THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

19 November 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

November 13, U.S. Attorney's Office, Northern District of Ohio – (Ohio) **Stow man charged with cyber crimes.** Authorities unsealed a federal indictment November 13 charging an Ohio man for attempting to install malware on the computer systems of Eaton Corporation while he was employed as a contracted financial analyst in May. The malicious code was discovered after the suspect disclosed its existence to a former coworker. Source: http://www.fbi.gov/cleveland/press-releases/2014/stow-man-charged-with-cyber-crimes

November 14, KING 5 Seattle – (Washington) **Seattle Public Schools security breach impacts thousands of students.** Seattle Public Schools notified the parents of at least 8,000 special education students November 13 of a November 11 security breach involving the private and personal information of their children including names, student identification numbers, and disabilities after a law firm retained by the district inadvertently sent the information to an individual involved in an ongoing case. Source: http://www.king5.com/story/news/local/seattle/2014/11/14/seattle-public-schools-admits-to-security-breach-impacting-thousands-of-students/19012537/

November 17, Softpedia – (International) **BusyBox devices compromised through Shellshock attack.** Researchers with Trend Micro identified a new version of the Bashlite malware that identifies devices on an infected system's network that use the BusyBox software for Linux, including routers, and can then attempt to compromise them using the Shellshock vulnerability. Source: http://news.softpedia.com/news/BusyBox-Devices-Compromised-Through-Shellshock-Attack-465087.shtml

November 17, Softpedia – (International) **Steam password stealer is stored on Google Drive.** A researcher with Panda Security analyzed and reported a piece of malware designed to steal passwords for the Steam gaming service that is being delivered from a Google Drive account. The account was still active when the researcher reported the malware November 16 and targets victims via a fraudulent link in Steam chat that downloads an executable file. Source: http://news.softpedia.com/news/Steam-Password-Stealer-Is-Stored-On-Google-Drive-465107.shtml

November 17, The Register – (International) **Attack reveals 81 percent of Tor users but admins call for calm.** A paper released by researchers at the Indraprastha Institute of Information Technology outlined a traffic confirmation attack method that the researchers stated could be used to identify users of the Tor anonymity network in 81 percent of cases if an attacker has sufficient resources. Source: http://www.theregister.co.uk/2014/11/17/deanonymization_techniques_for_tor_and_bitcoin/

November 17, Securityweek – (International) **Alleged creators of WireLurker malware arrested in China.** Authorities in China arrested three individuals for allegedly creating and distributing the WireLurker malware targeting Mac OS X, iOS, and Windows devices and shut down the Web site used to distribute the malware. Source: http://www.securityweek.com/alleged-creators-wirelurker-malware-arrested-china

November 17, Securityweek – (International) **Majority of top 100 paid iOS, Android apps have hacked versions: Report.** Arxan Technologies released their annual State of Mobile App Security report which found that there were cloned or repackaged versions of 97 percent of the top 100 paid Android apps and 87 percent for top 100 paid iOS apps, and that repackaged or cloned financial services apps existed for 95 percent of apps on Android and 70 percent in iOS, among other findings. Source: http://www.securityweek.com/majority-top-100-paid-ios-android-apps-have-hacked-versions-report

November 16, Softpedia – (International) **New variant of Dofoil trojan emerges with strong evasion features.** Fortinet researchers identified a new variant of the Dofoil botnet malware that contains several changes aimed at preventing the malware from being detected and analyzed. Source: http://news.softpedia.com/news/New-Variant-of-Dofoil-Trojan-Emerges-with-Strong-Evasion-Features-465050.shtml

November 15, Softpedia – (International) **New encryption ransomware offers file decryption trial.** Researchers at Webroot identified a new piece of encryption ransomware dubbed CoinVault that encrypts victims' files using AES-256 encryption, demands a ransom, and offers a free trial of the decryption performed if a ransom is paid. Source: http://news.softpedia.com/news/New-Encryption-Ransomware-Offers-File-Decryption-Trial-465027.shtml

November 14, Softpedia – (International) **Google misses trojan SMS app in Play Store for more than a year.** An SMS trojan named Thai Fun Content was identified by Malwarebytes researchers on the Google Play Store and was available for download for over 1 year. The app subscribes victims to a paid SMS service and charges victims $0.37 per day. Source: http://news.softpedia.com/news/Google-Misses-Trojan-SMS-App-in-Play-Store-for-More-than-a-Year-465005.shtml

November 18, WFXT 25 Boston – (Massachusetts) **BWH doctor tied up in armed robbery; patient data stolen from laptop.** Brigham and Women's Hospital in Boston notified approximately 1,000 patients of a potential privacy breach following the September 24 armed robbery of a doctor where thieves took a laptop and cellphone that contained patients' encrypted personal and medical information. The suspects forced the doctor to give them the pass codes after he was tied to a tree and authorities have two suspects in custody in connection to the robbery. Source: http://www.myfoxboston.com/story/27410047/brigham-womens-warning-of-privacy-breach-after-laptop-stolen

November 18, Securityweek – (International) **New variant of Matsnu trojan uses configurable DGA.** Researchers from Seculert found that a new variant of the Matsnu trojan (also known as Trustezeb) is using a configurable Domain Generation Algorithm (DGA) to attempt to create domain names that won't be detected by phonetic algorithms designed to look for nonsensical domain names. The malware can be instructed to take various actions, including downloading and executing files, updating itself, and reporting its status to its controllers. Source: http://www.securityweek.com/new-variant-matsnu-trojan-uses-configurable-dga

November 17, Securityweek – (International) **Research finds 1 percent of online ads malicious.** Researchers from universities in the U.S., U.K., and Germany presenting at the 2014 Internet Measurement Conference reported that their research looked at 600,000 online advertisements on 40,000 Web sites over a 3 month period and found that 1 percent of advertisements were malicious. Source: http://www.securityweek.com/research-finds-1-percent-online-ads-malicious

The State Department's Reluctance To Disclose Hacking Unsettles Lawmakers

Defense One, November 18, 2014: Lawmakers on both sides of the aisle are demanding answers. State's silence is somewhat at odds with the Obama administration's insistence that critical sectors, which include banking, energy and government, share information about threats and timely disclose breaches of personal information. "I'm troubled by the fact that when federal agencies are hacked, Congress and the public seem to be the last to know," Sen. Tom Coburn, R-Okla., ranking Republican on the Homeland Security and Governmental Affairs Committee told Nextgov. He is pushing for bipartisan legislation that would enforce stronger disclosure rules for these types of cyber events and provide citizens more transparency, Coburn said, "because the American people are often the most impacted by these events." Rep. Elijah Cummings, D-Md., ranking Democrat on the House oversight and government reform committee, sent State Secretary John Kerry a letter requesting more details on the attack. Cummings asked for, among other things, information on how the troublesome activity was first discovered, the manner in which employees were notified of the breach, and the types of data compromised. "The increased frequency and sophistication of cyberattacks upon both public and private entities highlights the need for greater collaboration to improve data security," Cummings said. He recently sent similar letters to hacked companies, including Home Depot, Target, Kmart, and Community Health Systems. After repeated inquiries during the past week, before the breach was made public, State declined to comment on when the incident began, how long it has been going on, and the number of federal employees potentially affected. The incident is one of many breaches with possible effects on federal personnel the government has been slow to disclose. During the past year, the Energy Department, the Office of Personnel Management, the National Oceanic and Atmospheric Administration, the U.S. Postal Service, the Nuclear Regulatory Commission, White House and State waited at least a month, oftentimes longer, to disclose breaches publicly. As reported earlier, State's unclassified email system was compromised in September or October, at the same time as a White House network. State's email has been down and access to public websites was disrupted, after the department on Friday disconnected networks to improve security, officials said. Speculation on the attackers has centered on hackers backed by a nation state, such as Russia or China. On Monday, it remained unclear why State officials waited until this weekend to take offline potentially infected systems . It's possible State waited to talk publicly and take down systems until it better understood exactly what was impacted by the cyberstrike, some security analysts said. "The priority is not necessarily, at the point of detection, to rush out and inform—you are taking the necessary remediating steps to abate the issue," said Steve Ward, a senior director at cyber firm iSight Partners. To read more click **HERE**

VA has not corrected security problems Washington

Free Beacon, 19 Nov 2014: Two years after a major security breach compromised the personal information of over 4,000 veterans, the Department of Veterans Affairs (VA) continues to suffer from systemic "security weaknesses," according to a new report from the Government Accountability Office (GAO). "While the Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, it has not fully addressed these weaknesses. … Until VA fully addresses previously identified security weaknesses, its information is at heightened risk of unauthorized access, modification, and disclosure and its systems at risk of disruption," the report found. The VA has experienced multiple high-profile breaches in recent years, and the report cautions that unless it corrects "underlying" security vulnerabilities in its systems, breaches are likely to continue and could result in unauthorized access and disclosure of personal information. Many of the weaknesses identified in the report are not new, but the inspectors say the agency has failed to sufficiently address some of the "previously identified vulnerabilities." The VA Inspector General released a report in February 2013 that identified deficiencies in "management controls intended to ensure that VA's critical systems have appropriate security baselines and up-to-date vulnerability patches," and made recommendations to resolve the problems. The VA said they completed the recommendations and would continue to improve those security controls but the recent inspection found that the VA failed to deliver on that promise. To read more click **HERE**

Google Releases Security Update for Chrome

US-CERT, November 19, 2014: Google has released Chrome 39.0.2171.65 for Windows, Mac and Linux. This update addresses multiple vulnerabilities, one of which could cause a denial of service condition. Users and administrators are encouraged to review the Google Chrome blog and apply the necessary updates. Source

Hackers attacked the U.S. energy grid 79 times this year

CNN, 19 Nov 2014 In fiscal year 2014, there were 79 hacking incidents at energy companies that were investigated by the Computer Emergency Readiness Team, a division of the Department of Homeland Security. There were 145 incidents the previous year. The outermost defenses aren't holding up. Between April 2013 and 2014, hackers managed to break into 37% of energy companies, according to a survey by ThreatTrack Security. Cybersecurity firm FireEye (FEYE) identified nearly 50 types of malware that specifically target energy companies in 2013 alone, according to its annual report. Energy firms get hit with more spy malware than other industries, according to a 2014 study by Verizon (VZ, Tech30). In March, TrustedSec discovered spy malware in the software that a major U.S. energy provider uses to operate dozens of turbines, controllers and other industrial machinery. It had been there for a year -- all because one employee clicked on a bad link in an email. And just last month, CERT revealed that a Russian malware called BlackEnergy had found its way onto the software that controls electrical turbines in the United States. Investigators didn't see any attempts to damage or disrupt machines. But the malware gives hackers a backdoor to plant destructive code in the future. So far, no computer virus has shut down any portion of the grid. But hackers are still breaking in, giving them the potential to flip switches off. "Our grid is definitely vulnerable," said David Kennedy, TrustedSec's CEO. "The energy industry is pretty far behind most other industries when it comes to security best practices and maintaining systems." Why are energy companies so vulnerable? One reason is that these industrial systems rely on 1970s-era technology. It doesn't get upgraded, because doing so would interrupt service, Kennedy said. At a power grid security conference in San Antonio, Texas in October, NSA director Admiral Mike Rogers told energy companies the power infrastructure just wasn't designed to stand up to today's attacks. "Power... is one of the segments that concerns me the most," he said, according to a transcript obtained by CNNMoney. So serious are the implications that DHS and FBI are now touring 12 American cities, hosting classified meetings with energy providers and utility companies to brief them on the danger. This confidential alert was sent to U.S. energy firms and their security consultants. Energy companies do take precautions. They have cybersecurity teams, and they separate their Internet-connected corporate computers from the stations that control critical machines. Firewalls and passwords help. And energy companies use so many different types of machines that taking out a city's power would take a calculated, coordinated effort by an army of hackers. David Whitehead is a research executive at Schweitzer Engineering Laboratories, which builds devices that monitor electrical current. He said it's easier to cause damage by shooting at power transformers with rifles -- like snipers did last year in Silicon Valley. Storms also currently pose a more potent threat of power outages than hackers. "There's all this doom and gloom about how fragile the grid is. But what do we have to fear in terms of power disruption? It's not a terrorist attack," Whitehead said. "It's mother nature." To read more click HERE

Michaels and Staples breaches carried out by same attackers?

Heise Security, 18 Nov 2014: The attackers that stole payment card information from consumers of Texas-based arts and crafts store chain Michaels and international office supply chain store Staples are likely the same ones. According to information received by Brian Krebs, the malware found in Staples stores and the one found in Michaels communicated with the same C&C networks. And while it's possible that these networks have been rented, it's also very unlikely, as creating them from scratch is easier and cheaper. The Michaels breach - actually, two breaches: one at its Aaron Brothers stores and the other at Michaels stores - took place between May 8, 2013 and February 27, 2014, and it is believed that the attackers managed to impact around 3 million payment cards via compromised POS systems. Rumours of

a Staples breach have been circulating since late October, and according to information shared by banks, it seems that the cash registers at a number of Staples stores were compromised between July and September 2014. According to sources close to the investigation, some 100 Staples stores were hit. Staples spokesman Mark Cautela confirmed that they are investigating, in conjunction with law enforcement, a "data security incident" that affected some of their stores. "We believe we have eradicated the malware used in the intrusion and have taken steps to further enhance the security of our network," he said. To read more click **HERE**

Google open sources Firing Range, a test tool for web app security scanners

Heise Security, 19 Nov 2014: Google has open source another security tool: it's called Firing Range, and it's an effective testing ground for a variety of automated web application security scanners. "Firing Range is a Java application built on Google App Engine and contains a wide range of XSS and, to a lesser degree, other web vulnerabilities," Claudio Criscione, Security Engineer at Google, explained in the announcement. Unlike other test applications that are already available, this one is aimed at automated solutions and not human testers. "Our testbed doesn't try to emulate a real application, nor exercise the crawling capabilities of a scanner: it's a collection of unique bug patterns drawn from vulnerabilities that we have seen in the wild, aimed at verifying the detection capabilities of security tools," he added. "We have used Firing Range both as a continuous testing aid and as a driver for our development, defining as many bug types as possible, including some that we cannot detect (yet!)." The tool was created by researchers from Google and the Polytechnic University of Milan because they needed a way to test Inquisition, a web application security scanning tool the company has created for in-house use. The source code for Firing Range can be found on GitHub. There's also a public instance open for use. "We hope that others will find it helpful in evaluating the detection capabilities of their own automated tools, and we certainly welcome any contributions and feedbacks from the broader security research community," Criscione concluded. This is the second security testing tool that Google has open sourced in the last two weeks. Earlier this month it has released nogotofail, a network security testing tool designed to probe device and apps for SSL certificate verification issues, HTTPS and TLS/SSL library bugs, SSL and STARTTLS stripping issues, and so on. To read more click **HERE**

320 breaches reported between July and September 2014

Heise Security, 19 Nov 2014: Consumers experienced a wide range of data privacy and security threats in the third quarter of 2014 as hackers successfully conducted large-scale attacks against financial services and retail companies as well as consumers' personal online accounts and identities. Between July and September of this year, there were 320 breaches reported worldwide, an increase of nearly 25 percent compared to the same period last year, and more than 183 million customer accounts and data records containing personal or financial information were either stolen or lost, according to SafeNet. Individuals also felt the data privacy pinch with breaches occurring across three major consumer activities: their banking, shopping, and online identities. Financial Services (42%) and Retail (31%) took the top spots among all industries in terms of the number of compromised customer accounts and data records. These were followed by breaches involving Technology and Personal Online Accounts (20%) such as email, gaming and other cloud-based services. In addition, Identity Theft also took the top spot among the types of data breaches, accounting for 46% of the total. "Consumers' heads must be spinning as criminals are easily getting access to their credit card, banking and personal information at every turn," said Tsion Gonen, chief strategy officer at SafeNet. "'Companies should assume a breach and plan accordingly. They need to implement technologies and programs that minimize the impact of a breach on top of the traditional prevention. As it is, these technologies are just not being used by to the fullest extent by either consumers or companies." "The retail industry has been consistently hit hard with breaches. Criminals want to have access to credit card and banking information for financial gain or to obtain personal information to use for identity theft. Customers have been very tolerant of these breaches, because they feel that this access can be corrected by someone else, like a bank replacing a stolen credit card. However, this new surge of online identity breaches is much more serious for individuals. Once your

personal photos or private messages have been accessed and leaked online, there's no fixing that. Those items will be forever in cyberspace for your future employers, friends and family to access," continued Gonen. "While it's not surprising that sophisticated cybercriminals are continuing to attempt these breaches, what is surprising is that again only 1% of breached records had been encrypted. Now is the time for customers to demand that their personal information be encrypted by companies," he added. By data breach type:

- Account Access: 86,393,338 records or 48%, and 39 data breach incidents or 12% of all incidents
- Financial Access: 58,453,288 records or 33%, and 52 data breach incidents or 16% of all incidents
- Identity Theft: 30,717,154 records or 17%, and 147 incidents or 46% of all incidents
- Nuisance: 3,195,285 records or 2%, and 46 incidents or 15% of all incidents
- Existential Data: 116,220 records or <1%, and 36 data breach incidents or 11% of all incidents.

By source

- Malicious Outsiders: Accounted for 173,835,350 data records stolen or 97%, and 172 data breach incidents or 54%
- Accidental Loss: Accounted for 2,795,235 data records lost or 1%, and 77 data breach incidents or 24%
- State Sponsored: Accounted for 2,075,584 data records stolen or 1%, and 24 data breach incidents or 7%
- Hacktivists: Accounted for 117,105 data records stolen or <1%, and 8 data breach incidents or 3%
- Malicious Insiders: Accounted for 52,011 data records stolen or <1%, and 38 data breach incidents or 12%.

To read more click **HERE**

One billion attacks were blocked during the third quarter 2014

Heise Security, 19 Nov 2014: Over a billion malicious attacks were detected and blocked during the third quarter, according to Kaspersky Lab. One third of Web attacks were carried out using malicious Web resources hosted in the United States. Attacks by mobile malware were detected in 205 countries, showing non-targeted mass attacks are becoming truly global. Q3 in figures:

- Over a billion malicious attacks were blocked on the computers and mobile devices of Kaspersky Lab users – 33.1 percent more than in the previous quarter.
- Two cyber-espionage campaigns – Crouching Yeti and Epic Turla – affected more than 2,800 high-profile victims in at least 10 industries, such as government institutions, embassies, military, research organizations and IT companies.
- About 110 million unique URLs that triggered web antivirus detections were recorded – 31 percent more than in Q2.
- 74,500 new mobile malware samples were added to Kaspersky Lab's collection. This is 14.4 percent more than in Q2.
- Over 7,000 mobile banking Trojans were detected – 3.4 times more than in the previous quarter.
- Banking Trojan attacks were detected in 70 countries, compared with 31 countries in Q2.

During the quarter there were also changes in the top five main sources of Web attacks. In Q2, the top five positions in the ranking were occupied by Germany, the US, the Netherlands, Russia and Canada, respectively. In Q3 the US made a big leap (+11.2 pp), landing in the top position with 33%. Germany dropped to third place (13.5%) and the Netherlands moved into second place (18%). Ukraine reached fifth place (4%), pushing Canada out of the Top 5. Russia remained in fourth position with 9%. "In Q3, Web antivirus modules were triggered at least once on almost one third of computers while owners were surfing the Web. This figure has been falling for a year: in Q3 2013 it was 34.1 percent, in Q1 2014 it fell

to 33.2 percent and starting from Q2 it 'froze' at 29.5 percent. This is due to a number of factors. First, browsers and search engines started helping to combat malicious sites. Second, there were fewer attacks involving exploit packs following the arrests of several developers. However, it would be naïve to expect the use of exploits to go down sharply: exploits remain the malware delivery method of choice in the case of targeted attacks," said Maria Garnaeva, Security Researcher at Global Research and Analysis Team, Kaspersky Lab. To read more click **HERE**

One-in-four have been victims of identity theft

Heise Security, 18 Nov 2014: Identity theft has ranked as the top concern amongst consumers questioned about their digital lifestyles, according to Centrify. The survey of 1,000 UK consumers, reveals that 81% of respondents cited that they were concerned, or very concerned about the prospect of having their identity stolen. Having credit card information stolen online is also extremely worrying, with 79% ranking it the second biggest concern above being a victim of cybercrime (73%). Surprisingly, cyber bullying was the least concerning, with just 40% of consumers showing any real concern, whilst privacy of social networks (59%) and email spam (68%) ranked much higher. The survey also reveals the numbers that have a high, medium, or low 'digital footprint' based on the amount of time they spend online in a typical week, emailing, texting and sharing or watching digital images, songs, games, videos and apps. 62% of those very concerned about identity theft have a medium digital footprint, 46% low, and 26% have a high digital footprint. Equally only 26% of those with a high digital footprint were concerned about having credit card information stolen off of an online shopping website, and their email accounts being spammed, showing that those that spend more time online are less concerned about their identity being stolen. One in four have definitely, or probably, been a victim of identity theft, 43% of which suggested it took more than one month to fix, and one in five saying it took more than 10 hours. 47% admitted to having to spend their own money to resolve the issue, with 28% noting they have spent at least 60 pounds (GBP), highlighting the need for increased password security. Tom Kemp, CEO for Centrify, comments: "According to our survey, online purchases were the top reason that users thought they became victims of identity theft, underscoring the importance of confidence in one's own online security. Consumers have very little faith in the absolute security of their passwords, as just 15% believe those passwords are very secure, regardless of the amount and type of characters used. Being able to manage our password security is crucial." Other research highlights:

- Online purchases were the top reason that users thought they became victims of identity theft, underscoring the importance of confidence in one's own online security.
- The groups that are most likely to say they have been victims of identity theft are those that probably best understand and notice the signs of identity theft: IT workers, online shoppers, higher-salary workers, the tech-savvy, and those with a high digital footprint.
- Those with the least confidence that their passwords are absolutely secure include, those that do less online shopping (12%), those aged 50-64 (11%), and those with a medium digital footprint (11%).
- A plurality of consumers are only somewhat confident that their passwords for personal accounts could not be cracked by a computer program, but few are very confident.

To read more click **HERE**

Microsoft Releases Out-of-Band Security Bulletin for Windows Kerberos Vulnerability

US-CERT, November 18, 2014: Print Document Tweet Like Me Share Microsoft has released security updates to address a remote elevation of privilege vulnerability which exists in implementations of Kerberos KDC in Microsoft Windows. Exploitation of this vulnerability could allow a remote attacker to take control of an affected system. US-CERT encourages users and administrators to review Microsoft Security Bulletin MS14-068(link is external) and Vulnerability Note VU#213119 for additional details, and apply the necessary updates. To read more click **HERE**

More Cloud Data Breaches 'Inevitable' in 2015, Forrester Says
Nextgov, 17 Nov 2014: If a new analysis holds true, cloud computing will continue to be the most disruptive technology around -- but get ready for more ugly data breach headlines. The inevitability of breached data in the cloud is the most provocative of 10 forecasts from Forrester Research in a new report, Predictions 2015: The Days of Fighting the Cloud are Over (link). The findings should raise eyebrows particularly for government customers, who put a premium on protecting sensitive information. "You can attempt to blame the software-as-a-service (SaaS) provider or the cloud platform for not protecting your data, but the breach won't happen because a hacker broke through their protections," the report stated. "You are a much easier target. The culprits will likely be common process and governance failures such as poor key management or lack of training or perimeter-based thinking by your security department. A breach of some form is inevitable. Whether the perpetrators find anything worthy of their effort is up to you." To help combat critical data breaches, IT managers should exercise caution and practice intelligent cybersecurity hygiene regardless of the cloud service provider and its standardized protections. One open port or bone-headed password is enough to get "owned." To read more click HERE

After Hack, NOAA Still Plans to Buy Supercomputers from IBM Unit Sold to Chinese Firm
Nextgov, 14 Nov 2014: A weather agency allegedly hacked by China intends to continue with plans for using forecasting computers provided by an IBM unit recently sold to a Chinese company. Lawmakers are voicing concerns about the contract, after the National Oceanic and Atmospheric Administration on Wednesday acknowledged attackers breached prediction and satellite systems. But NOAA says IBM's sale of its supercomputing business to Chinese-based Lenovo will not affect the agency's life-saving prediction capabilities. "IBM is obligated to continue upgrading the NOAA supercomputer system" and an update is scheduled to complete in January 2015, a NOAA official told Nextgov late Thursday. "This move will in no way impact NOAA's ability to provide timely and accurate forecasts to maintain public safety." Earlier in the year, the proposed Lenovo acquisition sparked espionage concerns, amid federal charges that Chinese military members cribbed trade secrets from U.S. organizations' networks. But the Committee on Foreign Investment in the United States, which reviews potential security risks posed by foreign takeovers of U.S. companies, cleared the deal. And the sale closed Oct. 1. The recently revealed hack and Lenovo controversy follow years of warnings from agency watchdogs about NOAA's computer insecurities. This summer, a federal inspector general blasted the agency for long neglecting tens of thousands of major cyber vulnerabilities that could compromise its environmental satellite program, the Joint Polar Satellite System, or JPSS. The IBM machines spun off to Lenovo, x86 servers, are part of that program. NOAA officials do not see the transaction as a security issue. "After reviewing the terms of the sale, NOAA determined the sale doesn't present a risk to the JPSS program," NOAA spokeswoman Ciaran Clayton said in an email. JPSS computers support satellite command and control, and generate forecast data crucial for aviation, emergency response and other daily activities. Lawmakers and federal investigators say they intend to examine NOAA's reliance on IBM technology now owned by China. The Government Accountability Office and NOAA will brief House Science Committee staff "on this issue in the near future, and have already been briefed by CFIUS," committee spokesman Zachary Kurz said in an email. "This is an issue we have been tracking for some time and will continue to monitor closely." As part of routine market research to explore contracting options, NOAA in August issued a request for information to survey all supercomputing vendors about their newest features, agency officials said. Rep. Frank Wolf, R-Va., told Nextgov that NOAA staff proactively told him IBM would be bidding on future work, because he is vocal on the issue of Chinese cyberespionage. Wolf said he is "absolutely" troubled by the possibility of national security threats from Lenovo's acquisition of IBM servers. "I am very concerned about any time a company is taken over by the Chinese," he said. The Chinese government "could put a chip in and do things that even the maintenance men might not be able to find." After Lenovo bought IBM's personal computer division in 2005, Wolf successfully pressured the State Department to keep the PCs off networks that contain classified material. "The question of stealing is both a national security issue and it's also a jobs issue because they look for information so they can use it in their production," he said. "And a lot of their gains in certain areas have been from what they've taken, not that they are smartest people in the

world. Now, the Chinese people are a wonderful people -- we're talking about the Chinese government." The inspector general at the Commerce Department, which oversees NOAA, "has ongoing work with the JPSS program," IG spokesman Clark Reid said, but declined to comment further. The number of critical cyber vulnerabilities in the satellite program have spiked by more than 60 percent since 2012, increasing from 14,486 security holes to 23,868 holes, according to an August IG report. IBM officials declined to comment on the NOAA computer project but said the U.S. government deemed the Lenovo sale free of any supply chain risks. "After a thorough review, the Committee on Foreign Investment in the United States found no conflict with U.S. security interests in the sale of IBM's x86 business to Lenovo," IBM spokesman Clint Roswell said. "IBM does not discuss the specifics of its federal client engagements." In October, after NOAA reportedly knew of unauthorized satellite system interference, it downplayed the problems. The agency told the public the National Weather Service had not received some satellite data, "potentially impacting" model forecasts and that the system was undergoing unscheduled maintenance. NOAA did not notify the IG about the intrusion until Nov. 4, Reid said, adding that the inspector is looking into the issue further. NOAA officials now state four agency websites were breached "in recent weeks" by an "Internet-sourced attack." It was agency staff who detected the infiltrations and "incident response began immediately," they added. Wolf said NOAA told him the incident was tied to the Chinese government, but agency officials declined to comment beyond their statement. The Washington Post first reported the hack Wednesday. This is not the first time NOAA satellite data has been hacked, nor is it the first time the Chinese have been accused of breaching satellites. Agency satellite data was stolen from a contractor's personal computer last year, but NOAA could not investigate the incident because the employee refused to turn over the PC, according to a July inspector general report. Several U.S. Earth observation satellites have also been probed by suspected Chinese hackers in recent years, according to federal officials. A 2011 report by the U.S.-China Economic and Security Review Commission characterized the events as successful interferences that might have been linked to the Chinese government. To read more click **HERE**

VA fails cybersecurity audit for 16th straight year

Federal News Radio, 17 Nov 2014: Despite what Veterans Affairs leaders said was progress toward shoring up their IT security processes, the department will receive a failing grade on a key annual cybersecurity audit — the 16th consecutive year in which it's fallen short. The VA inspector general won't publish the full details of the 2014 audit results until next year, but last week, the IG formally notified the department that it concluded, once again, that VA has significant material weaknesses with its compliance with the Federal Information Security Management Act, (FISMA). Stephen Warren, VA's chief information officer and executive in charge of the Office of Information and Technology, disclosed the audit result to reporters in advance of a Tuesday House Veterans Affairs Committee hearing that will scrutinize cybersecurity challenges within VA. "I was disappointed and I know the team was disappointed given the significant time and effort we applied this year," Warren said. "But we are going to continue to drive on this. We are going to continue to push so that we move forward on the rigorous, disciplined plan the team has put together so that when the audit team shows up next year they will continue to see the constant improvement they recognized even this past audit season." In its 2013 audit, the IG identified some 6,000 specific cybersecurity vulnerabilities and made 35 separate recommendations to close weaknesses. The corrective actions the IG has been recommending run the gamut of common IT functions, including identity and access management, incident response, configuration management and continuous monitoring. To read more click **HERE**