COLORADO SPRINGS
ISSA
INFORMATION SYSTEMS SECURITY ASSOCIATION, INC.

WWW.ISSA-COS.ORG

ISSA-COS NEWSLETTER

VOLUME 2 NUMBER 7 AUGUST 2013

INSIDE THIS ISSUE:

The Dog Days of Summer

As I sat down at my Mark IV Datamancer® to finish up this newsletter I realized that putting it together while completing some IA testing for my client and studying for my upcoming ITIL Foundations exam did not leave me any mental space for developing an opening article!

So… I hope to have something here next month. BTW—I am more than happy to fill this space with an article from *you*.

In the mean time I hope that you like this month's selection of articles. Hopefully, there won't be too many instances where you'll say, "I already knew that!"

Finally on page three you will find information on our upcoming ISSA-COS Board of Directors elections. Consider running!

Don Creamer

The ISSA Colorado Springs Newsletter incorporates open source news articles as a training method to educate readers on security matters in compliance with USC Title 17, Section 107, Paragraph a.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

In 'Golden Age' of Surveillance, US Has Big Edge

“You're commuting to where the information is stored and extracting the information from the adversaries' network.

We are the best at doing it. Period.".”

By Raphael Satter, Associated Press, July 2, 2013,

The saga of Edward Snowden and the NSA makes one thing clear: The United States' central role in developing the Internet and hosting its most powerful players has made it the global leader in the surveillance game.

Other countries, from dictatorships to democracies, are also avid snoopers, tapping into the high-capacity fiber optic cables to intercept Internet traffic, scooping their citizens' data off domestic servers, and even launching cyberattacks to win access to foreign networks.

But experts in the field say that Silicon Valley has made America a surveillance superpower, allowing its spies access to massive mountains of data being collected by the world's leading communications, social media, and online storage. That's on top of the United States' fiber optic infrastructure — responsible for just under a third of the world's international Internet capacity, according to telecom research firm TeleGeography — which allows it to act as a global postmaster, complete with the ability to peek at a big chunk of the world's messages in transit.

"The sheer power of the U.S. infrastructure is that quite often data would be routed though the U.S. even if it didn't make geographical sense," Joss Wright, a researcher with the Oxford Internet Institute, said in a telephone interview. "The current status quo is a huge benefit to the U.S."

The status quo is particularly favorable to America because online spying drills into people's private everyday lives in a way that other, more traditional forms of espionage can't match. So countries like Italy, where a culture of rampant wiretapping means that authorities regularly eavesdrop on private conversations, can't match the level of detail drawn from Internet searches or email traffic analysis.

"It's as bad as reading your diary," Wright said. Then he corrected himself: "It's FAR WORSE than reading your diary. Because you don't write everything in your diary."

Although the details of how the NSA's "PRISM" program draws its data from these firms remain shrouded in secrecy, documents leaked by spy agency systems analyst Edward Snowden to the *Guardian* and *The Washington Post* newspapers said its inside track with U.S. tech firms afforded "one of the most valuable, unique, and productive" avenues for intelligence-gathering.

The pool of information in American hands is vast. Redmond, Washington-based Microsoft Corp. accounts for more than 90 percent of the world's desktop computer operating systems, according to one industry estimate. Mountain View, California-based Google Inc. carries two-thirds of the world's online search traffic, analysts say. Menlo Park, California-based Facebook Inc. has some 900 million users — a figure that accounts for a third of the world's estimated 2.7 billion Internet-goers.

Electronic eavesdropping is, of course, far from an exclusively American pursuit. Many other nations pry further and with less oversight.

China and Russia have long hosted intrusive surveillance regimes. Russia's "SORM," the Russian-language acronym for System for Operational-Investigative Activities, allows government officials to directly access nearly every Internet service provider in the country. Initially set up to allow the FSB, the successor organization to the KGB, unfettered access to Russia's Internet traffic, the scope of SORM has grown dramatically since Vladimir Putin took power in 2000 and now allows a wide range law enforcement agencies to monitor Russians' messages.

Read the rest here:

http://www.dfinews.com/news/2013/07/golden-age-surveillance-us-has-big-edge?et_cid=3345776&et_rid=454841830&location=top

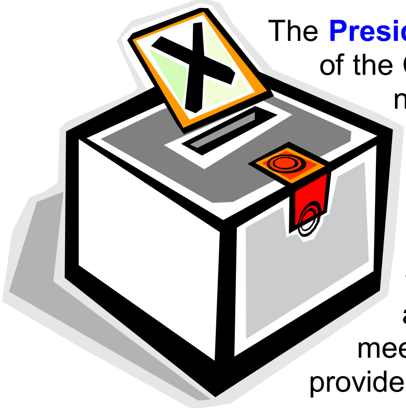
Elections for Your Board of Directors

To quote from the ISSA-COS By-Laws: *The business of the Chapter shall be managed by the Board of Directors. A Board quorum for business shall consist of at least four (4) board members present. This Board may, from time to time, establish special committees for various purposes as required.*

There are five positions (defined below) which are up for election on the ISSA-COS Board of Directors. The other positions on the Board (**Executive Vice President**, **Recorder** and a **Member at Large** position) will be elected in 2014. The **Communications Officer** position will also be up for re-election in 2014 to restore a proper balance to which positions are up for election and which are not. With the exception just mentioned these are all two-year positions.

Who is qualified to run for a position on the Board (again, quoting from the ISSA-COS By-Laws)? *The officers of the Chapter must be General Members in good standing as of the date of their election.*

THE FOLLOWING OFFICES (WITH JOB DESCRIPTIONS) ARE UP FOR ELECTION THIS YEAR:



The **President** shall be the executive head of the Chapter and shall preside at all meetings of the Chapter. The President shall have the power to call special meetings with a nominal five (5) day notification to the general membership if deemed necessary for the benefit of the Chapter. The President shall also have the power to assign the duties of the monthly reconciliation of the bank account to any officer other than the Treasurer.

The **Vice President** shall attend to the duties of the President in the absence of the President and Executive Vice President and shall attend to any other duties as the President may require. The Vice President shall have the power to call a meeting of the Board without the consent of the President. The Vice President shall provide liaison with standing committees within the Chapter.

The **Treasurer** shall be responsible for Chapter financial administration as outlined in Article VIII. The Treasurer shall receive all Chapter membership dues from ISSA and receive and disperse other monies incidental to Chapter activities. The Treasurer shall maintain an accounting of articles of value belonging to the Chapter, and shall keep an accurate accounting of all treasury receipts, expenditures, and deposits.

The **Communications Officer** shall maintain sufficient membership address lists as to ensure that all members in good standing are notified of meetings, and that all other correspondence necessary to the conduct of the Chapter is received by the members. At the direction of the President, the Communications Officer shall also transmit and respond to all correspondence of the Chapter, and perform any other duties customarily associated with the office of Communications Officer. The Communications Officer shall approve content of Chapter sponsored websites and newsletters. Additionally, the Communications Officer shall be responsible for the publication of the Chapter Newsletter and/or website, either directly or by supervising an appointed editor/webmaster.

The **Member at Large** shall be responsible for acting as a liaison between the ISSA-COS members and the Board, annually assessing the Board's performance, and coordinating all committees not established as standing committees.

There will be a Nominating Committee selected at the November 14th meeting. You may volunteer for one of the two positions on this Committee.

Elections will occur at the December luncheon meeting and assumption of office will occur at the end of the December meeting.

House Is a 'Hacker's Dream'

By Emma Dumain. Roll Call, July 26, 2013

An enterprising computer hacker or foreign intelligence agent would have little problem hacking into the House of Representatives' information technology systems, an unauthorized review of the chamber's cybersecurity found.

Vulnerabilities on the House side of the Capitol complex include exposed, unattended cables and network equipment as well as a lack of policing at security checkpoints, according to two systems administrators who work on a contract basis for multiple House members — including those who sit on sensitive committees such as the Intelligence panel.

The chamber also appears to lack sufficient authentication for contractors who call the House's official computer "help desk" to request activation passwords for the BlackBerrys of members or staff.

"It's a hacker's dream," one of the administrators said.

In an anonymous July 8 memo to House security stakeholders, that administrator wrote that he conducted the review "out of genuine regard for the safety and continued operation of the Congress."

A congressional office that employs the administrator says the memo was hand-delivered to the two relevant House offices — House Security, part of the House Sergeant-at-Arms Office, and Information Security, part of the office of the House Chief Administrative Officer — earlier this month as a courtesy and out of concern for the issues being raised.

The memo, obtained by CQ Roll Call, indicates points around the House office buildings where individuals with sophisticated technology expertise and malicious intent could tap into the computer system and wreak havoc.

"Think of your house," said the second administrator, in discussing his colleague's report. "You have a front door and a back door. If someone has the keys to either door, they can get inside. If they know what they're looking for, they can take it."

The same goes for a hacker: Once he or she can get inside the House's network or a member's BlackBerry, the possibilities are limitless, because a hacker knows what to look for and how to get it.

As observed by CQ Roll Call, help desk attendants readily offer such passwords to contractors over the phone without asking any other questions to ensure the contractors' identity or their authorization to make such requests.

"To believe that other countries don't send intelligence agents onto this campus is beyond naive," the memo notes.

Prime opportunities for hacking, according to the memo, exist in some secluded areas around the Capitol, where wireless access points, or WAPs, sit exposed.

The WAP is a lightweight physical device, about the size of a small dinner plate, that sends out the wireless signal. WAPs, the administrators say, should be mounted on the wall or ceiling, or somewhere generally out of reach.

With a WAP on a piece of furniture in a secluded public area — such as the first-floor atrium in the Rayburn House Office Building — anyone could come and replace it with a "state-engineered clone device" or possibly a network tap.

"A person can sit in here for long periods of time without surveillance," the memo said of the atrium. Indeed, a CQ Roll Call reporter spent several hours in the atrium on a quiet Friday afternoon, sitting on the floor surrounded by cables and Ethernet cords and periodically fiddling with the WAP itself. The foot traffic was negligible and never once did a Capitol Police officer come by.

Read the rest here:

http://www.rollcall.com/news/house_is_a_hackers_dream-226687-1.html?pg=1

Attack on South Korean targets part of a larger cyber-espionage campaign

The March 20 cyber-attack on South Korean financial services and media firms, known as Dark Seoul, was thought to be significant not only for the high-profile nature of the targets but also for the use of a Master Boot Record (MBR) wiping functionality that erased the hard drives of infected PCs.

By InfoSecurity, July 8, 2013

According to McAfee Labs, however, Dark Seoul is notable for another reason: it can be linked back to an ongoing, persistent operation against South Korea known as Operation Troy, which has been targeting the world's most wired nation since at least 2009. And, the threat appears to come from within.

"McAfee Labs can connect the Dark Seoul and other government attacks to a secret, long-term campaign that reveals the true intention of the Dark Seoul adversaries: attempting to spy on and disrupt South Korea's military and government activities," the security firm noted in a white paper dissecting the issue

(http://www.mcafee.com/us/resources/white-papers/wp-operation-troy.pdf).

"The attackers have attempted since 2009 to install the capability to destroy their targets using an MBR wiper component, as seen in the Dark Seoul incident. From our analysis we have established that Operation Troy had a focus from the beginning to gather intelligence on South Korean military targets. We have also linked other high-profile public campaigns conducted over the years against South Korea to Operation Troy, suggesting that a single group is responsible."

Aside from the obvious reference to trojan viruses, the term "Operation Troy" has been given to the campaign because of a liberal sprinkling of Roman and Trojan terms throughout the attack code, which McAfee said most likely points to a group called the NewRomanic Cyber Army Team as the perpetrators.

The latest attacks managed to create a significant disruption of ATM networks in South Korea, while denying access to funds. But in addition to wiping the MBR to render systems unusable, creating an instant slowdown to operations within the target, Operation Troy is also focused on stealing and holding data hostage and announcing the theft in an Anonymous-style hacktivist approach.

"Public news media have reported only that tens of thousands of computers had their MBRs wiped by the malware," McAfee said. "But there is more to this story: The main group behind the attack claims that a vast amount of personal information has been stolen. This type of tactic is consistent with Anonymous operations and others that fall within the hacktivist category, in which they announce and leak portions of confidential information."

McAfee uncovered that in 2011, one of the same financial institutions was hit with destructive malware that caused a denial of service. "The attackers left a calling card a day after the attacks in the form of a web pop-up message claiming that the NewRomanic Cyber Army Team was responsible and had leaked private information from several banks and media companies," the firm said, noting that they also referenced destroying the data on a large number of machines (i.e., MBR wiping).

The attackers who conducted the operation remained hidden for a number of years prior to the March 20 incident by using a variety of custom tools. While analyzing malware components from before the March 20 incident, McAfee found both similar and identical attributes of the files involved that link them to the 3Rat remote administration tool client used on March 20, as well as to samples dating to 2010. The firm said that it's also possible that the campaign known as 10 Days of Rain is a byproduct of Operation Troy; some of the analysis suggests that the malware Concealment Troy was present in these attacks.

"This spying operation had remained hidden and only now has been discovered through diligent research and collaboration," McAfee noted. "We also suspect the attackers had knowledge of the security software running within the environment before they wiped the systems, given that some of the variants used in the attack were made to look as if they were antimalware update files from before March 20."

Read the rest here:

http://www.infosecurity-magazine.com/view/33341/attack-on-south-korean-targets-part-of-a-larger-cyberespionage-campaign/

New algorithm quickly identifies most dangerous risks in a power grid amid millions or billions of possible failures

By Jennifer Chu, Phys.org, July 1, 2013

Each summer, power grids are pushed to their limits, as homes and offices crank up the air conditioning in response to rising temperatures. A single failure in the system—such as a downed power line or a tripped relay—can cause power outages throughout a neighborhood or across entire towns.

For the most part, though, a failure in one part of the grid won't bring down the entire network. But in some cases, two or more seemingly small failures that occur simultaneously can ripple through a power system, causing major blackouts over a vast region. Such was the case on Aug. 14, 2003, when 50 million customers lost power in the northeastern United States and Ontario—the largest blackout in North American history. Even more recently, in July 2012, India experienced the largest power outage ever, as 700 million people—nearly 10 percent of the world's population—went without power as a result of an initial tripped line and a relay problem.

To help prevent smaller incidents from snowballing into massive power failures, researchers at MIT have devised an algorithm that identifies the most dangerous pairs of failures among the millions of possible failures in a power grid. The algorithm "prunes" all the possible combinations down to the pairs most likely to cause widespread damage.

The researchers tested their algorithm on data from a mid-sized power grid model consisting of 3,000 components (in which there are up to 10 million potential pairs of failures). Within 10 minutes, the algorithm quickly weeded out 99 percent of failures, deeming them relatively safe. The remaining 1 percent represented pairs of failures that would likely cascade into large blackouts if left unchecked.

The speed with which the researchers' algorithm works is unmatched by similar existing alternatives, according to one of its co-developers, Konstantin Turitsyn, the Esther and Harold E. Edgerton Assistant Professor in MIT's Department of Mechanical Engineering.

"We have this very significant acceleration in the computing time of the process," Turitsyn says. "This algorithm can be used to update what are the events—in real time—that are the most dangerous."

Turitsyn and graduate student Petr Kaplunovich will present their work, supported by the MIT Skoltech Initiative, in a paper at the IEEE Power and Energy Society Meeting in July.

A zero missing rate

In power systems lingo, a pair of failures is referred to as an "N minus 2 contingency"—"N" being the number of components in a system, and "2," the number of failures in a power grid at any given moment. In recent years, researchers have been developing algorithms to predict the most dangerous N-minus-2 contingencies in an electric grid. But while such algorithms successfully identify dangerous pairs of failures, Turitsyn says that most of them don't guarantee that these pairs are the only failures of concern. In other words, there may be failures that these algorithms missed.

"They don't provide guarantees that the ones you assume to be safe are really safe," Turitsyn says. "If you want to have some guarantees that the system is safe, you want the system to rely on algorithms that have zero missing rates."

Taking this angle of approach, Turitsyn and Kaplunovich developed an algorithm to comb through all possible pairs of component failures in a power grid (for example, a downed transmission line, or a generator short-circuit), weeding out failures that don't result in any overloads and are unlikely to cause widespread damage, and certifying them as safe. The pairs that are left can be flagged as potentially dangerous.

On a qualitative level, the algorithm essentially identifies spheres of influence around a power failure. While every part of a grid responds in some way to a single failure, the intensity of the response centers on a few grid components, and may only be felt locally, within a single neighborhood, or local region. If two failures are relatively "close," spheres of influence can overlap, intensifying the response and increasing the likelihood of a catastrophic cascade.

Read the rest here:

http://phys.org/news/2013-07-algorithm-quickly-dangerous-power-grid.html

Parenting in the Information Age: A Practical Guide

Research conducted in Hong Kong shows that blocking websites is no substitute for hands-on digital parenting. Former Hong Kong government CIO, Jeremy Godfrey, says governments should assist parents and teachers in getting up to speed, so they can help children have a positive and safe online experience.

By Jeremy Godfrey, InfoSecurity, June 27, 2013

A headline in the *Independent* read: "We need to help protect children from internet porn, say teachers." A *Daily Mail* columnist called on the government to "ensure that internet feeds are porn-free unless over-18 users specifically request it." The *Daily Mirror* reported a mother bemoaning: "I caught my 8-year-old sending NAKED pics of herself."

Every week we see news articles about children being exposed to inappropriate material online and comment pieces proposing (or opposing) various solutions. On one side of the debate are proponents of measures such as compulsory filtering by internet service providers (ISPs). On the other side are those who argue that these measures are ineffective, promote a dangerously false sense of security, and that they unacceptably interfere with freedom of communication.

HOW CAN WE KNOW WHO'S RIGHT?

A few years ago, when I was responsible for internet governance in the Hong Kong government, we were facing a similar debate. Religious organizations and conservative groups were arguing for the government to amend the law on obscene and indecent publications to make some sort of filtering mandatory. Liberal political groups and internet freedom advocates were vehemently opposed.

Instead of waiting to see whether either side of the debate could gather overwhelming support for its position, we decided to see if we could collect any hard evidence on the effectiveness of filtering software, compared with other techniques to promote childrens' online safety. This soon became a more general study on effective parenting in the information age.

FACT FINDING

We started with a program of qualitative interviews with parents and teenage children. We asked them about their perceptions of the benefits and risks of using the internet. We asked them about the techniques that parents used to guide and supervise their children's use of the internet. And we asked them how effective they thought the techniques were.

Among lower-income, less-educated parents, the main concern was the amount of time their children were spending online. Parents did not know what their children were doing, but they assumed it was distracting them from schoolwork. A typical supervision technique was to limit time spent online, and to pull the power plug out of the wall if children refused to comply.

Better-off, better-educated families had a greater appreciation both of the risks and the benefits of being online. They also had a closer relationship with their children. One father told us that he had come across his son looking at pornographic material online. He engaged his son in a discussion about the differences between the soft-porn magazines of his youth and the harder-core online material available today.

We followed-up with a large program of quantitative research, involving 2,500 families. When we presented this research at the United Nations' Internet Governance Forum, we were told this was the most thorough survey of its kind ever carried out.

We asked a wide range of questions about demographics – age, income level, parental education level and parental familiarity with the internet. We surveyed about parenting style – whether they were authoritarian, engaged or laissez-faire. We also queried about the techniques used to promote internet safety, including the use of filtering software, not allowing computers in bedrooms, regularly talking to children about their online experiences, setting rules, etc. We asked about parents' and children's awareness of and their concerns about different sorts of online risks.

Finally, we asked how satisfied parents were with their effectiveness in guiding and supervising children's use of the internet.

THE RESULTS

Based on the data we gathered, we used statistical techniques to see what factors could best explain why some parents were satisfied with their ability to supervise their children online, while others were not. The most surprising result was that use of filtering software was correlated with *lower levels* of parental satisfaction regarding their ability to guide and supervise children's use of the internet.

Read the rest here:

http://www.infosecurity-magazine.com/view/33175/parenting-in-the-information-age-a-practical-guide/

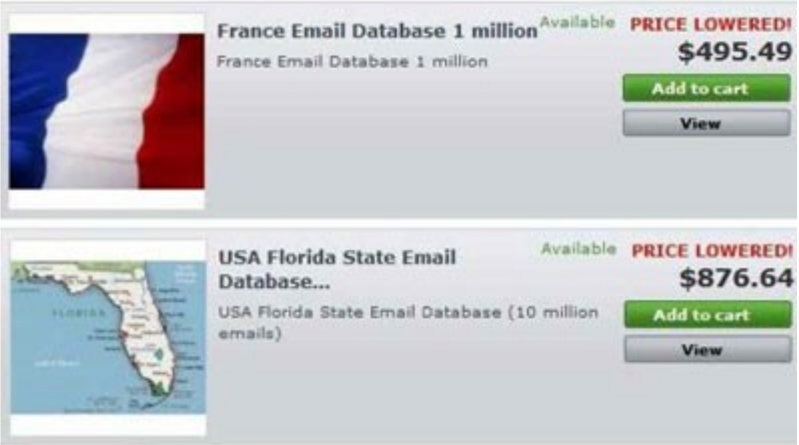
Current cybercrime market is all about *Cybercrime-as-a-Service*

By Zeljka Zorz, Help Net Security, July 2, 2013

The cybercrime market is constantly evolving, and it is currently full of knowledgeable individuals who have focused on their core competencies to offer services to those who have not the skills, patience or time to make what they want or need for their criminal exploits.

"The marketplace contains many stakeholders, ranging from formal, legitimate organizations selling vulnerabilities to parties that meet their strict eligibility criteria to underground websites that allow individuals to offer illegal services," say McAfee CTO Raj Samani and Senior Threat Research Engineer François Paget in their latest white paper titled *Cybercrime Exposed* (http://www.mcafee.com/sg/resources/white-papers/wp-cybercrime-exposed.pdf).

Research-as-a-Service offerings are more gray market than black. The offers are made by commercial companies that find and sell zero-day vulnerabilities to buyers of their choosing (often governments), and by brokers who help vulnerability sellers to get as much money as possible for their knowledge, and help buyers to remain anonymous and acquire information about vulnerabilities they might not otherwise be able to get their hands on.



France Email Database 1 million

France Email Database 1 million

Available

PRICE LOWERED!

$495.49

USA Florida State Email Database...

USA Florida State Email Database (10 million emails)

Available

PRICE LOWERED!

$876.64

Prices range from $5,000 and more for Adobe Reader zero day vulnerabilities, to $100,000 or even $250,000 for iOS ones.

Another Research-as-a-Service offering is the identification of targets - for example, a list of email addresses for spamming that often belong to users in a specific country or state, of a specific profession or gender, or users of a specific service.

The Crimeware-as-a-Service system includes developers selling exploits, malware, spyware, bots, spamming tools, tools for obfuscating the malicious nature of software (polymorphic builders, crackers, cryptors, and so on), as well as hardware for hacking or stealing (for example card skimmers) and services including checking files against security software

The Cybercrime Infrastructure-as-a-Service model allows wannabe criminals to rent botnets for DDoS attacks or for sending out spam or malware, bulletproof hosting schemes, and so on. The services are tailored to any and every budget.

Finally, the Hacking-as-a-Service option allows budding cyber crooks to skip doing research, building tools, and developing an infrastructure to launch an attack, as there are services out there that outsource the entire process. Examples include password hacking services, DDoS services, and sale of stolen credit card and bank login information.

According to the researchers, bank login information is sold for a higher price than credit card info, and EU bank logins are sold for a higher price (4–6% of the account balance) than American ones (2% of it). Verified PayPal, Moneybookers, Netteier account login info is worth even more (6-20%), and Western Union transfer details cost 10% of the transferred amount.

Read the rest here:

http://www.net-security.org/secworld.php?id=15173

New whitepaper on cybercrime, systemic risk and global securities markets

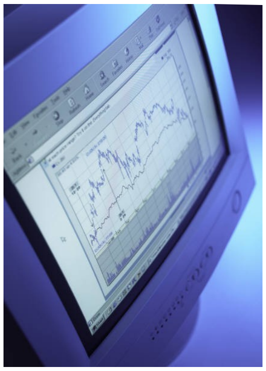
By Help Net Security, July 16, 2013

The Research Department of the International Organization of Securities Commissions (IOSCO) today published a joint Staff Working Paper, with the World Federation of Exchanges (WFE), entitled Cyber-crime, securities markets and systemic risk.

The report explores the evolving nature of cyber-crime in securities markets and the threat it poses to the fair and efficient functioning of markets. Importantly, it highlights the urgent need to consider cyber threats to securities markets as a potential systemic risk.

The first part of the report assesses what is known of the cyber-threat so far. It also presents a framework for monitoring the extent of cyber-crime in securities markets going forward. This is in line with IOSCO´s commitment to identifying emerging risks in a proactive way.

The report also points out that certain types of cyber-crime constitute more than an 'IT issue' or simple extension of financial crime. While cyber-crime in securities markets has not had systemic impacts so far, it is rapidly evolving in terms of actors, motives, complexity and frequency. The number of high-profile and critical 'hits' is also increasing. The report warns that underestimation of the severity of this emerging risk may lay open securities markets to a black swan event.



On the other hand, efforts to neutralize cyber-crime in securities markets can be assisted through high levels of awareness and a concerted cross-border, cross-sectoral, collaborative approach.

The second part of the report provides the results of a survey to the world exchanges. The survey explores the experiences of exchanges in dealing with cyber-crime and perceptions of the risk. The focus on exchanges is not due to any perceived or particular vulnerability. The survey is intended as part of a series of surveys exploring the experiences of different groups of securities market actors.

The survey revealed that a significant number of exchanges are already under attack with 53% suffering an attack in the last year. Attacks tend to be disruptive in nature, rather than motivated by financial gain. This distinguishes these cyber-crimes from traditional crimes in the financial sector such as fraud and theft.

Read the rest here:

http://www.net-security.org/secworld.php?id=15231

Read the White Paper Here:

http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

The European Parliament has voted in favor of a new directive on cybercrime

By InfoSecurity, July 5, 2013

By a vote of 541 to 91, with 9 abstentions, EC proposals for a directive on stiffer penalties across Europe for cybercriminals have been adopted by the European Parliament. Denmark has chosen to opt out of the directive, preferring to maintain its own system.

European member states now have two years to implement the proposals, which are an attempt to impose a more standard response to cybercrime across the Union. In general it introduces stronger penalties. It increases penalties for illegally intercepting communications, and producing or selling tools that enable this. The penalty for attacking national infrastructures, such as power plants or government networks, is set at five years in prison - which is generally higher than most nations' current sanctions.

"The perpetrators of increasingly sophisticated attacks and the producers of related and malicious software can now be prosecuted, and will face heavier criminal sanctions," said Cecilia Malmstrom, European Commissioner for Home Affairs in a statement.

But not all MEPs are happy with the outcome. During the debate on Tuesday, MEP Jan Philipp Albrecht warned, "we're not getting any more security from this directive, simply tougher and tougher punishments". He suggested that responsibility should be taken by the operators of the IT networks to ensure that all loopholes are closed.

In a statement issued last month, Albrecht warned that Europe's new approach would likely weaken rather than strengthen security. "The blunt new rules on criminalising cyber attacks... take a totally flawed approach to internet security. The broad strokes approach to all information system breaches, which would apply criminal penalties for minor or non-malicious attacks, risks undermining internet security."

Read the rest here:

http://www.infosecurity-magazine.com/view/33308/the-european-parliament-has-voted-in-favor-of-a-new-directive-on-cybercrime/

Things CEOs Hate To Pay For and How They Can Help You Make Your Case for Security

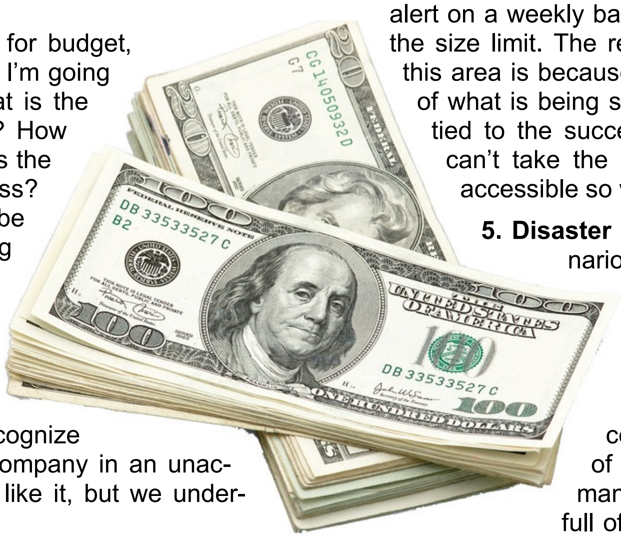
When Making the Case for a Security Budget, Don't Just Provide Numbers and Statistics...

By Mark Hatton, SecurityWeek, July 02, 2013

As a CEO, I hate spending money on things that don't help grow my business or improve the products and services we bring to market. While I know there are necessary evils in business that require funding, the thought of spending money on things that are only used in a worst-case scenario are not attractive options to me when it comes to the allocation of limited and important resources. Having spent the majority of my career in the cyber security business, I am well aware that many of my CEO brethren lump security spending into the same bucket as other less desirable expenditures and believe me, I get it.

When the case is being made for budget, my management team expects that I'm going to ask some tough questions. What is the payoff? Where does the risk exist? How likely are we to be affected? What is the potential impact to our business? These are questions that need to be answered. Bottom line, I'm looking for them to prove their case as to why the risk or reward to the business warrants the expenditure.

Executives make purchasing decisions everyday based upon need over want, because they recognize that the failure to do so puts the company in an unacceptable position of risk. We don't like it, but we understand it.



Here are five other things that we hate spending money on but are willing to do so in order to protect the business. Looking at the rationale for spending money in these areas can help you make the case to your own executive team why cyber security needs to be a priority in your company.

1. Insurance – in business and in your personal life, insurance is a check nobody ever wants to write. But we understand that protecting our critical assets against a catastrophic event is a necessity. Failure do so would be putting the company at risk of serious harm or even "going under" from a single event.

2. Legal Services – while I personally love our attorneys, life would be much simpler without the legal wrangling over contracts, leases and other complicated legal documents. But to try to do it alone would be crazy. Being protected under the law is a must for corporations, both private and public, and it's well worth the expenditure to have these experts on your team.

3. Compliance – government regulations and compliance initiatives have been on the rise in recent years and show no signs of slowing down. Failure to comply can lead to fines and penalties that could be devastating to large corporations and catastrophic for small to mid-size businesses. Ensuring compliance is a top concern of all management teams, no matter how costly.

4. Data Storage – billions are spent each and every year on data storage solutions and yet I seem to get an alert on a weekly basis telling me that my email is over the size limit. The reason we hate spending money in this area is because we know that a large percentage of what is being stored does not contain critical data tied to the success of the business. However, we can't take the chance that important data is not accessible so we make the additional investment.

5. Disaster Recovery – again, worst-case scenario expenditure, but one that is absolutely necessary. With many businesses existing solely upon their information and intellectual property (IP), the the sudden catastrophic loss of its data center due to weather, or other form of disaster, could spell the end for many businesses. In today's market full of information-based companies, the potential for systems and data to be unavailable is a non-starter.

Hopefully you noticed a common theme throughout these examples of things we don't like to spend money on, but do anyway. In each case, the potential cost to the business of not making the investment far exceeds the actual spend. In other words, these are all critical services that are necessities and not choices. Cyber security is simialr and touches all of the examples above. Failure to protect your company's critical data is not an option and can have wide-reaching implications beyond the walls of your own business. Depending upon the industry you are in, the compliance and legal issues that would result from a cyber-attack would put you at much more than further financial risk. A complete loss of data or IP could also put you quickly out of business.

Read the rest here:

http://www.securityweek.com/things-ceos-hate-pay-and-how-they-can-help-you-make-your-case-security

The Technology You Need to Protect Against Mass Surveillance

By Seth Schoeneff, Gizmodo, July, 18, 2013

In the past several weeks, EFF has received many requests for advice about privacy tools that provide technological shields against mass surveillance. We've been interested for many years in software tools that help people protect their own privacy; we've defended your right to develop and use cryptographic software, we've supported the development of the Tor software, and written privacy software of our own. This article looks at some of the available tools to blunt the effects of mass surveillance.

I. The things users want to keep private

There are many different kinds of electronic surveillance and many aspects of our communicative activities we may want to keep private. The online privacy landscape can be daunting in part because each different tool addresses different kinds of monitoring and privacy threats.

For example, most web browsers now include a "private browsing mode" which limits the web history kept *on your own computer*, preventing others who access your computer from learning about your browsing, but which has no effect on the data that's transmitted over the Internet, and doesn't try to stop, say, your Internet service provider from knowing where you went online.

Similarly, some privacy settings on services like Google and Facebook limit the display of some account history and information either *to you* or *to your friends*, but don't do anything at a technical level to stop Google or Facebook themselves from accessing or recording the communications and activities you send through their sites.

Even when we use cryptography to hide the content of our communications, there's a distinction to be drawn between *transport encryption* (protecting the communications as they travel between your computer and a service provider, like Gmail or your cell phone carrier) and*end-to-end encryption* (protecting them all the way between your device and the device of the person you're talking to, so that no intermediaries can read them at any stage). Accessing a webmail account over a secure HTTPS connection is an example of the former; it prevents your ISP, as well as people on your wifi network, from reading your mail as it travels between you and your mail provider. Using email encryption software like PGP is an example of the latter; it prevents even your webmail provider itself from reading the mail.

As we'll discuss in more detail in part two of this series, it's relatively easy to use transport encryption to prevent network operators from reading your communication. It's more work to use end-to-end encryption to keep communications private from an intermediary like an IM provider, cell phone carrier, or email service. And it's quite difficult to conceal the fact that communications happened between one user and another—it's much easier to hide *what you said* in an IM, phone call, or email than to conceal *that you contacted a particular friend* via IM, phone, or email at a particular moment.

Finally, you might want to hide your physical location when you're communicating. By default, Internet service providers along the way see, and most Internet sites you interact with store, your Internet protocol address (IP address), which can be used to figure out where you connected to the Internet from. This gives services a potential profile of your whereabouts over time, and even the potential to infer other information such as who else was with you and where you spent the night.

Here, we'll look at a few options to increase the use of cryptography to protect the contents of your on-line communications. As we'll discuss in Part 2, these technologies can't offer complete protection against every kind of surveillance, or against every possible eavesdropper; still, making encryption mainstream should help increase everyone's privacy baseline.

II. Privacy for Connections to Web Sites: HTTPS Everywhere

The technology we use to secure our communications with web sites against eavesdropping as our data travels over the Internet is HTTPS. Major web sites have been gradually migrating toward supporting or requiring HTTPS connections, which provide an important kind of protection against mass surveillance targeted against the Internet infrastructure itself.

Your web browser already supports HTTPS, but for some sites you might or might not use a secure connection. (For example, a secure connection for Google Search or for Wikipedia is available, but is optional.) To address this problem, EFF developed HTTPS Everywhere, a browser add-on that tries to make sure your connection to web sites is secure whenever the web site you're visiting supports it.

Even with HTTPS Everywhere, you can only have a secure connection with web sites that choose to offer HTTPS. Some still don't. If you use a site that still doesn't offer a secure HTTPS connection, please ask the site operators to start supporting HTTPS.

Read the rest here:

http://gizmodo.com/the-technology-you-need-to-protect-against-mass-surveil-823081362

Starting A Career in Digital Forensics

This is a two-part article. The links to both parts are at the end of this excerpt.

By John J. Barbara, DFINews, February 8, 2013

Can anyone remember when computers and cell phones did not impact our daily lives? Today, the majority of us take for granted that these technological marvels are necessary for our daily existence. However, this has not come without a concomitant price, that being the enormous proliferation of cybercrime which is directly related to the prevalence of these devices. Cybercrime has now reached epidemic proportions, causing the loss of billions of dollars annually. Daily, crimes such as identity theft and fraud, online child exploitation, child pornography, hacking, and intellectual property theft continue to make headlines. Many illegal drug deals are arranged using e-mail and/or text messaging. Frequently, cell phones containing probative information are encountered at crime scenes. Digital surveillance systems routinely capture crimes as they are being committed. Not surprisingly, many individuals post information about their criminal offenses on one or more of the social networking sites!

RESPONDING TO CYBERCRIME

Not too long ago there were few public sector agencies fully equipped and staffed to perform analysis on digital media. Many employed examiners whose prior experience consisted of being a sworn officer or investigator. Internal and external training programs were limited and not formalized. There was a paucity of forensic software and hardware and it was expensive. Due to the scarcity of trained examiners and the associated costs, there were even fewer private sector agencies offering digital forensic services. Likewise there were virtually no undergraduate or graduate programs to assist in preparing an individual for a career in digital forensics. However, over the past ten years or so, the landscape has dramatically changed with the expansion of digital forensics services in both the public and private sectors. External training programs and technical certifications are now commonplace as are undergraduate and graduate degree programs in digital forensics. The diversity and complexity of currently available forensic software and hardware tools far exceeds what was available just several years ago.

"WHAT DO I DO?"

A question often asked is, "What education and training is necessary to work in digital forensics?" There is not one easy, simple answer to this question. First of all, an individual has to make a choice of career pathways, namely do they wish to work in the public sector or in the private sector. These divergent paths may eventually lead to:

- Different types of employers.
- Working with different types of employees.
- Needing different qualifications.
- Working on distinct types of cases.
- Having different job expectations.
- Differences in salaries and benefit packages.

THE PUBLIC SECTOR

Examiners are routinely employed by government regulatory agencies, the intelligence agencies, the military, and by many federal, state, county, and local law enforcement agencies. Before choosing a public sector career path, there are a number of important points to consider, some of which may include:

- Funding is normally provided via taxing authorities.
- Agency requirements to follow certain federal, state, or local mandates which could impact hiring and promotional opportunities.
- Requiring prospective employees to undergo a thorough background investigation which normally includes fingerprinting, drug testing, and/or polygraph examination.
- Examiners mandated to sign contracts to remain with the agency for a period of time after they are trained.
- Agency requirements for random drug testing.
- Law enforcement agency examiners being exposed to some of the most appalling types of cybercrime, namely child exploitation cases and child pornography.
- Examinations and reports being confidential and not intended for general discussion and dissemination.
- Strict security access requirements to the area where examinations are conducted and where digital evidence is stored.
- Examiners assisting investigators at violent crime scenes (homicide, suicide, rape, etc.) to retrieve and/or image computers in unsafe, potentially contaminated environments. Frequently this occurs outside of the normal work hours or work day.
- Shortages of trained personnel and large case backlogs.
- Agencies instituting "quotas" regarding the amount/type of work examiners are expected to complete within a defined time frame.

The rest of Part 1 may be found here:

http://www.dfinews.com/articles/2013/02/starting-career-digital-forensics-part-1#.UaWxVtJGCSo

Part 2 may be found here:

http://www.dfinews.com/articles/2013/05/starting-career-digital-forensics-part-2?et_cid=3347843&et_rid=454841830&location=top

SSH Keys - Improved Security Controls or Improved Protocol?

As the use of Secure Shell (SSH) keys and related encryption services evolves and expands, security experts question what drives that evolution and are looking for ways to maximize the security effectiveness of the ubiquitous technology.

By Jeff Hudson, SecurityWeek, July 11, 2013

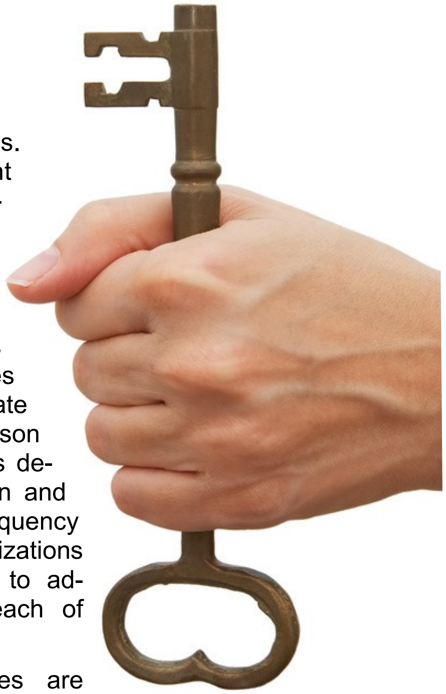
Recently, the Ponemon Institute found that most enterprises believe the largest security threat to their cryptographic assets is SSH key pairs, which are heavily entrenched in both data centers and cloud computing platforms. Simply put, enterprises fear attackers can easily compromise corporate access and data, thanks to weaknesses in traditional SSH key escrow and management processes.

New research suggests the fear is justified. The most recent APT1 report from Mandiant claims that 100 percent of attacks are related to compromised credentials, including SSL and SSH, and the Dell SecureWorks' Counter Threat Unit found that one in every five Amazon Machine Images (AMIs) stored in Amazon Web Services (AWS) has unknown SSH keys. Can modern enterprises trust a key-based encryption platform, especially if it relies on SSH and cloud-based services to protect data? A plethora of compromise possibilities exist thanks to that combination, with new attacks, hacks, and interceptions occurring daily by the hundreds. Yet, as always, security comes down to trust.

The question of trust may not be easy to answer, but some practices and technologies can ease the burden of uncertainty and reestablish credibility for SSH and key-based security infrastructures. Before delving into specific tips and tricks, though, one must truly understand the magnitude of the problem.

Cryptographic keys and digital certificates establish the trust for every business and government activity we rely on, from online payments to airline operations to cloud services. Not surprisingly, then, organizations have on average more than 17,000 keys and certificates, including SSH keys. The average network has thousands of systems that use SSH for elevated and privileged access. Yet the Ponemon Institute found that only 51 percent of organizations surveyed knew how many keys and certificates were in use in their enterprise.

Cybercriminals are counting on this fact: they are leveraging organizations' lack of visibility and their inability to respond to attacks on keys and certificates as the easiest route in. As a result, cybercriminals are successfully stealing intellectual property by exploiting this new attack vector – keys and certificates. Advanced persistent threats (APTs), targeted attacks, and compromised Certificate Authorities (CAs) are just some of the ways criminals are using weaknesses in key and certificate management to poison the trust organizations depend on for protection and security. Given the frequency of such attacks, organizations have very little time to address this major breach of trust.



Two major issues are generating vigorous discussion among those that SSH-based security impacts—which turns out to be a significant number of organizations. The majority of the Global 2000 use SSH keys for their digital communications.

The first issue is that organizations categorically do not have enterprise-wide visibility or controls in place that continuously monitor and manage SSH keys within their networks.

Without clear visibility or understanding of how SSH keys are used on the network there is little ability to respond to an attack that takes advantage of trusted SSH keys. The compromise of SSH keys within an environment allows an attacker to move seamlessly, undetected, and with elevated privileges from system to system. This enables them to steal valuable intellectual property.

The second issue affecting the SSH community is the need for improved protocols that enhance security and forensics. These protocols will also prove an important and ongoing defense against more sophisticated attacks, which are powered by ever-increasing computing potential.

There is a danger that organizations will not address these issues equally—that they will put more resources into protocol development while eschewing management improvements, or vice versa. Either way, strengthening only one element leaves significant gaps in overall SSH security.

Read the rest here:

http://www.securityweek.com/ssh-keys-improved-security-controls-or-improved-protocol

News Ripped From the Headlines

July 2, The Register – (International) **Crimelords: Stolen credit cards…keep 'em. It's all about banking logins now.** Research by McAfee revealed details of the stolen financial and user information markets, showing the going rate for bank login details, credit card information, user account information, and other products and services available in underweb communities. Source: http://www.theregister.co.uk/2013/07/02/mcafee_cybercrime_exposed/

July 5, Softpedia – (International) **Private Exploit Pack: New browser exploit kit advertised on hacker forums.** A new browser exploit kits named Private Exploit Pack was found being advertised on hacker forums. The exploit pack works on Windows XP, 7, and 8, and contains exploits for Java, Internet Explorer, PDF, and Microsoft Data Access Components. Source: http://news.softpedia.com/news/New-Browser-Exploit-Pack-Private-Advertised-on-Hacker-Forums-366008.shtml

July 5, Softpedia – (International) **New service allows fraudsters to instantly generate scans of fake documents.** A researcher discovered a service on a Russian underweb market that allows cybercriminals to generate fake passports, ID cards, utility bills, and credit cards for use in fraudulent activities. Source: http://news.softpedia.com/news/New-Service-Allows-Fraudsters-to-Instantly-Generate-Scans-of-Fake-Documents-365941.shtml

July 9, Softpedia – (International) **McAfee details 4-year cyber espionage campaign against South Korea.** Symantec published a report on a 4-year cyberespionage campaign that targeted South Korean financial, government, military, and broadcasting organizations dubbed 'Operation Troy'. Source: http://news.softpedia.com/news/McAfee-Details-4-Year-Cyber-Espionage-Campaign-Against-South-Korea-366571.shtml

July 9, Softpedia – (National) **FAA's Civil Aviation Registry vulnerable to hackers, report finds.** The Office of the Inspector General for the U.S. Department of Transportation issued a report that states the Federal Aviation Administration (FAA) has not implemented needed security controls to make sure the systems of the Civil Aviation Registry cannot be breached. The reported stated the FAA was not in compliance with policies for PII encryption and account access controls. Source: http://news.softpedia.com/news/FAA-s-Civil-Aviation-Registry-Vulnerable-to-Hackers-Report-Finds-366697.shtml

July 12, Softpedia – (International) **Experts reveal how Chinese APT hackers abuse Dropbox and WordPress.** A report by Cyber Squared detailed how a Chinese advanced persistent threat (APT) group utilized cloud-based platforms in attacks such as the 2012 attack on the New York Times. Source: http://news.softpedia.com/news/Experts-Reveal-How-Chinese-APT-Hackers-Abuse-Dropbox-and-WordPress-367652.shtml

July 12, Health IT Security – (Texas) **Texas Health Harris Methodist Hospital reports data breach.** Patients admitted to Texas Health Harris Methodist Hospital Fort Worth between 1980 and 1990 were notified after the hospital discovered a portion of a microfiche that contained the patient's personal information and was meant to be destroyed by its paper-shredding vendor, Shred-It, was found in a park. As a result, the hospital changed its paper destruction vendors. Source: http://healthitsecurity.com/2013/07/12/texas-health-harris-methodist-hospital-reports-data-breach/

July 23, Help Net Security – (International) **U.S. the number one source of web attacks.** Imperva published its Web Application Attack Report, which found that retailers suffer twice as many SQL injection attacks as other industries, and that the U.S. was the largest source of Web attacks. Source: https://www.net-security.org/secworld.php?id=15269

July 23, U.S. Securities and Exchange Commission – (International) **SEC charges Texas man with running Bitcoin-denominated Ponzi scheme.** The U.S. Securities and Exchange Commission charged the founder and operator of Bitcoin Savings and Trust with running a Ponzi scheme that raised an amount of Bitcoins initially valued at $4.5 million and which currently exceeds $60 million. Source: https://www.sec.gov/servlet/Satellite/News/PressRelease/Detail/PressRelease/1370539730583#.Ue_Wfl21FKB

July 23, Softpedia – (National) **US Army sergeant admits to stealing information from Army computers.** A sergeant in the U.S. Army pleaded guilty to accessing the Army Knowledge Online accounts of two individuals without authorization. She initially gained access by tricking the help desk into giving her temporary passwords and used the information she obtained to harass the targeted individuals. Source: http://news.softpedia.com/news/US-Army-Sergeant-Admits-Stealing-Information-from-Army-Computers-370209.shtml

We interrupt this program to warn the Emergency Alert System is *hackable*

Publicly available SSH key makes it possible to hijack nation's warning system.

By Dan Goodin, Ars Technica, July 8 2013

The US Emergency Alert System, which interrupts live TV and radio broadcasts with information about national emergencies in progress, is vulnerable to attacks that allow hackers to remotely disseminate bogus reports and tamper with gear, security researchers warned.

The remote takeover vulnerability, which was fixed in an update issued in April, affected the DASDEC-I and DASDEC-II application servers made by a company called Digital Alert Systems. It stems from a recent firmware update that mistakenly included the private secure shell (SSH) key, according to an advisory published Monday (http://www.ioactive.com/pdfs/IOActive_DASDEC_vulnerabilities.pdf) by researchers from security firm IOActive. Administrators use such keys to remotely log in to a server to gain unfettered "root" access. The publication of the key makes it trivial for hackers to gain unauthorized access on Digital Alert System appliances that run default settings on older firmware.

"An attacker who gains control of one or more DASDEC systems can disrupt these stations' ability to transmit and could disseminate false emergency information over a large geographic area," the IOActive advisory warned. "In addition, depending on the configuration of this and other devices, these messages could be forwarded and mirrored by other DASDEC systems."

Other advisories warning of the vulnerability were published here (http://ics-cert.us-cert.gov/advisories/ICSA-13-184-02) and here (http://www.kb.cert.org/vuls/id/662676) by the Industry Control Systems Cyber Emergency Response Team and the US CERT. The US CERT advisory, which also warns against vulnerabilities in the One-Net E189 Emergency Alert System device sold by Digital Alert Systems' parent company Monroe Electronics, was published two weeks ago.

The warnings come five months after hackers took over the emergency alert system of a Montana TV station and broadcast a bogus emergency bulletin warning TV viewers of an imminent zombie apocalypse. Devices used by stations in Michigan, California, Tennessee, and New Mexico were also reportedly commandeered. "Civil authorities in your area have reported that the bodies of the dead are rising from the grave and attacking the living," at least one of the prank messages said. The advisories from IOActive and the CERT groups didn't say if the February attacks were carried out by exploiting the SSH key vulnerability.

The Emergency Alerting System is designed to enable the US president to deliver speeches to the entire country within 10 minutes of a disaster occurring. Application servers such as the DASDEC-I and DASDEC-II interrupt regular programming broadcast by TV and radio stations and relay an emergency message, which is preceded and followed by alert tones. In addition to tampering with the delivery of legitimate emergency messages, attackers who use the SSH key to log in to vulnerable systems could make unauthorized changes to the server and glean potentially sensitive configure information that could lead to additional hacks.

Read the rest here:

http://arstechnica.com/security/2013/07/we-interrupt-this-program-to-warn-the-emergency-alert-system-is-hackable/

Employees admit to accessing or stealing private company information

By Help Net Security, April 15, 2013\

Can anyone remember when computers and cell phones did not impact our daily lives? Today, the majority of us take for granted that these technological marvels are necessary for our daily existence. However, this has not come without a concomitant price, that being the enormous proliferation of cybercrime which is directly related to the prevalence of these devices. Cybercrime has now reached epidemic proportions, causing the loss of billions of dollars annually. Daily, crimes such as identity theft and fraud, online child exploitation, child pornography, hacking, and intellectual property theft continue to make headlines. Many illegal drug deals are arranged using e-mail and/or text messaging. Frequently, cell phones containing probative information are encountered at crime scenes. Digital surveillance systems routinely capture crimes as they are being committed. Not surprisingly, many individuals post information about their criminal offenses on one or more of the social networking sites!

In a survey of 1,000 employers by LogRhythm, 80 percent do not believe any of their workers would view or steal confidential information, while three quarters (75 percent) admitted to having no enforceable systems in place to prevent unauthorised access to company data by employees.

Interestingly, a third of those employers believe that they do not need such systems at all. In addition, around two thirds of companies surveyed (60 percent) do not regularly change passwords to stop ex-employees being able to access sites or documents.

However, in a corresponding survey of 2,000 employees, 23 percent admitted to having accessed or taken confidential data from their workplace, with one in ten stating that they do it regularly. The most accessed confidential data related to details of colleague salaries (38 percent) and details of colleague bonus schemes (23 percent).

94 percent of those who had accessed confidential information or stolen company data had never been caught.

“There is a clear gap between businesses’ internal security procedures and the harsh reality of employee behaviour,” said Ross Brewer, vice president and managing director for international markets at LogRhythm. “In an era where data breaches are considered inevitable, and with the government urging for greater consideration of cyber threats within businesses, the amount of employers who are doing nothing about unauthorised access across their networks – and the even higher number who don’t perceive any risk at all when it comes to employee data theft – is staggering.”

“Even more worrying than the lack of systems in place to stop employees stealing data is that many organisations still have no idea what’s happening on their networks at all. With recent government proposals to increase the sharing of cyber threat intelligence among businesses, the first stage must be to ensure that more employers have the right level of visibility to track suspicious or abnormal behavior on their own networks – but this is clearly not happening,” continued Brewer.

When asked, more than a quarter (27 percent) of employers could not identify the biggest threats to their confidential data, while 14 percent did not even know whether employees have stolen data – even though they believe employees would do so.

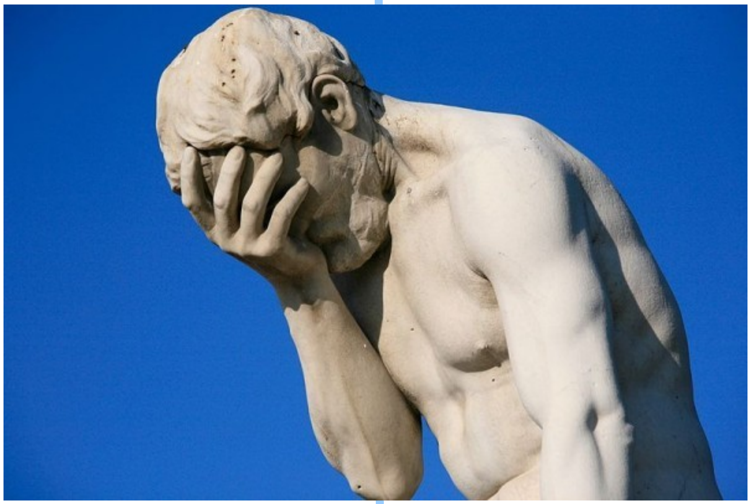
Read the rest here:

http://www.net-security.org/secworld.php?id=14746

The State Department's Cybersecurity Office Sounds Like an Awful Mess

By Adam Clark Estes, Gizmodo, July 23, 2013

There are government that finish projects on time, use technology to improve performance and protect Americans from imminent harm. Then there's the State Department's cybersecurity office. It seems to have a hard time just keeping the lights on.



A damning new report (http://oig.state.gov/documents/organization/212277.pdf) by the State Department's inspector general casts this anti-hacking office in a pretty dismal light. The so-called Bureau of Information Resource Management's Office of Information Assurance (IRM/IA) is responsible for safeguarding the secrets from dozens of embassies and consulates around the world, but based on the wording of the report, it operates like a rudderless ship. Broadly speaking, the report said that the office "wastes personnel resources," "lacks adequate management controls" and "has no mission statement." That's just the beginning, too.

The inspector general's office has plenty more bad things to say about the IRM/IA and its performance. They also take a dim view of the head of the bureau who's apparently never around to provide leadership or even guidance for the employees. On top of that, the office's regulations haven't been updated since 2007, which is eons ago in terms of developments in cybersecurity. All things told, the office "is not doing enough and is potentially leaving Department systems vulnerable," says the report.

Experts are unsurprisingly unimpressed with how the IRM/IA is performing. If this office isn't doing its job keeping America's secrets safe, it really does put our national security at risk. If any cybersecurity office should be held accountable for shortcomings, it should be this one, and this report is the beginning of that process. "This report reads like a what-not-to-do list from every policy, program, and contracting perspective," Scott Amey, general council for the Project on Government Oversight, told *Mother Jones* this week. "With stories about foreign entities hacking US government systems and questions about non-authorized access to classified information, this latest IG report causes major concerns about the State Department's ability to protect government systems."

Read the rest here:

http://gizmodo.com/the-state-departments-cybersecurity-office-sounds-like-879586167

Budget cuts force DHS to scale back cybersecurity programs

By Homeland Security News Wire, July 22, 2013

Sequestration-mandated federal budget cuts are beginning to have an effect on DHS cybersecurity efforts. Since March, the department has been forced to cancel two conferences and three training sessions for utility companies on how to defend against cyberattacks.

The *Wall Street Journal* reports that One of the cancelled conferences, which was due to take place next month, was for the Industrial Control Systems Joint Working Group (ICSJWG), a unit established to facilitate information sharing and reduce the risk to the U.S. industrial control systems.

“I was amazed they cancelled the [spring conference] because they had probably already spent a lot of money,” Dale Peterson, founder and CEO of Digital Bond, a control systems research and consulting firm said.

The *Journal* notes that the cancelled conferences were important for establishing public-private partnerships for cybersecurity defense of critical infrastructure

“Those two conferences [in May and August] are the main places where they can establish those partnerships,” Peterson told the *Journal*.

DHS’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) recently sent a memo to the CEOs of electric companies telling them to be vigilant about cybersecurity threats. The memo was sent after an alert in early May warning about “increasing hostility against U.S. critical infrastructure organizations,” according to a memo obtained by the *Journal*.

The memo outlined several rules that should be established by private critical infrastructure companies to shield themselves better against cyberthreats:

Read the rest here:

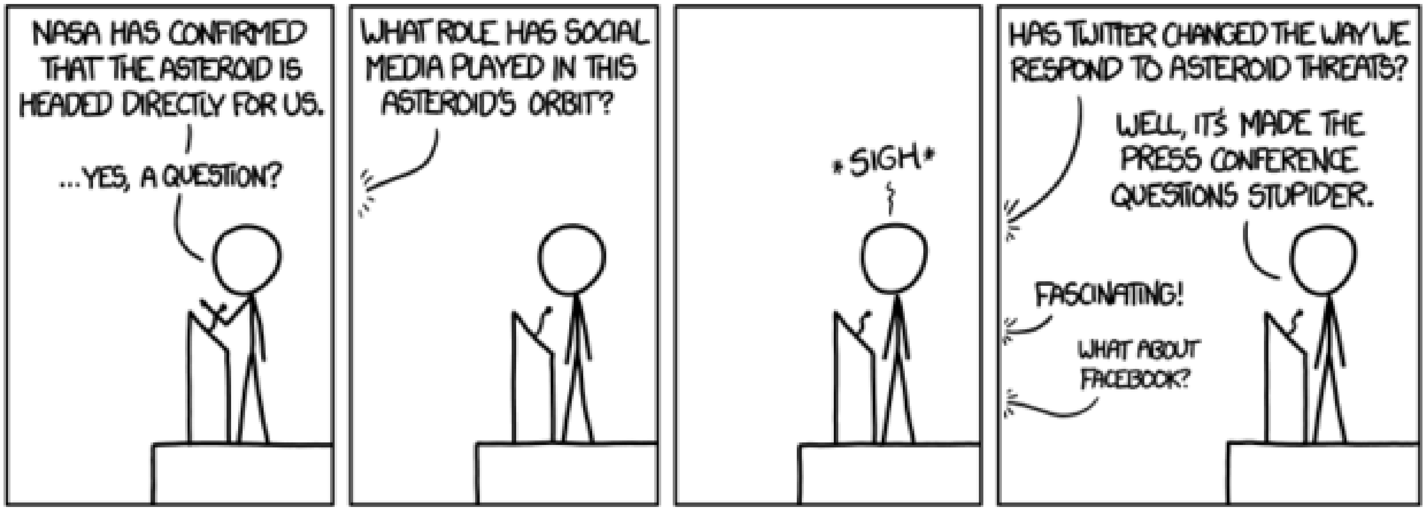
http://www.homelandsecuritynewswire.com/dr20130721-budget-cuts-force-dhs-to-scale-back-cybersecurity-programs

Volunteers Needed

Deborah Johnson is soliciting volunteers for the next ISSA-COS conference committee. Please contact her if you have an interest in helping on this committee. The venue is being narrowed down, but there are other planning tasks that need to be handled as well, such as marketing and publicity, brochures, programs, sponsors, door prizes, etc. so if you would like to take on any of these roles, let her know.

If you are interested in helping please contact her (*djohnson@swcp.com*).

Thank you in advance!


NASA HAS CONFIRMED THAT THE ASTEROID IS HEADED DIRECTLY FOR US.
...YES, A QUESTION?
WHAT ROLE HAS SOCIAL MEDIA PLAYED IN THIS ASTEROID'S ORBIT?
SIGH
HAS TWITTER CHANGED THE WAY WE RESPOND TO ASTEROID THREATS?
WELL, IT'S MADE THE PRESS CONFERENCE QUESTIONS STUPIDER.
FASCINATING!
WHAT ABOUT FACEBOOK?

Training: The next Security + training session will be September 7 at Colorado Technical University. Watch for more information to come via e-mail as we get closer.

Date	Time	Location
Aug 8	11:00 to 1:00	Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121
Sep 12	5:30 to 7:30	Bambino's
Oct 10	11:00 to 1:00	Bambino's
Nov 14	5:30 to 7:30	Bambino's
Dec 6	11:00 to 1:00	**Carrabba's North**

Information Systems Security Association
Developing and Connecting Cybersecurity Leaders Globally
Colorado Springs Chapter

WWW.ISSA-COS.ORG

Chapter Officers:

Mark Spencer—Chapter President
Dr. George J. Proeller—President Emeritus
Tim Hoffman—Executive Vice President
David Willson—Vice President
Melody Wilson—Treasurer
Lora Woodworth—Recorder
Don Creamer—Communications Officer
Jeff Pettorino—Member at Large
Brian Kirouac—Member at Large

Position Chairs:

Deborah Johnson—Coins
James Stephens—Director of Training

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Soon, Your Smartphone Could Be Powered by Pee

By Jamie Condliffe, Gizmodo, July 17, 2013

Plugging your phone into the main is for suckers. What you really need is one of a new breed of microbial fuel cells to drive your phone—so you can power it with pee.

A team of researchers from the University of the West of England, UK, have developed the new, small microbial fuel cell (MFC) which can turn organic matter—in this particular case, that happens to be your pee—into electricity.

To do that, the fuel cells are filled with special bacteria which chow down on the chemicals in the urine to fuel their own metabolic processes—in turn producing electrons, which are stored by the cell and used to provide power.

Read the rest here:
http://gizmodo.com/soon-your-smartphone-could-be-powered-by-pee-812526447

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing ™, Woodland Park, Colorado