Colleagues,

Get ready for the 4th annual Cyber Focus Day! Our first conference of the year is on March 30th, 8:00am to 5:00pm, at the University of Colorado, Colorado Springs Campus (UCCS)! We have several excellent speakers, great topics, and it’s FREE to members! Military, government, and contractor personnel (with a .gov or .mil e-mail address) may also attend at no cost. Our Cyber Focus Day offers industry, government, military, academia, training, and other cybersecurity professionals a great opportunity to get up-to-date information on today’s rapidly evolving cyber risks, threats, and challenges. It’s also a great opportunity to earn continuing education credits. Speakers and topics include:

- Noel Kyle, Program Manager, Cyber Education & Awareness Branch, U.S. Dept of Homeland Security
  **Topic:** Closing the Gap: Forging Pathways to a Cybersecurity Career

  **Topic:** Should We Be Afraid of the Russians? A Case Study in Collaboration from the 2016 Elections
  - George Nazarey, Senior Systems Engineer, FireEye
  - Paul Parker, Vice President of Federal Engineering, Infoblox Federal, Inc.
  **Topic:** M-Trends 2017
  - Michael Seguinot, Federal Director, Exabeam
  **Topic:** DNS Security, Threats and Solutions
  - Lynne VanArsdale, Health Information Exchange Innovations Program Manager
  **Topic:** Duality of Modern Man – Everyone’s an Insider

A Note From Our President

By Ms. Colleen Murphy

If you haven’t already, please register now at: [https://www.fbinc.com/e/cfd/attendereq.aspx](https://www.fbinc.com/e/cfd/attendereq.aspx). Spread the word, let your co-workers know about the conference; let’s make this the biggest, best Cyber Focus Day ever!

Have you been a member of ISSA for

(Continued on page 11)

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.
How to secure a smartphone for the tweeter-in-chief


As President Donald Trump takes office, he has also taken up a new, digital symbol of the presidency. Before, during and since the campaign, he used an Android smartphone to conduct his business and tweet prolifically, directly reaching millions of followers. But when he was inaugurated, Trump surrendered that device and accepted in its place a smartphone that has somehow been made more secure.

It is a key move for a man who might now be not only the 45th commander-in-chief but also America’s first president with such devotion to Twitter. Many private companies deal with issues like this, in which employees joining the ranks already have a mobile phone they use for their personal life. Should that device be connected to company systems? Or should workers be issued a cumbersome second phone for work-only purposes? There are federal recommendations about that, but few firms are handling data as sensitive as the president’s phone might be.

A presidential smartphone is probably the most attractive target imaginable for foreign governments’ hackers. Attacking the phone could provide access to the highest secrets of national security, and near-constant real-time information about exactly where the president is, raising the potential for physical threats. Securing a phone like that requires several layers of protection.

Exactly what has been done to protect the president’s phone is intentionally left unclear to the public. But as a scholar of mobile security, I know that beyond overall network security measures, there are several technological approaches to securing a smartphone for special use. The most secure, however, is also among the least practical and least likely: ensuring the phone cannot connect to the internet at all. So how might have government cybersecurity specialists locked down Trump’s new phone?

**Hiding key information**

One level of protection is what is called “security by obscurity.” Many people presumably had Trump’s pre-presidential phone number. Now, relatively few people will have his new number. Similarly, his old phone’s internal device identifiers, such as its unique 15-digit International Mobile Equipment Identity number, or IMEI, may not have been as carefully guarded as those for his new phone. Keeping that information secret means the first hurdle for potential attackers involves figuring out which phone to attack in the first place.

Another layer of security involves ensuring the device was made by a trusted manufacturer, using trusted components, reducing the risk that the hardware would have any vulnerabilities that an attacker could exploit. Similarly, anyone who worked with or handled the phone at any step would have to be prevented from tampering with it to introduce any weaknesses.

Adding even more security in the physical device itself would be a specialized computer chip to add significant encryption capability for data stored on the phone or transmitted to or from it. Called a “Trusted Platform Module,” this hardware element is required by the Defense Department in all new devices handling military information. In addition, it could be used to ensure that any attempts to tamper with the phone, its settings or the operating system installed would be identified immediately.

**Custom configuration**

The phone also might be configured to connect only with certain predetermined phone and data networks that are regularly screened against intrusions. Limiting its contact with the internet would, of course, be key -- though that would also significantly limit the phone’s usefulness to a president whose routine involves constant connection.

To handle that middle ground -- finding a compromise between a full, unrestricted internet connection and a completely disconnected device -- Trump’s phone likely has some degree of customization. This could include a custom operating system, such as the Android variants the Department of Defense has developed.

Read the rest here:
Great news! The Freemium program was officially sanctioned by the ISSA International Board. They are now in the process of rolling out this program to all chapters who wish to participate. From an International perspective, the rules governing the program remain the same: Full time students, not fully employed in Cybersecurity, etc. Rather than being a separate membership type (as it was during the trial) we will provide a chapter unique payment code for them to use in the payment block when they join as a “Student” member. Students who don’t meet the Freemium criteria can still enroll as “Student” members, too. However, they will have to pay the current student membership rate of $55. At our next chapter board meeting we’ll need to discuss the mechanics of how we use this new tool. In the meantime, if you have someone you believe would meet the criteria for the Freemium payment waiver, please have them contact me. I will capture the information required to confirm eligibility and then I can provide them the payment code so they can join.

We are holding steady on our membership—~481 members as of the end of February. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

We still need more mentors! We have more people who want mentoring than we have mentors to support the program. Please contact Melissa Absher or me if you can support this worthwhile program for the chapter. It’s a good block to have on your resume when you submit your application for Senior Member, Fellow, or Distinguished Fellow.

Finally, 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.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

<table>
<thead>
<tr>
<th>New Members</th>
<th>February</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lynn Patterson</td>
<td></td>
</tr>
<tr>
<td>Francis Westley</td>
<td></td>
</tr>
<tr>
<td>Jacqueline Stewart</td>
<td></td>
</tr>
<tr>
<td>Albert Davila</td>
<td></td>
</tr>
<tr>
<td>Patrick Pivarnik</td>
<td></td>
</tr>
<tr>
<td>Jeff Dillard</td>
<td></td>
</tr>
<tr>
<td>Reid OLear</td>
<td></td>
</tr>
<tr>
<td>Bradley Goss</td>
<td></td>
</tr>
<tr>
<td>Joseph Squire</td>
<td></td>
</tr>
<tr>
<td>John Clagnaz</td>
<td></td>
</tr>
<tr>
<td>Patrick Light</td>
<td></td>
</tr>
<tr>
<td>David Zarsky</td>
<td></td>
</tr>
</tbody>
</table>
The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. The current cycle opened December 2, 2016 and applications will be accepted until July 10, 2017, at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2016 ISSA International Conference. Submissions received after August 1, 2016 will be considered in the following cycle.

Familiarize yourself with the Fellow Program, and the submission guidelines (http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/Fellow_Program/Fellow_Policies_Revised_June.pdf). If you have questions, contact Shawn or The ISSA Fellow Manager (fellow@issa.org) or call 866 349 5818 (US toll free) extension 4082.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

- 5 years of ISSA membership and 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify.

For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application.

To access the Senior Member application go to: https://www.issa.org/?Senior_member_App

For the Senior Member endorsement form go to: https://www.issa.org/?Senior_Mem_Endorse

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Shawn and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

- 8 years of association membership, 3 years of volunteer leadership in the association and 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty
ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards
245 E Taylor St  (behind Johnny’s Navajo Hogan on North Nevada)
Colorado Springs
(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

developing and teaching courses.

- All Fellow applications require a nomination to qualify

To access the Fellow application go to:

https://www.issa.org/?Fellow_App

To nominate a Fellow go to:

https://www.issa.org/?Fellow_Nom

To submit a Fellow letter of recommendation go to:

https://www.issa.org/?Fellow_Recommend

- 12 years association membership, 5 years of sustained volunteer leadership in the association, and 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

- All Distinguished Fellow applications require a nomination to qualify.

To access the Distinguished Fellow application go to:

https://www.issa.org/?Distinguished_Fellow

To nominate a Distinguished Fellow go to:

https://www.issa.org/?D_Fellow_Nom

To submit a Distinguished Fellow letter of recommendation go to:

https://www.issa.org/?Fellow_Recommend

Please help us identify candidates that we can recognize in our chapter! Please contact:

Shawn P. Murray, Chapter Recorder
5871charlois@gmail.com, 719-362-0666

(Continued from page 4)
Training Committee Update

Training and Education Update

The past month we had great participation and attendance at our first Mini-Seminar for 2017! Thank you everyone who attended and helped to make the day great. The Training Committee is gearing up for the first Security+ Seminar to be held April 1st and 8th at Colorado Technical University. We also discussed ways to expand our training offerings and collaborate with industry partners and the Pikes Peak Chapter of (ISC)^2 to expand our cadre of volunteer trainers. As always, this program succeeds and grows based on participation and feedback from our members so please feel free to stop me at a meeting, or drop the team an e-mail at Training@issa-cos.org.

Sincerely,
Luke Ingerman, C|CISO, CISSP, CAP
ISSA-CoS, VP of Training and Education

Mini-Seminars

Mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Mini-seminars provide continuing education, professional collaboration, and career broadening for members. They’re also a great opportunity for members to share their knowledge and experience with other members of the Chapter, and gain experience as a speaker, by volunteering to present a topic. Mini-seminars are generally held on a Saturday, from 9am – noon.

Additional details will be provided through the Chapter website (https://www.issa-cos.org), e-mails, and chapter meetings.

Security+ Seminars

Security+ Exam Prep Review Seminars are generally offered two times a year. All material has been reviewed and updated per the 2015 CompTIA SY0-401 criteria. The Security+ Seminar provides a comprehensive review of the CompTIA Security+ material to help students prepare for the Security+ exam. The 12-hour seminar is taught by certified Security+ or CISSP Chapter members, on two consecutive Saturdays, 9:00am to 4:00pm. Watch for Security+ seminar registration details in future newsletters.

Security+ Seminar #1 will be held on April 1st and 8th at Colorado Technical University (CTU).
To register, please visit https://www.eventbrite.com/e/issa-security-seminar-april-1-8-2017-tickets-28864574720
Security+ Seminar #2 will be held on June 3rd and 10th

CISSP Seminar

The CISSP Exam Prep Review Seminar is offered once each year. The CISSP Seminar provides a comprehensive review of the (ISC)^2 CISSP material to help students prepare for the CISSP exam. All material has been reviewed and updated per the 2015 (ISC)^2 Common Body of Knowledge (CBK) criteria. The 40-hour seminar is taught by certified CISSP Chapter members, on five alternating Saturdays, 8:15am - 4:45pm. Watch for CISSP Seminar registration details in future newsletters.

CISSP Seminar will be held on 29 Jul, 12 & 26 Aug, 9 & 23 Sep

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 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.

If you have ideas/suggestions/requests for training initiatives, please email our Training Committee leads at: Training@issa-cos.org.
A man detailed his escape from a burning house. His pacemaker told police a different story.

By Cleve R. Wootson, Jr., Washington Post, February 8, 2017

As the fire spread through Ross Compton’s $400,000 home, the Middletown, Ohio, man knew he had to get out, but first he had to grab a few things. Fifteen things, in fact, investigators determined.

He packed some of his clothes and other belongings in a suitcase. He put the stuff that wouldn’t fit in other bags. He grabbed his computer. He made sure to pick up the charger for his medical device. Then, he told dispatchers, he used his cane to break a window and hurl the bags out. After that, he says, he rushed out of the burning house.

Investigators were suspicious early on, said Deputy Fire Chief Jeff Spaulding. It seemed like a lot of work for someone escaping a burning house — especially a man who needed a pacemaker and an external heart pump to survive.

There were other suspicious signs. Spaulding, who was on his way to work when he was diverted to the fire, noticed signs that the blaze had started in several locations. And as the smell of smoke receded, Spaulding could smell gasoline.

Weeks later, as investigators mulled how to make an arson charge stick, they realized that they had a way of corroborating just how much scrambling Compton was doing during the fire: His pacemaker was tracking every beat of his heart.

“We’d be able to see did he exceed his threshold limit,” Spaulding told The Washington Post. “Or did his pulse drop below a certain rate. It won’t say what you’re doing, obviously, but it would help corroborate his story. It was much more informative than we thought.”

It disproved Compton’s story instead, Spaulding said.

After investigators were granted a search warrant, a technician collected data from Compton’s heart during a noninvasive procedure. “All he had to give us was his time,” Spaulding said.

Now, Compton is charged with aggravated arson and insurance fraud in the Sept. 19 fire. A grand jury indicted him last month after a doctor testified that he couldn’t have done the things he claimed during the fire.

A cardiologist who reviewed the medical data for the investigation concluded that “it is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions,” according to court documents obtained by the Middletown Journal-News.

Read the rest here:

7th ANNUAL CYBER SECURITY TRAINING & TECHNOLOGY FORUM (CSTTF)
August 30th & 31st, 2017
Double Tree Hilton Hotel • Colorado Springs, CO

https://www.fbcinc.com/e/csttf/
Will your organization be breached this year? I ask this question all the time in my classes. Most say no, their company will not be breached. But when asked if another company will, most say yes. So where is the disconnect? What makes your company more secure than your neighbors?

If you ask most senior IT or security executives whether their organization will be breached this year, and, if so, could they have prevented that breach, the answer will likely be Yes and Maybe respectively. Ask the C-Suite the same questions and their answers are likely No and Yes. Security and IT professionals rank security number one; whereas the C-Suite ranks security number nine. (The Economist, “The Cyber-Chasm”)

Data breaches are increasing and the lack of preparedness is causing huge recovery costs and loss of business and customers. (Ponemon, “2016 Cost of Data Breach study”)

If you suffer a breach what are the ramifications:
Potential class-action lawsuit or an investigation and fines by a regulatory agency? Assuming you can’t prevent the breach, can you avoid lawsuits by disgruntled customers or investigations by a State Attorney General (AG), the FTC, SEC, HHS, PCI (Purchase Card Industry), etc.? Prevent, probably not, but successfully defend; most likely!

The common factor in most of data breach class-action lawsuits as well as investigations by regulatory agencies is the allegation that the breached company failed to implement “reasonable security or protections” to prevent the breach. Logically then, if you implement “reasonable security and protections” you should be able to confidently defend your security practices and actions.

Reasonable Security

If you haven’t thought about what constitutes “reasonable security” lately or ever maybe the time to do so is right now! Most of us have become numb to the weekly news reports of another data breach, and shortly thereafter the report of a class-action suit being filed. Sadly these reports are only a small percentage of the actual number of breaches. Realistically the number is closer to two or more a day. Once a company is outed as having been breached, the potential for damage to the company’s reputation and the threat of a lawsuit hangs in the air. These are not the only threats plaguing breached companies though. Many companies have also found themselves suddenly being investigated and possibly fined by regulatory agencies such as the FTC, SEC, HHS or a State AG.

Since most of the data breach class-action suits and regulatory investigations claim breached companies did not implement “reasonable security or protections,” it is logical to assume that “reasonable security” is the antidote to getting sued or fined. This article will look at some of the claims and allegations made in the lawsuits and agency findings as well as the requirements or guidance provided by regulatory agencies and States in order to develop a clear definition and standard for “reasonable security.” As we will see, most of the allegations against breached companies include a failure to implement or properly utilize software, hardware and techniques which are very basic. Bottom-line, most companies are not even implementing the basics.

Class-Action Complaints

A sample of the allegations in the 13 class-action lawsuit complaints I researched include: the breached companies did not use encryption, failed to use good passwords, didn’t use a firewall or improperly configured the firewall, did not use or failed to properly update antivirus, failed to implement good vendor security, failed to segment networks separating sensitive information from common or public networks, failed to implement adequate intrusion detection systems, failed to notify customers in a timely manner, continued to utilize outdated software/hardware and, or failed to properly implement a legally or contractually required standard like PCI. These companies include Target, Home Depot, Anthem, Experian, Trump Hotels, Wendy’s, Wyndham, just to name a few.

(Continued on page 9)
Compliance Failures

Of the 13 class-action lawsuits which I reviewed, 10 of the breached companies were alleged to have failed to use or improperly used encryption. Security practitioners for years have been encouraging companies to use encryption, and many data privacy laws such as HIPAA and some enacted by various States have stated that there would be no requirement to notify if the data that was breached was encrypted.

- The complaints also alleged, in some cases specifically and others more broadly, that the breached companies failed to implement various industry standards and “best practices.” “Best practices” is a term frequently used in the security industry. One of the most popular set of so-called “best practices” is “The CIS Critical Security Controls for Effective Cyber Defense.” Many States recommend “best practices” as part of a good or reasonable security program and refer to the CIS Critical Security Controls for Effective Cyber Defense as an example of “best practices.” As stated, many of the 13 companies researched did not even implement basic security standards or did not do so competently. Therefore, it would appear that the recommended best practices really equate to “basic practices.”

Basics: Inventorying the assets a company possesses that store or transmit data; restricting administrative access to a need to know; implementing intrusion detection (IDS) and boundary defenses, e.g. firewalls, etc., would all constitute commonsense basics.

In five of the 13 complaints, the breached companies failed to destroy sensitive information once it was no longer needed.

Basics: Draft and implement a policy that identifies the data to be destroyed and when, on a continuing basis, similar to implementing regular backups.

In one regard the research indicates companies are getting better with regard to security issues that have been highlighted for years. Only two of the 13 complaints claimed that the breached company did not utilize good passwords. The complaints against Wendy’s and Target allege they did not assign strong passwords to their security solution in order to prevent application modification.

Basics: Require the implementation of good passwords. Not words or easily guessed passwords.

⇒ In five of the complaints, the companies failed to employ regular updates to software or replace outdated hardware or software. Security is a process and cannot be treated as a “set and forget” concept.

Basics: Implement a policy and procedures to ensure updates are accomplished. This is a huge task for many companies since software updates, in many cases, should be sandboxed and tested prior to implementation. But, ignoring it creates vulnerabilities.

⇒ Three of the complaints alleged that the companies either did not have a firewall or the firewall was improperly configured.

Basics: As stated above, perimeter defenses are key. You have to be able to detect at least basic to intermediate attacks. No one and no security can prevent all intrusions, but not implementing basics in an attempt to detect intrusions is tantamount to negligence.

⇒ The above are just some of the allegations. See the “Reasonable Security - Breached Companies Spreadsheet” for all of the research.

Data Breach Victims Common Failures

The allegations are not that companies were tricked or did not implement the latest and greatest security, but did not do the basics. For instance, none of the 13 class-action complaints alleges that any of the companies negligently clicked on an email attachment or link that introduced malware to the network causing the breach. It is unlikely a company would be accused of being negligent any time soon for a mistake or an incident wherein an employee was tricked by a hacker. Mistakes happen, but companies must still show due diligence in their efforts to protect data.

One thing is clear in all of the complaints: All breached companies were on notice about the pervasiveness of hackers and the overwhelming potential for such companies to be the next victim. In fact four of the 13 companies had previously suffered a breach that was publicly known. Realistically, most of the companies likely suffered a breach previously but the breach did not become publicly known.

If by law or contract you are subject to a particular standard, e.g. GLBA, HIPAA, PCI, etc., or regulatory guidance, it likely behooves you to at least strive to meet that guidance or standard and ensure legal compliance. If some of the requirements don’t make sense for your company, you may be able to make a sound business argument as to why that requirement in the guidance or standard was not applicable to your company and circumstances and may actually cause greater security issues.

States Guidance

We can also find some guidance as to what might be considered “reasonable security” by reviewing guidance provided by States in their privacy and data breach laws. The following States, and to some degree most states, all advocate or require any business that collects personal information to implement “reasonable security” protections or practices. This is not an exhaustive list but a sampling.

⇒ California: “Requires businesses to use ‘reasonable security’ procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure.”

⇒ Oregon: Businesses “shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information,

⇒ Rhode Island: Businesses “shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization.”

(Continued on page 10)
At this point you may be noticing that “reasonable” is a very subjective standard. In some instances though, like California, the guidance includes a recommendation to review and seek to implement the CIS Critical Security Controls for Effective Cyber Defense.

Regulatory Guidance and Standards

When it comes to federal regulatory guidance and rules, the FTC, via the “Standards for Safeguarding Customer Information (Safeguards Rule),” appears to be the most active in investigating and pursuing breaches. The Safeguards Rule states in part: “This part [§314.1], which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act (GLBA), sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.” Companies must show due diligence in protecting customer information, due diligence being defined as, “the care that a reasonable person exercises to avoid harm to others or their property.”

A review of an FTC action against a breached company should shed some light on what “reasonable security” may look like. For instance, in the Petco case, the FTC claimed that Petco:

1. Created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, in violation of bank rules;
2. Did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
3. Failed to employ sufficient measures to detect unauthorized access or conduct security investigations;
4. Failed to encrypt personal information; and,
5. Stored customer information in files that could be accessed anonymously by using a commonly known default user ID and password.

As stated by Joel Hanson in his 2008 article, “If a business is attacked by hackers or other kinds of thieves stealing sensitive consumer information, the FTC may not take action against the business if it finds that the business has employed reasonable and appropriate measures to secure the personal information of its customers. Such measures include adequate security software, protections against well-known hacking methods, limiting the time personal information is stored, limiting access to networks, and having a method of detecting and investigating unauthorized access. Further, businesses should take precautions against the threat of insider theft of consumer information.”

FCC Guidance

The guidance by the FTC states,

A sound data security plan is built on 5 key principles:

1. Take stock. Know what personal information you have in your files and on your computers.
2. Scale down. Keep only what you need for your business.
3. Lock it. Protect the information that you keep.
5. Plan ahead. Create a plan to respond to security incidents.

Each of these principles includes further details for implementing “reasonable security.”

Again, the term reasonable is used, but with very little specific guidance and criteria. In most guidance wherein the term reasonable is use, the organization then points practice criteria like the CIS Critical Security Controls for Effective Cyber Defense or various standards like NIST and ISO. Meeting a “reasonable security” standard requires implementing and deploying a plan that you, the leadership of the company, can confidently defend. One that will make it difficult for an attorney in a class-action suit, or an agency like the FTC or State Attorney General to claim you were negligent in your effort to protect data. Certainly you should assume that “reasonable security” would include meeting “basic security” standards.

Getting Started

1. First, start with an assessment looking at the risks to your organization relative to the loss or theft of data, as well as known vulnerabilities in your software, and the processes and procedures you use;
2. Draft a plan to address risks and correct deficiencies and vulnerabilities. Implement the security basics that make sense for your organization by choosing from the myriad of guidance and standards that exist, and work from there;
3. Capture how you will implement and accomplish security in your organization in a written plan that is very detailed. Train all employees so your new plan, as well as the policies and procedures are thoroughly understood and implemented by the entire workforce;
4. Finally, ensure your security plan/policy includes measures for identifying a data breach and the steps to follow once this identification is made. Such steps include, sample statements to release to the public, which vendors to call for support, conducting forensics, how to notify customers and shareholders and when, etc.

There is a growing trend wherein companies employ a law firm to oversee and manage their incident response. Using a law firm to hire and manage vendors, such as a forensic examiner, security company, public affairs company, etc., will ensure that any communication between you, the vendors and the law firm are, for the most part, protected under the attorney-client privilege.

Preparation is the Key

Despite what many believe, security is not rocket science. It is commonsense and hard work. Do what’s right and stand by your decisions. Burying your head in the sand won’t make it go away or make it better. The goal is not to prevent a breach. The goal is to prepare for that ever
looming breach, lower risk and reduce or eliminate liability to minimize or eliminate the threat of a lawsuit or fines, by implementing a “reasonable security” program you can confidently defend.

End Notes

1 “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category; companies that have been hacked and will be hacked again.” See, Federal Bureau of Investigation Speeches, RSA Cyber Security Conference, San Francisco, CA (March 2012).
2 Less than 24 hours after the Anthem breach was publicly acknowledged a lawsuit was filed. See, Schenker, Lisa, “Anthem in legal crosshairs as three class-action lawsuits filed over breach.” Modern Healthcare (Feb. 2015).
4 See “Reasonable Security Breached Companies Spreadsheet” at: http://www.psatec.com/downloads/, or at: https://cyberwarandtheboardroom.wordpress.com/about/, wherein I reveal my research on class-action lawsuit complaints.
5 The standards referred to here are not legally required or such as HIPAA or GLBA, or contractually required such as PCI, but are industry recommended standards.
6 CIS Critical Security Controls, at: https://www.cisecurity.org/critical-controls.cfm
7 Id. at note 4.
10 California Civil Code §§ 1798.29, 1798.80 et seq.
11 Oregon § 646A.600 to .628, 2015 S.B. 601, Chap. 357.
12 Rhode Island Gen. Laws § 11-49.2-1 et seq.
16 Id.
18 This does not refer to a technical vulnerability scan, e.g. vulnerability assessment or penetration test, which should be accomplished at least annually, but this refers to seeking to understand the vulnerabilities in your processes and procedures and how you physically control access to and the flow of sensitive data.

David Willson is a licensed attorney, CISSP and owner of Titan Info Security Group. He focuses on helping companies with risk management, cyber security, risk assessments, policy review and development, incident response investigation management, messaging, reputation management, cyber awareness training, and cyber and data protection legal issues, among other issues. He can be reached at: david@titaninfosecuritygroup.com.

Cyber Focus Day

(Continued from page 1)

five years? Do you have 10 years of relevant professional experience? If so, you may be eligible to become an ISSA Senior Member. Have you been a member of ISSA for eight years, and served for three years in a leadership role? Do you have five years of significant performance in the profession such as substantial responsibilities in leading a team or project, performing research with some measure of success, or faculty developing and teaching courses? If so, you may be eligible to become an ISSA Fellow. These are the general criteria from ISSA International’s website to apply for Senior Member or Fellow recognition. Don’t miss out on getting the professional recognition you’ve earned. Talk to the Recognition Committee, or any Board member, about how to apply. We’ll help you with your submission, endorsement from the Chapter, and for Fellow candidates, a nomination from a current Fellow or Distinguished Fellow.

Colleen
The New 8570 Certification

By Kurt Danis, ISSA-COS, February 22, 2017

On February 3, 2017, the DoD Deputy Chief Information Officer for Cybersecurity approved the Global Industrial Cyber Security Professional (GICSP) certification. The new cert is part of the GIAC certification family.

As a result, DISA updated the 8570 baseline certification chart. The chart (shown here) can also be viewed or downloaded from:

http://iase.disa.mil/iawip/Pages/iabaseline.aspx

Background on GIAC certifications.

According to Wikipedia, the SANS Institute founded the GIAC certification entity in 1999 and the term GIAC is trademarked by The Escal Institute of Advanced Technologies. In a nutshell, GIAC is focused on the certification business; and SANS is focused on the training business.

As of January 21, 2017, GIAC claims to have granted 89,827 certifications worldwide. GIAC certifications are stratified into two general levels:

- The "silver" level certification is achieved upon completion of a multiple choice exam.
- The "gold" level certification can be obtained by completing research paper and has the silver level as a prerequisite.

Readers must admit that many of the GIAC research papers are quite useful for research and education artifacts. Furthermore, many are available free on the web. See the SANS Reading Room.

Clearly, the GIAC reputation is evidenced by the professional quality of their research papers. On the flip side, the reader should also be aware that earning and maintaining a GIAC certification comes at a higher cost than many other certs. Of course, the benefits may outweigh the costs. In conclusion, the astute practitioner should research Continuing Professional Experience/Education (CPE) requirements before investing in any professional certification.

The following sites provide CPE requirements for five popular cybersecurity certification vendors:

http://www.giac.org/certifications/renewal#CPE_categories
https://www.isc2.org/maintaining-your-credential.aspx
https://certification.comptia.org/continuing-education/how-to-renew/earn-continuing-education-units
http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/Maintain-Your-CISA.aspx
https://cert.eccouncil.org/ece-policy.html (addresses recertification requirements. CPE requirements only appear on blog pages.)
By Brian X. Chen, New York Times, February, 01, 2017

Modern homes today are getting internet-connected light bulbs, thermostats, TVs and speakers. So with a simple voice command or the touch of a button on our smartphones, we can set the temperature, turn on a light or prepare the TV to record a program.

What could go wrong?

A lot more than most people are prepared for, it turns out. If one of these devices gets hijacked, hackers could potentially snoop around for sensitive data like financial or health information. Or they could use a network of compromised devices to perform a widespread attack that takes down major websites, which is what happened last October.

The good news is that so far, online attacks on home devices are relatively uncommon. Only 10 percent of American consumers said they were victims of the crime in a recent study done for the Hartford Steam Boiler Inspection and Insurance Company. However, those who experienced such an attack through their home gadgets reported losses of $1,000 to $5,000 from the incidents.

“There’s still this whole sort of, ‘Gee whiz, it’s so cool’ thing that’s going on” with internet-connected home appliances, said Lee Tien, a lawyer for the Electronic Frontier Foundation, a nonprofit that focuses on digital rights. “That’s also what often gets us into trouble.”

As smart home devices become more popular, they will become bigger targets for hackers. So it behooves us to get ahead of the curve by securing our home appliances, using these tips from security experts who have closely studied smart home accessories.

When shopping for an internet-connected home device like a smart speaker, lighting system or television set, a good rule of thumb is to go with a trusted brand.

Larger, well-regarded companies like Amazon or Google have a background in developing products with security in mind, said Liviu Arsene, an analyst for Bitdefender, which sells security hardware for protecting smart home accessories. Before buying a product, consumers should do a web search on it to see if the company regularly issues software updates that fix security vulnerabilities, he said.

People should also carefully read company privacy policies. David Britton, a vice president in the fraud and identity department of Experian, the credit reporting agency, said people should be curious about whether companies themselves were a threat to user privacy.

“What are they capturing about you?” he said. “Is the data leaving the device? Is it being sent back to the mother ship?”

Consider the smart speakers from Amazon and Google. Amazon said its Alexa smart assistant, which is used in its Echo speakers, automatically downloads software updates to defend against new security threats. Data from the Echo is also uploaded to Amazon’s servers only after people utter the wake word “Alexa,” the company said. That minimizes the likelihood that the device will record conversations unrelated to requests intended for Alexa.

Google said its Home speaker similarly issued regular software updates and employed advanced security features, like a technique that disables the device if its software is tampered with. The company added that the speaker processed speech only after the words “O.K. Google” or “Hey Google” were detected.

But other large brands occasionally engage in behavior that customers may find objectionable. The smart TV maker Vizio, for example, made headlines with revelations from the investigative news site ProPublica that it kept a detailed record of customer viewing habits and shared it with advertisers, who could then use the information to identify other devices you owned.

Read the rest here:
Your Medical Device Is In My Internet of Things

By Martin McKeay, Security Intelligence, February 25, 2017

A few months ago, I was at a birthday party with one of my sons when another young man took out a medical device that had a long, thin tube leading back into his pocket. When asked, he identified it as his insulin pump, which he needed to check and set appropriately before having a piece of cake. “It’s capable of connecting to my phone via Bluetooth, but I’ve never set it up and wouldn’t know what to do with it anyway,” he said.

Our short conversation highlighted many of the issues we should be concerned with when the world of medical devices meets the Internet of Things (IoT). This young man was carrying a device that his life literally depends upon, and while he knows the basics of the device, he doesn’t understand the full extent of its capabilities or vulnerabilities. Unluckily, the same can probably be said of the device’s manufacturers.

Securing the Medical Device

Honestly, security has been low on the priority list for most medical device manufacturers. Reliability is a much bigger concern, as it should be. But cybercriminals have been picking away at them since at least 2008, when researchers explained how a pacemaker could be subverted to give life-threatening shocks to its owner. While companies have taken threats like this seriously and in general fixed the problems quickly, preventing this type of vulnerability through increased focus in the software development and testing areas has not become a priority for most organizations.

But this will likely be changing in the near future: The U.S. Food and Drug Administration (FDA) has released a draft of proposed guidelines for medical device manufacturers, the succinctly named “Postmarket Management of Cybersecurity Medical Devices.” This paper laid out basic guidelines for understanding and compensating for the risks that medical IoT devices will likely face, patching and how such vulnerabilities will be reported to the FDA and the device users.

Perhaps the most important part of the paper is that it described potential suggestions for dealing with the people researching medical IoT devices. In other words, it recommended what to do when a white-hat hacker finds a vulnerability in a device and reports it.

I found this paper from the FDA to be filled with good advice — not just for medical IoT manufacturers, but for anyone who’s developing a program for external researchers to report issues. In other words, a bug bounty program.

While the FDA paper doesn’t explicitly talk about paying for vulnerability research, it does discuss about many of the considerations that go into making such a program. There’s significantly more to the paper, most of it fundamental to any good security program, but this is what stood out the most to me.

Additional Guidelines

External to the FDA, but also pushing in the right direction for the security of medical IoT devices, a group of security professionals called I Am The Cavalry published a Hippocratic Oath for Connected Devices. While the oath calls for some of the same controls the FDA’s guidance pointed toward, it goes far beyond, listing five core cybersecurity capabilities, including security by design and resilience. Perhaps we’ll see the FDA adopt several of the points from this Hippocratic Oath to encourage manufacturers to take further steps to secure their devices development through to deployment and beyond.

My one criticism of the FDA’s guidelines is that they leave too much of the decision of what should be reported and how specific risks and vulnerabilities should be graded to manufacturers. The outline does include a few good examples of what controlled and uncontrolled risks are, but leaves it up to the manufacturer to judge where the line is.

We’ve seen multiple examples of manufacturers who refuse to acknowledge reported vulnerabilities in all industries, not just medical devices, which points to the need for concrete, defined reporting regulations rather than general ones. The guidelines are in comment phase, so there’s hope this will change as they approach finalization.

Read the rest here: https://securityintelligence.com/your-medical-device-is-in-my-internet-of-things/
In recent years, a growing number of data breaches have resulted from the improper data removal and insecure storage of drives. Organizations face a myriad of internal and external challenges with preventing sensitive personal and corporate information from being accessed or breached from solid state drives (SSDs), according to the Blancco Technology Group.

According to over 300 IT professionals surveyed in the United States, Canada, Mexico, United Kingdom, France, Germany, India, Japan and China, 62 percent of organizations believe encryption is sufficient to protect data from being accessed or breached. On top of this, 70 percent said they rely on encryption to prevent data loss/theft from SSDs and 35 percent reformat the drives.

Moreover, when IT assets containing SSDs hit their end-of-life and are ready to be disposed of, recycled or resold, over half (56 percent) of organizations either send them to IT asset disposition vendors/recyclers to erase the data or outsource the task to an IT security consultant.

**Key findings**

- **SSDs contain a myriad of sensitive personal and business information.** 47 percent of organizations store both personal information (from employees) and business data on SSDs.

- **Loss/theft of drives and employees leaking data for personal gain rank low on the list of SSD security challenges.** Loss or theft of hard drives (8 percent) and employees leaking data for monetary gains/personal benefits (5 percent) were at the bottom of SSD security challenges for organizations.

- **Organizations prioritize efficiency and cost over data security when selecting IT asset disposition vendors/recyclers.** 49 percent of organizations consider efficiency and cost to be the most important factors when selecting an IT asset disposition vendor. Yet, only 16 percent factor in the vendor’s ability to permanently remove all data and 13 percent prioritize certifications and recommendations from governing bodies and institutions into their decision-making process.

- **Although confidence in SSD security practices is high, monitoring of ITAD vendors/recyclers is a low priority.** Although 89 percent of the survey’s respondents are either ‘very confident’ or ‘confident’ that data cannot be accessed or breached after SSDs have been discarded, recycled or resold, 27 percent admitted they don’t have any formal process for monitoring how ITAD vendors/recyclers erase data from SSDs.

Why protecting data on SSDs is critical

“Our study’s findings underscore the difficulty many organizations face with managing, storing and protecting data on SSDs and are symptomatic of a larger data security problem,” said Richard Stiennon, Chief Strategy Officer of Blancco Technology Group. “Many organizations and individuals place a great deal of their trust and reliance in encryption and reformattting to prevent data loss/theft from SSDs and minimize their exposure to a potential data breach.

Read the rest here: https://www.helpnetsecurity.com/2017/02/01/ssd-security-challenges/
This Smart AI Can Now Steal Code to Write Its Own Programs

By David Nield, Science Alert, February 28, 2017

Our artificial intelligence systems are continuing to get smarter, with scientists demonstrating that a system called DeepCoder is now clever enough to borrow bits of code from other programs to solve basic problems.

But the team behind the tool don't want to put human programmers out of a job — they want to make it easier for people to build programs without any coding knowledge.

DeepCoder is a project run by Microsoft and the University of Cambridge, using deep learning techniques to mimic the neural network of a brain, where vast amounts of data are processed and evaluated to make decisions.

That means AI can think for itself without those choices being hard-wired into the code to begin with, not unlike Google's human-beating Go system.

"All of a sudden people could be so much more productive," MIT's Armando Solar-Lezama, who wasn't involved in the work, told New Scientist. "They could build systems that it [would be] impossible to build before."

Given a list of inputs and outputs, DeepCoder can figure out which pieces of code will bring about the desired result, and its developers say the system could potentially enable people to simply describe an idea for a program to create.

Human coders will already be familiar with borrowing bits of other publicly available programs, but a system like DeepCoder can search much faster and think much more quickly than previous AI systems.

It could also combine bits of code in ways that humans haven't even thought of yet.

And rather than running each bit of code through a trial and error process — as earlier versions of the system did — DeepCoder can now predict in advance which fragments are going to be useful and which aren't.

The system is even able to get smarter as it goes, learning from its choices.

That means we could soon be producing programs that spot bugs in software or identify objects in photos much faster — and all without human coders having to lift a finger.

Want a program that moves all your photos from one computer to another, resizing them along the way? One day, you might just have to ask.

We should point out that the technology still needs to be tested by independent researchers, as it's yet to be published in a peer-reviewed journal. But the team is being conservative about its claims regarding its current capabilities, so this looks like the real deal.

For now, DeepCoder can only solve simple programming problems that require around five lines of code, but the researchers are hoping to scale up the system and make it easier to operate for non-coders in the future.

Read the rest here: http://www.sciencealert.com/smart-ai-can-now-steal-code-to-write-its-own-programs
Study: Cybersecurity Skills Gap To Widen To A Massive 1.8 Million Worker Shortfall By 2022

By Sarah Kuranda, CRN, February 24, 2017

The cybersecurity skills gap – widely recognized as one of the biggest challenges facing the IT security industry – is only going to continue to widen in the years to come, a recent report found.

The deficit of cybersecurity professionals is now expected to grow to more than 1.8 million workers globally by 2022, according to the Global Information Security Workforce Study, sponsored by the Center for Cyber Safety and Education and surveying over 19,000 cybersecurity professionals. That is a 20 percent increase over what the same study predicted two years ago.

The study also noted that the security industry seems to have a challenge recruiting millennial workers in particular, with only 12 percent of the workforce under 35.

Many security solution providers cite the security talent shortage as one of the greatest challenges facing their businesses today. Global Managing Director of Accenture Security Kelly Bissell said there simply isn't enough talent to go around in the security industry.

"The war for talent is on," Bissell said.

That war for talent is leading to real-world implications when it comes to security effectiveness, the study found. It said the skills deficit is already starting to impact businesses, with 46 percent of companies saying that it is already causing a "significant impact" on customers and leading to increased security breaches.

However, Bissell said the gap is so large that it is no longer enough for companies like Accenture to recruit personnel from the competition. He said Accenture has doubled down on its investment in training and security boot camps to develop the next generation of security practitioners in the marketplace.

The talent shortage is particular hard on the SMB side of the market, the study found. It said only 23 percent of security professionals work for companies with fewer than 500 employees, although SMB companies make up the majority of the business market.

Sam Heard, president of Lakeland, Fla.-based Data Integrity Services, said he has also seen the talent shortage accelerate.

"There are more bad guys than good guys, for sure," Heard said.

Heard said his business, which offers tech support and managed services to SMBs in Florida, has worked to close the gap by working with local colleges. He said Data Integrity Services provides the colleges with some curriculum or current security technology, so students can use different vendor’s products to learn, train and even get certified on before graduation.

Bissell said Accenture would continue to funnel significant investments into developing security talent, as it is important to have "boots on the ground" when it comes to solving major cybersecurity issues for clients. He said companies like Accenture and other solution providers have a responsibility to help solve this issue for clients.

Read the rest here:

88% of companies concerned about cyberattacks

By Tim Ross, Bloomberg, February 20, 2017

The threat of cyber attacks and political instability resulting from rising populism are among the biggest worries for businesses around the world, according to a study of companies in 79 countries.

The number one issue for executives working in business continuity and resilience is the threat from hackers, with 88 percent of companies included in the survey saying they are "extremely concerned" or "concerned" at the risk.

For the first time, political upheaval ranked among the top 10 threats, following the U.K.’s vote to leave the European Union and the election of Donald Trump in the U.S., according to the report by the Business Continuity Institute and the British Standards Institution.

"Cyber-attacks and data breaches continue to cost organizations billions of dollars annually, a sum that is only likely to go up with the increasing integration of new pieces of technology into daily operations," BCI Executive Director David Thorp said in the foreword to the report. "Politics too has been a dominant topic this year, certainly more than in the recent past."

The study comes as governments and businesses seek to strengthen resilience to cyber attacks. Companies on both sides of the Atlantic are also grappling with political uncertainty over changes to commerce policies, from taxes to trade tariffs, being planned in the U.S. and the U.K.

Read the rest here:
https://www.bloomberg.com/politics/articles/2017-02-21/threat-of-cyber-attack-is-biggest-fear-for-businesses-survey
ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.
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.

Article for the Newsletter?
If you would like to submit an article...

Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at:
doncreamer@outlook.com

Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Please Note: Address Change

Should you have a submission for the ISSA-COS Newsletter there has been an address change. Submissions should now be sent to doncreamer@outlook.com. My old “q.com” account is no more.