



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



PREPAREDNESS UPDATE #017 - FRIDAY, OCTOBER 26, 2007

Local

Capital Connections Meeting: December, 14, 2007, 1:00 p.m. to 3:30 p.m. Location: TBD

Planned Featured Presentations: "ISLAM (THE BASICS)"; "ILLINOIS COMMUNICATION NETWORK" (the IL Public/Private partnership to keep utilities going during disasters)



Local Sangamon County Area Training

Title	Date/Time	Contact
Command & General Staff Course*	Nov. 5-9, 2007 (Springfld)	IL Fire Safety www.fsi.uiuc.edu/documents/forms/General%20Registration.pdf

*Meets NIMS IC 300 & 400 requirements

Agricultural

Article claims increased ethanol production in the U.S. will lead to increased food prices & inflation -

[//money.cnn.com/news/newsfeeds/articles/prnewswire/TO12622102007-1.htm](http://money.cnn.com/news/newsfeeds/articles/prnewswire/TO12622102007-1.htm)

\$5.9 million grant offering for "Outreach & assistance for socially disadvantaged farmers & ranchers" -

www.csrees.usda.gov/funding/rfas/outreach.html

Biological, Laboratory/testing & Medical

Presidential Directive HSPD-21 on Public Health & Medical Preparedness (10/18/07) -

www.whitehouse.gov/news/releases/2007/10/20071018-10.html

Emergence of antimicrobial resistance Strep pneumonia infections (MA) – CDC Weekly Report

www.cdc.gov/mmwr/preview/mmwrhtml/mm5641a2.htm?s_cid=mm5641a2_e

D.C. Fire & EMS personnel also dealing with Staph (MRSA) infection - [www.emsresponder.com/web/online/Top-EMS-](http://www.emsresponder.com/web/online/Top-EMS-News/DC-Fire-and-EMS-Dealing-With-Staph-Infection/1$6400)

[News/DC-Fire-and-EMS-Dealing-With-Staph-Infection/1\\$6400](http://www.emsresponder.com/web/online/Top-EMS-News/DC-Fire-and-EMS-Dealing-With-Staph-Infection/1$6400)

Chemical, Heavy Metals, Environmental & Toxic Substance

- No report at this time -

Cyber & Other Communication & GPS Updates

<<<See Supplemental>>>

Energy, Environment, Water & Utility Items

Author speaks about how easy it is to hack into our nation's power grid -

www.internetevolution.com/author.asp?doc_id=136047&f_src=dnewsalert

Florida proposes two new nuclear power stations - [/news.yahoo.com/s/ap/20071017/ap_on_go_co/terrorist_surveillance](http://news.yahoo.com/s/ap/20071017/ap_on_go_co/terrorist_surveillance)

Byron Nuclear Power Station (Ogle Co, Illinois – South of Winnebago Co) shuts down

a reactor due to leaky pipes found on inspection - www.rstar.com/homepage/x1302706007

Security guard force pulled from Jardine water treatment plant (Chicago – Largest capacity water filtration system in the world) after caught sleeping & not where they were supposed to be -

www.suntimes.com/news/metro/614148.CST-NWS-water22.article;

How it (Jardine) works - www.algor.com/news_pub/cust_app/jardine/jardine.asp

California wild fires sit. report - www.fema.gov/emergency/reports/2007/nat102307.shtml



Explosive, Incendiary & Man-Portable Air Defense systems (MANPADs)

A 'would-be' suicide bomber accidentally blows-up himself, his mother, sister & brother when he tried to leave his house and his mother tried to stop him - www.news.com.au/heraldsun/story/0,21985,22593708-5012750,00.html

USA Today reports on a Classified report that O'Hare missed 60% of fake bombs hidden on undercover agents (75% at LAX) - www.usatoday.com/printedition/news/20071018/1a_lede18_dom.art.htm

"Kitchen Sink" (Chemical) bomb awareness -

www.boston.com/news/nation/articles/2007/02/19/fbi_anticipates_new_terrorist_weapon_kitchen_sink_bombs/

IEDs seen as a rising threat in the U.S. - www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101902703.html

Female suicide bomber blows up a minibus taxi in Russia - www.nytimes.com/aponline/world/AP-Russia-Suicide-Bomber.html?ex=1350792000&en=568108bff819aa02&ei=5088&partner=rssnyt&emc=rss

Suicide bombing on the rise worldwide - [/usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2007&m=October&x=20071011104652dmslahrellek0.8995325&chanlid=washfile](http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2007&m=October&x=20071011104652dmslahrellek0.8995325&chanlid=washfile)

Study finds black gay men, lesbians, & Bisexual individuals have significantly fewer mental disorders than 'whites' (who typically have higher suicide rates) - www.mailmanschool.org/news/display.asp?id=572 Risk Factors & suicide rates - www.afsp.org/index.cfm?fuseaction=home.viewpage&page_id=052AE75C-03F4-C6CA-029712654E43848C

Information, Finance & Technology



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



Tamil Tiger gang arrested for ATM fraud in NY - www.nydailynews.com/news/crime/file/2007/10/16/2007-10-16_sri_lankan_terror_gang_busted_in_atm_hei-2.html

Website discusses how websites are being used for propaganda by radical Islamic - www.jamestown.org/terrorism/news/article.php?articleid=2373721

Study of 500 closed Secret Service cases reveals ID thieves have a 50-50 chance of going to jail - www.infoworld.com/article/07/10/23/ID-thieves-50-50-chance-of-prison_1.html

<<<Also See Supplemental>>>

International Events

Article on the "Saffron Revolution" (Burmese Monk Protest) - [//english.safe-democracy.org/2007/10/11/the-explosion-of-the-saffron-revolution/#more-334](http://english.safe-democracy.org/2007/10/11/the-explosion-of-the-saffron-revolution/#more-334)

Radiological & Nuclear

Morris, IL still in the running to be the nation's spent fuel rod recycler – U.S. DOE decision delayed - www.suburbanchicagonews.com/heraldnews/news/608918.4_1_JO18_NUCLEAR_S1.article

About \$60 million in U.S. funds went to make ports in Britain, Pakistan & Honduras 100% radiologically screened for containers headed to the U.S. - www.upi.com/International_Security/Emerging_Threats/Briefing/2007/10/15/3_ports_start_100percent_cargo_scanning/2799/

Six U.S. Navy personnel punished for forging inspection documents on nuclear powered submarine cooling systems - www.cnn.com/2007/US/10/22/sub.misconduct/index.html?section=cnn_latest

Suspicious Packages & Substances

- No report at this time -

Tactical Weapons, Trends & Mass Trauma Activities

Israel's prevention of suicide hijackings into Tel Aviv - www.mailmanschool.org/news/display.asp?id=572

An increasing number of mainland European militants are traveling to Pakistan for terrorism training attacks against the west - www.latimes.com/news/nationworld/world/la-fg-jihad14oct14_0_4029080_full_story?coll=la-home-center

York Region & the Toronto's Star News agencies report gun trafficking between New York & Canada - www.yorkregion.com/News/Richmond%20Hill/article/53730; www.thestar.com/News/article/267022

Custom-built trap door in trucks used to siphon thousands of gallons of gasoline from stations during broad daylight (FL) - www.floridatoday.com/apps/pbcs.dll/article?AID=20071019/BREAKINGNEWS/71019001/1086

A stolen tanker w/7,100 gallons of diesel fuel was found in SE D.C. – [//blogs.abcnews.com/rapidreport/2007/10/fuel-tanker-hij.html](http://blogs.abcnews.com/rapidreport/2007/10/fuel-tanker-hij.html)

At least 16 coal fired power stations nationwide have been scrapped due to global warming concerns - www.foxnews.com/story/0,2933,303061,00.html

Concealed weapons on campus movement - [//concealedcampus.org/](http://concealedcampus.org/)

LTTE suicide bomber (Black Tiger) attacks Sri Lanka military base October 22 & killed 34 - www.thestar.com/News/article/269414

Transportation

Air passengers will no longer have to remove bulky headwear, such as turbans, if it will make them feel uncomfortable to do so (TSA) - [/news.yahoo.com/s/ap_travel/20071016/ap_tr_ge/travel_brief_turban_screening;_ylt=Av2C5D44kZzrRxFy7abbCoQ8sM0F](http://news.yahoo.com/s/ap_travel/20071016/ap_tr_ge/travel_brief_turban_screening;_ylt=Av2C5D44kZzrRxFy7abbCoQ8sM0F)

A small piece of low-level radioactive isotope (moister-density gauge use) fell of a truck and caused a highway closure (TX) - www.chron.com/disp/story.mpl/ap/tx/5227480.html

As the Great Lakes recede, cargo ships must reduce weight to navigate - www.nytimes.com/2007/10/22/nyregion/22oswego.html?_r=2&oref=slogin&oref=slogin

New law requires airlines to complete background checks on ALL employees (Oct 1, 2007) - http://www.usatoday.com/news/nation/2007-10-21-airports_N.htm

Gaps in aircraft security - www.charleston.net/news/2007/oct/22/disturbing_gaps_aircraft_security19794/

(Other) Training, Exercise, Response & Policy

Egypt releases a top HAMAS leader although wanted by Palestinian & Israeli authorities for terrorist attacks over recent years – May have been linked to secret hostage exchange. www.jpost.com/servlet/Satellite?cid=1192380554462&pagename=JPost/JPArticle/Printer

Top Yemen Qaeda suspect convicted of bombing of the U.S.S. Cole surrendered to authorities - www.canada.com/topics/news/world/story.html?id=f55dc3b0-50ad-4705-a34d-7f433ec8807b&k=52761

EMS preparedness funding bill being considered by the Senate - [www.emsresponder.com/web/online/Top-EMS-News/EMS-Funding-Bill-on-Senate-Agenda/1\\$6343](http://www.emsresponder.com/web/online/Top-EMS-News/EMS-Funding-Bill-on-Senate-Agenda/1$6343)

Rushville (IL) hospital get's a \$250K telemedicine grant - www.pjstar.com/stories/101707/REG_BELO7MJP_049.php



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



Concerns raised over possible terrorist attacks on the U.S. launched from Latin American (Hezbollah a big concern) - [//news.scotsman.com/latest.cfm?id=1666102007](http://news.scotsman.com/latest.cfm?id=1666102007)

Sweden drug smugglers try to smuggle cocaine to Sweden from Peru using postcards – Drug sniffing canines are credited. www.thelocal.se/8829/20071018/

FBI Congressional report on Terrorist Screening Center - www.fbi.gov/congress/congress07/boyle102407.htm

“It is easier to fight for principles than to live up to them.” – Alfred Adler

Dates:

40 days of protest to end abortion Sept 6 - Nov. 6, 2007 - www.40daysforlife.com/chicago/

Students for Concealed Carry on Campus (SCCC) to stage a demonstration across U.S. by wearing empty holsters Oct. 22 – Oct. 26, 2007 [//concealedcampus.org/index.htm](http://concealedcampus.org/index.htm)

Islamo-Facism Awareness Week Oct. 22 – Oct. 26, 2007 protests targeting students on campuses www.terrorismawareness.org/
Law Enforcement should remain vigilant to possible conflicts, due to the nature of the groups involved...

Capital Connection December 14, (1:00p – 3:30p);

National Mobilization to end the Iraq War planned for Oct 27 – Chicago one of the sites - [//madpeace.org/?q=taxonomy/term/23&PHPSESSID=76013839d91e698eb51701a0a82cf4bf](http://madpeace.org/?q=taxonomy/term/23&PHPSESSID=76013839d91e698eb51701a0a82cf4bf)

Daylight Savings Time Ends ~ November 4, 2007 ~

Judith Miller Appearance (Co-Author of Germs:...& Other BioT books - to speak on Press Freedom), UIS, November 7th (7:30p)
Free, ticket details being worked out. [//en.wikipedia.org/wiki/Judith_Miller_%28journalist%29](http://en.wikipedia.org/wiki/Judith_Miller_%28journalist%29)

Website Links

Look-ups:

Federal Inmate Locator - www.bop.gov/iloc2/LocateInmate.jsp;

Federal Sex Offender Look-up - www.nsopr.gov/;

Gang Identification & Expert Witness - www.gangsor.us/index.html; www.knowgangs.com/; [//gangresearch.net/](http://gangresearch.net/); www.ngcrc.com/;

www.nmgf.org/; www.iir.com/nygc/; www.gangscrossamerica.com/

IL Agency Directory - www.illinois.gov/teledirectory/searchbyagency.cfm;

IL Employee Directory - www.illinois.gov/teledirectory/searchbyname.cfm;

IL Sex Offender Look-up - www.isp.state.il.us/sor/;

IL Methamphetamine Manufacturer Registry - www.isp.state.il.us/meth/

Terrorism Database – www.tkb.org

Urban Legends (debunking) - [//urbanlegends.about.com/](http://urbanlegends.about.com/); www.snopes.com/

Preparation:

NEW: Adult vaccination recommendations (CDC) - www.cdc.gov/mmwr/preview/mmwrhtml/mm5641a7.htm?s_cid=mm5641a7_e

CDC & Red Cross Preparedness for Public Health emergencies - [//emergency.cdc.gov/preparedness/](http://emergency.cdc.gov/preparedness/);

Cyber scam updates - www.us-cert.gov/;

Federal Ready.Gov - www.ready.gov/;

Ready.Illinois - www.ready.illinois.gov/;

Statistics:

FBI 2006 Crime Statistics available - www.fbi.gov/ucr/cius2006/index.html;

Illinois Health Statistics - www.idph.state.il.us/health/statshome.htm;

Illinois Suicide Prevention Training - www.isp.net/calendar.htm;

National Health Interview Survey Results - www.cdc.gov/nchs/about/major/nhis/quest_data_related_1997_forward.htm;

US Census demographics by zip code - [//zipskinny.com/](http://zipskinny.com/)

Reporting:

Suspicious terrorism or criminal activity that could lead to terrorism –

<Your Local Law Enforcement Center First>

FBI Springfield, 900 East Linton Avenue, Springfield, Illinois 62703, springfield.fbi.gov (217) 522-9675

State & Regional Fusion Centers - www.fas.org/irp/agency/ise/state.pdf

Training:

Emergency Management - FEMA: training.fema.gov/IS/crslist.asp, IEMA:



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



Fire: www.nfaonline.dhs.gov/

Law Enforcement: Homeland Security: www.fletc.gov/training/programs/state-local/state-and-local-training-links/; Bureau of Justice Assistance: bjatraining.ncjrs.gov/;

Public Health: CDC www2a.cdc.gov/PHTN/media.asp#LiveCourses; Public Health: IL IDPH Learning Management System www.idphlms.com/; UIC www.publichealthlearning.com/Public/Catalog/

Weapons, Equipment & Tactics:

Chain Whip 46" sharpened "Daggertail" - www.amazon.com/Chain-Blade-Whip-Stainless-Daggertail/dp/B000PJC7PC?tag=dogpile-20

Cell phone stun guns - www.tbotech.com/cellphonestungun.htm

Coin knives - www.eloi.net/

NEW: License Plate Flipper - www.platflipper.com/

Miniature low resolution 33 hr camcorder can hide in a gum stick box - www.spygadgets.com/spy-cameras/spycameras.htm

Pepper Spray Ring - www.planetmace.com/pepper-spray-ring.html

Taurus Judge Handgun 45-410 - www.taurususa.com/video/taurus-theJudge-video.cfm

Gun-shaped belt buckles (\$1) - www.icedoutstreets.com/files/details.php?pid=242

<Supplemental>

October 15, The Detroit Free Press – (National) **Phony check schemes are bouncing back.** According to the National Consumer League, schemes involving fake checks cost the victims on average between \$3,000 and \$4,000. The schemes come in various forms, but the most common current scams include big lottery or jackpot winnings and work-from-home scams. In both cases, recipients receive checks featuring a larger sum of money than requested or desired, and wire the difference back to the fraudsters before they are informed by their banks that the checks were fraudulent. A senior vice president of the fraud services department for Comerica Bank in Auburn Hills, Michigan said that the checks look so authentic that even bank tellers are not able to identify them as fake. However, the bank official recommended that people tell their banks where and how they received the check before depositing it. Source: <http://www.freep.com/apps/pbcs.dll/article?AID=/20071015/COL07/710150377/1002>

October 14, St. Louis Today – (National) **Child ID theft is a growing financial problem.** According to the Federal Trade Commission, identity theft reports for victims under 18 years old increased from 6,512 in 2003 to 10,835 in 2006 representing 5 percent of all identity thefts. The report lists teens as particularly vulnerable because of their increased access to the internet. One concern is that the identity theft may go unnoticed until many years later, when the victim becomes an adult and applies for a credit card. Authorities say that often the crime is committed by the children's own parents or relatives, who apply for credit using the child's social security number. These crimes can go unreported because victims who do eventually discover the crimes do not seek legal ramifications against loved ones. The vice president of public education at Experian, one of the three major credit bureaus, advises parents to "monitor their child's online activity; do not ignore the junk mail the child receives; if they sign up their child for a magazine subscription to put it under their name; and do not let children keep their Social Security cards in their wallets." Moreover, if parents suspect their children's identity was stolen, they should check immediately to see if a credit file was created on their child. Source: <http://www.stltoday.com/stltoday/business/stories.nsf/yourmoney/story/088AB3C9CBEAAF8786257373000E9D6B?OpenDocument>

October 15, Computerworld – (Ohio) **'Management Glitch' is blamed in Ohio tape theft.** An Ohio state official must surrender a week of future vacation time as punishment for a "management glitch" that led to the theft of a backup tape holding Social Security numbers and other personal data on more than 100,000 state employees and taxpayers. The state issued the punishment late last month to the payroll team leader for the Ohio Administrative Knowledge System ERP project of the Ohio Department of Administrative Services, according to the department's communications office. The tape was stolen in June from an intern's car. An official from the office also noted that although the tape was his department's responsibility, it was regularly handled by individuals from other agencies. "Part of the problem is that [the data] was outside of any one person's hands. There were people coming in from agencies to do data migration and testing" who were adding data to the drive, he said. "One lesson that the state learned is that we need to throw more resources at security and privacy when we have an issue like that," he added. An analyst at Enterprise Strategy Group Inc. in Milford, Massachusetts, said the minimal punishment indicates that there is not a widespread security problem. "If there was a pattern of incompetence," she said, "then typically the person would lose their job." Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=305393&taxonomyId=17&intsrc=kc_top



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



October 15, IDG News Service – (National) **Researcher: Mac OS, Linux probably have URI issues too.** The problems with URI protocol handlers that are registered unnecessarily and with little thought given to security are not just limited to Windows, researchers say. In fact, an analyst at Ernst & Young Global, and one of the researchers who has been studying the problem most closely, says he hopes to present more details on how other Unix-based operating systems like Linux and Mac OS X may also be susceptible to what are known as URI (Uniform Resource Identifier) protocol handler flaws at the Toorcon hacking conference, being held next week in San Diego. In an interview, he said that he had not yet found a way to run unauthorized code on Unix-based operating systems, but that he and his fellow researchers had discovered a number of issues that looked like they could be grounds for further research. The problem they have been researching over the past few months has to do with the URI protocol handling technology, used to launch programs from within Web browsers. Probably the best known of these protocols is mailto, which is used to launch the mail client from within the browser. But any software developer can register their own application with the operating system. To date, hackers have found ways to run unauthorized software on the PC by sneaking commands into specially crafted Web links that use the URI protocols of several well-known applications. Microsoft had originally said that it was up to software developers to make sure their programs check the links so that they do not include malicious code, but this week it agreed to put some checks within the Windows operating system as well. Source: <http://www.thetimesherald.com/apps/pbcs.dll/article?AID=/20071015/NEWS01/710150307/1002>

October 15, Computerworld – (National) **Commerce bank thwarts a major database hack.** A Midwestern bank last week said it was able to deflect most of a hacking attempt on its database, but not before some customer information was divulged. Commerce Bank NA, which operates in Missouri, Kansas, Illinois, Oklahoma and Colorado, last week said a hacker had breached a database with about 3,000 customer records and accessed 20 of them. The hacking was quickly detected and stopped, said the unit of Kansas City, Missouri-based Commerce Bancshares Inc. Officials added that law enforcement agencies were notified of the breach. The bank said that it is contacting all customers who may have been affected and that it will provide them with free credit monitoring services for 24 months. Commerce Bank did not disclose how the hackers accessed its database. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=305311&taxonomyId=17&intsrc=kc_top

October 12, IDG News Service – (National) **Critical Oracle patches coming this week.** Oracle Corp. will release security updates for its products next week fixing 51 vulnerabilities in its products. Included in the Critical Patch Update, set to be released Tuesday, will be critical updates for the company's flagship Oracle Database. Twenty-seven database bugs will be fixed, but five of the bugs can be "exploited over a network without the need for a username and password," Oracle said in a note on next week's patches. Fixes are also planned for Oracle's Application Server, E-Business Suite and Enterprise Manager software. There will also be patches for three vulnerabilities in the company's PeopleSoft Enterprise products. After the database software, the Application Server and E-Business suite will get the most patches with 11 and 8 bug fixes, respectively. No patches are planned for Oracle's Collaboration Suite and JD Edwards products. Oracle's 10g and 9i databases will both be patched next week. The software vendor releases its updates on a quarterly basis, meaning that these updates typically contain a lot of patches. For example, July's updates contained 45 fixes. Following next Tuesday's release, the next Critical Patch Update is set for January 15. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9042438&taxonomyId=17&intsrc=kc_top

October 15, RCR Wireless News – (National) **VZW intros new opt-out policy for dissemination of calling records.** Verizon Wireless is requiring customers to opt out of allowing the carrier to share their customer proprietary network information (CPNI), a new policy that could spark protest from the carrier's customers. CPNI comprises users' calling records and includes the numbers of incoming and outgoing calls and time spent on each call, among other data. Verizon Wireless last week began sending letters notifying customers that they have 30 days to opt out of the program by calling an 800 number before their information would be shared. "In order to better serve your communications needs and to identify, offer and provide products and services to meet your requirements, we need your permission to share this information among our affiliates, agents and parent companies (including Vodafone) and their subsidiaries," the company informed subscribers. "Unless you provide us with notice that you wish to opt out within 30 days of receiving this letter, we will assume that you give the Verizon Companies the right to share your CPNI with the authorized companies as described above." CPNI has become a contentious issue in recent years as telecommunications firms and others seek to leverage their networks by delivering highly targeted ads. The Federal Communications Commission earlier this year strengthened its privacy rules regarding CPNI following the pretexting scandals that darkened the industry last year. Source: <http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20071012/FREE/71012004/1002>



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



October 15, Computerworld – (National) **Privacy concerns dog IT efforts to implement RFID.** Privacy concerns related to the use of radio frequency identification technology are reaching new heights, as legislators increasingly look to restrict RFID deployments and corporate employees criticize efforts to use it in identification badges. At the same time, champions of the technology contend that not enough is being done to promote the value of RFID. For example, they say, it can be used to track tainted foods or counterfeit drugs or to reduce inventory-tracking costs. IT executives attending the RFID World conference in Boston last month said employee fears have forced some companies to change or even cancel plans to use badges embedded with RFID technology. The manager and counsel for technology policy and state government affairs at the AeA, formerly known as the American Electronics Association, noted that more and more state legislatures are seeking to limit the use of RFID technology. While RFID privacy concerns “are taken very seriously in state governments across the U.S.,” most legislators do not understand the value of the technology, he contended. Aderson said 50 bills aimed at limiting RFID were introduced in 19 states in 2007, and three became law. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=305197&taxonomyId=17&intsrc=kc_top

October 16, Identity Theft Assistance Center - (National) **Don't be tricked by scams that use your financial information to commit fraud.** The Identity Theft Assistance Center (ITAC) released a report in which it warns consumers of three of the most common scams involving personal information and access to financial accounts. “Everyone should have a healthy dose of skepticism when it comes to responding to urgent requests for personal information or access to your financial accounts,” said ITAC’s executive director. The official further discussed the three most common methods used by fraudsters to steal personal and financial information: phishing, which involves emails leading to counterfeit websites; pretexting used by people posing as some type of representative and trying to obtain Social Security numbers, driver license, financial accounts, etc; and fake checks, which are usually sent on behalf of non-existent lotteries, foreign businesses, and work-at-home offers. Source:

http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20071016005136&newsLang=en

October 15, The Associated Press - (National) **TSA laptops with personal info missing.** Two laptop computers containing the names, addresses, birthdays, commercial driver’s license numbers and, in some cases, Social Security numbers of 3,930 people, are missing and considered stolen. The information pertained to drivers participating in the Hazardous Materials Endorsement Threat Assessment, which collects information for security-clearance purposes from commercial drivers across the country, who transport hazardous materials. The two computers were in the possession of a contractor working for the Transportation Security Administration (TSA). The TSA spokesman said that none of the information on the computers has been misused yet. Some were outraged at the news of the security breach, especially on the eve of the new Transportation Worker Identification Credential (TWIC) program, according to which 750,000 employees with access to port areas will have to undergo background checks. However, the spokesman stated that the TWIC program will run through TSA computers, not the contractor’s. Source:

http://ap.google.com/article/ALeqM5jVsOSGHmxE5jv_4QU9UxSKo2ggQOD8S9TH7G2

October 16, Computerworld – (National) **Newest Windows update snafu puzzles Microsoft.** For the second time in a month, Microsoft Corp. has had to defend Windows Update against charges that it upgraded machines without users’ permission. So far, it has no explanation for the newest instance of unauthorized updating. In a post published late Friday to a company blog, the program manager for Microsoft Update denied that Windows’ update mechanism was to blame for reports of settings being changed without user interaction, updates downloading and installing, and systems rebooting. “We have received some logs from customers and have so far been able to determine that their AU [Automatic Update] settings were not changed by any changes to the AU client itself and also not changed by any updates installed by AU,” he said. Claims started to trickle in shortly after the rollout last Tuesday of multiple security patches that machines running Windows Vista had updated on their own, even though users had set Automatic Update to require their approval before downloading and/or installing patches. Some users also reported that machines had rebooted, which caused data loss in applications that had been left open. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042759&intsrc=hm_list

October 15, Computerworld – (National) **Researcher posts unofficial patch for Windows URI bug.** A researcher beat Microsoft to the patch punch Sunday by publishing an unofficial fix for a critical flaw in Windows XP and Server 2003 on PCs with Internet Explorer 7. KJK::Hyperion, a.k.a. “Hackbunny,” a researcher believed to live in Italy, posted a link to the 16KB patch on both his Web site and the Full Disclosure security mailing list Sunday. KJK’s patch, dubbed “ShellExecuteFiasco,” blocks the execution of malformed URLs



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



and forces normalization of valid URLs. URL normalization, which can include tasks such as changing a URL to all-lowercase and stripping out the "www" part of the address, is a technique used by search engines to reduce indexing of duplicate pages. Users, who apply the patch, do so at their own risk, KJK warned. "The present patch is dramatically under-tested and it has undergone [sic] no quality assurance procedure whatsoever, so please deploy with the greatest care," he said in the notes accompanying the fix. "It has a very good chance of misbehaving and making your system unusable." His patch targets the URI (Universal Resource Identifier) vulnerability that Microsoft acknowledged last week. On Thursday, the company's security group issued an advisory that spelled out the problem, which could allow attackers to compromise systems running Internet Explorer 7 if users clicked on malicious links embedded in e-mail messages or posted on a Web page. Microsoft also said it would release a fix, but would not commit to a schedule. The unsanctioned patch can be downloaded from KJK's Web site. Source: http://www.infoworld.com/article/07/10/15/Researcher-posts-unofficial-patch-for-Windows-URI-bug_1.html

October 15, Computerworld – (California) **Governor vetoes bid to make retailers liable for banks' breach-related expenses.** In a move that is likely to come as a major relief to retailers nationwide, California's governor on Saturday vetoed legislation that would have made merchants in his state financially liable for the costs incurred by financial institutions because of retail data breaches. In a statement explaining his reasons for refusing to sign the bill, formally known as AB 779, the official said that it "attempts to legislate in an area where the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers." The measure, which was approved last month by both the California State Assembly and Senate, would have required retailers in California that get hit by data breaches to reimburse banks and credit unions for the cost of alerting customers and reissuing credit and debit cards. It would also have prohibited merchants from storing specific types of authentication data taken from the magnetic stripes on the back of payment cards, while requiring the use of so-called strong authentication technologies for protecting cardholder data. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042630&intsrc=hm_list

October 16, IDG News Service – (National) **Google testing YouTube antipiracy system.** Google has unveiled a test version of a much-awaited antipiracy system for its wildly popular yet controversial YouTube video-sharing site. The system, called Video Identification, has been far from a secret. Google executives have been mentioning its development since the company acquired YouTube in November of last year. YouTube, which lets people upload and share clips, is the most popular video site, but some angry video owners have taken the company to court alleging copyright infringement. The best-known plaintiff is global media conglomerate Viacom, which sued Google in March for \$1 billion over the unauthorized uploading of video clips from its TV shows and movies. In its complaint, Viacom alleged that, as of March, almost 160,000 of its video clips had been uploaded to YouTube without permission and had been viewed over 1.5 billion times. The antipiracy system became news in July, when an attorney representing Google in the Viacom case said during a routine hearing that Video Identification would be ready by September. When describing the system, Google has consistently stressed that it will not block videos from being uploaded, but rather take action, if necessary, after they have been added to the YouTube site. In other words, Google has never planned to place uploaded videos in a holding queue while it checks whether they can be made available on YouTube. Instead, Google will match uploaded clips against a repository of legitimate videos provided by their owners using digital fingerprinting technology and will take whatever action the copyright owner has requested, such as removing the clip or leaving it up on YouTube. It remains to be seen whether this highly anticipated system will help to appease those video content owners, who argue that YouTube does not do enough to prevent and combat piracy on its site and that instead it profits from the unauthorized and illegal uploading of copyright clips. Source: http://www.infoworld.com/article/07/10/16/Google-testing-YouTube-antipiracy-system_1.html

October 15, IDG News Service – (National) **Apple faces potential environmental lawsuit.** The Center for Environmental Health on Monday said that it has given Apple 60 days' legal notice -- a step required by California law before a lawsuit is launched. The action is based on the report by environmental group Greenpeace released earlier Monday that found hazardous materials in Apple's iPhone. The Greenpeace tests revealed chemicals that included "phthalates" in the vinyl plastic earphone wiring at levels that are prohibited in young children's toys in San Francisco and the European Union (EU). Under California's Proposition 65 law, products that can expose consumers to phthalates or other chemicals that are reproductive toxins or carcinogens must carry a warning label, according to the Center for Environmental Health. Apple representatives were not immediately available for comment on the lawsuit or the Greenpeace report. Source: http://www.infoworld.com/article/07/10/15/Apple-being-sued-based-on-Greenpeace-report_1.html

October 17, IDG News Service—(New York; National) **Facebook to beef up safety.** Facebook will step up the policing of pornography, harassment, and inappropriate behavior on its social networking site, settling a consumer fraud investigation by the attorney general



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



(AG) of New York State. Facebook users can now report complaints about pornography, harassment, or inappropriate contact either by clicking on links on the Web site or by sending e-mail to the abuse@facebook.com address. The company will respond to these complaints within 24 hours, and it will allow an independent examiner appointed with the approval of the New York AG, to monitor the company's compliance for the next two years. The social networking site has been in hot water with attorney generals throughout the U.S. over perceptions that it is a haven for pornography and sexual predators. Late last month, the New York AG's office subpoenaed Facebook documents and sent its CEO a letter detailing preliminary findings of an investigation into Facebook's safety measures. Investigators posing as minors on Facebook were repeatedly solicited by adult predators, and the site did a poor job of responding to complaints from investigators posing as minors or their parents, the AG's office said. Source:

http://www.infoworld.com/article/07/10/17/Facebook-to-beef-up-safety_1.html

October 17, IDG News Service – (National) **Feds question intelligence of crybaby typosquatting convict.** A so-called typosquatter, who served pornographic advertisements on domains such as Bobthebiulder.com and teltubbies.com, has been fined again by the Federal Trade Commission (FTC). John Zuccarini has agreed to give up \$164,000 in typosquatting revenue he is alleged to have raked in, the FTC said Tuesday in a statement. Five years ago, a federal court had barred Zuccarini from registering domains that are misspellings of legitimate brands, a practice called typosquatting, but he ignored the order, according to a staff attorney with the FTC. "He was engaging in practices that violated certain provisions of the order," she said. "He had certain domain names that were transpositions or misspellings of popular domain names." After his 2002 settlement, Zuccarini tearfully pled guilty in 2003 to typosquatting and child pornography charges brought by the U.S. Attorney for the Southern District of New York. However, he resumed the domain name registration scam after being released from prison in late 2005. This time around, however, his hundreds of Web sites were used to advertise legitimate products rather than pornography. "I seemed like he was linking his domain names to affiliate marketing programs where they had all sorts of ads," she said. Though typosquatting has been illegal in the U.S. for about 10 years, the government has been largely unable to crack down on the practice because typosquatters often operate outside of federal jurisdiction. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042944&intsrc=hm_list

October 16, Computerworld – (National) **Storm botnet divides, preps for sale to spammers.** The hackers behind the pernicious, persistent Storm Trojan are getting ready to slice off pieces of the botnet created by their malware so that they can "sell" the compromised computers to spammers and denial-of-service attackers, a researcher said today. That is the most likely explanation for the encryption added to secure the command-and-control traffic between the bot herder and some bots, said a senior security researcher at SecureWorks Inc. According to this specialist, who has closely tracked Storm since its debut in January, the newest variants include a 40-byte key that encrypts the command traffic. Unlike other bot-building Trojans, Storm uses peer-to-peer (P2P) rather than IRC (Internet Relay Chat) to receive commands, a tactic that has made its bots harder to take down. "One possibility is that they're splitting [the botnet] and selling off individual botnets to spammers," he said. "If they're going to sell, they need to have it so each botnet is on a separate network. The easiest way to do that is to scramble the peer-to-peer Overnet traffic." Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042883&intsrc=hm_list

October 16, The Associated Press – (International) **Cisco cooperating with Brazil tax evasion investigation.** Cisco Systems Inc., the world's largest manufacturer of computer network equipment, said it is cooperating with Brazilian authorities who raided offices across the country to break up an alleged tax evasion scheme. Police refused to name which company may have benefited from the plot, but a police statement described the firm as an "American multinational, leader in the sector of high-technology services and equipment for corporate networks, Internet and telecommunications." A Cisco spokesman said the company is "cooperating fully with the investigation" but declined to say whether Cisco's Brazilian facilities had been raided Tuesday, or if any Cisco executives were among those arrested by police. "We are currently in the process of establishing what exactly has happened and cannot comment further until we have more information," he said in an e-mail. About 650 police and tax agents executed 93 search warrants Tuesday, arresting 40 people involved in an alleged ring to help the unnamed U.S. company avoid import, sales and corporate taxes, the federal police statement said. Tax agents also seized \$10 million in merchandise, a commercial jet and 18 vehicles in the raids, tax officials said in a separate statement. The scheme, allegedly set up by Brazilian businessmen to benefit the U.S. firm, prompted a two-year police investigation that focused on at least \$500 million in products shipped to Brazilian clients from tax havens like Panama, the Bahamas and the British Virgin Islands, in order to avoid local taxes, the police statement said. Those goods could have generated \$833 million in tax revenue for the Brazilian government, police said. Source: http://www.iht.com/articles/ap/2007/10/16/business/LA-FIN-Brazil-Cisco.php?WT.mc_id=rssap_business



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



October 17, IDG News Service—(New York; National) **Facebook to beef up safety.** Facebook will step up the policing of pornography, harassment, and inappropriate behavior on its social networking site, settling a consumer fraud investigation by the attorney general (AG) of New York State. Facebook users can now report complaints about pornography, harassment, or inappropriate contact either by clicking on links on the Web site or by sending e-mail to the abuse@facebook.com address. The company will respond to these complaints within 24 hours, and it will allow an independent examiner appointed with the approval of the New York AG, to monitor the company's compliance for the next two years. The social networking site has been in hot water with attorney generals throughout the U.S. over perceptions that it is a haven for pornography and sexual predators. Late last month, the New York AG's office subpoenaed Facebook documents and sent its CEO a letter detailing preliminary findings of an investigation into Facebook's safety measures. Investigators posing as minors on Facebook were repeatedly solicited by adult predators, and the site did a poor job of responding to complaints from investigators posing as minors or their parents, the AG's office said. Source:

http://www.infoworld.com/article/07/10/17/Facebook-to-beef-up-safety_1.html

October 17, IDG News Service – (National) **Feds question intelligence of crybaby typosquatting convict.** A so-called typosquatter, who served pornographic advertisements on domains such as Bobthebuilder.com and telubbies.com, has been fined again by the Federal Trade Commission (FTC). John Zuccarini has agreed to give up \$164,000 in typosquatting revenue he is alleged to have raked in, the FTC said Tuesday in a statement. Five years ago, a federal court had barred Zuccarini from registering domains that are misspellings of legitimate brands, a practice called typosquatting, but he ignored the order, according to a staff attorney with the FTC. "He was engaging in practices that violated certain provisions of the order," she said. "He had certain domain names that were transpositions or misspellings of popular domain names." After his 2002 settlement, Zuccarini tearfully pled guilty in 2003 to typosquatting and child pornography charges brought by the U.S. Attorney for the Southern District of New York. However, he resumed the domain name registration scam after being released from prison in late 2005. This time around, however, his hundreds of Web sites were used to advertise legitimate products rather than pornography. "I seemed like he was linking his domain names to affiliate marketing programs where they had all sorts of ads," she said. Though typosquatting has been illegal in the U.S. for about 10 years, the government has been largely unable to crack down on the practice because typosquatters often operate outside of federal jurisdiction. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042944&intsrc=hm_list

October 16, Computerworld – (National) **Storm botnet divides, preps for sale to spammers.** The hackers behind the pernicious, persistent Storm Trojan are getting ready to slice off pieces of the botnet created by their malware so that they can "sell" the compromised computers to spammers and denial-of-service attackers, a researcher said today. That is the most likely explanation for the encryption added to secure the command-and-control traffic between the bot herder and some bots, said a senior security researcher at SecureWorks Inc. According to this specialist, who has closely tracked Storm since its debut in January, the newest variants include a 40-byte key that encrypts the command traffic. Unlike other bot-building Trojans, Storm uses peer-to-peer (P2P) rather than IRC (Internet Relay Chat) to receive commands, a tactic that has made its bots harder to take down. "One possibility is that they're splitting [the botnet] and selling off individual botnets to spammers," he said. "If they're going to sell, they need to have it so each botnet is on a separate network. The easiest way to do that is to scramble the peer-to-peer Overnet traffic." Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042883&intsrc=hm_list

October 16, The Associated Press – (International) **Cisco cooperating with Brazil tax evasion investigation.** Cisco Systems Inc., the world's largest manufacturer of computer network equipment, said it is cooperating with Brazilian authorities who raided offices across the country to break up an alleged tax evasion scheme. Police refused to name which company may have benefited from the plot, but a police statement described the firm as an "American multinational, leader in the sector of high-technology services and equipment for corporate networks, Internet and telecommunications." A Cisco spokesman said the company is "cooperating fully with the investigation" but declined to say whether Cisco's Brazilian facilities had been raided Tuesday, or if any Cisco executives were among those arrested by police. "We are currently in the process of establishing what exactly has happened and cannot comment further until we have more information," he said in an e-mail. About 650 police and tax agents executed 93 search warrants Tuesday, arresting 40 people involved in an alleged ring to help the unnamed U.S. company avoid import, sales and corporate taxes, the federal police statement said. Tax agents also seized \$10 million in merchandise, a commercial jet and 18 vehicles in the raids, tax officials said in a separate statement. The scheme, allegedly set up by Brazilian businessmen to benefit the U.S. firm, prompted a two-year police investigation that focused on at least \$500 million in products shipped to Brazilian clients from tax havens like Panama, the Bahamas and the British Virgin islands, in order to avoid local taxes, the police statement said. Those goods could have generated



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



\$833 million in tax revenue for the Brazilian government, police said. Source: http://www.iht.com/articles/ap/2007/10/16/business/LA-FIN-Brazil-Cisco.php?WT.mc_id=rssap_business

October 18, Marketwire – (National) **TCS and Glowlink win \$8 million DoD contract.** TeleCommunication Systems, Inc. (TCS) a global leader in mission-critical wireless communications, and Glowlink Communications Technology, Inc., a premier manufacturer of satellite monitoring equipment, today announced they have won a satellite hardware and services contract valued at approximately \$8 million to support the spectrum management of the Wideband Global SATCOM Satellite (WGS) system and to continue support for the monitoring and service of the Defense Satellite Communications System (DSCS) satellites. This award is a follow-on contract to an earlier award in January valued at about \$700,000 for spectrum management at two Wideband SATCOM Operations Centers (WSOCs). The contract has a three-year period of performance, beginning this month, and is expected to provide approximately \$1 million of products and services before the end of calendar year 2007. WGS offers continuation and augmentation of the services currently provided by the DSCS and the Global Broadcast Service (GBS) Ka services provided by GBS payloads on ultra-high frequency follow-on satellites. WGS is a high-capacity satellite communications system designed to support the warfighter with newer and far greater capabilities than those provided by current systems, yet it is compatible with existing control systems and terminals. Source: <http://money.cnn.com/news/newsfeeds/articles/marketwire/0316842.htm>=

October 18, Computerworld – (National) **States ask for Microsoft oversight until 2012.** A group of state attorney generals urged a federal judge on Tuesday to hold Microsoft Corp. to a 2002 antitrust settlement another five years so that the company cannot stymie embryonic Web 2.0 rivals of its Windows operating system. According to six states -- California, Connecticut, Iowa, Kansas, Minnesota and Massachusetts -- and the District of Columbia, Microsoft could use its Internet Explorer browser as a "chokepoint" to block moves that might unseat Windows' dominant position on the desktop. Although the states had said they would ask for an extension last month in a hearing before a U.S. District Court judge, the motion filed Tuesday formalized the request. Key parts of the consent decree that Microsoft struck with the U.S. Department of Justice and 20 states back in 2002 are scheduled to expire November 12. In August, federal regulators and those from New York, Louisiana, Maryland, Ohio and Wisconsin told the judge that the decree had done its job. The group of five other states plus Washington, D.C., dubbed the California group, disagreed. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043119&intsrc=hm_list

October 17, Techworld – (National) **Backing up clogs enterprise systems.** Backup volumes in many organizations have grown so large that they are causing business disruption by tying up systems, storage, and network capacity and hogging valuable IT resources, according to a recent survey commissioned by storage management software vendor BridgeHead Software. More than half (59 percent) of IT executives said that the volume of data they are forced to backup is disrupting business operations or will do so eventually, according to a survey of 472 IT executives in the U.K. and North America. And the problem is not going away, with 93 percent saying that their routine backup volumes are continuing to increase. The problem is consuming IT resources for long periods with 37 percent admitting that daily backups of primary data now take them more than nine hours, while 19 percent said it took them more than 12 hours. More than two-thirds (84 percent) of those polled felt they could benefit by reducing the volume of data they routinely back up. One of the most effective ways of reducing the pressure on backups is to take information that is static or seldom accessed and archive it off primary storage systems according to BridgeHead Software's CEO. Source: http://www.infoworld.com/article/07/10/17/Backing-up-clogs-enterprise-systems_1.html

October 17, IDG News Service – (National) **Cafe Latte attack steals data from Wi-Fi PCs.** If you use a secure wireless network, hackers may be able to steal data from your computer in the time it takes to have a cup of coffee. At the Toorcon hacking conference in San Diego this coming weekend, a security researcher will demonstrate a technique he has developed to attack laptops that use the WEP encryption system to log on to secure wireless networks. Developed in the late 1990s, WEP was the default method of securing Wi-Fi networks. Though the WPA (Wi-Fi Protected Access) system replaced it, about 41 percent of businesses continue to use WEP. That percentage is even higher among home users, security experts say. That is unfortunate because WEP has been riddled with security problems. In fact, WEP was blamed for the recent TJX Companies data breach in which thieves were able to access 45 million credit- and debit-card numbers. To date, however, researchers have tended to focus on exploiting WEP flaws in order to break into wireless networks. That generally meant that the attacker would roll up near the WEP-encrypted router, crack the WEP key used to encrypt network traffic, and then log on to the network. The researcher, a senior wireless security researcher with AirTight Networks, has taken a look at the client side of things and developed a way of tricking a WEP-enabled client into thinking that it is logging on to a network that it already knows. His technique, which he calls the Cafe Latte attack, allows an attacker to circumvent firewall protection



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



and attack the laptop or to set up a “man in the middle” attack and snoop on the victim’s online activity. “Until now, the conventional belief was that in order to crack WEP, the attacker had to show up at the parking lot,” he said. “With the discovery of our attack, every employee of an organization is the target of an attack.” Source: http://www.infoworld.com/article/07/10/17/Cafe-Latte-attack-steals-data-from-Wi-Fi-PCs_1.html

October 17, IDG News Service – (National) **Couple swarmed by SWAT team after 911 ‘hack.’** A Washington State teenager is facing 18 years in prison on charges that he used his computer to access Orange County, California’s 911 emergency response system and convinced the sheriff’s department into storming an area couple’s home with a heavily armed SWAT team. The nineteen-year-old, of Mulkiteo, Washington is not only facing charges of unauthorized computer access, but he is also facing assault charges by proxy, meaning that authorities want Ellis to be convicted as if he, and not the SWAT (Special Weapons And Tactics) team, pointed weapons at the victims. The incident took place late in the evening of March 29, when Ellis allegedly used his computer to call the Orange County 911 dispatch and, during the course of a 38-minute telephone conversation, convinced dispatchers that he had murdered someone on the premises and was about to do it again. Within minutes, fire, police and a helicopter team had been dispatched to the home of the Lake Forest, California couple, whom authorities declined to identify. A spokeswoman with the Orange County District Attorney’s office characterized the suspect as a “computer hacker,” but declined to explain exactly how the attack was carried out. “One of the reasons that we’re not disclosing exactly how he did it is because we don’t want to teach other computer hackers how to do it,” she said. Still, it is not clear that Ellis’s alleged hack involved anything more complicated than tricking the 911 system into thinking he was calling from the Lake Forest couple’s number. County officials said Wednesday that he did not exploit a technical flaw in the 911 system’s software. Authorities said that the suspect had made nearly 200 fake 911 calls to dispatch systems in California, Arizona, Washington and Pennsylvania. He is set to be arraigned Monday in Santa Ana, California. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043098&intsrc=hm_list

October 18, Government Executive – (National) **Tighter security over power plant computer systems urged.** Current regulations to protect the control systems that support power plants nationwide fall short of federal recommendations, posing a serious threat to electric infrastructure and national security, witnesses testified at a hearing before the House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology on Wednesday. One lawmaker threatened legislation if standards do not improve. The hearing was prompted by a simulation that highlighted vulnerabilities in the computers that run water, power and chemical plants. In the March Aurora Generator test, researchers from the Idaho National Laboratories created a video for the Homeland Security Department simulating a cyberattack on a power plant’s control system. The attack caused a generator to self-destruct. The government and industry experts who testified cited flaws in regulations set by the North American Electric Reliability Corporation (NERC). Certified as the electric reliability organization by the Federal Energy Regulatory Commission on July 20, 2006, NERC is charged with improving the reliability and security of the bulk power system in North America through the development and enforcement of reliability standards. Recognizing weaknesses in these standards, the National Institute of Standards and Technology (NIST) released recommendations of its own for the IT security of networked digital control systems used in industrial applications. One senator said that NERC standards focus on the bulk power system as a whole, but do not properly address the threat of regional outages or the security of the IT components that support the electric grid. Source: http://www.govexec.com/story_page.cfm?articleid=38319&dcn=todaysnews

October 19, The Union Leader - (New Hampshire) **AG alerts consumers to possible e-mail scam.** New Hampshire’s attorney general (AG) released a warning of a scam involving a fake home heating refund. The fraudster sends an email entitled “urgent notification” saying that the recipient should click on a link in the message to receive \$480.58 from the U.S. Department of Energy. However, those who follow the instructions and go to the attached link expose their computer to a virus allowing the hacker to trace personal information. The AG advised consumers to be suspicious of this type of email and to verify the message with the business or agency in question. Government agencies do not contact people via email. Source: <http://www.msnbc.msn.com/id/21373715/>

October 19, E-Security Planet – (National) **Code Green brings data loss prevention to SMBs.** A new Data Loss Prevention (DLP) appliance has been launched by Code Green Networks Inc. of Santa Clara, California. The new CI-750 appliance enables small offices with 50-250 users and distributed enterprises to protect sensitive data leaving the organization. The company’s founder says small businesses face identical challenges as larger organizations in terms of protecting confidential data and safeguarding intellectual property - including having to comply with the same federal and state regulations and guidelines as organizations with more resources at their disposal. This is especially true with new guidelines set forth by the Federal Trade Commission (FTC) for protecting personal



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



information, and recent amendments to the Federal Rules of Civil Procedure (FRCP) regarding the protection of electronic communications for e-Discovery purposes. However, unlike their large enterprise counterparts, small businesses typically do not have in-house security experts or compliance officers advising them on what they should be doing to secure their data. As a result, they are not quite in step with their larger industry counterparts when it comes to deploying technology and instituting and enforcing data protection policies. The appliance costs \$10,000, which the company's owner says is a price point intended for small businesses.

Source: <http://www.esecurityplanet.com/prevention/article.php/3706186>

October 19, Computer World – (National) **Attacks exploiting RealPlayer zero day in progress.** Attackers are exploiting a zero-day vulnerability in RealPlayer in order to infect Windows machines running Internet Explorer, Symantec Corp. said late Thursday. The security company issued an alert that rated the threat with its highest possible score. According to a warning issued to customers of its DeepSight threat network, Symantec said an ActiveX control installed by RealNetworks Inc.'s RealPlayer program is flawed. When combined with Microsoft Corp.'s Internet Explorer (IE) browser -- which relies on ActiveX controls to extend its functionality -- the bug can be exploited and malicious code downloaded to any PC that wanders to a specially crafted site. Only systems on which both RealPlayer and IE have been installed are vulnerable. Symantec also referenced a blog that had posted some information about the RealPlayer vulnerability Wednesday morning. The blogger, identified only as Roger, claimed that the NASA space agency has warned workers not to use IE because of an unspecified problem with RealPlayer. Roger quoted from what he claimed was a NASA bulletin. "The malware appears to be spreading through a large variety of common and highly-respected Internet sites," the NASA warning reportedly said. "However it does not appear these sites are themselves infected. The affected sites are serving solely as a mechanism to attract potential victims." NASA's public affairs team at the Ames Research Center in northern California was not available for comment Thursday night. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043319&intsrc=news_ts_head

October 19, BBC – (International) **Mobile phone use backed on planes.** Cellular phone use is currently prohibited on planes because there is evidence that it interferes with onboard communication and navigation systems. Research published in 2003 found that mobile phone signals skewed navigation bearing displays by up to five degrees. But now, regulators around Europe are calling for consultation on the potential introduction of a technology that permits mobile calls without risk of interference with aircraft systems. If given the go ahead, the service would allow calls to be made when a plane is more than 3,000 meters high. Individual airlines would then decide if they wanted to introduce the technology. The European Union has recommended to member states that the plan go ahead and space on the airwaves has been reserved for the technology. The proposed system utilizes an on-board base station in the plane which communicates with passengers' own handsets. The base station - called a pico cell - is low power and creates a network area big enough to encompass the cabin of the plane. The base station routes phone traffic to a satellite, which is in turn connected to mobile networks on the ground. A network control unit on the plane is used to ensure that mobiles in the plane do not connect to any base stations on the ground. It blocks the signal from the ground so that phones cannot connect and remain in an idle state. The regulator said that the technology could be implemented next year. Source: <http://news.bbc.co.uk/2/hi/technology/7050576.stm>

October 18, The Star Tribune – (Minnesota) **Globalstar signs agreement to increase satellite messaging capacity to 10 times and further expand Simplex data coverage.** Globalstar, Inc., a provider of mobile satellite voice and data services to businesses, governments, and individuals, today announced that Radyne Corporation business unit AeroAstro will supply Globalstar with the necessary network upgrades that will enhance both the receiver sensitivity and the overall customer messaging capacity of the Globalstar Simplex data network. According to the recently signed agreement, AeroAstro will provide Globalstar with the ground network upgrades needed to expand the current subscriber messaging capacity of the Globalstar Simplex data network by 10 times and increase receiver sensitivity of the network by up to 40 percent. Increased receiver sensitivity will further expand the geographic coverage area of Globalstar's gateway earth stations and is expected to improve Simplex message transmission reliability, which already exceeds 99 percent in the gateways' primary coverage area. Deliveries of the necessary upgrades are scheduled to begin in early 2008. Globalstar's Simplex data network is used to support a variety of aviation flight-following, emergency asset, fleet and personal tracking applications. Simplex data modem integrated solutions are also used for a number of remote monitoring and alarm applications, both within and beyond the reach of traditional wireless and terrestrial infrastructure. Information such as GPS location coordinates, remote status and other sensor information can be sent to customers using the Globalstar Simplex network. Source:

<http://money.cnn.com/news/newsfeeds/articles/primenewswire/129109.htm>



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



October 22, The Associated Press – (National) **Study IDs identity thieves.** A study conducted by the Center for Identity Management and Information Protection at Utica College and funded by the Department of Justice revealed that approximately 3 million Americans are victims of identity theft every year. The study, which analyzed cases between 2000 and 2006, also found that “42.5 percent of offenders were between the ages of 25 and 34, another 18 percent were between the ages of 18 and 24, two-thirds of the identity thieves were male, and nearly a quarter of the offenders were born outside the United States.” Moreover, “eighty percent of the cases involved an offender working solo or with a single partner,” the report found. It seemed that most of the methods used by fraudsters did not involve the internet. A large percentage said they only stole “fragments of personal identifying information, as opposed to stealing entire documents, such as bank cards or driver’s licenses.” The study also found that “insider” employees were the offenders in just one-third of the cases. Employees who stole identity information often worked in the retail industry, the report found. Source: http://news.yahoo.com/s/ap/20071022/ap_on_re_us/identity_theft_study;_ylt=AmOIs50Fmlrhf28iRm0xx5as0NUE

October 21, The Associated Press and The Dallas Morning News – (National) **Grocery chain loses \$10 million in e-mail scam.** Supervalu, a Minnesota-based supermarket chain, received two emails from people posing as American Greetings Corp. and Frito-Lay employees, who asked payments to be sent to new bank accounts. The store complied and wired \$6.5 million to the fake American Greetings account and almost \$3.6 million to the phony Frito-Lay account. Fortunately, the F.B.I. intercepted the transaction before it was finalized and captured the money. However, American Greetings, Frito-Lay and Supervalu are now disputing which company should receive the money. No one has been charged yet. Source: http://www.dallasnews.com/sharedcontent/dws/bus/stories/DN-supervalu_22bus.State.Edition1.27d66b9.html

October 22, IDG News Service – (National) **With attack code circulating, RealPlayer fix coming.** One day after Symantec researchers discovered software that attacked a critical unpatched vulnerability in RealNetworks’ media player, Real says that a fix for the issue is imminent. “Real has created a patch for RealPlayer 10.5 and RealPlayer 11 that addresses the vulnerability identified by Symantec,” wrote RealNetworks General Manager of Product Development in a Friday blog posting. “Real will make this patch available to users via this blog and our security update page later today,” he said. Users of RealOne Player, RealOne Player v2, and RealPlayer 10 should upgrade to the 10.5 version of the product or the RealPlayer 11 beta code and should install the patch, he said. The attack exploits a flaw in an ActiveX browser helper object, software that RealPlayer employs to help users who are experiencing technical difficulties, so the PC must be using the Internet Explorer browser to be affected by this particular attack, Symantec said. The attack only works on Windows systems, RealNetworks said. Linux, Mac and RealPlayer 8 users are not affected. Attackers were using a complicated network of advertising Web sites to launch the attack from a Web site that has been spotted hosting malicious code several times over the past two years, Symantec said. Users who do not have the patch can turn off ActiveScripting within IE as a workaround to the problem. Very technical users can also set kill bit on the Class identifier (CLSID) FDC7A535-4070-4B92-A0EA-D9994BCC0DC5 to disable the ActiveX control, Symantec said. Source: http://www.infoworld.com/article/07/10/22/RealPlayer-fix-coming_1.html

October 22, Computerworld – (California) **IT staff acts as wildfire advances on Pepperdine’s data center.** The CIO of Pepperdine University had little warning that a wildfire was soon to threaten the campus’ data center when he woke without power at 5 a.m. Sunday. Within a matter of hours, brush fires came within 100 feet of the data center -- and there was a point, he said, where “we had serious concern that the data center itself was going to be jeopardized.” The CIO quickly left for the data center and, as he drove to it, could see light from the fire on the other side of a ridge. Other administrators were responding as well, and by 5:30 a.m., the campus administration had called a meeting of the university’s Emergency Operations Committee. Wildfires are an ongoing threat in the area, and the university is prepared for that contingency, as well as other threats. It routinely sends its backup tapes to Iron Mountain Inc. for protection. In addition, the latest tape backup copies were moved to a fireproof safe. The ERP applications were shut down, and the hard drives were removed and also safely stored. All that work was completed in 35 minutes, he said. It was still before 8 a.m. While the IT staff scrambled, the fire advanced toward the data center building and nearby university administration building. Firefighters from Los Angeles County and other jurisdictions acted immediately. There were about 25 firefighters in the way of the advancing fire “whose entire goal was to protect the buildings,” he said. “They were able to contain those fires and keep them from spreading further,” he said. Pepperdine’s University Data Center never went offline, ensuring the campus of network services, including voice communications. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043421&intsrc=hm_list

October 21, IDG News Service – (National) **Storm Worm now just a squall.** The Storm Worm’s days may be numbered, according to a University of California researcher. The researcher said that, despite the intense publicity that the Storm network of infected



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



computers has received, it has actually been shrinking steadily and is a shadow of its former self. On Saturday, he presented his findings at the ToorCon hacker conference in San Diego. Storm is not really a computer worm. It is a network of computers that have been infected via malicious e-mail messages and are centrally controlled via the Overnet peer-to-peer protocol. The researcher said he has developed software that crawls through the Storm network and thinks that he has a pretty accurate estimate of how big Storm really is. Some estimates have put Storm at 50 million computers, a number that would give its controllers access to more processing power than the world's most powerful supercomputer. But the real story is significantly less terrifying, he said. In July, for example, he said that Storm appeared to have infected about 1.5 million PCs, about 200,000 of which were accessible at any given time. He guessed that a total of about 15 million PCs have been infected by Storm in the nine months it has existed, although the vast majority of those have been cleaned up and are no longer part of the Storm network. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043419&intsrc=hm_list

October 19, CNN – (International) **Official: International hackers going after U.S. networks.** About 140 foreign intelligence organizations are trying to hack into the computer networks of the U.S. government and U.S. companies, a top counterintelligence official said. The national counterintelligence executive told CNN it is not accurate to blame only the Chinese government for recent penetrations of government computer systems. Because it is easy for hackers to disguise where an attack originates, he said, the best course of action is to tighten up one's own networks rather than to place blame. The nation's electronic systems are too easy to hack, and the number of world-class hackers is "multiplying at bewildering speed," he said. That, he said, has transformed the nature of counterintelligence: "If you can exfiltrate massive amounts of information electronically from the comfort of your own office on another continent, why incur the expense and risk of running a traditional espionage operation?" He also warned that hackers could create chaos by manipulating information in electronic systems the government, military and private industry rely on. "Our water and sewer systems, electricity grids, financial markets, payroll systems, air and ground traffic control systems ... are all electronically controlled, electronically dependent, and subject to sophisticated attacks by both state-sponsored and freelance terrorists," he said. The government must develop a better system for warning the private sector and universities about attacks, he said, and some laws might need to change: "We've got to rethink the adequacy of our legal authorities to deal with the cyber thieves and the vandals who I call the Barbary pirates of the 21st century." Source: <http://www.cnn.com/2007/US/10/19/cyber.threats/index.html>

October 21, IDG News Service – (National) **AT&T sues Vonage for patent infringement.** - AT&T Inc. on Friday filed a lawsuit against voice-over-IP (VoIP) provider Vonage Holdings Corp. seeking damages for alleged patent infringement. The lawsuit comes just days after Vonage settled a patent-infringement lawsuit with telecommunications provider Sprint Nextel Corp. In a filing with the U.S. District Court for the Western District of Wisconsin, AT&T alleged that Vonage willfully infringed an AT&T patent related to telephone systems that allow people to make VoIP calls using standard telephone devices. In the legal filing, AT&T said it tried to reach an agreement with Vonage to license the patent but failed, which forced the lawsuit. Vonage announced on October 8 that it settled its suit with Sprint Nextel for \$80 million. As part of that agreement, Vonage agreed to license VoIP patents from Sprint, including more than 100 patents covering technology for connecting calls from a traditional phone network to an IP network. Vonage is also in the process of resolving a patent-infringement dispute with Verizon Communications Inc. Earlier this year, a court found that Vonage had infringed on Verizon patents and ordered an injunction that could have prevented Vonage from signing up new customers. Vonage won an injunction staying the order and is appealing the original infringement ruling. Vonage in August said it was close to rolling out work-arounds for two of the three patents Verizon claimed. Vonage is one of the largest independent VoIP providers in the U.S., with nearly 2.5 million customers. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9043420&taxonomyId=17&intsrc=kc_top

October 20, RCR Wireless News – (National) **FTC works to quash call list urban legend.** The Federal Trade Commission (FTC) faces a dilemma as it once again attempts to kill a wireless urban legend that just won't die. "The Federal Trade Commission today reiterated that despite the claims made in e-mails circulating on the Internet, consumers should not be concerned that their cellular phone numbers will be released to telemarketers in the near future, and that it is not necessary to register cellular phone numbers on the national Do Not Call Registry to be protected from most telemarketing calls to cellular phones," the agency stated. While the Do Not Call list accepts registrations of landline and wireless numbers alike, the Federal Communications Commission has a permanent ban on telemarketers using automated dialers to call cellular phone numbers. There are 145 million wireline and wireless numbers in the registry. The FTC has repeatedly posted "The Truth about Cellphones and the Do Not Call Registry" advisory several times since the program was crafted by the Federal Communications Commission and FTC in 2003. The agencies attribute rumors about



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



telemarketers getting their hands on mobile-phone numbers and other falsehoods associated with the Do Not Call registry to an industry effort aborted several years ago to launch a wireless 411 directory. The FTC does not presently highlight the fact that under current law consumers must re-register with the Do Not Call Registry. The reason is the agency does not know whether legislation to make the registry permanent will be approved by Congress this year. In the meantime, an FTC spokesman said a major campaign to remind consumers to re-register will be rolled out in early 2008 if lawmakers fail to get legislation approved. Source:

<http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20071020/SUB/71019016/1005>

October 22, WIBW – (Kansas) **Alert: credit card scam.** Kansas's Attorney General's office released a warning of a scam involving people calling and claiming that the recipient's credit card record shows an unusual purchase. They gain the victim's trust by saying they know the name and the last four digits of the recipient's social security number. Subsequently, they ask for the credit card three-digit code in order to get rid of the purchase. The officials warn people not to give their code numbers because the scammers probably have their credit card information, but need the three-digit code to make purchases. Source:

<http://www.wibw.com/home/headlines/10730386.html>

October 22, The Houston Chronicle – (Texas) **Agency says seniors being targeted by medical ID scam.** The program director with the Houston's Better Business Bureau Education Foundation announced Monday that her office received reports of scammers targeting seniors by posing as telemarketers. The fraudsters claim that the seniors' Medicare cards are no longer valid and that they need to sign up for a new one. Then, they ask for a bank account number and when they are refused "they yell at people, they tell them they are stupid and will call back repeatedly in hopes of scaring the seniors into giving out their banking information," according to the director. Source: <http://www.chron.com disp/story.mpl/metropolitan/5236214.html>

October 23, IDG News Service – (National) **ID thieves have a 50-50 chance of going to prison.** If you are a convicted identity thief, you have about a 50 percent chance of avoiding jail. That is one of the findings of a new study of closed U.S. Secret Service case files, released Monday by Utica College's Center for Identity Management and Information Protection. This is the first time researchers have been allowed to sift through the Secret Service's data. The study's authors based their findings on an analysis of 500 closed Secret Service cases. "Prosecutors had a slightly better chance of sending a convicted identity thief to prison than not (51 percent) and could expect to see the imprisoned offender sentenced to three years or less of incarceration," the report said. The college has been working with a number of partners, including the Secret Service, IBM, and the Federal Bureau of Investigation, since the Center's creation in mid-2006 to study the methods used by ID thieves and to help corporations and law enforcement prevent this type of crime. Technology like printers, mobile phones, and computers were used in about half of the cases, but the Internet was the exclusive tool of ID thieves only about 10 percent of the time. The median loss from identity theft was just over \$31,000, but in one case, investigated by the Secret Service's Dallas field office, the defendant spent millions on luxury vehicles and then managed to set up shell companies and defraud investors. Losses totaled \$13 million. "In general," however, "the more offenders involved in the case, the higher the victim loss," the study stated. According to Javelin Strategy & Research, identity theft cost U.S. businesses and consumers an estimated \$49.3 billion in 2006. Source: http://www.infoworld.com/article/07/10/23/ID-thieves-50-50-chance-of-prison_1.html

October 23, The Associated Press – (International) **British, Dutch police close pirate site.** British and Dutch police shut down what they say is one the world's biggest online sources of pirated music Tuesday and arrested the Web site's 24-year-old suspected operator. The invitation-only OiNK Web site specialized in distributing albums leaked before their official release by record companies, the International Federation of the Phonographic Industry said. Many among OiNK's estimated 180,000 members paid donations "to upload or download albums, often weeks before their release, and within hours albums would be distributed through public forums and blogs across the Internet." Users were invited to the site if they could prove they had music to share, the IFPI said. The IFPI said more than 60 major albums were leaked on OiNK so far this year, making it the primary source worldwide for illegal prerelease music. Prerelease piracy is considered particularly damaging to music sales as it leads to early mixes and unfinished versions of artists' recordings circulating on the Internet months before the release. Police in Cleveland, in northeast England, said they were tracing the money generated through the Web site, expected to amount to hundreds of thousands of dollars. The arrest of a 24-year-old IT worker at a house in Middlesbrough, northeast England, followed a two-year investigation by Dutch and British police and raids coordinated by Interpol. Cleveland police said the man, whose name was not released, was arrested on suspicion of conspiracy to defraud and infringement of copyright law. OiNK's servers, in Amsterdam, were shut down by Dutch police, the IFPI said. Source: http://news.yahoo.com/s/ap/20071023/ap_on_hi_te/britain_pirate_web_site;_ylt=Apf5aM4kxV_81NcBxsmuS0MjtBAF



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



October 22, Computerworld – (Colorado) **Update: World Series ticket sales to resume after Colo. stall.** After a 26-hour delay, the Colorado Rockies baseball team will at last be able to sell its tickets for World Series home games at Coors Field. Sales should begin Tuesday at noon MDT on the Rockies' Web site. When its automated ticketing vendor's servers crashed early Monday morning, the Rockies struck out as they tried to sell tickets to three home World Series games, set to begin on Saturday. "It's been an extremely frustrating day for our fans and the entire Rockies' organization," said the Rockies' team president in a statement. "Our Web site, and ultimately our fans and our organization, were the victim of an external, malicious attack that shut down the system and kept our fans from being able to purchase their World Series tickets." The National League team, which will face the American League champion, the Boston Red Sox, beginning Wednesday night in Boston, had announced last week that it would sell its World Series tickets via an online process to make it fair for all ticket buyers for the first World Series to involve a Colorado team. Only about 500 tickets had been sold online before the outage occurred, 10 minutes after the tickets went on sale Monday. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043598&intsrc=hm_list

October 22, Computerworld – (National) **Adobe patches critical PDF vulnerability.** Adobe Systems Inc. patched its Reader and Acrobat programs Monday to fix a flaw that exposed most Windows XP users to exploits arriving in malicious PDF files. The patches are included in updates to Reader, the for-free PDF rendering utility, and Acrobat, Adobe's full-featured application; both have been tagged as Version 8.1.1. "Critical vulnerabilities have been identified in Adobe Reader and Acrobat that could allow an attacker who successfully exploits these vulnerabilities to take control of the affected system," Adobe warned in the bulletin that detailed the patch availability. "A malicious file must be loaded in Adobe Reader or Acrobat by the end user for an attacker to exploit these vulnerabilities." Only users of Microsoft Corp.'s Windows XP who have Internet Explorer 7 installed are at risk of such attacks, Adobe added. The patches come a little more than two weeks after Adobe acknowledged the bug and posted a complicated work-around that required users to edit the Windows registry. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9043543&taxonomyId=17&intsrc=kc_top

October 23, The Associated Press – (International) **Report: China starts work on first direct undersea cable to US.** A group of phone companies has begun constructing the first undersea telecommunications cable directly linking China with the United States, a news report said Tuesday. The fiber-optic cable will go into operation next July ahead of the Beijing Olympics, the Chinese government's Xinhua News Agency said. The project, dubbed the Trans-Pacific Express, comes amid explosive growth in telephone and Internet traffic between China and the United States. Its developers say it will have 60 times the capacity of current cable connections between the two countries. Current U.S.-Chinese cable links run through Japan, but Beijing sees Tokyo as a regional rival and has long wanted an independent connection to the United States. Construction of the new cable began Monday in the Chinese coastal city of Qingdao, Xinhua said. Its developers are state-owned China Telecom Ltd., China Netcom Ltd. and China Unicom Ltd., Verizon Communications Inc. of the United States, Taiwan's Chunghwa Telecom Co. and South Korea's KT Corp. The cable is to have connections to South Korea and Taiwan, but none to Japan, according to its developers. Verizon said last year the system would extend more than 18,000 kilometers (11,000 miles) and represent an investment of US\$500 million. The route of the cable is intended to minimize potential disruption from earthquakes by avoiding seismically active areas, Xinhua said. A quake in January severed an undersea cable near Taiwan, disrupting communications throughout Asia. Source:

<http://www.iht.com/articles/ap/2007/10/23/business/AS-TEC-China-US-Sea-Cable.php>

October 22, Newsfactor.com – (National) **Comcast impersonates users to control P2P traffic.** Comcast interferes with peer-to-peer traffic on its cable network by masquerading as users and resetting connections, *The Associated Press* reported on Friday. Apparently in an effort to maintain quality of service, Comcast cut off uploads of files to BitTorrent and other P2P networks. While observers agree that an Internet service provider needs to be able manage its traffic, the way Comcast is going about this -- by impersonating customers -- is troubling to many. "Comcast is in an interesting position because the amount of outbound and inbound traffic is constrained in their network," said the CEO of Sonic.net, a California internet service provider. "In an asynchronous network, as the amount of outbound traffic grows, inbound rates will decrease." Thus in order to maintain service quality for inbound traffic, which is important to all users, Comcast is throttling outbound P2P traffic. But the way Comcast is doing it -- by "injecting TCP resets that are forged as coming from the customer," according to the Sonic.net exec -- is "pretty weird." The *AP* story offered an apt metaphor: it is as if an AT&T operator broke into a phone conversation and impersonated one of the speakers, saying, "I have to go now, goodbye" and closed the connection. "That's a fundamental line that's been crossed," he said. Yet, he added, Comcast might have no choice. "The



Sangamon County Office of Bioterrorism Preparedness

Ray Cooke, MPH, EMT-B, Director, 2801 N Fifth Street, Springfield, Illinois 62702 (217) 971-7331 rayc@co.sangamon.il.us
Melanie Dennison, Chief Editor



peer-to-peer software is so insidious in how it tries to work around throttling, that forging may be the only way to stop the traffic," he said. Source: http://news.yahoo.com/s/nf/56178;_ylt=Aj8vkLHNYtXJLkfgl0T.HrsjtBAF