Thanks and Good Bye

Colleagues,

I want to give everyone a big THANK YOU for all the help with the CSTTF conference. It was another successful conference. This year we had 5 Keynote speakers. The attendance at the conference was approximately 500 which breaks last years and 23 vendors. This conference gets better every year. Everyone seemed to enjoy the event and most stayed for the whole event.

We celebrated our 25th anniversary as a ISSA chapter with a social on the first night of the conference. It was a good time by all. Talking about how the chapter has grown!

Federal Business Council sponsored the 25th anniversary event and has already put in the invoice for the conference. The chapter will see a check for $4000 for this event. We do have the event in October that we need to support with FBC. This partnership has helped this chapter to grow.

At the end of the conference I did announce that I was resigning as the President of the chapter effective 26 August. I have moved to Alaska to take on a new job, and feel that I no longer can provide the leadership that this chapter needs and deserves. It has been a pleasure to be part of this chapter for the last 12 years. This is a great chapter, and I will miss the meetings, conferences and training.

The board members did meet and are ready to moved forward

(Continued on page 3)
A Cute Internet Star Flirts. All He Wants Is Your Password.

By Amanda Hess, NY Times, July 20, 2016

Jack Johnson — whose six-second bursts of comedy on Vine have propelled him to a fledgling pop-rap career — is one of the internet's biggest stars. Last week he told his nearly four million Twitter followers to send him their passwords. And in an hour, tens of thousands of fans complied — all for the slim chance to see a personalized video from Mr. Johnson pop up inside their accounts.

At first glance, this stunt, which Mr. Johnson called "#HackedByJohnson," looks like another case of teenagers traipsing through a social media minefield, oblivious to the real-world consequences.

But Mr. Johnson's fans are not naïve. Handing over their passwords to some strange, cute boy actually constitutes a minor act of youthful rebellion. The whole encounter delivers a heady mix of intimacy and transgression — the closest digital simulation yet to a teenage crush.

Mr. Johnson, 20, is not your traditional teenage heartthrob. While his partner in the duo Jack & Jack, the 19-year-old Jack Gilinsky, looks like a standard-issue junior American hunk — square jaw, pillowy lips, visible abs — Mr. Johnson seems more sidekick material, a scrappy runt with the charm of a man twice his size. He raps like Eminem's sweeter younger brother and carries himself with a Biebersque swagger. But unlike Justin Bieber, who canceled his concert meet-and-greets earlier this year because they left him "drained and unhappy," Mr. Johnson thrives on serving his fans.

And fan interaction has become a starmaking talent in and of itself.

To charm millions of strangers simultaneously, Mr. Johnson hops among Vine, Twitter, Snapchat and Instagram, tailoring his persona to fit each platform.

"The #HackedByJohnson tactic breaks through the surface of social media and reaches that rare private space, the inside of the fan's personal account."

On Vine, he's a sketch comic dealing in nerdy situational humor. On YouTube, he performs pop-rap about his chill California lifestyle. And in person, he acts as a hype man for his legions of fans.

When Tee Bradshaw, 20, first met Mr. Johnson at a Minneapolis concert in February, he flirtatiously took note of her cotton-candy-pink hair. "It looks almost edible," Ms. Bradshaw recalled Mr. Johnson's telling her. Mr. Johnson and Mr. Gilinsky each took a braid in one hand and held it in front of their faces like a novelty mustache, posed for the cameras, and posted the photo to their official Instagram account. The caption: "FRESHEST HAIR IN THE GAME."

"It made me feel really special," Ms. Bradshaw said, "to know that he thought that moment was worthy of being seen by literally everyone."

With #HackedByJohnson, Mr. Johnson has digitized — and supersized — that feeling.

The skill on display lands somewhere between improv and pickup artistry. For each "hacking" video, Mr. Johnson studied the lucky user's social-media profile, twisted his finger around a personal detail, held a cellphone camera within kissing distance and hit record. "Our picture in your icon is cute as hell," he tells one fan. "Where was that, was that Cleveland? I dunno. But anyways, we look good. Damn, we could be a couple maybe. But seriously: I hope your summer is going great."

Ms. Bradshaw sent her Twitter password to Mr. Johnson "at least 50" times, she said, until a mysterious new video popped up in her account: 16 seconds of Mr. Johnson sitting at a keyboard, playing a little melody and staring soulfully into the lens. "What's good, Tee?" he says. "I just wrote this one for you."

Read the rest here:
First, As we take a breath after completing another successful Cyber Security Training & Technology Forum (CSTTF) I would like to personally thank all the members who helped support the conference. The chapter wouldn’t be successful without your efforts. We are continuing to increase our membership—up to ~456 members as of the end of August. We will lose a few members as graduating students move on to new jobs and locations and we transfer them to new chapters. Congratulations on graduation; we will miss you but appreciate having had the opportunity to know you. Overall, we are successfully increasing our membership with renewals and new memberships—both general and students. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in, particularly as the new school year starts! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

Next, I would like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

We will continue to push our Freemium student program. We currently have 39 Freemium students as well as several other student members. We will be trying to track participation metrics to support our case for making the Freemium program a permanent program within ISSA. I would personally appreciate hearing from our Freemium students periodically regarding what activities they have participated in as well as their perspective on those activities. Were they relevant and useful? Any ideas to improve our activities would also be welcome. Your inputs will be critical to our ability to “sell” the Freemium program to the ISSA International board so please take a couple of minutes and provide some feedback to us.

The easiest way would be a quick email to me at dreed54321@comcast.net.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

(Continued from page 1)
and to continue to operate and move forward.

I want to thank everyone that been part of my membership in the last 12 years. George and Mark who supported and encourage me to be involved. As Vice President with Pat, we worked so well together and will never forget how right looks like. Melody for her advice and support. Colleen for doing training and growing what the chapter provides for the members. Shawn for stepping up at short notice to speak at the chapter meetings and conferences. Grace, Paul and Warren as the ones that were there for every event to do what needed to be done. Bill for the website, it still looks great. Don for doing the newsletter. Plus all other members that I have worked with and did not mention.

Cindy
Mini-seminar: 15 Oct, 9am-Noon:

Our next mini-seminar will be 15 October, 9am to noon. Topics to be covered during this mini-seminar will be announced later. These mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Please note that there will be no mini-seminar in September.

Are you missing out on a great opportunity for FREE continuing education credits? Are you missing out on an opportunity to share your knowledge/experience with your fellow Chapter members? Come to our mini-seminars and collaborate with your colleagues!

The idea of these "mini-seminars" is for members to give a 30 min or 1 hour (or longer) presentation on a topic of interest. Those giving the presentations would earn CPES/CEUs for the time spent preparing their presentation, and those attending would earn CPES/CEUs for their attendance and participation in any discussions. If you’re interested in presenting a topic, please email our Training Committee leads at: Training@issa-cos.org and let us know the topic you’d like to present and approximately how much time you’d like for your presentation. If there’s a topic you’d like us to cover during a mini-seminar, please let us know and we’ll see if someone in the Chapter is willing to develop a presentation for it.

Security+ Seminar:

No additional Security+ Seminars are currently planned for the rest of the year. If you are interested in attending a Security+ Seminar, please email our Training Committee leads at: Training@ISSA-COS.org and let us know. Security+ Seminars will start again next year, in March and June.

CISSP Seminar:

This year’s CISSP Seminar started 30 July and will be held on five alternating Saturdays: 30 Jul, 13 & 27 Aug, and 10 & 24 Sep. Do you already hold the CISSP certification? Did you know you can attend the CISSP Seminar for a refresher at no cost and obtain CPES? This is another great way to maintain your certification, and is an excellent benefit of being a member of ISSA-COS. If interested in attending any of the CISSP Seminar classes, please email the Training Committee leads at: Training@issa-cos.org to ensure we have a seat available for you, and to ensure we have a CPE certificate for you.

CISSP Study Guides:

Did you know that (ISC)² members are able to purchase the CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 7th Edition for a 50% retail discount? Log into (ISC)², and scroll down to the Security Central section. From there, look for the section that says: (ISC)² Textbook Discounts Get 50% off the Official CBK guides to all (ISC)² certifications. Click on the link provided.

Prefer a different CISSP study guide, or want an additional CISSP study guide? Sybex and Shon Harris both have updated their CISSP study guides, per the 2015 CISSP Common Body of Knowledge (CBK). Both books are now available. Ensure you purchase the 7th edition of either book (updated per the 2015 CBK) to get the latest and most current information.

SANS Courses in Colorado Springs:

SANS is coming to Colorado Springs! We’ve been working with SANS, trying to get them to bring their courses to Colorado Springs, in addition to Denver. SANS currently has the following courses scheduled on different dates, different locations in the Springs, with discussions ongoing for future courses. Based on responses and comments from the survey we did a couple months ago, these courses are what many of you requested. Register quickly, they may fill up soon!


(Continued on page 5)
Professional Outreach Director News

ISSA-COS has seen tremendous growth in companies wanting to sponsor meetings, introduce the Board of Directors to their technical accomplishments, and generally become very active in our organization. If you are a company who would like to network with our members, contact me, Suzanne Chance, the Professional Outreach Director, at suzanne.chance@gmail.com. We can connect you with the right people, whether they are ISSA-COS members or companies in the Colorado Springs area. Remember--we have well more than 430 members and are growing quickly. We would love to bring the right people together for everyone's benefit. Networking is a key perk that comes with involvement in our highly active and experienced chapter. It's good for you and good for us. We have many ways to connect you with qualified members seeking jobs, or desirable companies seeking cyber professionals.

Cheers!
Suzanne

(Continued from page 4)

SEC504: Hacker Tools, Techniques, Exploits and Incident Handling – December 5-10 - https://www.sans.org/community/event/sec504-colorado-springs-05dec2016-staff

Physical and Cybersecurity for Critical Infrastructure Training Course

This course will be taught in Colorado Springs on September 29, 2016, and it appears to be free, and provides 8 continuing education units.

The Texas A&M Engineering Extension Service (TEEX) is offering a new course for practitioners managing physical and cybersecurity. The course is the result of a partnership between TEEX, the NPPD Office of Infrastructure Protection and Office of Cybersecurity and Communications, and the FEMA National Training and Education Division. The new course, MGT 452 - Physical and Cybersecurity for Critical Infrastructure, encourages collaborative efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our Nation’s critical infrastructure.

Participants will identify physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure, and explore resources that can be applied to improve security within an organization, business, or government entity. The target audience is critical infrastructure owners and operators and individuals responsible for physical and/or cybersecurity within their organization, including Federal, State, local, regional, tribal, and territorial government officials, and owners and operators of small businesses and non-profit organizations. This instructor-led course is 8 hours in length and offers 8 CEUs. For more information, contact nerrtc@teex.tamu.edu.

Continuing Education (CEU/CPE) Ideas:

Do you know there are numerous free or low cost CEU and CPE options available? Check out the ISSA-COS web page (http://www.issa-cos.org/), Training Classes, “On-Line Training” link for suggested sites.

Volunteer Opportunities:

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs or (ISC)2 CPEs? We’re always looking for members to teach one or more of the Security+ or CISSP domains. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA or (ISC)2 criteria. If you would like to volunteer to teach one of the Security+ or CISSP domains, or if you have questions, please contact our Training Committee leads at: Training@issa-cos.org.

If you have ideas/suggestions/requests for training initiatives, please email our Training Committee leads at: Training@issa-cos.org.
America’s Electronic Voting Machines Are Scarily Easy Targets

By Brian Barrett, Wired, August 11, 2016

This week GOP presidential candidate Donald Trump openly that this election would be “rigged.” Last month, Russia decided to take an active role in our election. There’s no basis for questioning the results of a vote that’s still months away. But the interference and aspersions do merit a fresh look at the woeful state of our outdated, insecure electronic voting machines.

We’ve previously discussed the sad state of electronic voting machines in America, but it’s worth a closer look as we approach election day itself, and within the context of increased cyber-hostilities between the US and Russia. Besides, by now states have had plenty of warning since a damning report by the Brennan Center for Justice about our voting machine vulnerabilities came out last September. Surely matters must have improved since then.

Well, not exactly. In fact, not really at all.

Rise of the Machines

Most people remember the vote-counting debacle of the 2000 election, the dangling chads that resulted in the Supreme Court breaking a Bush-Gore deadlock. What people may not remember is the resulting Help America Vote Act (HAVA), passed in 2002, which among other objectives worked to phase out the use of the punchcard voting systems that had caused millions of ballots to be tossed.

In many cases, those dated machines were replaced with electronic voting systems. The intentions were pure. The consequences were a technological train wreck.

“People weren’t thinking about voting system security or all the additional challenges that come with electronic voting systems,” says the Brennan Center’s Lawrence Norden. “Moving to electronic voting systems solved a lot of problems, but created a lot of new ones.”

The list of those problems is what you’d expect from any computer or, more specifically, any computer that’s a decade or older. Most of these machines are running Windows XP, for which Microsoft hasn’t released a security patch since April 2014. Though there’s no evidence of direct voting machine interference to date, researchers have demonstrated that many of them are susceptible to malware or, equally if not more alarming, a well-timed denial of service attack.

“When people think that people think about doing something major to impact our election results at the voting machine, they think they’d try to switch results,” says Norden, referring to potential software tampering. “But you can do a lot less than that and do a lot of damage… If you have machines not working, or working slowly, that could create lots of problems too, preventing people from voting at all.”

The extent of vulnerability isn’t just hypothetical; late last summer, Virginia decertified thousands of insecure WinVote machines. As one security researcher described it, “anyone within a half mile could have modified every vote, undetected” without “any technical expertise.”

The vendor had gone out of business years prior.

The WinVote systems are an extreme case, but not an isolated one. Other voting machine models have potentially vulnerable wireless components; Virginia’s just the only one where a test proved how bad the situation was.

The worst part about the current state of voting machines is that they don’t even require outside interference to undo an election. “They’re all computers. They run on tens of thousands of lines of code,” says Norden. “It’s impossible to have a perfectly secure, perfectly reliable computer.”

That’s true, but in fairness, most computers aren’t quite this imperfect, either.

A Good Kind of Audit

So electronic voting machines aren’t ideal. The good news is, it’s entirely possible to mitigate any potential harm they might cause, either by malice or mistake.

First, it’s important to realize that electronic voting machines aren’t as commonplace as one might assume. Three-quarters of the country will vote on a paper ballot this fall, says Pamela Smith, president of Verified Voting, a group that promotes best practices at the polls. Only five states—Delaware, Georgia, Louisiana, South Carolina, and New Jersey—use “direct recording electronic” (DRE) machines exclusively. But lots of other states use electronic machines in some capacity. Verified Voting also has a handy map of who votes using what equipment, which lets you drill down both to specific counties and machine brands, so you can see what’s in use at your polling station.

Read the rest here: https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/
Not everything belongs on the Internet, and the American electoral process is a textbook example. But 31 states don’t see it that way.

The recent cyberattack on the Democratic National Committee has raised the specter of an Internet-based assault on the democratic process in the U.S., leading computer security experts to call on the federal government to do more to protect the voting process from hackers.

Since national elections involve some 9,000 separate jurisdictions, and they use a variety of technologies, the problem at first appears to be hopelessly complex. But there is a simple way to manage the risk of cybercrime: keep voting off the Internet.

Many states are currently exposing their systems to the risk of cyberattack by allowing voters to return absentee ballots via poorly secured e-mail, Web portals, or Internet-connected fax machines.

Internet-based voting has obvious potential benefits, especially for voters who live outside the country and for people in the military. But most security experts agree that it is not technically feasible to guarantee the security of online voting systems at this point.

Congress passed a law in 2009 that made it mandatory for states to electronically deliver blank ballots to voters in the military and overseas. But it said nothing about the electronic return of completed ballots. The authors of the legislation “knew there were unsolved security issues,” says Pamela Smith, president of Verified Voting, a group that advocates for the accuracy and transparency of elections. But if the law had gone so far as to issue a blanket restriction on online voting, it may not have passed. Instead, the door remained open for more states to begin offering voters the option to return their completed ballots using the Internet.

Of the 31 states that now do this, 29 allow it only for military and overseas voters, and several of those impose fairly tight restrictions on the process, according to Verified Voting. Utah extends the option to voters with disabilities, too. Alaska allows any voter in the state to use a Web portal to return a completed ballot.

Four other states besides Alaska use Web portals. Six states, including Florida, a crucial swing state for the 2016 presidential election, allow electronic ballot return only via fax, despite the fact that many fax machines now send data over the Internet. Twenty allow at least some voters to use either e-mail or fax to deliver their ballots.

Read the rest (and see the map) here:
How Hackers Could Get Inside Your Head With ‘Brain Malware’

By Victoria Turk, TechRepublic, August 3, 2016

Despite the efforts made to improve cybersecurity at many organizations, there are too many systems with aging infrastructure and vulnerabilities that leave companies at risk, with ransomware one of the most sinister threats, according to a new Cisco report.

Hackers have spyware in your mind. You’re minding your business, playing a game or scrolling through social media, and all the while they’re gathering your most private information direct from your brain signals. Your likes and dislikes. Your political preferences. Your sexuality. Your PIN.

It’s a futuristic scenario, but not that futuristic. The idea of securing our thoughts is a real concern with the introduction of brain-computer interfaces—devices that are controlled by brain signals such as EEG (electroencephalography), and which are already used in medical scenarios and, increasingly, in non-medical applications such as gaming.

Researchers at the University of Washington in Seattle say that we need to act fast to implement a privacy and security framework to prevent our brain signals from being used against us before the technology really takes off.

“There’s actually very little time,” said electrical engineer Howard Chizeck over Skype. “If we don’t address this quickly, it’ll be too late.”

I first met Chizeck and fellow engineer Tamara Bonaci when I visited the University of Washington Biorobotics Lab to check out their work on hacking teleoperated surgical robots. While I was there, they showed me some other hacking research they were working on, including how they could use a brain-computer interface (BCI), coupled with subliminal messaging in a videogame, to extract private information about an individual.

Bonaci showed me how it would work. She placed a BCI on my head—which looked like a shower cap covered in electrodes—and sat me in front of a computer to play Flappy Whale, a simple platform game based on the addictive Flappy Bird. All I had to do was guide a flopping blue whale through the on-screen course using the keyboard arrow keys. But as I happily played, trying to increase my dismal top score, something unusual happened. The logos for American banks started appearing: Chase, Citibank, Wells Fargo—each flickering in the top-right of the screen for just milliseconds before disappearing again. Blink and you’d miss them.

The idea is simple: Hackers could insert images like these into a dodgy game or app and record your brain’s unintentional response to them through the BCI, perhaps gaining insight into which brands you’re familiar with—in this case, say, which bank you bank with—or which images you have a strong reaction to.

Bonaci’s team have several different Flappy Whale demos, also using logos from local coffee houses and fast food chains, for instance. You might not care who owns your weak spot for Kentucky Fried Chicken, but you can see where it’s going: Imagine if these “subliminal” images showed politicians, or religious icons, or sexual images of men and women. Personal information gleaned this way could potentially be used for embarrassment, coercion, or manipulation.

“Broadly speaking, the problem with brain-computer interfaces is that, with most of the devices these days, when you’re picking up electric signals to control an application… the application is not only getting access to the useful piece of EEG needed to control that app; it’s also getting access to the whole EEG,” explained Bonaci. “And that whole EEG signal contains rich information about us as persons.”

And it’s not just stereotypical black hat hackers who could take advantage. “You could see police misusing it, or governments—if you show clear evidence of supporting the opposition or being involved in something deemed illegal,” suggested Chizeck. “This is kind of like a remote lie detector; a thought detector.”

Of course, it’s not as simple as “mind reading.” We don’t understand the brain well enough to match signals like this with straightforward meaning. But with careful engineering, Bonaci said that preliminary findings showed it was possible to pick up on people’s preferences this way (their experiments are still ongoing).

“It’s been known in neuroscience for a while now that if a person has a strong emotional response to one of the presented stimuli, then on average 300 milliseconds after they saw a stimulus there is going to be a positive peak hidden within their EEG signal,” she said.

The catch: You can’t tell what the emotional response was, such as whether it was positive or negative. “But with smartly placed stimuli, you could show people different combinations and play the ‘20 Questions’ game, in a way,” said Bonaci.

When I played the Flappy Whale game, the same logos appeared over and over again, which would provide more data about a subject’s response to each image and allow the researchers to better discern any patterns.

“One of the cool things is that when you see something you expect, or you see something you don’t expect, there’s a response—a slightly different response,” said Chizeck. “So if you have a fast enough computer connection and you can track those things, then over time you learn a lot about a person.”

Read the rest here:
The history of ransomware

By Ryan Francis, CSO, July 20, 2016

Ransomware has been the most pervasive cyber threat since 2005. According to publicly available information, ransomware infections have outnumbered data breaches 7,694 to 6,013 over the past 11 years.

Over the years there have been two distinct varieties of ransomware which remain consistent: crypto and locker based. Crypto-ransomware is ransomware variants that actually encrypt files and folders, hard drives, etc. Whereas Locker-ransomware only locks users out of their devices, most often seen with Android based ransomware.

New-age ransomware involves a combination of advanced distribution efforts such as pre-built infrastructures used to easily and widely distribute new strains as well as advanced development techniques such as using crypters to ensure reverse-engineering is extremely difficult. Additionally, the use of offline encryption methods are becoming popular in which ransomware takes advantage of legitimate system features such as Microsoft’s CryptoAPI, eliminating the need for Command and Control (C2) communications.

Terrance DeJesus of Solutionary’s Security Engineering and Research Team (SERT) takes a look back at the highlights and the evolution of ransomware throughout the years.

1989—Aids Trojan

The very first ransomware virus, the AIDS Trojan, was created by Harvard-trained Joseph L. Popp in 1989. 20,000 infected diskettes were distributed to the World Health Organization’s international AIDS conference attendees. The Trojan’s main weapon was symmetric cryptography. It didn’t take long for decryption tools to recover the file names, but this effort set in motion over almost three decades of ransomware attacks.

2006—Archiveus

Almost two decades (17 years) after the first ransomware malware was distributed, another strain was released. Unfortunately, this new strain was much more difficult to remove and used RSA encryption for the first time in ransomware history. The Archiveus Trojan encrypted everything in the “My Documents” directory on a system and required users to make purchases from specific Web sites to obtain the password to decrypt the files. Archiveus was also the first known ransomware variant to use Asymmetric encryption.

The unnamed Trojan of 2011

Jump five years and mainstream anonymous payment services make it much easier for hackers using ransomware to collect money from their victims without revealing their identity. Product related ransomware Trojans began to go mainstream that same year. A Trojan ransomware that mimicked a user’s Windows Product Activation notice informed users that their system’s Windows installation had to be re-activated due to fraud. A fake online activation option was offered but was ultimately a dead end for the users trying to resolve their issue, requiring users to call an international number. The malware claimed that this call would be free, but the call was actually routed through a rogue operator who placed the call on hold, causing the user to incur large international long distance charges to go along with their ransomware infection.

2012—Reveton

A major ransomware Trojan known as Reveton began to spread throughout Europe. Based on the Citadel Trojan, the piece of ransomware claimed the computer under attack had been used for illegal activities and that in order to unlock the system the user would be required to pay a fine using a voucher from an anonymous prepaid cash service. In some strains, the computer screen displayed footage from the computer’s webcam to give the illusion that the ‘criminal’ was being recorded. Shortly after this incident, there was a flurry of “police-based” ransomware including Urausy and Tohfy.

Researchers discovered new variants of Reveton in the United States, claiming to require the payment of a $200 fine to the FBI using a MoneyPak card.

2013—Cryptolocker

September 2013 was a pivotal moment in ransomware history as CryptoLocker was born. CryptoLocker was the first cryptographic malware spread by downloads from a compromised website and/or sent to business professionals in the form of email attachments made to look like customer complaints. CryptoLocker infections spread rapidly because threat actors leveraged the already existing GameOver Zeus botnet infrastructure. Operation Tovar in 2014 put a halt to the GameOver Zeus Trojan and CryptoLocker campaigns by targeting the Peer-to-Peer infrastructure used for distribution and support.

2014—Cryptodefense

Read the rest here:
http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html#slide1
How to Keep Cars Safe from Cyberattacks

By Sean Allocca, Forensic Magazine, August 24, 2016

In the age of the Internet of Things, even our automobiles come equipped with GPS, Bluetooth, and Wi-Fi that makes driving safer and easier. But with these new technological advances, so comes the danger of cyberattacks.

Researchers demonstrated how easily hackers can access sensitive equipment in a moving vehicle like the driver's radio, media console, and even the brakes and steering systems. A reporter documented one such takeover of a Jeep SUV in 2015. The hackers were able to remotely kill the engine while the vehicle was driving on a highway.

Now, new research from the University of Arkansas at Little Rock tackles the unusual problem of keeping cars safe from cyberattacks.

"These cars have become the trend of the future," said associate professor and project leader Dr. Shucheng Yu. "There could be some very severe consequences if someone hacked into the car. A car can be fully controlled by the hacker if it is not protected."

Through a National Science Foundation grant, the research focuses on developing a security protocol to protect the internal communication system in vehicle, known as the Controller Area Network (CAN).

By creating an extra layer of security, the team showed how the CAN system can be protected in two ways. The first security feature authenticates messages sent through the network by creating a security code. The second feature protects against "replay attacks," when a hacker tries repeatedly sending old messages to break into a network.

"There are many ways that hackers can control CAN," said researcher Zachary King, an undergraduate who participated in the project. "Once they access it, hackers can pretty easily control your car however they want. We are proposing to add a layer of security, so if an unauthorized person accesses it, they still wouldn't be able to control your vehicle."

Read the rest here: http://www.forensicmag.com/article/2016/08/how-keep-cars-safe-cyberattacks?et_cid=5493033&et_rid=454841830&location=top&et_cid=5493033&et_rid=454841830&linkid=http%3a%2f%2fwww.forensicmag.com%2farticle%2f2016%2f08%2fhow-keep-cars-safe-cyberattacks%3fet_cid%3d5493033%26et_rid%3d%subscriberid%26location%3dtop

Global cybercrime costs will exceed $6T annually by 2021

By Jessica Davis, Healthcare IT News, August 30, 2016

The cost of cybercrime around the globe will exceed $6 trillion annually by 2021 – more than double the annual cybercrime costs of 2015, according to a recent Cybersecurity Ventures report, sponsored by security firm Herjavec Group.

These costs include data damage and destruction, stolen money, loss of productivity, intellectual property theft, personal or financial data theft, fraud, embezzlement, business disruption after the attack, investigation, restoration and deletion of hacked data and systems.

The healthcare industry topped the list of most cyberattacked industries in 2015, followed by manufacturing, financial services, government and transportation agencies.

Further, cybersecurity defense costs are projected to exceed $1 trillion cumulatively from 2017 to 2021, according the report. And by 2020, more than 25 percent of identified enterprise attacks will involve Internet of Things, as 85 percent of security experts believe half of IoT products are insecure.

"Due to the anonymous and impersonal nature of the attack surface, cybercriminals test your assets from outside and in, looking for the most profitable ways to exploit the holes in corporate cyber defenses," Robert Steadman, vice president, Security and Compliance Consulting for Herjavec Group, said in a statement.

"The lack of user awareness when combined with a significant uptick in criminal activity (and improved tactics) has given rise to a number of large scale private and public sector breaches that have resulted in a global epidemic of issues surrounding confidentiality, integrity and availability of data and services," he added.

Ransomware attacks have risen a whopping 300 percent in 2016, the report found. And cybercriminals produced malware at a rate of 230,000 new samples per day in 2015. However, 2016 figures are predicted to be much higher. Even worse, a new zero-day vulnerability was discovered every day in 2015.

"Due to the anonymous and impersonal nature of the attack surface, cybercriminals test your assets from outside and in, looking for the most profitable ways to exploit the holes in corporate cyber defenses," Robert Steadman, vice president, Security and Compliance Consulting for Herjavec Group, said in a statement.

"The lack of user awareness when combined with a significant uptick in criminal activity (and improved tactics) has given rise to a number of large scale private and public sector breaches that have resulted in a global epidemic of issues surrounding confidentiality, integrity and availability of data and services," he added.

Ransomware attacks have risen a whopping 300 percent in 2016, the report found. And cybercriminals produced malware at a rate of 230,000 new samples per day in 2015. However, 2016 figures are predicted to be much higher. Even worse, a new zero-day vulnerability was discovered every day in 2015.

90 percent of security incidents stem from exploits against defects in software, according to the report. Furthermore, over 90 percent of corporate executives aren’t prepared for a major attack and are unable to read a cybersecurity report.

Risk and the Pareto Principle: Applying the 80/20 rule to your risk management strategy

By Joe Fantuzzi, RiskVision, August 30, 2016

Enterprises these days are putting more resources into monitoring and managing business risk. And with good reason – in light of a growing number of vulnerabilities and advanced threats, they’re dealing with a more complex risk environment that also impacts their technology partners and other third parties.

Of course, unknown and hidden vulnerabilities increase enterprise risk by leaving organizations susceptible to data theft, cyber espionage and other business disruptions. For regulated industries, vulnerability exploits can also result in hefty financial penalties and additional audits. What also may be less obvious, but eventually costlier, is that these vulnerabilities can often leave an organization susceptible to attack for years down the road.

Take the Yahoo breach as an example of the long and far reaching tail of business risk. While the breach itself likely dated back to 2012, it reared its head four years later in August 2016 when a hacker publicly announced that he had just placed 200 million Yahoo login credentials – including MD5-hashed passwords and date of births – for sale on the underground marketplace. And will this breach manifest in other ways down the road? More than likely.

While organizations are investing in Threat and Vulnerability Management (TVM) solutions to understand their exposure to risk, they’re also realizing that it’s nearly impossible to address the explosion of vulnerabilities that they’re suddenly detecting in their environment. A TVM solution might be a step in the right direction, but organizations also need to approach their risk posture more strategically.

Research indicates that the majority of risk (about 80 percent) is sourced to a fraction of their vulnerabilities (20 percent or less.) Looking ahead, that means organizations need to prioritize the vulnerabilities that present the most risk. By focusing on critical flaws with the potential for damage, enterprises can make a huge dent to business risk, while also streamlining threat management processes to be more efficient, cost effective and smarter.

Threat and vulnerability management and the Pareto Principle

In light of these threat trends, it’s not surprising that enterprise organizations are paying more attention to their risk posture and actively monitoring business risk – the growing number of cyberattacks and insider breaches that are often buried inside millions of events and vulnerabilities.

How can organizations hope to wrap their arms around all of those vulnerabilities hidden in their network? The short answer is that they probably can’t – and shouldn’t try. In order to truly understand their risk posture and address the threats that have the potential to cause the most damage, they need to be more strategic.

To start, organizations need to understand the Pareto Principle – otherwise known as the 80-20 rule – and how it applies to their threat environment. At a high level, the Pareto Principle, named for economist Vilfredo Pareto, stipulates that roughly 80 percent of the effects or results are attributed to 20 percent of the causes or invested input.

It’s a universal concept that also applies to users’ vulnerability environment. From a risk standpoint, that means that approximately 80 percent of the business risk that can cause the most harm comes from just 20 percent of the vulnerabilities.

So, in order to successfully gauge risk and develop an effective risk strategy, organizations will not only need to find vulnerabilities, they’ll need to identify and determine the right vulnerabilities – the ones that present the biggest risk both to their business and security posture.

In short, this is the equivalent of “finding a needle in a stack of needles.” The ability to locate, triage and then patch the most serious vulnerabilities is a lot more challenging than simply finding them. For that, organizations will need to invest in business risk and intelligence technologies which often includes some kind of Threat and Vulnerability Management (TVM) solution, designed to streamline the aggregation and correlation of asset vulnerability data with threat intelligence, while scoring risk and analytics prioritizing actions that tightly align with business objectives. In fact, solutions now provide risk intelligence coupled with TVM capabilities, which can also be offered from the cloud to accommodate an enterprise’s unique environment and scale as it grows.

But that’s just the beginning. Whatever solution that’s adopted needs to incorporate three salient macro-dimensions that will help enterprises to apply the Pareto Principle to their risk environment – rapidly identifying 20 percent of the most critical vulnerabilities while more effectively mitigating 80 percent of the impact.

**The Data Model:** Like the foundation of a building, the ability to locate, query and prioritize the data is where it all starts, essentially setting the stage for an effective Pareto Principle approach to risk.

Read the rest here: https://www.helpnetsecurity.com/2016/08/30/risk-management-strategy-pareto-principle/
Corporate directors focusing on cybersecurity

By Mike Freeman, San Diego Union Tribune, August 19, 2016

Pity the weary sysadmin who's just finished silencing the loudspeakers in the company's computers to keep data behind the air gap: processor fans can also be used to whisper your secrets.

As high profile data breaches continue to grab headlines, corporate boards need to make sure they're deeply involved in the cybersafeguards at their companies.

"They have to accept responsibility," said David Finn, a former federal prosecutor who spent 16 years leading Microsoft's efforts to fight cybercrime, counterfeiting and fraud. "It's not just a server room issue. It's a board room issue."

A group of national cybersecurity experts will discuss cyberthreats next week at the Corporate Directors Forum at Qualcomm's headquarters at 5775 Morehouse Drive. The San Diego non-profit helps corporate board members with training and networking.

Finn, who is now chief operating officer at AppEsteem in Seattle, will join Illumina Chief Information Officer Norm Fajeldheim and FBI Cyber Division Section Chief Philip Celestini on Tuesday (Aug. 23) for the Corporate Directors Forum meeting, which begins at 5:30 p.m.

After a high profile hack three years ago at Target that compromised personal data of millions of shoppers, the retailer's board ousted CEO Gregg Steinafel. The average cost of a data breach globally last year was $4 million, up 29 percent from two years earlier, according to a study by the Ponemon Institute, an independent research group. It costs companies on average $158 for every record lost or stolen in a breach.

"It is a very significant issue that is not going away anytime soon," said Finn in an interview. "Just look at the press over the last several years, whether it's recent hacks of the Democratic National Committee, Ashley Madison, JP Morgan, Anthem, Home Depot, Neiman Marcus, The Office of Personnel Management. It goes on and on."

Corporate boards sometimes view cyberthreats as an information technology department problem. They also may feel they lack the knowledge to oversee cybersecurity efforts.

But ballooning security budgets are bringing more scrutiny to the cyberthreat, with corporate directors often unsure what they need to spend to be safe.

Finn said cybersecurity needs to be tackled not as a technology issue but a "classic risk management issue."

"Given that you can't eliminate the risk completely, you have to prioritize your assets," he said. "You have to identify risk from third parties, look at whether your leadership has the understanding they need, make sure you are funded properly, think about disclosures if you are compromised. You need to have policies and procedures in place."

Federal guidelines from the U.S. Commerce Department's National Institute of Standards and Technology, the U.S. Securities and Exchange Commission and other agencies can help corporate boards get a handle on cybersecurity, he said.

"It can be addressed," he said. "I don't think board members need to fear it."

Read the rest here:
http://www.theregister.co.uk/2016/06/24/israeli_researcher_fans_fears_heres_another_way_to_cross_the_airgap/
Shadow Brokers Leak Just Revealed How The NSA Broke American-Made Encryption

By Thomas Fox-Brewster, Forbes, August 19, 2016

If the Shadow Brokers’ leak of NSA files is legit, as is now all but confirmed, they have offered a glimpse into how the intelligence agency exploited security systems created by American tech vendors. And one of the vulnerabilities has offered proof of just how the US’ finest digital spies were able to snoop on encrypted communications, in particular those provided by Virtual Private Networks (VPNs).

The weakness resided in Cisco’s PIX product, discontinued back in 2009, according to an analysis by London-based security researcher Mustafa Al-Bassam. The so-called BENIGN-CERTAIN exploit dropped by the Shadow Brokers was not dissimilar to the infamous Heartbleed hacks of 2014: the snoop would send specially-crafted requests to a Cisco PIX server – in this case what’s known as an Internet Key Exchange (IKE) packet – that would cause the device to dump pieces of its memory. Keep doing that and eventually the hacker could get the passwords for the PIX devices. The firewall could then be hacked.

As PIX firewalls were used to run VPNs using a protocol called IPSec, any organizations using the Cisco product for such supposedly-secure communication could have been spied on by the NSA with apparent ease. Al-Bassam gave the vulnerability a cute name to boot: PIXPocket.

Though Al-Bassam wasn’t able to test the exploits on a real Cisco firewall, others were. Researcher Brian Waters tweeted to show how he was able to grab test passwords for his PIX box.

A Cisco spokesperson said: “There is not a current PIX version to evaluate or update, and PSIRT has confirmed for me that the investigation so far has not identified any new vulnerabilities in current products related to the exploit you mention.” The spokesperson also pointed FORBES to the company’s end-of-life policy.

But whilst Cisco stopped selling PIX kit in 2009, many are believed to still use the tool. Using Shodan, a search tool for internet-connected devices, it was possible to find more than 2,000 servers just entering “PIX”. Many appeared to be Cisco products.

Even if few PIX tools remain in use, according to Al-Bassam, the leak would indicate that between 2002 and 2008, the NSA was able to break Cisco security. “Rewind a little bit and you had the biggest governments and businesses on PIX, and an intelligence agency potentially with a command line tool to get access. And nobody even understands how. That is crazy,” said British malware researcher Kevin Beaumont.

“The Snowden files made reference to the NSA having VPN access… I think we may know how finally.”

Read the rest here:

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
By Dan Goodin, ArsTechnica, August 2, 2016

Shortly after Carnegie Mellon University professor Lorrie Cranor became chief technologist at the Federal Trade Commission in January, she was surprised by an official agency tweet that echoed some oft-repeated security advice. It read: "Encourage your loved ones to change passwords often, making them long, strong, and unique." Cranor wasted no time challenging it.

The reasoning behind the advice is that an organization's network may have attackers inside who have yet to be discovered. Frequent password changes lock them out. But to a university professor who focuses on security, Cranor found the advice problematic for a couple of reasons. For one, a growing body of research suggests that frequent password changes make security worse. As if repeating advice that's based more on superstition than hard data wasn't bad enough, the tweet was even more annoying because all six of the government passwords she used had to be changed every 60 days.

"I saw this tweet and I said, 'Why is it that the FTC is going around telling everyone to change their passwords?'" she said during a keynote speech at the BSides security conference in Las Vegas. "I went to the social media people and asked them that and they said, 'Well, it must be good advice because at the FTC we change our passwords every 60 days.'"

Cranor eventually approached the chief information officer and the chief information security officer for the FTC and told them what a growing number of security experts have come to believe. Frequent password changes do little to improve security and very possibly make security worse by encouraging the use of passwords that are more susceptible to cracking. The CIO asked for research that supported this contrarian view, and Cranor was happy to provide it.

The most on-point data comes from a study published in 2010 by researchers from the University of North Carolina at Chapel Hill. The researchers obtained the cryptographic hashes to 10,000 expired accounts that once belonged to university employees, faculty, or students who had been required to change their passcodes every three months. Researchers received data not only for the last password used but also for passwords that had been changed over time.

"The UNC researchers said if people have to change their passwords every 90 days, they tend to use a pattern and they do what we call a transformation," Cranor explained. "They take their old passwords, they change it in some small way, and they come up with a new password."

The researchers used the transformations they uncovered to develop algorithms that were able to predict changes with great accuracy. Then they simulated real-world cracking to see how well they performed. In online attacks, in which attackers try to make as many guesses as possible before the targeted network locks them out, the algorithm cracked 17 percent of the accounts in fewer than five attempts. In offline attacks performed on the recovered hashes using superfast computers, 41 percent of the changed passwords were cracked within three seconds.

A separate study from researchers at Carleton University provided a mathematical demonstration that frequent password changes hamper attackers only minimally and probably not enough to offset the inconvenience to end users.

Over the past few years, organizations including the National Institute of Standards and Technology in the US and UK government agency CESG have also concluded that mandated password changes are often ineffective or counterproductive. And now, thanks to Cranor, the FTC has also come around to this thinking. But don't count on everyone doing away with regular password changes.

By studying the data, the researchers identified common techniques account holders used when they were required to change passwords. A password like "tarheels#1", for instance (excluding the quotation marks) frequently became "tArheels#1" after the first change, "taRheels#1" on the second change and so on. Or it might be changed to "tarheels#11" on the first change and "tarheels#111" on the second. Another common technique was to substitute a digit to make it "tarheels#2", "tarheels#3", and so on.

Contrary to what you've been told, frequent changes can be counter-productive.
How states use facial recognition to sniff out driver's license fraud

By Russell Brandom, The Verge, August 15, 2016

By the time the law caught up with him, Ronald Carnes had been on the run for 40 years. He'd been moving from state to state after escaping from a North Carolina prison in 1973, finally landing in Waterloo, Iowa, under a pair of assumed names.

He probably could have spent the rest of his life that way if it weren't for a facial recognition program in the Iowa Department of Motor Vehicles. Scanning through the driver's license database, the program found Carnes' face in the system under two different names, tipping police off to the fraud.

Those scans have become one of the most popular uses of facial recognition technology. Deep learning makes it easy and cheap to scan millions of photos for duplicates and fraud, and since it doesn't involve any extra data collection or access — you just need to find matching entries, not link them to an identity — privacy groups see it as one of the more benign forms of facial scanning. Forty-three of the 50 states have used some form of that technology, with seven of those states adopting the system for driver's licenses in the last three years. (The holdouts are California, Missouri, Louisiana, Mississippi, Maine, New Hampshire, and Vermont.) But while the scans are still limited, some worry those systems could be the first step toward something more troubling.

One of the driving forces behind the new DMV systems has been a wave of federal requirements — and newly available federal money to meet those new standards. The Real ID Act was passed in 2005 in response to the 9/11 Commission's identification requirements — including the requirement that driver's licenses be stored in digital form. States are still in charge of their own licenses, but if licenses don't meet the new federal requirements, they'll stop being valid for use in airports as early as 2018.

The act itself doesn't say anything about facial recognition, but it strongly encourages states to find ways to reduce fraud. Many have seen facial scans as a natural way of doing that, particularly since the act has come with a wave of federal grants for any state that needs money to try out a new fraud detection method.

During the same period, the FBI developed a powerful facial recognition system, which became fully operational in April of 2015. If the FBI needs to put a name to a face, the bureau can now scan through over 411 million photos spread across state and federal databases. Combined with the State Department's partner countries, that system can catch fugitives as far away as Nepal, as it did in the Neil Stammer case.

Read the rest here:

Hacker shows Reg how one leaked home address can lead to ruin

By Darren Pauli, The Register, Juny 20, 2016

It takes nothing more than a home address for hacker "Nixxer" to find enough information to ruin your life.

Nixxer is one of Australia's most skilled good-guy social engineers and at a recent event, and in subsequent chats with The Reg, demonstrated the potential damage rather than actually ruining a life. But the arsenal he showed - a mix of open source intelligence, custom tools, a knack for correlation and experience in how to siphon personal information - show how identity theft and worse are not hard to accomplish. And also how the most locked-down Facebook accounts leak like sieves.

Nixxer himself is a ghost. He doesn't use his real name and his real-self can't be found online.

His hacker identity is, however, used in public at events like the Unrestcon security confab in Melbourne, where he demonstrated how he can find enough information to access bank accounts.

To the gallows

On this occasion, Nixxer targeted an address that will lead to a family man in Kansas, US. Nixxer selected the address through a random search of online clipboard Pastebin for the keyword "dox" - the name given to private personal information made public.

Those records did not yield a name and Nixxer did not know if the street address was even real.

But it didn't take long to verify the address, through Google's and Microsoft's online mapping services, and in geospatial databases. Along the way he found not only details of the the man he sought but also the previous owners of the property. Checks against other public databases revealed how much the house cost, allowing the social engineer to make estimates on the household income necessary to purchase the home. He reckoned the combined income was about US$120,000.

Read the rest here:
http://www.theregister.co.uk/2016/07/20/silver_tongue_hacker_shows_how_one_home_address_can_lead_to_ruin/
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.

A Nostalgic Virus Is Infecting Windows Machines

They don’t make them like this anymore.

Anyone who visited FossHub on Tuesday to download either Start Menu replacement Classic Shell or the audio editor Audacity is at risk of having downloaded a trojan that feels like something out of the early 90s. The malicious code was written by a hacking crew calling themselves Pegglecrew.

YouTuber danooct1 explains that Pegglecrew’s program is both brand new and largely undetected by sites like VirusTotal. Even the fake installer is almost identical in file size to the original. Opening the infected version of either Audacity or Classic Shell appears to do nothing, but on reboot the user is greeted with the following message:

Read the rest here:
http://gizmodo.com/a-nostalgic-virus-is-infecting-windows-machines-1784817228