The Security Blanket

(We've got you covered!)

Volume 1, Issue 1. September 2001

Welcome to the first issue of the Security Blanket, the Information Security Office's (ISO) monthly newsletter. The ISO is responsible for State of Iowa enterprise security including security policies and procedures, security operations, security planning, information assurance, and security awareness. The Security Operations Team performs network vulnerability assessments, operates an Intrusion Detection System and a test network, serves as an incident response team, and consults on various network security issues. The purpose of the ISO is to help provide Information Assurance and enhance the quality of service that state agencies give to the citizens of Iowa through improved security awareness and practice. We're here to help you and your agency protect your information assets in an increasingly computer-dependent environment. The purpose of this newsletter is to distribute information and resources that can aid state employees and agencies in protecting their information and their information systems.

To this end ISO Newsletters will contain the following:

- A letter from the CISO
- Current ISO activities and Security services/opportunities
- Helpful Hints – Easy activities employees can perform to improve security
- Upcoming classes/consultations or training and testing opportunities
- Articles related to information security
- Points of Contact for security services, questions, or concerns
- Links to helpful resources

We at the ISO hope this service is of help to you in the challenging times ahead.

In This Issue:

From the CISO

Welcome to the initial issue of *The Security Blanket*, the Enterprise Information Security Office's information assurance newsletter. This newsletter is intended to raise security awareness within the state of Iowa at all levels, provide important information concerning information assurance, and report on the activities of the office. If you have questions, concerns, or comments, please contact the editor, Bill Hubbard, at William.Hubbard@itd.state.ia.us.

In my opening dialogue, I'd like to share a few things with you about information assurance and the thoughts and beliefs of the security office. First of all, what exactly is information assurance? Information assurance, as we define it, goes beyond the standard information protection principles and includes detecting events, recovering systems when necessary, and responding appropriately. We like to say, "Protect, detect, restore, respond."

Enterprise Information Security Office
Mission Statement

Our mission is to identify and protect the information and information systems entrusted to the state through the development, deployment, and institutionalization of a structured, cost-effective process that provides reasonable assurance that valuable business and personal information will be: 1) Identified and prioritized based on value and privacy; 2) Adequately safeguarded from misuse and theft regardless of the technologies used and changes in business models; 3) Maintained in a manner that satisfies legal requirements and 4) Leveraged for business needs.

Protection, of course, includes all the components necessary to maintain the confidentiality and integrity of the information entrusted to the state. In this area, we also include availability of information and information systems to authorized users when needed. We have all seen in the news how sites and systems can be overwhelmed by traffic, bringing them "down" and affecting availability. Availability has traditionally been something of an oversight, but more and more Internet attacks are taking advantage of past omissions in system planning, forcing more of an emphasis on keeping information and capabilities available.

Detection is just that, detecting that an event is occurring or has occurred. In today's environment, it is impossible to remove all the security risks; therefore, we try to reduce the risk to a manageable level, identify the risk that remains, and prepare for the eventuality that something bad might happen. Detection of an occurring event is difficult to do without full time staff dedicated to that endeavor. ITD has personnel assigned to monitor and operate an enterprise intrusion detection system. This system mainly monitors ITD's environment and the Campus Backbone. We check the system as much as time permits, and are working towards real-time notifications via e-mail and pagers/cell phones. Our goal is to identify significant events and start the remediation process as soon as we practically can.

Enterprise Information Security Office
Guiding Principles

We believe that the traditional objectives of maintaining information confidentiality and integrity, while providing appropriate availability, are non-negotiable.

- The state is entrusted with the information and owns the accountability for its protection.
- Security exists only to mitigate risk.
- Security must be an enabler.
- Security input must be value added.
- Security input must be practical and fast.

Restoration means that systems are recovered. If a system is subject to an intrusion, we want to get it back up and running as quickly as we can, all while ensuring that we don't destroy any evidence that might be available. The evidence may be an important piece of the final step, which is respond. Respond can mean many things; it might mean getting law enforcement involved, changing a policy, or implementing additional controls. Most intrusions occur simply because patches and service packs aren't kept up to date – one response to that would be to update the machine and put a process in place ensuring that it is kept that way.

So, that's information assurance. It is something that requires constant vigilance; you never reach an endpoint with security. There is *always* something else to do. The bad guys are too good at coming up with new tools and exploits for us to be able to relax.

I'd like to finish up by talking about the thoughts and beliefs of the security office. The Information Security Office has responsibilities across the enterprise and includes the participating agencies as defined in Iowa Code Section 14B. In fulfilling our duties, we constantly keep our mission in mind. It is a pretty important mission, and one that we take seriously. Security is one of the key foundations that digital government is being built upon – without its key enabling attributes digital government will ultimately fail. Citizen confidence will have to be high if they are going to use on-line services, and one incident can make a huge impact. The citizen's privacy and economic well-being must be protected, even if they don't understand that they need to be protected. The state has an important role as the caretaker of citizen information and the security office believes that we work for the citizen above and beyond anybody else. In our daily activities, we use our guiding principles to influence decisions and the things we do. When things get frustrating or we don't know where else to turn, they serve as our beacon and are reminders of what our role is. In other words, they help us stay focused and give others an indication of what to expect from us.

Enterprise Information Security Office Core Values

- Integrity First
- Service Before Self
- Excellence in All We Do

Finally, the bedrock of security is people, not technology. It takes people to put policies and procedures in place, and people must implement, manage, and use the systems. One of the unfortunate truths about security is that it always boils down to the trust of the individual. Even in highly secure systems, individual trust is an important factor. We trust users not to share passwords or put confidential information in e-mails. We trust administrators to secure the systems and monitor them effectively while not taking advantage of their additional access and other capabilities. Because of that, security personnel and those that have important functions relating to the security of systems must be held to a higher ethical standard. Our core values are borrowed from the United States Air Force. As a former active duty officer and current reservist, these values have been instilled in me for a very long time and I saw few reasons to alter them for our use; therefore, we have adopted them as is. These values provide a guide for our inner belief system and serve as a model for all to follow.

In future issues, I will expand upon the concept of information assurance and address other issues we should all be concerned about. If you have questions or comments on this column, or would like me to focus on something specific, please send an e-mail to Kip.Peters@itd.state.ia.us.

Return to Table of Contents

Current Activities

New Enterprise Security Website http://www.itd.state.ia.us/security/

This is the main contact point for enterprise security information and resources. The new **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

Return to Table of Contents

Helpful Hints – Password Guidelines

Since your password acts as a personal key, it provides access to computer systems and applications. It also gives each user certain permissions and capabilities. Therefore, you should select passwords according to the following guidelines:

- Passwords should contain a minimum of 8 alphanumeric characters (a mix numbers and of upper and lower case letters) including at least one special character. You can use pass "phrases" to help you do this. For example, 'Can I have three scoops of ice cream?'

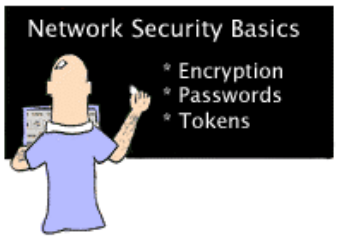
can become “CIh3soic?” as a password. It is easier to remember than random characters and just as secure.

- Passwords should be changed at least every 60 days. Never re-use a password.
- System default and initial passwords should be changed immediately upon receipt. (Passwords like “administrator”, “guest”, “user”, null passwords, etc. need to be changed ASAP
- Passwords should not be written down or recorded on-line in any form, and passwords should not be shared with anybody.
- Passwords should not be words or combinations of words, even if combined with other alphanumeric or special characters. (For a poor example: “Hawks6%”)
- Passwords should not be a user ID in any form, all the same alphanumeric character, or published examples of good passwords.

With password-cracking tools easily available on the Internet today, poor passwords can be cracked in seconds, while more difficult ones (8+ mixed characters) can take hours or days. Also, remember that your password is **your** personal key to your workstation or network. If someone else uses your password, his or her activities will be recorded as being done by **you**.

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.

Oct. 15-22, 2001 - SANS Network Security 2001, San Diego, CA
http://www.sans.org/NS2001/NS2001.htm
This is the largest security education conference and expo in the world.

December 6, 2001 - Energy Vulnerability Assessment
The US Department of Energy Office of Critical Infrastructure Protection (DOE-OCIP), Iowa’s Emergency Management Division (EMD), Iowa’s Department of Natural Resources (DNR), and Iowa’s Information Technology Department (ITD) will join forces to assess and exercise Iowa’s energy. More details will be provided when they are available. For more information on activities of the DOE-OCIP, please see these sites:
http://ocip.anl.gov/
http://www.naseo.org/events/outlook/2001/presentations/scalingi.PDF

Return to Table of Contents

Feature Articles

Most feature articles in this newsletter will be short, informative, and be published in the ISO newsletter in its entirety. The first feature article in this volume is an exception to this general rule, however. It provides an excellent introduction to home network security, and while not short, covers multiple security topics briefly, enabling the home user to easily understand a variety of security issues relating to home network and computer use.

Home Network Security (From CERT)*

This year, we have seen a significant increase in activity resulting in compromises of home user machines. In many cases, intruders then use these machines to launch attacks against other organizations. Home users have generally been the least prepared to defend against attacks. Many home users do not keep their machines up to date with security patches and workarounds, do not run current anti-virus software, and do not exercise caution when handling email attachments. Intruders know this, and we have seen a marked increase in intruders specifically targeting home users who have cable modem and DSL connections.

Most of the subscribers to the CERT Advisory Mailing List and many visitors to our web site are technical staff responsible for maintaining systems and networks. But all of us know people who have home computers and need advice about how to secure them. We recently released a document on our web site providing some basic security information and references for home users. The document, "Home Network Security," is available on our web site at:

http://www.cert.org/tech_tips/home_networks.html

We encourage the technical readers of our mailing list to reach out to your parents, children, and other relatives and friends who might not be as technically oriented, point them to this document and help them understand the basics of security, the risks, and how they can better defend themselves. We have a long road to travel in educating home users on the security risks of the Internet. But all of us working together to educate home users will improve the security of the Internet as a whole.

*CERT (Computer Emergency Response Team) is a center of Internet security expertise which studies Internet security vulnerabilities, handles computer security incidents, publishes a variety of security alerts, does research for long-term changes in networked systems, and develops information and training to help people improve security at their site.

The Five Worst Security Mistakes End Users Can Make

The security professionals at SANS have made several ‘lists’ regarding common security risks, concerns, flaws, and weaknesses of systems and behavior. The following is one such list, but a commentary on why these are risks may be helpful to non-security personnel.

1) Opening unsolicited e-mail attachments without verifying their source and checking their content first.
Most viruses spread via e-mail. They are hidden in attachments or are disguised as legitimate traffic. When a user inadvertently opens an e-mail message with a virus (usually a file or message heading with an .vbs or .exe extension on it – the Anna Kournikova.vbs virus comes to mind) the virus could simply muck-up their own workstation, but is more likely to have a disastrous effect on their e-mail community. A good security practice is to check the source of the e-mail: if you don't know or trust the source delete the message without opening it. Make sure you have some kind of virus protection system for your e-mail system, too. (McAfee for example.) If you don't you are increasing the risk of viruses getting into your network. Another easy safeguard is to perform a virus check on an e-mail you have doubts about. The fifteen seconds it takes to do that could save hours of repair time later. (Scanning downloaded files from the Internet before opening or executing them is similarly good security practice.)

2) Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, and Netscape.
Installing security patches should be done by technical staff, so most employees don't really need to worry about this. Check your agency's policies, however, to understand whom needs to do what. (Of course, it's your task to secure your own home systems.)

3) Installing screen savers or games from unknown sources.
This risk is similar to point #1. If it is not from a trusted source, then don't trust it and don't use it. On occasion some screen savers and games have had malicious programs imbedded in them. When installed or run, a Trojan horse (a hidden malicious program) can install backdoors into a system, in essence allowing a hacker access to a system or network. All downloads of code should be coordinated with your departmental techies, as well.

4) Not making and testing backups.
Again, your departmental technical personnel or system administrators should do this activity. Techies - check your policies, and if this isn't covered in those policies, do the testing and backups yourself, if necessary.

5) Using a modem while connected through a local area network.
Use either the modem or the LAN; don't do both at the same time. If a hacker gets access to your machine via the modem and you're connected to a LAN, he can bypass many of the security defenses of the LAN. Also, if a virus or other malicious program executes on your machine when you have both connections open, you could infect the state's network via that LAN connection. There are other bad things that can happen with this scenario as well, so the best practice is to simply only open one communication connection at a time.

William Hubbard

Introduction to InfraGard

What is InfraGard? InfraGard is a Partnership between private industry and the U.S. Government, represented by the FBI. InfraGard was developed in 1996 in Cleveland to promote the protection of critical systems. The InfraGard initiative encourages the sharing of information between the government and the private sector members. The goal of InfraGard is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

Why do we need InfraGard?

Historically, it was easier to protect critically important infrastructure pieces, as they were owned and operated by government entities. An example of this was the phone company. There used to be one, government controlled company, and today there are dozens of deregulated telecommunication companies. In fact, today over 90% of the critical infrastructures we rely upon are privately owned and operated. As big a departure in terms of control, it is an even bigger departure in terms of securing these assets.

Since these systems are owned and operated by private industry, they have responded to market forces to make them more efficient and competitive. To this end, these systems are becoming more automated. To further increase the efficiency of these systems, they have become more interconnected. This creates situations where one system may be adversely affected or compromised by an incident in a seemingly unrelated system.

The ability to disrupt systems from the Internet has become much simpler, and the tools needed to do so are widely available on the Internet. The skill required to use a hacking tool designed to disrupt a computer system has decreased tremendously. With the Internet having no international boundaries, greater possibilities and opportunities exist, either intentionally or accidentally, to bring down systems for critical systems.

Often times, the victims of intrusions do not even know that they were broken in to. The disruption of services could be attributed to technological errors or other causes. The government and the private sector have a wealth of information on threats to our systems, and this wealth needs to be shared and analyzed.

The InfraGard program intends to do just that. In fact, Iowa has it's own InfraGard chapter! The Iowa chapter meets on the third Thursday of each month at the Principal Insurance building in downtown Des Moines Iowa. For more information on InfraGard and our chapter's activities, please contact Kip Peters. For membership queries, please contact Bill Hayen. For information on the federal InfraGard initiative please see: http://www.infragard.net/.

Larry Brennan

Feeling insecure? Grab your Security Blanket and make the monsters go away!

Return to Table of Contents

Linked Articles

ZDNet Security - Wireless LANs dealt new blow
The latest blow to WLAN's security reputation is the worst yet--an attack that enables an eavesdropper to capture network traffic and uncover a user's secret key.

ComputerWorld - Taking A Look Behind The Scenes At The NIPC
In an interview, Ronald Dick, director of the NIPC, reveals how the agency handled the Code Red worm.

San Francisco Chronicle - High-speed Net Users Sitting Ducks for Hackers
Is it open season on PCs without firewall protection?

ZDNet Tech Update - Is China's Guandong province ground zero for hackers?
One possibility of who is behind the latest cyber attacks and why they are doing it.

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)

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.

The ISO Code:

Integrity…Service…Excellence