The Security Blanket

Issue 13
Jan/Feb 2002

Security… It is our passion
It stirs our hearts, we tremble with anticipation just to be close to it
Sublime, seductive, variable, demanding
It taunts us with visions of perfection, yet dances just beyond our reach
Always and forever, we follow the path that leads toward our heart's desire…

Yeah, we need to get out more. And while we're doing that, please peruse this issue, and maybe you can find something to help you be a little more secure.

In This Issue:

From the CISO

Business Continuity

Business continuity is often one of those things that people don't think about, or possibly one of those things that people don't like to think about. The issue of business continuity exists because you just never know what might happen. Much like an insurance policy, your business continuity policies and procedures exist for when something bad happens. What could that be? It could be a water-leak two floors above yours that eventually floods your area on a weekend. It could be a chiller pump, and a backup pump, that goes out of service at the same time, eliminating the cool air from entering your server farm. It could be a tornado, an earthquake, a power spike, a loss of power, or an airplane diving into your building. The possibilities are endless - which is why preparation is essential. Joseph Nye, Dean of the John F. Kennedy School of Government at Harvard, once said, "Security is like oxygen. You never notice it until it's gone." Business continuity is kind of like that in a different way - you never think you'll need it, and you may not notice it's there, but if you ever need it business continuity will save your bacon.

What does business continuity entail? Essentially, and briefly, it consists of identifying your essential functions and putting measures in place to have the ability to continue providing those functions in the face of a variety of events. When something bad happens, you retain the ability to function. That's it. Sounds simple, but it can be complicated, and it can be very, very expensive. To make it sound easier, think of business continuity in terms of risk management. Ask four simple questions:

1. What can hurt me?
2. How can it hurt me?
3. How critical am I?
4. What can I do to protect myself?

You actually go through this process many times on a personal basis each and every day. I need to go to work, but it's cold, so I should put a coat on. I have to drive to Marshalltown today, so I should put some gas in the car because I only have a quarter tank left. I need to mow the lawn, so I'm going to fire up my trusty lawnmower, but I should probably wear proper attire while mowing, including protecting my feet, my legs, and my eyes. The reality of it is that we are so ingrained to do this on a regular basis that it's never really thought about. But, as we have seen in the last year or so, bad things happen, even to us. We need to do our part, in our areas of responsibility, to ensure that we can continue to function in the event of an emergency.

Kip Peters

Return to Table of Contents

Feature Articles

The Business Continuity Plan – Risk Assessments

While creating a business continuity plan for your organization, don't forget to perform a risk assessment of your facility. This is especially true of those items that are not owned by or directly controlled by your organization. Oftentimes it's taken for granted that a service or utility will be available because it's always been available in the past. This is wishful thinking and can create problems during an emergency.

Some topics to research during your assessment are the primary and backup sources for:

- Power
- UPS system
- Generator system
- Heating and cooling systems
- Related facility concerns, such as chilled water system, etc.
- Fire suppression
- Water detection
- Monitoring humidity levels and temperature ranges
- Feeds from other information networks that are critical to your business units
- Physical security requirements, such as limited access
- Other related topics.

Besides the physical infrastructure of your organization, an important aspect that should not be overlooked during an assessment is the issue of people resources. Especially if your organization is small in size, much may be riding on a sole individual or small group of key individuals. Are there backups for these critical individuals? With all of the recent retirements, terminations and other staff reductions, backups may be missing for essential employees. These problem areas should be identified before an emergency. Remember that a disaster may disable or eliminate a key individual critical to your emergency response.

Controls should also be verified and rated as to their effectiveness for the above bulleted items and the related redundancies of these controls. A new control may be needed as a result of your assessment, or some controls may need to be updated as a result of changing technologies.

At the end of your assessment, recommendations are made on how to minimize or mitigate the risk of business impact for your organization. Prioritize your recovery strategies with alternate solutions for different risks. With the limited funding available during our current budget crisis, management will appreciate various options.

To aid you with your assessment, there is a wealth of planning templates available via the Internet. Pick and choose those forms or templates from the sources that seem to be the best fit for your organization. Following is a list of a few of the resources available via the Internet:

Weather & National Disasters

- US National Weather Service (www.nws.noaa.gov) - warnings, observations, forecasts, forecast models, weather safety, and the NWS education information center
- US Geological Survey (www.usgs.gov) - scientific information to describe and understand the Earth; minimize loss of life and property from natural disasters; and mange water, biological, energy and mineral resources
- GuaranteeedWeather.com (www.guaranteedweather.com) - news, resources, tools, case studies, research, and solutions needed to understand and manage weather risk

Publications

- Contingency Planning & Management (www.contingencyplanning.com) - technology, products, services, information and management strategies that support business continuity
- Disaster Recovery Journal (www.drj.com) - disaster recovery and business continuity publication, the main publication of the Disaster Recovery Institute

Risk Analysis & Assessment

- The Geneva Association Homepage (www.genevaassociation.org) - formed by major insurance companies to research world-wide insurance activities in sectors of the economy
- The Society for Risk Analysis (www.sra.org) - research of emerging issues in risk analysis and risk management in both the U.S. and internationally
- Risk Theory Society (www.aria.org/rts/) - research on risk theory and risk management
- Risk and Insurance Management Society, Inc. (www.rims.org) - information on the practice of risk management

Disaster Information & Reference

- Disaster News Network (www.disasternews.net) - reports of disaster response information, including appropriate response, preparedness and mitigation.
- Disaster Response: Principles of Preparation (216.202.128.19/dr/flash.htm) - text of book can be viewed in its entirety online
- Natural Disaster Reference Database (ndrd.gsfc.nasa.gov) - NASA's site for disaster news, history, current conditions and preparedness
- National Fire Protection Agency (www.nfpa.org) - scientifically based codes and standards, research, training, and education
- The Disaster Center (www.disastercenter.com) - A U.S. based information center offering worldwide information about disasters, weather, preparedness and links
- Crisis Navigator (www.crisisnavigator.de/auinede.html) - an international Internet resource guide to issues about crisis and business continuity management. Specialists and consultants from around the world contribute papers related to these topics.
- Business Continuity & Disaster Recovery Associates (www.businesscontinuity.com) - insight into business continuity management, disaster recovery, emergency management, crisis management, disaster control, business recovery and continuity management functions.

Wes Hunsberger

Return to Table of Contents

CERT: More Than A Breath Mint

Most of you have probably heard of the term CERT at one time or another. A CERT is a coordination center and response team. The most famous computer security CERT is the Coordination Center at Carnegie Mellon University. The Defense Advanced Research Projects Agency (DARPA) formed the Carnegie Mellon CERT Coordination Center (CERT/CC) in 1988. It has now grown into a team of security professionals that help coordinate responses to cyber attacks and identify solutions to security problems. The information they create is released free of charge to the security community. CERT/CC is a great resource for system administrators and can offer quite a bit of help to those interested in maintaining secure systems.

The biggest public face of CERT/CC is its public advisories and incidents. They release alerts on the most serious threats that face cyber security. An example of their public advisories is the Microsoft SQL worm, CERT Advisory CA-2003-04 (http://www.cert.org/advisories/CA-2003-04.html). The worm was discovered in the wild on Saturday January 25th, 2003 and CERT/CC released an advisory that same day describing the worm. Their advisories come with a description, impact, and solution. You can trust that if CERT/CC releases an advisory, the impact of the vulnerability is usually high. This means that if CERT/CC released an advisory on a new vulnerability, you should probably apply the software patch in a hurry!

Incident handling is CERT/CC's main focus. They help administrators with servers that have been hacked and they help handle proper disclosure of many security vulnerabilities. Administrators can visit the CERT/CC website at http://www.cert.org and find checklists to find out if they have been hacked. If they have been hacked, there are lists on the web site about how to recover systems and bring them back online after an attack. CERT/CC also provides steps on how to secure your systems so that you don't get hacked in the first place. CERT/CC will even provide personal assistance to administrators that report an incident and need a hand.

Carnegie Mellon
Software Engineering Institute

Administrators that wish to communicate with CERT/CC can do so through their web site. People may contact CERT/CC to subscribe to their advisory mailing list, report a new security vulnerability, request help with a problem, or report a security incident. Their web site is a great resource full of information useful to security conscious administrators. I highly recommend browsing through their web site and seeing what free help they have to offer.

CERT/CC Advisories
http://www.cert.org/advisories/

Incident Reports
http://www.cert.org/incident_notes/

Current Malicious Internet Activity
http://www.cert.org/current/current_activity.html

CERT/CC Tech Tips
http://www.cert.org/tech_tips/

Jared McLaren

Return to Table of Contents

Identity Theft

Identity theft is a crime where a person's legal identity is stolen and used to conduct financial fraud. Identity thieves steal information about a victim such as bank account information, Social Security number and driver's license number in order to open accounts in the victim's name or to change the victim's account information. In 2001, there were over 86,000 cases of identity theft reported in the United States, with 324 of those cases in Iowa. (http://www.consumer.gov/idtheft/statemap/iowa.pdf) The total number of identity theft cases leapt to over 162,000 in 2002 in the United States. Though the 2002 Iowa numbers haven't been released yet, it is safe to assume that we will see a proportional increase in Iowa.

The damage from identity theft is considerable, both to financial institutions and victims. Since most identity thieves are never caught, financial institutions cover a majority of the costs from fraud. GAO Report # GAO-02-363 (http://www.consumer.gov/idtheft/reports/gao-d02363.pdf) shows that credit card fraud related to identity theft cost companies $1.1 billion in 2000. "This is a crime that is almost solely on the shoulders of the victim to resolve," said Beth Givens, director of the Privacy Rights Clearinghouse. The average victim will pay over $1,000 to have their good credit restored and it could take years for their credit record to be rectified. During this time, the victim will not be eligible for home, car or student loans, nor will they pass a credit check required for some jobs. The possible non-financial repercussions to the victim of identity include criminal investigation, arrest and even conviction, according to the GAO Report.

While you can't prevent identity theft, you can minimize your risk by managing your personal information wisely. Basic, everyday transactions are often the target of identity thieves. A check written at a department store, a credit card receipt from dinner, and other records of day-to-day financial transactions that require the sharing of personal information are all targets for identity thieves.

Here are some steps to help you not be a victim of identity theft:

- Order your credit report from the three major credit bureaus each year and check to see if all the information is correct. (Equifax, Experian, and Trans Union)
- Follow up with creditors if bills do not arrive on time, as the identity thief may have taken your bill and use that information to conduct fraud in your good name.
- Shred or tear up papers that you do not intend to keep that contain personal, financial or account information. Examples of these are credit card offers, credit card checks, papers with personal identification numbers (PINs), etc.
- Be careful when sharing personal information in person, over the phone and on the Internet.
- Be careful what you keep in your purse or wallet. If your purse or wallet is stolen, report it right away to the police and follow up with your credit-card company, credit union, and insurance company so they can stop activity on your accounts.

- Keep a copy of all the contact information of your financial companies safe at home so you can quickly contact each institution for reporting stolen credit cards, checks, and insurance cards.

Lastly, both the State of Iowa and the Federal Government have resources and sites to help citizens defend against and cope with Identity Theft.
State of Iowa: http://www.state.ia.us/government/ag/consumer/consumer_info.html
Federal Trade Commission: http://www.consumer.gov/idtheft/
The Information Security Office has copies of the FTC publication "ID Theft – When Bad Things Happen to Your Good Name" which is available upon request.
Request FTC ID Theft Guide

Larry Brennan

Return to Table of Contents

Current Activities

Let's see, things we've been up to… security policy development, testing lab, IDS, working towards the departmental integration… lots of stuff. In the future we're also planning a cyber-event exercise. Cool!

Information Security Office Service Offerings

Would you like to have a vulnerability assessment performed on your systems? Do you need help with an incident? Are you looking for security services? Check out the ISO Service Offerings!

Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates. (Security Services are listed in the last quarter of the web page.)

- Security Consulting
- Vulnerability Assessments
- Physical Security Vulnerability Assessments
- Network-Based Intrusion Detection System
- Enterprise Business Continuity
- Incident Response
- Test Lab
- Awareness Briefings
- Enterprise IT Business Continuity

Certification and Accreditation Process

It just wouldn't be a proper C&A update without major changes… so here are this month's:

Management of the Certification and Accreditation Process has been transferred to the Enterprise Quality Assurance Office, yet will continue to utilize the ISO for security testing and validation when appropriate. The C&A Process will eventually be integrated into the existing auditing process.

Certification and Accreditation is also being integrated into the ITD Project Management process, so that all new projects will automatically be reviewed for security issues and should earn accreditation before being put into production.

I will continue to be the primary contact for the C&A Process, so if you have any questions, feel free to contact me.

Marie Hubbard

Information Security Officer Distribution List

The Information Security Office has a distribution list with which we can easily send out security mailings to security contacts within the State of Iowa. Mailings include the Security Blanket, Security Quickies, Lunch & Learns, Security Alerts, Daily News and Virus Reports, security events, or other announcements. Some contacts also disseminate the ISO mailings to their departmental personnel. If you are interested in being included in this distribution list, drop a note to Security Awareness.

If you would prefer to only get the Daily News and Virus Report, which is sent out every business day, send the note with this subject heading: Security Awareness.

Security Awareness Tutorial

The Security Awareness Tutorial (SAT) is an online/CD-ROM based training course that covers security topics like Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. It is divided into separate lessons, so you can complete the lessons at different times if needed.

The SAT is currently being used by ITD for security awareness training. Because the Information Security Office has Enterprise-wide responsibilities, the SAT is also

available to State of Iowa Enterprise agencies at no charge. In addition, the SAT is available to non-Enterprise agencies and non-State of Iowa organizations as well, for a licensing fee.

For more detailed information such as system requirements and course content you can visit http://www.itd.state.ia.us/security/education.html#tutorial. Contact William Hubbard if you have questions regarding the SAT content, and Cory Oelberg for access to the course.

UPCOMING SERVICES

Risk Assessment
A standard risk assessment methodology for Enterprise systems is under development. Training will be provided on how to best utilize the methodology, and staff assistance will be available for agency assessments.

Vulnerability Profiling
A vulnerability profiling service utilizing existing Enterprise components is planned for later this quarter. The ISO will be taking a more proactive stance toward vulnerabilities by instituting alerts to appropriate personnel and developing response procedures to facilitate risk mitigation for state systems.

OTHER ACTIVITIES

Enterprise Security Website
The ISO site contains Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's a free resource of Enterprise and ITD security information.

Educational Extras
Extra resources are available here for State of Iowa security awareness efforts and home personal computer security. New additions include the CERT Home Computer Security Guide, the CIAC Home Security Guide, and others.

Information Security Outreach
In an effort to assist with the federal security awareness outreach effort and to aid state employees, security awareness materials are being offered to Enterprise departments. These materials include the ISO "Guidelines for Information Security and Internet Usage", the Federal Trade Commission's "Safe at Any Speed" and "Identity Theft" guides, and password help sheets, all of which are designed to be beneficial both in the work place and at home. If you or your department would like to obtain some of these free documents contact Security Awareness.

New Policies, Guidelines, and Procedures

We have a new ITD Web Proxy Policy, an ITD Windows 2000 Public Access Kiosk Guideline, and check out some Procedures and Guidelines from Other Sources on our website. Some newer ones include Securing Web Applications (OWASP Project) and Building and Configuring More Secure Websites.

You can find a complete list of Enterprise and ITD security policies, guidelines and procedures, as well as great industry guidelines at http://www.itd.state.ia.us/security/reading.html.

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about information sharing, security training, conferences, programs, and security vendor announcements.

The Information Security Office's Lunch &Learn Program continues. These informal meetings cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. Change of location or time will be announced via e-mail, and sent to departmental Information Security Officer contacts.

Planned Future Sessions Include:

- ITD and Enterprise Policies
- Safe Data Removal
- Business Continuity
- Secure Application Development

An updated schedule and past presentations (lots of them - in .pdf, .ppt, and/or video) are available at the Lunch & Learn site.

Please remember - we'll supply the place, the conversation, and the riveting power-point slideshows, but you will need to bring your own lunch. Questions or topic ideas on the Lunch & Learn program can be directed to William Hubbard.

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing info.

Security Vendors

SANS Offerings:
Each month SANS offers at least one training conference in a major U.S. city. In the next few months there are several upcoming events, but especially notable is the SANS 2003 event, March 5 –12, in San Diego. For this (and others) see:
http://www.sans.org/SANS2003

SANS also offers online and onsite security courses for those who are unable to travel much, but still wish to participate. Visit http://www.sans.org/newlook/home.php for more info. SANS also offers a free Webcasts on security, auditing, and network administration. Visit http://www.sans.org/webcasts/ for further enlightenment.

If **State of Iowa employees** are interested in an Enterprise-shared SANS session, drop a note to Security Awareness, and note your specific interest, if known (Security Essentials, Securing Windows, Auditing, etc.). If there is enough response the ISO may be able to organize a reduced-cost session specifically for state employees. SANS often can arrange a special on-site session for a reduced cost. Details:
http://www.sans.org/onsite

Sun Microsystems
Sun is conducting beta tests for its "Solaris Security Administrator" certification exams, and is offering a free certification program for those that help to test it. They recommend that a tester have 6-12 months experience administering security on Solaris.
http://www.netsys.com/cgi-bin/displaynews?a=464

Microsoft: (Vendor Announcements)

The Microsoft Security Update Offers Home User Edition
Microsoft is making non-technical alerts available for home users. This service is designed to make it easier for home users to keep aware of and deal with new vulnerabilities and patches. Visit the following site for more information or to sign up:
http://www.microsoft.com/security/security_bulletins/decision.asp

Free MSDN Webcasts
Microsoft offers free 90-minute live, interactive webcasts on a variety of topics, including security. Customers can see code and application demos online, and ask the presenter technical questions, or listen to their peers ask questions.
Register at: http://www.microsoft.com/usa/webcasts/upcoming/default.asp
Recorded sessions can be found at:
http://www.microsoft.com/usa/webcasts/ondemand/default.asp.

Microsoft Online Training
Microsoft offers online training for a number of their products. Government workers also get discounts. To register for a course, or just to check them out, visit their website:
http://www.msgovernmenttraining.com/offer/

Other Events:

BlackHat Windows Security 2003 Briefings and Training
Feb. 24-27, Sheraton Seattle Hotel & Towers in Seattle, WA
Subjects include policies, deep knowledge, networking and integration, and application development, as well as Microsoft .NET, Microsoft IIS, Microsoft SQL Server, and Microsoft Internet Security and Acceleration (ISA) Server 2000. For more information see: http://www.blackhat.com/html/win-usa-03/win-usa-03-index.html

InfoSec World Conference and Expo 2003
March 10-12, Orlando, FL
This large annual event features hands-on experts, the latest security topics, live demos, optional pre- and post-conference workshops, and more. For more details visit:
http://www.misti.com/northamerica.asp?page=4&region=1&subpage=2&id=OS03&disp=showconf

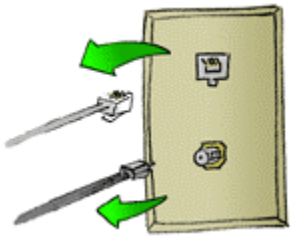
RSA Conference 2003, April 13-17, San Francisco, CA
The RSA conference has four main components: General Sessions, Expo, Tutorials, and Class Tracks. See http://www.rsasecurity.com/conference for details.

Return to Table of Contents

Helpful Hints

Always On, Always Vulnerable

Today, people have many Internet connection options to choose from. Anything from s-l-o-w modems, to faster DSL, and *speedy* cable modems, home users can choose the price and speed combination that's right for them. When your system has a connection to an ISP, however, it is also possible that someone could connect to your system through that ISP.



Got a modem? Make sure the modem's auto-answer is turned off. Even better, disconnect the modem whenever you aren't using it. Do you use an always-on connection? Very convenient, but at the same time that means the system is also always open to attack.

When you're not using your ISP, make sure you aren't accepting incoming traffic. Switch the connection off, or configure your firewall to accept only the specific traffic you want to allow, like automatic updates from your anti-virus vendor. Connecting to the Internet from home can be a blast, but it is important to remember that whenever you are looking at the Internet, the Internet is looking back at you.

William Hubbard

Return to Table of Contents

Linked Articles

Featured Links:

Pillars of Your Community
To err is human. But can you really forgive the security disasters a careless employee might bring to your company? Here's how to teach users that they're your company's best defense against information security breaches. January 2003 CSO Magazine

Iowa Homeland Security Initiative (pdf)
This is the final report of Iowa's Homeland Security Advisor regarding the Homeland Security Initiative in the State of Iowa.

Education

Helpful Security Guides:
Connecting to the Internet Securely - Protecting Home Networks - the Dept. of Energy, CIAC, has developed a guide on securing the home network, CIAC-2324
http://www.consumer.gov/idtheft/ Federal Trade Commission's guide to Identity Theft
CERT Home Computer Security Website – an informative security guide for home users.
It's a Great Time to Check Your Security – a compilation of basic and advanced guides.
Security Linux 101 - a guide to securing Linux systems.
Securing Systems with chroot – a guide for defending against buffer overflows.
Closing the Floodgates - DDoS Mitigation Techniques

Microsoft Revamps Security Updates for Home Users
Microsoft Corp. on Tuesday continued the expansion of its security response process, unveiling a new security mailing list specifically for home or other non-technical users. Feb. 11, 2003, eWeek

See Also:
The Microsoft Security Update - Home User Edition
Microsoft is now offering a free e-mail alert service for home users, the Microsoft Security Update newsletter.

Rooting Out Vulnerabilities at the Source
Sanctum Inc. released a new application designed to enable developers to perform security testing and vulnerability assessments of their software during the development process. February 10, 2003, eWeek

What It Takes To Develop Defense In Depth
Defense in depth should be thought of not as a set of independent steps to be executed separately, but as a series of related and overlapping technical and nontechnical security measures that, when strategically deployed together, have a greater effect than their individual components. Feb 04, 2003, ComputerWorld

Forensics on the Windows Platform, Part One
Forensics on the Windows Platform, Part Two
In Part One the wider legal issues raised by computer forensics and the benefits of pre-investigation preparation are discussed. Part Two concentrates on the areas of a Windows file system that are likely to be of most interest to forensic investigators and the software tools that can be used to carry out an investigation. Jan/Feb. 28, 2003, SecurityFocus

Who is at risk from cyberattack?
It may come as no surprise that utility firms often come under assault from hackers, but some of Symantec's findings are not as predictable. Feb. 5, 2003, ZDNet UK News

Worm spread worldwide in 10 minutes
It only took 10 minutes for the SQL Slammer worm to race across the globe and wreak havoc on the Internet two weeks ago, making it the fastest-spreading computer infection ever seen. Feb 5, 2003, CNN

How to toughen the weakest link in the security chain
The guiding tenet of computer security is that an organization's overall security is only as strong as its weakest link: the human element. Jan. 8, 2003, ComputerWorld

Instant Insecurity: Security Issues of Instant Messaging
As with most things Internet based, the increasing use of instant messaging has led to an associated increase in the number of security risks. Jan 13, 2003, SecurityFocus

Microsoft Baseline Security Analyzer V1.1 (Product Review)
MBSA 1.1 is a multi-threaded security scanner that analyzes an individual computer or a group of computers for missing security patches and other common security mis-configurations. (Dec.19, 2003, SecurityFocus)

How to prevent data loss
Some tips to help you avoid data loss. (Jan. 28, 2003, Computerworld)

Are You Infected? Detecting Malware Infection
Some tips on malicious code and how to detect certain infections. Feb. 13, 2003, SecurityFocus

Homeland Security

Internet Attack Rattling Assumptions
Disruptions from the weekend attack (Slammer Worm) on the Internet are shaking popular perceptions that vital national services, including banking operations and 911 centers, are largely immune to such attacks. Jan. 28, 2003, ITToolBox

Ashcroft proposes vast new surveillance powers
A sweeping new anti-terrorism bill drafted by the Justice Department would dramatically increase government electronic surveillance and data collection abilities, and impose the

first-ever federal criminal penalties for using encryption in the U.S. (Feb. 7, 2003, Security Focus)

See also:

Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act
Ashcroft may be preparing a comprehensive sequel to the USA Patriot Act. (Includes link to the draft proposal - Feb. 7, 2003, Center for Public Integrity)

Homeland IT added to GAO's high-risk list
The Homeland Security Department in general and its IT operations in particular are new areas of high risk for failure, the General Accounting Office notes. Jan. 30, 2003, GNC

Sen. Edwards introduces information security bill
Sen. John Edwards has introduced a bill that would require agencies to identify vulnerabilities in their systems and set up timetables for eliminating them. Jan. 20, 2003, GNC

Think Federally, Secure Locally
Cyber threats may be global, but cyber security is everyone's responsibility. Jan. 1, 2003, CIO Magazine

Cyberthreats Not to Be Dismissed, Warns Clarke
Says vulnerabilities still 'underappreciated' as threat to nation's critical infrastructure. Jan. 6, 2003, ComputerWorld

Cyber Crime

Experts Search for Ways to Fight Cybercrime
Cyber terrorism is a real threat, but identity theft and child exploitation shouldn't be ignored, conference attendees say. Feb. 12, 2003, PCWorld

Tackling identity theft
A fourth man has been arrested as part of the largest identity theft case in U.S. history. Jan. 29, 2003, CNN

eBay account hijacked, bidders bilked in `rampant' fraud
For a couple of days last month someone was auctioning Sony camcorders from Kevin Pilgrim's eBay account. But the auctioneer wasn't Pilgrim, who lives in Raytown, Mo. Jan. 30, 2003, Centre Daily

Feds pull suspicious .gov site
In a move that raises questions about the security of governmental domains, the Bush administration has pulled the plug on a .gov Web site pending an investigation into the authenticity of the organization that controlled it. Feb. 5, 2003, C/Net

FTC sees surge in identity theft
Complaints about identity theft have risen 73 percent from a year ago, according to a new report from the Federal Trade Commission. Jan. 22, 2003, ZDNet

A crime wave festers in cyberspace
Cyber crime, long a painful side effect of innovations of Internet technology, is reaching new dimensions, security experts say. Jan 28, 2003, IHT

Pair who hacked court gets 9 years
Former computer consultant tried to dismiss pending cases. Feb. 7, 2003, MSNBC

FBI investigating theft of data on international students by hacker
University of Kansas officials said Thursday they believe the "hole" that allowed a computer hacker to download personal information about 1,450 of the school's international students has been patched. Jan. 24, 2003, USAToday

Ruling shields AOL on 'hostile code'
In what legal experts describe as a first, a federal appeals court has upheld a ruling that America Online and other Internet service providers are not liable for "hostile code" sent between subscribers. Jan. 23, 2003, C/Net

California disclosure law has national reach
A new California law requiring companies to notify their customers of computer security breaches applies to any online business that counts Californians as customers, even if the company isn't based in the Golden State. Jan. 6, 2003, SecurityFocus

Judge orders Internet providers to help trace online pirates
Internet providers must abide by music industry requests to track down computer users who illegally download music, a federal judge ruled Tuesday in a case that could dramatically increase online pirates' risk of being caught. Jan. 21, 2003, SFGate

News

NIPC Advisory 02-002: Encourages Heightened Cyber Security as Iraq - US Tensions Increase
The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq. Feb. 11, 2003, NIPC

Class Action Lawsuit launched over missing hard drive
A class-action lawsuit has been launched against the company responsible for losing a VHS cassette-sized computer drive with personal information affecting up to one million people. Feb. 4, 2003, SNP

Trustworthy Yet?
Microsoft is making significant strides to clean up its security mess, but Trustworthy Computing still has a long way to go. Feb. 2003, InfoSec Magazine

Information Systems Security Association Announces Review of Security Certifications
Global Voice of Information Security Will Create a Certification Roadmap to Help Guide Industry Professionals. Jan. 27, 2003, News Alert

Security Vendor Cuts Ties With CERT
A prominent U.K.-based security vendor well-known for finding dangerous vulnerabilities in a variety of software said on Monday that it would no longer work with the CERT Coordination Center after CERT personnel gave advance notice of several new vulnerabilities to a software vendor and some government officials. Jan. 28, 2003, eWeek

The New Security Threat: Lawyers
What's the security problem you fear most? Is it viruses, Trojans or computer crackers? How about lawyers? Jan. 27, 2003, OSOpinion

The Briscoe Syndrome
Fear of terrorism and a desire to cooperate with law enforcement has led many corporate insiders to pony up sensitive information on their customers to anyone with a badge... with no court order required. Dec. 29, 2003, SecurityFocus

Was the FBI's Response to Slammer Too Slow?
The recent creation of the Department of Homeland Security likely hampered the government's handling of the worm, insiders say. Jan. 28, 2003, PCWorld

Sprint DSL's Gaping Security Hole
Sprint DSL customers are at risk of having their e-mail addresses and passwords stolen -- even when their computers are powered off -- due to weak security controls on their DSL modems. Jan. 23, 2003, Wired News

Silence Isn't Golden for Security
Like cancer used to be among friends in the 1960s, security is taboo as a discussion topic among many CIO's today. Jan. 20, 2003, ComputerWorld

Texas auditors urge systems consolidation
The Texas State Auditor's Office today issued a report citing information resources and technology management as a major risk area for the state and recommended that Texas create a plan to consolidate the state's IT projects. Jan. 22, 2003, GNC

News Homepage links:

Centre Daily: http://www.centredaily.com/mld/centredaily/
Center for Public Integrity: http://www.publicintegrity.org/dtaweb/home.asp
CIO: http://www.cio.com/
C/Net: http://news.com.com/
CNN: http://www.cnn.com/
Computer World: http://computerworld.com/
CSO Online: http://www.csoonline.com/
eWeek: http://www.eweek.com/
GNC: http://www.gcn.com/
InfoSec Magazine: http://www.infosecuritymag.com/
IHT: http://www.iht.com/frontpage.html
ITToolbox: http://security.ittoolbox.com/news/
MSNBC: http://www.msnbc.com/news/default.asp
News Alert: http://www.newsalert.com/bin/userinfo/
NIPC: http://www.nipc.gov/index.html

OSOpinion: http://www.osopinion.com/
PCWorld: http://www.pcworld.com/news/
Security Focus: http://online.securityfocus.com/
SFGate: http://sfgate.com/
SNP: http://www.securitynewsportal.com/index.shtml
USAToday: http://www.usatoday.com/usafront.htm
Windows Web Solutions: http://www.windowswebsolutions.com/
Wired News: http://wired.com/
ZDNet UK News: http://news.zdnet.co.uk/
ZDNet: http://www.zdnet.com/

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: Charter Projects: Transition Security Issues, Security Planning, Certification and Accreditation Process
515-725-0385

Paul Schmelzel: Security Operations: Vulnerability Assessments, Intrusion Detection, Incident Response, Test Lab
515-281-5956

Larry Brennan: Critical Infrastructure Assurance Coordinator, Iowa Crisis Action Team
515-725-0365

Wes Hunsberger: 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 20 Vulnerabilities

The FBI's NIPC and the SANS Institute published a revised list of the top twenty Internet security vulnerabilities along with instructions on how to fix them.

Iowa Homeland Security

This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more.

Homeland Defense Journal

This is the federal Homeland Defense journal homepage.

Stay Safe Online

A site dedicated to educating citizens and helping them secure their home systems. Sponsored by the National Cyber Security Alliance.

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

*Cause we just **Love** Security!*