# THE CYBER SHIELD

*Cyber News for Counterintelligence / Information Technology / Security Professionals*

*29 May 2014*



**Purpose**
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

**Source**
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

**Publisher**
* SA Jeanette Greene
Albuquerque FBI

**Editor**
* CI SA Scott Daughtry
DTRA Counterintelligence

**Subscription**
To receive this newsletter please send an email to scott.daughtry@dtra.mil

**Disclaimer**
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

**NMCIWG Members**
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

**Distribution**
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data


## Survey: Cybercrime on the rise

AP, 28 May 2014: The hackers are winning, according to a survey of 500 executives of U.S. businesses, law enforcement services and government agencies released Wednesday. The 12th annual survey of cybercrime trends found that online attackers determined to break into computers, steal information and interfere with business are more technologically advanced than those trying to stop them. The survey was co-sponsored by San Jose, California-based business consulting firm PwC, the U.S. Secret Service, the CERT Division of Carnegie Mellon University's Software Engineering Institute and CSO security news magazine. Three out of four respondents said they had detected a security breach in the past year, and the average number of security intrusions was 135 per organization, the survey found. "Despite substantial investments in cybersecurity technologies, cyber criminals continue to find ways to circumvent these systems" Ed Lowery, who heads the U.S. Secret Service's criminal investigative division, said in a written statement. Lowery said companies and the government need to take "a radically different approach to cybersecurity," which goes beyond antivirus software, training employees, working closely with contractors and setting up tighter processes. The top five cyberattack methods reported in the survey were malware, phishing, network interruption, spyware and denial-of-service attacks. And 28 percent of respondents said the attackers were insiders, either contractors or current and former employees or service providers, according to the survey. To read more click **HERE**

## Deadline set for Senate action on cybersecurity

The Hill, 28 May 2014: The Senate needs to pass a major cybersecurity bill by August, or else the effort could be lost for the year, House Intelligence Committee Chairman Mike Rogers (R-Mich.) warned on Wednesday. "If we don't have something moving by August, I think it gets lost in the haze, and it will be a very long time until we actually get a bill passed that will actually have an impact," he said at a cybersecurity forum at George Washington University. The Senate has struggled to pass a companion measure to his Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House more than a year ago. Since then, revelations from Edward Snowden about programs at the National Security Agency have derailed the effort and heightened concerns about government snooping. The bill would allow companies to share information about possible cyber threats with each other and the government. President Obama had threatened to veto the bill if it ever came to his desk. Last month, Senate Intelligence Committee Chairwoman Dianne Feinstein (D-Calif.) and ranking member Saxby Chambliss (R-Ga.) announced that they had reached a deal on a draft bill for the upper chamber. The legislation has not yet been formally introduced, but several privacy advocates have voiced similar concerns that they had about the House bill. Rogers on Wednesday said he was "cautiously optimistic that we can find some agreement within the next 30 days to try to get something moving." If the Senate does pass a bill, "I promise you, it will be the fastest conference committee known to man, because I'll be the chairman of it," he added. He said he had hoped that the massive data breach at Target late last year would help convince the public of the need for a new cyber bill, but the backing had not yet materialized. The hack might have exposed 110 million shoppers' personal or financial data, and led the company's chief executive to resign earlier this month. "We were hoping that that would be the catalyst for people to understand just how serious this is," Rogers said. To read more click **HERE**

*May 28, Norfolk Virginian-Pilot* – (Virginia) **Chesapeake tech company CEO charged with bribery.** The founder of now-defunct ACS Systems and Engineering based out of Chesapeake, Virginia, was indicted May 23 for allegedly paying $50,000 in bribes to contractors with Military Sealift Command in exchange for more than $1.1 million in contracts. A second person was charged for allegedly accepting bribes from the former CEO, while five others have already pleaded guilty as part of broader investigation into bribery at the sealift command. Source: http://hamptonroads.com/2014/05/chesapeake-tech-company-ceo-charged-bribery

**12 Quick Internet Safety Tips That Will Save Your Digital Life from Getting Hacked**
Business Insider, 27 May 2014: If we've learned anything about cyber security in 2014, it's that hackers are becoming more of a threat than ever before. Within the past two months companies such as Microsoft, AOL, and eBay have been the victim of security breaches. If you've been laid back about your online habits, now might be a great time to change your ways. Here are some tips to help prevent your digital life from being stolen, whether it is a password breach or an internet-wide vulnerability.

- Make sure you've got a super strong, unique password. In other words, ensure that your password is difficult to guess. One way to come up with a creative password is to brainstorm a random sentence. Take the first letter of each word in that sentence and use that acronym as the base for your password.
- Don't use the same password for multiple services. Using the same term for all of your passwords leaves your entire digital life vulnerable to attack. This means that if a hacker has one password, he or she has all of your passwords.
- Enable two-factor authentication. Many services, including Google, offer two-factor authentication for logging into your account. Instead of simply entering a username and password to log in, the website will prompt you to enter a code sent to your smartphone to verify your identity.
- Apply software updates when necessary. Apple, Google, and Microsoft typically include security bug fixes and patches in their most recent software updates. So don't ignore those annoying prompts and keep your software up-to-date.
- Carefully read the permissions before installing apps. This is one of the most prominent ways in which malicious apps can gain access to your personal information. These types of issues have been especially present in the Google Play store. A lot of apps ask for a lengthy list of permissions, and that doesn't mean they're all ill-intentioned. But it's important to be aware of the types of information your apps are accessing, which can include your contacts, location, and even your phone's camera.
- Check the app publisher before installing. There have been numerous instances in which scammers have published apps in the Google Play store posing as another popular app. For example, in late 2012 an illegitimate developer posted an imposter app in Google Play pretending to be "Temple Run." A quick look at the publisher shows that the app comes from a developer named "apkdeveloper," not the game's true publisher Imangi Studios.
- Avoid inserting hard drives and thumb drives you don't trust into your computer. If you find a random USB stick, don't let your curiosity tempt you to plug it in. Someone could have loaded malware onto it hoping that an interested person was careless enough to insert it into their device. If you don't trust the source, you're better off not putting your computer at risk.
- Make sure a website is secure before you enter personal information. Look for the little padlock symbol in front of the web address in the URL bar. Also, make sure the web address starts with the prefix https://. If these things aren't there, then the network isn't secure and you shouldn't enter any data you wouldn't want made public.
- Don't send personal data via email. Sending critical information such as credit card numbers or bank account numbers puts it at risk of being intercepted by hackers or cyber attacks.
- Keep an eye out for phishing scams. A phishing scam is an email or website that's designed to steal from you. Often times, a hacker will use this email or website to install malicious software onto your computer. These web entities are designed to look like a normal email or website, which is how hackers convince their victims to hand over personal information. Phishing scams are typically easy to spot, but you should know what to look out for. Many of these emails contain spell errors and are written in poor grammar.

*May 27, KMGH 7 Denver* – (Colorado) **Computers with patient test data stolen from Denver VA hospital.** The Veterans Affairs hospital in Denver notified about 239 patients after two bio-medical computers containing data from tests were stolen from a pulmonary lab at the hospital the week of May 19. The pulmonary application data was encrypted while the application itself was password protected. Source: http://www.thedenverchannel.com/news/front-range/denver/computers-with-patient-test-data-stolen-from-denver-va-hospital

*May 27, WBBM 2 Chicago* – (Illinois) **More than 120 iPads stolen from school in Lawndale.** Police are investigating after thieves stole 123 iPads worth nearly $50,000 from Charles Hughes Elementary School in Chicago May 26 by smashing windows in the building. Source: http://chicago.cbslocal.com/2014/05/27/more-than-140-ipads-stolen-from-school-in-lawndale/

*May 28, SecurityWeek* – (International) **Compromised Apple IDs used to hold iPhones for ransom.** Users of Apple mobile devices reported attackers using compromised Apple IDs to enable Lost Mode through Apple's iCloud service, using the service to lock devices and demand a ransom to unlock them. The ransom messages bear the name of an Oracle engineer that was likely chosen at random by the attackers, according to a Symantec researcher. Source: http://www.securityweek.com/compromised-apple-ids-used-hold-iphones-ransom