures, distributed denial of service attacks, response teams, management and awareness issues and much more. The conference is designed for anyone with responsibility for or involvement or interest in information and network security, and has sessions for those new to security as well as for seasoned professionals. Over 3000 information security professionals from around the world are expected to attend.

Return to Table of Contents

Feature Articles

ITD Business Continuity Planning

Wes Hunsberger is in the process of creating a current business continuity plan for ITD. A business continuity plan is designed to carry an organization through the recovery effort associated with a disaster. Functions deemed critical for various reasons are kept in some form of operation. The continuity of certain business operations ensures that citizens and/or other organizations are still given critical services to maintain their standard of living. Using the relevant parts of the contingency plan developed for Y2K, the current plan is being developed from a critical business function point of view. Selected critical business functions that have been obtained so far from interviews with the administrators are:

- Database / Data Access / Datawarehouse Services, from Customer Liaison
- Iowa Financial Accounting System (IFAS), from Customer Liaison
- IOWAccess / E commerce / Web Hosting, from Digital Government
- Mainframe Storage and Processing Power, from Operations

- Open Systems / Server Farm, from Operations
- Networking Services / Campus Backbone Network, from Operations

A critical business function is a service or product that is critical to the functioning of state government, and these functions usually take a "big-picture" view of the department. Not all department divisions and offices support critical functions. Wes is in the process of interviewing all division administrators and directors to obtain their views of the critical business functions within their areas. Wes is also asking the administrators and their staff to review the function questionnaire and vital records document that has been developed. It is important that the proper tools are gathered while developing the plan. The correct tables, inventories, diagrams, calling trees and other documents will make the recovery process possible. Suggestions for improvements will be included in the final versions of the documents, and these updated documents will be the major tool used to collect function information within the department.

It is important to note that critical business functions are the connections between the ITD business continuity plan and the Emergency Management Division's (EMD) continuity of operations plan. What this means, is that ITD will develop our own list of critical business functions that we will use in developing our own business continuity plan. EMD will in turn make their own decision on which of our critical business functions are absolutely critical to the functioning of state government or the support of our citizens. For example, of the critical business functions defined by ITD for the Y2K contingency plan, eight of these twelve functions made it into EMD's continuity of operations plan.

As the department's critical business functions are the basic building block for the ITD business continuity plan, each critical business function will be represented on the department's disaster response team. Each function will have two members, a staff member with primary responsibility and a backup staff member.

There are some special projects being developed immediately to be included in the business continuity plan. Three critical areas have been identified to be developed as soon as possible: (A) a networking redundancy plan, (B) a storage and backup plan including desktop storage and (C) an alternate location for file storage. Wes is working with other personnel within ITD to develop these supporting documents.

Questions or comments regarding the ITD Business Continuity Plan may be directed to Wes Hunsberger.

Home PC Security

Home PC security is important not only for protecting your own personal data but also for protecting your machine from becoming compromised and used in a distributed denial of service attack (DDoS). A distributed denial of service attack is when many compromised machines are used to attack a targeted system causing that system to no longer function properly, or to function at all. Protecting your home PC is even more important today with the popularity and accessibility to "always on" Internet connections like DSL and cable modems. Please be aware that this is an introduction to securing your home PC, however, and not a "how to". All of the topics discussed herein can be found on the Internet, though, with step-by-step instructions on how to implement solutions.

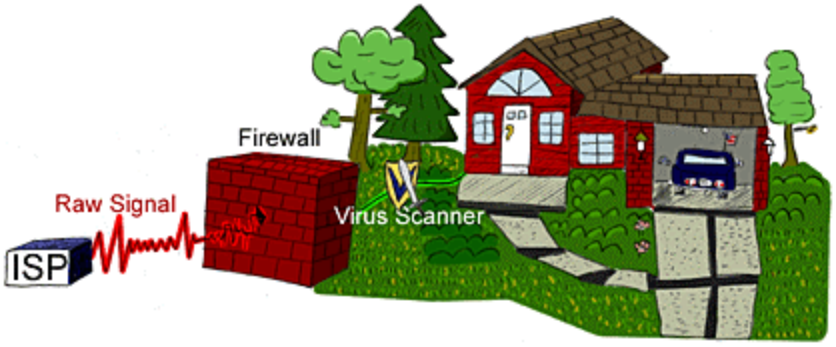
The first line of defense is securing the operating system on your machine. (Whether you have Microsoft Windows or Linux, many of the steps you can take to secure your PC are the same.) First, if you are using Windows, it is important to disable file and print sharing. If you must use them, secure the sharing as much as possible. There are many references on the Internet where you can find ways to secure or limit access to this, but if at all possible, disable file and print sharing. (One such reference is www.nwinternet.com/~pchelp/security/issues/sharing.htm.) With file and print sharing turned on, an attacker can take over your machine and add or delete files and programs. They can add programs that log every keystroke you make in order to capture passwords, or they can put Trojans on your machine and then make it part of a distributed denial of service attack.

The next step in securing your operating system is to make sure that all services you do not need are turned off. Linux is especially known for starting many services from the default build that are not needed for normal use. Find out what you need to use and stop the services that are not necessary. Every service that runs has the potential for another vulnerability that could allow an attacker to compromise your system. The more services you have running the greater potential you have for running a system that is not secure.

The final step in operating system security for your home PC is to keep your system up-to-date and patched. Vendors are always putting out new patches for security holes that have been found in their products, and by keeping up with patches you can protect yourself from hackers. Hackers see these patches become available as well, and then they find ways to exploit the vulnerability that the patch fixed. They search for machines that are not patched and can quickly compromise them. If your system is patched it can be quickly passed over by attackers because they want an easy way in. (For Microsoft products, the most convenient method of checking for new patches and updates, and if your PC is vulnerable to something, is visiting the Windows update site: windowsupdate.microsoft.com/default.htm)

The second line of defense is to buy anti-virus software for your PC. Good anti-virus software can scan emails that you receive and scan Web sites as you browse them. It can protect your system from viruses and worms that could compromise your PC and wipe out the entire hard drive or add a backdoor that would allow an attacker to take over your PC whenever they chose. Installing anti-virus software and keeping it updated weekly is one of the most important ways of keeping your machine clean. (One example of an anti-virus vendor is McAfee, at www.mcafee.com)

The third line of defense is to use a personal firewall. A personal firewall can protect your PC from hackers trying to connect to it. There are many options out there for personal firewalls, ranging from free programs to ones you must buy. The two most popular are Zone Alarm and Black Ice. Zone Alarm is extremely popular because it is free and easy to use. Black Ice is also popular but it is one that you must pay for, but with it you get customer support and an extremely easy interface to work with. (Zone Alarm: www.zonelabs.com, and Black Ice: www.networkice.com/products/soho_solutions.html)



The fourth line of defense is for the more technical savvy user that wants to see what is really talking to their machine: an Intrusion Detection System. The most popular one by far is a program called Snort. Snort works on both Windows and Linux machines. It works well for home machines as well as for entire networks. If you are interested in it as a home user you can refer to www.snort.org. If you are interested in more information on what a Network Intrusion Detection System is and what it can do for your agency's network, please refer to the IDS article is this issue about the new service the ITD Security Operations Team is offering.

All of these steps will help make a system more secure. By minimizing the services on your machine, disabling file and print sharing, and keeping your system current with the most recent patches, your system will be difficult for an attacker to crack. Add anti-virus software, to help protect your system from viruses and worms, along with a personal firewall and you will have a good solid fortress to protect your PC.

Paul Schmelzel

Read your Security Blanket for a warm, fuzzy feeling inside!

Return to Table of Contents

Linked Articles

Cyber Attack During the War on Terrorism: A Predictive Analysis - From the Institute for Security Technology Studies, Dartmouth College, Hanover, N. H. USA

This report analyzes the possibility of cyber attacks against U.S. and allied information infrastructures in response to anticipated military strikes against terrorists and nation-state sponsors. While many have speculated about the possibility for such cyber attacks, this report provides a detailed, fact-based assessment of the situation. It examines recent trends and precedents and sets out in detail the potential types, targets, and sources of cyber attacks that we should be prepared for. It also makes concrete recommendations for protective actions.

Information Technology - Essential But Vulnerable: How Prepared Are We For Attacks?

Testimony of Richard D. Pethia, director of the CERT Center Software Engineering Institute at Carnegie Mellon University in Pittsburgh, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations (ComputerWorld, Sept., 27, 2001)

Meet the World's Baddest Cyber Cops

They're not the feds, but they're taking down hackers, organized criminals, script kiddies,

and other threats to your company. A report from the front lines (ZDNet, Sept 28, 2001)

Terrorism Fight Could Prompt New Cyber Attacks
A congressional committee was told today that the U.S. war on terrorism could increase the number cyber attacks aimed at U.S. companies already struggling to repair an increasing array of vulnerabilities to Internet connected systems. (ComputerWorld, September 26, 2001)

Cyberterrorists: Our Invisible Enemies
We are already engaged in an escalating confrontation that holds frightening consequences for our economy--its called cyber terrorism. Rob Fixmer says the numbers of our invisible enemies are growing each day. (ZDNet, Sept. 24, 2001)

U.S. Commission Eyes Cyberterrorism Threat Ahead
A special congressional commission examining terrorism is concerned that future attacks against the U.S. might occur in conjunction with a cyber attack that would maximize the destructive effects of physical weapons such as bombs or chemical assaults. (ComputerWorld, September 17, 2001)

Senate OKs Use of Carnivore Against Terrorism
In response to last week's terrorist attacks, the U.S. Senate has approved expanding the permissible uses of the FBI's e-mail surveillance system formerly known as Carnivore to include the investigation of acts of terrorism and computer crimes. The measure also allows broader use of Internet tapping by law enforcement authorities and calls on the government to "make better use of its considerable accomplishments in science and technology" to combat terrorism. (ComputerWorld, September 17, 2001)

FBI Operation Penetrates Hacker Underground
The FBI has gained a foothold in the hacker underground thanks to an 18-month undercover operation launched during the height of the U.S. military's 1999 bombing campaign in Kosovo. (ComputerWorld, Sept. 11, 2001)

The U.S. Recruits New Hackers
The government desperately needs experts to fight hackers. So they've recruited a 63-year-old retired aerospace engineer, a mid-western mother of three, and a long-haired former teen golfing champ to do the job. The National Science Foundation is handing out $8.6 million worth of two-year training scholarships in computer security, in return for two years of government service. (Wired News, Sept. 7, 2001)

Return to Table of Contents

Points of Contact

Kip Peters: CISO, Enterprise Security
Marie Hubbard: Security Operations Team Coordinator
Larry Brennan: Critical Infrastructure Assurance Coordinator
Wes Hunsberger: Physical Security and Business Continuity

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/

The Enterprise Security website. Lots of security and state security information and resources! Curious about viruses and hoaxes? Policies and Procedures? Educational Resources? This is a great place to start! For security-related links go to Education, then Links.

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 (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. http://www.sans.org/top20.htm

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