The Security Blanket

(We've got you covered!)

Volume 1, Issue 4. December 2001

In This Issue:

From the CISO

Have you ever purchased anything on-line? I actually don't do that very often, but when I do it's usually very nice. You pick the items, provide a delivery address and credit card number, and the stuff arrives. Pretty neat, unless you're trying to match a pair of pants and a shirt. Somehow they never seem to look the same as they did on the monitor. Purchasing clothes, CDs, software, books, and other goods and services on-line is a benefit of the Internet that a lot of people take advantage of. You can buy virtually anything from anywhere without having to cross a border. That's one side of the story – the other side is that there are other people out there who want your information. You knew that was coming, didn't you?

I've only had one bad experience with purchasing on-line. I bought something from Australia, something similar to what a friend had brought back with him after visiting earlier this year. "That's cool," I thought, and figured I had to have one. So, I checked it out on the Internet and good enough, there it was, along with a bunch of other cool stuff. So I ordered two items and about two weeks later they arrived. It was really neat because at the time the American dollar was worth almost two Australian dollars, so a $70 item cost me less than $40, and the shipping was an unbelievable $4. Oh, and no tax.

The bad part hit about three weeks later. I received a letter from my credit card company asking me to call them about a fraud issue they wanted to discuss. What had happened was someone tried to use that credit card for on-line betting, but the creditor rejected it because the request came from out of the country. Putting two and two

together, along with the fact that I hadn't purchased anything on-line since Australia or months before, I determined that the company in Australia was the culprit. I notified them about what happened and they were nice about it, but the damage was done. I was lucky for the following reasons, and I recommend that you do the same:

- Find a credit card with zero liability. I'm responsible for $0 of anything purchased using this card that I didn't authorize.
- Use one credit card for on-line purchases, and don't use it for anything else. This way, you can both limit your exposure and also make it easier to track back where an incident may have occurred.
- Use a smart credit card. This is not an advertisement, but I use a First USA Smart Visa that allows me to use a smart card reader (first one free from First USA) with certain vendors. Using the reader means the credit card information is not used and the transaction is much more secure. By the way, I also get 5% back from certain vendors, such as Amazon.com.
- Be careful about where you buy. Is it a reputable vendor? Who is their e-commerce partner? Do they share information about their security and privacy practices? You want to be as sure as you can that the vendor has done the due diligence necessary to protect you and your information.

If you follow these guidelines, I think you'll find your e-commerce experience safer and more satisfying. If you have any questions or concerns, please contact me. And, as always, if you ever have any security concerns, let us know.

Kip Peters

Return to Table of Contents

Current Activities

Information Security Office Service Offerings

(Service rates are available at: http://www.iowaccess.org/government/its/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 Marie Hubbard.

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. The filming is complete! Look for the tutorial at the Enterprise Security Website by the end of the year.

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.

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. The current Enterprise Security Policy can be accessed here, as well. 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.

Return to Table of Contents

Helpful Hints

Dumpster Diving and Shredding

Though it is unglamorous, dumpster diving, or searching through people's trash, can be one of the most effective ways of gathering information on a target victim or network. How many times have we casually thrown away billing statements, password notes, system information, or a draft of some confidential document? The trashcan can be a great source of information for both hackers and thieves alike.

The best way to safely minimize this threatening garbage is to shred confidential documents before throwing them away. Papers with server IP Addresses, customer accounts numbers, credit card numbers, confidential business plans, confidential personal information, and system passwords are all examples of documents that should be shredded before throwing them out. Don't just crumple and toss papers, they can be uncrumpled, too. And while burning confidential documents to destroy them might be appealing while you're shivering at your desk in the cold winter months ahead, it just isn't safe or practical for the office.

Shredding is the best method of destroying confidential documents. And if you can manage to get a crosscut shredder, do so. That type not only destroys the paper strips that most shredders make (which *really* makes it difficult to piece papers back together), it can also give you a great supply of confetti for the office New Year's party. By shredding confidential documents prior to throwing them away, we can greatly reduce the risk of having the confidential information discovered and used to compromise the State or ourselves. Happy Shredding!

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.

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
Dec. 18 12-1pm	Top Security Issues for Win2000 Grimes Bldg., North Conference Room
Jan. 8 12-1pm	How Attacks are Perpetrated Against Us 1LC and 2LC, Hoover Building, B Level
Jan. 22 12-1pm	Home Computer Security 1LC and 2LC, Hoover Building, B Level

Change of location or time will be announced via e-mail, and sent to departmental L&L security contacts. The past presentations (Introduction to the Information Security Office, and Critical Infrastructure Assurance and Cyber Terrorism - in .pdf and video) and an updated schedule are available at http://www.itd.state.ia.us/security/education.html#lunchnlearn.
Questions regarding the Lunch & Learn program can be directed to William Hubbard.

Terrorism Conference
January 16, 2002. STARC Armory, Camp Dodge, Johnston, Iowa. Sponsored by EMD.

Topics and presenters currently planned include:

Public and Private Partnerships	American Red Cross
Cyber Terrorism	ITD, State of Iowa
FEMA's Updated Responsibilities	FEMA Region VII, Eric Jenkins
Public Health Support for BIO Terrorism	Iowa Dept. of Public Health
Civil Support Team	LT. Col. Dan Robbins
Terrorism Planning	IEMD, Dan Lee
National Pharmaceutical Stockpile "Thinking outside the box"	CDC, Steve Reissman
Training and Exercises	Connie Gilbert
Incident Command/Unified Command	Chuck Eddy and Scott Siberski
Facilitated WMD Tabletop Exercise:	DOJ Tech Assist from contractor.

To view the Conference Flyer and Application, see:
http://www.itd.state.ia.us/security/education.html#conference. Other questions? Contact: Thomas Baumgartner.

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

Return to Table of Contents

Feature Articles

Biometrics and You

There are many technologies that may be used today to prove your identity to a system. You may use a password, a pin code, a magnetic access card, or any number of devices. With such normal devices used for authentication, there is always a security risk of shared passwords, lost pin codes, or stolen access cards. Wouldn't it be easiest to have a unique method of identification that you can always have with you? This is where biometrics comes in handy. Biometrics can be defined as measurable biological characteristics that can be used to uniquely identify the identity of an individual. There are many physical characteristics you have that no one else has. Everyone has a unique fingerprint - even identical twins. Patterns found within someone's eye are also something unique to every person on the planet. Our hands, voices, and faces can also be used as reliable means of identification that can be extremely difficult to duplicate. These are the types of things that you won't forget at home in your coat pocket!

The purpose of biometrics is to take the verification of identity and turn it into a mode of authentication. This can be quite effective in today's computer-driven world. There are affordable fingerprint identification devices available on the market today that will allow you to log onto your computer by simply pressing your thumb on a handheld device. Sounds easy, doesn't it? This is a simple way to avoid having to type in your username and password and yet still prove that you are "you". It may seem that many methods of biometrics are only in Hollywood movies, but they are used every day in real life. Retina scanners and voice recognition systems are other popular biometric devices. Authentication with a retina scanner uses a utility that analyzes the pattern of blood vessels in your eye. This pattern within your retina is just as unique as a fingerprint and even harder to copy. Voice scans are also used to uniquely identify a person by their patterns of speech. Biometrics has even gone so far as to identify people by their face structure. This can make a video camera an even more powerful tool to identify individuals.

Now that we know what kind of basic forms of biometrics are available and in use today, let's discuss how some are being used in the real world. The international airport in Amsterdam is starting to use methods of iris scanning in combination with a smart card that helps speed up the identity of incoming overseas travelers. This is currently in its trial period and will be put into full swing by mid-2002 when limited-access areas within the airport are also going to be controlled by iris scans. The system they are using, created by Iridian Technologies, takes 247 independent unique variables in an iris to identify a person. That's quite a bit of input from your eye!

Another interesting bit of information about biometrics in action dates back to last year's Super Bowl. Did you know that all of the footage taken from the crowd at last year's game was matched against a national database of wanted criminals with a biometric method of face recognition? This form of biometrics is extremely effective at identifying individuals without having to interact on a physical level. Sounds pretty high-tech, doesn't it?

I hope this has given you an idea of how biometrics works and how it might become part of your life. Biometrics can effectively be used with computerized devices

to make identifying you quick, easy, and painless. Whether you're a frequent airport traveler, a tech administrator checking out new products, or just out enjoying a televised football game, your life will someday involve the use of biometrics.

Jared McLaren

You are Our Most Important Security Asset!

Discussions of security seem to swirl around how much money, how much hardware, how much software, and how many people it takes to secure a network, a building, or a computer. While it is impossible to secure anything for free, the best security doesn't cost very much. Indeed, the most important security asset any company or department can have is the security-conscious worker.

You are the most important link in the security chain. Each employee needs to follow good security procedures to keep the entire department safe. When one security breach occurs, others may quickly follow. The following examples are all common mistakes we need to guard against.

If someone sets a weak password (or a good one that they leave taped to their monitor) they could nullify all the expensive security hardware and software in place and allow an attacker to compromise their system. If someone turns off their anti-virus software (or doesn't have any installed) they could expose every single PC in the complex to whatever virus they might receive. All of us have to be convinced that being secure is as important to us as fast response time or using some piece of software.

If someone uses outside mail or communication processes – Internet Messaging, or a Hotmail account, for example – they bypass all the expensive safeguards in the mail system and could bring a virus attack directly into the network. Allowing a fast-moving virus or worm into the state network would almost guarantee some network failure and a time-consuming response to the infection. The recent Goner.A worm is an excellent example of this. While many State e-mail systems were protected against the worm coming in to an account on the server, people who use POP3 e-mail and Instant Messaging brought the worm inside the network, where it couldn't be stopped until the anti-virus companies could publish updates. We employees could have avoided the situation in two ways, by not using outside messaging systems and by not opening suspicious and obviously non-work oriented e-mail.

With regard to physical security, when someone props a security door open, they make the room and all its contents available to anyone who walks by. State employees have been known to let others into secure areas even when the employees don't know them. Certainly this was not the intent of those who locked the door and passed out access cards!

It is impossible to protect someone who refuses to follow good security practices – whether we are talking about physical security provided by a bodyguard or electronic security provided by the network. Unless everyone works inside the rules, the state's systems can be exposed and harmed by intruders or automated e-mail, Internet, and other forms of attack. Don't let the uninformed fool you - You are security at the State of Iowa. If any one of us does not take security precautions seriously, the rest of the security process cannot succeed.

John Maxwell, William Hubbard

Return to Table of Contents

Linked Articles

Clarke Presses Industry on Security
The White House is calling on the information technology industry to assist in government efforts to strengthen the state of cybersecurity and is also urging vendors to ensure that what they sell is secure. (Federal Computer Week, Dec. 5, 2001)

US Government Unveils Protection Policy
The US government has finalized a new data encryption standard, which it believes will help the country to protect its critical information infrastructures, as well as provide secure electronic government services. (ITToolbox, Dec. 5, 2001)

US Cyber Security Chief Asks Vendors To Do More To Protect Users
The president's computer security adviser asked technology executives Tuesday for a shopping list of changes, including bundled security software for high-speed Internet users and a new way to get software updates on personal computers. (SiliconValley, Dec. 4, 2001)

Instant messaging: Open door for hackers?
Instant messaging systems used by millions around the world are vulnerable to the same types of lightning attacks spread by e-mail causing billions of dollars in damages. (ZDNet, Dec. 3, 2001)

Record-Breaking Year For Security Incidents Expected
The U.S. government and private industry should prepare for a record-setting number of Internet security incidents in the year ahead, a panel of industry experts recently told Congress. (ComputerWorld, Nov. 26, 2001)

Global Cyber Crime Treaty Signed
The United States, Canada, Japan and South Africa joined their counterparts in 26 other countries in signing the Council of Europe1s Convention on Cybercrime to harmonize laws and penalties for crimes committed via the Internet. (NewsBytes, Nov. 26, 2001)

Search engines find the forbidden
Search-engine spiders crawling the Web are increasingly stumbling upon passwords, credit card numbers, classified documents and even computer vulnerabilities that can be exploited by hackers. (ZDNet News, Nov. 26, 2001)

How to finally give viruses the heave-ho!
Merely owning anti-virus software is not enough to protect your PC from infection. The software requires a certain amount of care and feeding beyond the initial purchase. Fortunately, a few minutes of prevention can prevent hours of frustration during a real attack. (ZDNet News, Nov. 13, 2001)

Users Are The Weakest Link, Security Experts Warn

With corporate network users viewed as the No. 1 cyber threat to sensitive business data, experts say companies should shift their security focus to where the real threat is: inside the firewall. (ComputerWorld, Nov. 15, 2001)

Group Pushes Standards For Vulnerability Disclosure
Microsoft and a handful of security firms have formed an organization to propose standards that would give vendors time to fix security flaws in their software before those vulnerabilities are publicly disclosed. (ComputerWorld, Nov. 19, 2001)

Broadband ISPs Shouldn't Knock Down Firewalls
Citing finicky configuration problems, the major high-speed providers discourage their use -- a backward and dangerous policy. (BusinessWeek, Nov. 20, 2001)

Will hackers keep the cyberpeace?
Six days after the attacks on the World Trade Center and Pentagon, a major European hacker group issued an unorthodox plea to the rest of the computer underground for cyberpeace. (ZDNet Nov. 20, 2001)

Back to School – Security Training
Internet security (or the lack of) is gaining headlines with new exploits being exposed to the public every week - if not every day. (SC Magazine, Nov. 2001)

'Dark Web Space' Hides Net Nasties
Results of a three-year study on Internet 'reachability' have confirmed that the web is partitioned and littered with pockets of 'dark web space', which are home to some of the Internet's nasties. (ITToolbox, Nov. 14, 2001)

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
http://www.iowahomelandsecurity.org/

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

From all of us at the ISO – "Have A Safe And Happy Holiday Season!"