That will help guide the future of the chapter, document some of our initiatives such as how we plan our three (3) conferences each year working with the Federal Business Council, and developing marketing materials to help advertise our chapter to many who still don’t know about us. The one new thing we will be rolling out very soon is our new web site. This is long overdue but we have a few folks, namely Tim Hoffman and Bill Welker, doing outstanding work to make this happen so be on the lookout for that rollout soon. All of this is important as we go forward because we will be having leadership changes at the end of the year.

When I became President I said I would give it my all during my time at the helm but that I would not serve as the Chapter President forever. In December it will be two (2) years for me as Chapter President, and I think that’s long enough. I’m going to give all my efforts over the next six (6) months and then give someone else an opportunity to lead us. We will have other opportunities on the board opening up as well and our very

(Continued on page 3)
We don't cover stupid, says cyber insurer that's fighting a payout

By Lisa Vaas, Naked Security, May 28, 2015

During the Cold War the communist rulers of the Soviet Union invented all sorts of propaganda, deception and interrogation techniques that are still widely copied (and often condemned) because they work. Some of those techniques have been updated and continue to serve the current rulers of Russia. One of them involves the Internet and is particularly useful in Russia.

In 2013, California healthcare provider Cottage Health System discovered that security on one of its servers had been disabled, leaving tens of thousands of patients' files potentially open and exposed on the internet.

Those files included patients’ names, addresses, dates of birth, and in a few cases, their diagnosis, lab results and procedures performed.

Cottage was sued, along with inSync, a Laguna Hills-based company responsible for putting the records in a secure location online.

Imagine the expenses rolling in: Class action lawsuit, ka-ching!

Cyber forensic investigators to figure out what happened, security consultants to analyse and scrub the malware away, affected patients notified and (typically, at any rate) offered credit monitoring services, business lost due to newly cautious customers - all of it costs big bucks, ka-ching, ka-ching!

Good thing the healthcare provider had insurance to cover such a data breach, eh?

Well, it would have been a bit of a relief, if the insurer hadn’t scratched its head and shrugged its shoulders, pointing to a clause in the policy that means it doesn’t have to pay out when the insured party has been bone-headed about its security.

Cottage’s insurer, Columbia Casualty, earlier in May filed a complaint against Cottage Health System, claiming that whatever money it had to pay out under the policy would have to be paid right back to it, for the same reasons that the class action lawsuit had been filed: because the healthcare provider allegedly failed to follow “minimum required practices” as spelled out in the insurance policy.

Specifically, the insurer is claiming that Cottage "stored medical records on a system that was fully accessible to the internet but failed to install encryption or take other security measures to protect patient information from becoming available to anyone who 'surf' the internet."

The patient data had been exposed for about two months, starting in October 2013.

It’s not like the company was jumped on by cyber attackers, per se. Rather, the data was accessible via the public internet and to Google search.

That makes it tough to know who might have accessed the data.

In fact, anyone could have viewed the records during those two months, the complaint states, adding that the "extent of the breach is enormous."

While Cottage is looking for about $4 million (about £2.6 million) from its insurer to cover both damages related to the incident as well as potential fines from a Department of Justice investigation of possible violations of HIPAA - the federal Health Insurance Portability and Accountability Act - Columbia is looking to recoup anything it has to pay out.

Some of the alleged security failings that Columbia is hoping will get it out of paying damages:

Read the rest here: https://nakedsecurity.sophos.com/2015/05/28/we-dont-cover-stupid-says-cyber-insurer-thats-fighting-a-payout/?utm_source=Naked%2520Security%2520Feed&utm_medium=feed&utm_content=rss2&utm_campaign=Feed&utm_source=Naked+Security++Sophos+List&utm_campaign=8b0e9d6552-naked%252Bsecurity&utm_medium=email&utm_term=0_31623bb782-8b0e9d6552-148533189
Membership Update

We are still waiting to receive information from ISSA International about the pilot test of a student sponsorship program. As soon as we receive that we will put our implementation plan together to get it off the ground as soon as possible. In the interim, we have decided to go ahead and use our old sponsorship approach to get several students who are expiring soon (or have recently expired—note, I only mean that in the sense of their ISSA membership J). I will be sending out emails to students that I’m aware of. However, I will ask that all current student members who are coming up for renewal to drop me an email (address below) that includes your name, membership number and expiration date so I can get this resolved for folks as quickly as possible. We’ve got lots of upcoming activities, and we want to ensure everyone stays informed of everything. That information will also let me prioritize some test cases as we get the ISSA International program off the ground. More information will be published about this great opportunity for our chapter as it becomes available.

I’d like to reiterate Pat’s call for volunteers. In addition to all the board positions that need filled each year, we also have many committee positions that are always in need of support. Some of those positions are leadership positions but just as important are the team members who get the work done. If you have a skill—we all have at least a few of those—we have an opportunity for you to use those skills to improve the chapter. So please, take a few minutes to assess your time and if you have some—please consider volunteering for the chapter. We are all busy, but it’s important that we share the load to have an active, exciting chapter that meets all of our needs as members.

Last, and of course not least, I’d like to welcome those new members on behalf of the Chapter! When you are 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

A Note From Our President

capable Vice President Cindy will address those in her newsletter column. We’re announcing changes early so that if you are interested in serving on the Board you will have an opportunity to meet with the current incumbent, learn more about what serving on the chapter board entails, and decide whether this is the right time for you to step up and serve in a leadership role. I hope some of you will give it serious consideration. It’s my belief we need to keep the leadership fresh because we need new ideas to keep our chapter interesting, exciting, and focused on providing great value to our members. I will find a new role that allows me to contribute and support the chapter as needed.

Thanks for all you do and please consider how you can serve your chapter going forward.

Cheers!

Pat

New Members
May
Michael S. Bourda
Jeremiah Bess
Lance Youngblood
Thomas C Johnson
Paul Grey
An Important Note From Our Chapter Vice President

June and July Luncheons

The lunch meetings for June and July will be at Bambino’s located on Circle and Plate. Mark the dates – 10 June and 8 July at 11:00 am. To sign up for June meeting go to Eventbrite at http://www.eventbrite.com/e/issa-colorado-springs-june-2015-meeting-tickets-17018258068?aff=eac2. Bambino’s will only seat 85 people so signing up early is advised.

Bambinos will be closing their doors at their current location of Circle and Platte in August. They will be moving to a downtown location thus this will be our last meetings there.

There will be no dinner meetings for June and July.

CSTTF – August 19th and 20th

Federal Business Council (FBC) and ISSA-COS will again host the 5th Annual Cyber Security Training and Technology Forum (CSTTF). It is set to convene on August 19th and 20th at the DoubleTree by Hilton located on Cheyenne Blvd. CSTTF 2015 will bring together cyber experts from the DoD, federal government, business, research, and academia to address a variety of current cyber topics.

This year there will be two unique tracks. One track will be dedicated to emerging information technology advancement. The other track will be dedicated to the NIST National Initiative for Cybersecurity Education (NICE) track.

We need at least fourteen volunteers for the conference. The positions will be helping with sign in, answering questions at the ISSA-COS table, and introducing and bring the microphone to personnel with questions during the sessions.

If you are interested in volunteer, please contact me at thombuc@aol.com.

December Elections

Every December ISSA-COS conducts their annual election. This year is no different. We are looking for a volunteer to handle the election this year. The duties are minimal – count the ballots and ensure everyone who votes is in good standing as a member.

The current positions will be open and are for two years:

- **President** - Will be the executive head of the Chapter and shall preside at all meetings of the Chapter. The President shall have the power to call special meetings with a nominal five (5) day notification to the general membership if deemed necessary for the benefit of the Chapter.

- **Vice President** - Will attend to the duties of the President in the absence of the President and shall attend to any other duties as the President may require. The Vice President shall provide liaison with standing committees within the Chapter.

- **Communication Officer** - Will maintain sufficient membership address lists as to ensure that all members in good standing are notified of meetings, and that all other correspondence necessary to the conduct of the Chapter is received by the members. At the direction of the President, the Communications Officer shall also transmit and respond to all correspondence of the Chapter, and perform any other duties customarily associated with the office of Communications Officer.

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

More information on the duties and persons who are currently holding these positions will be provided in future newsletters.

If you are interested in running for any of the positions above or have questions please contact me at thombuc@aol.com.

Cindy
Canary box aims to lure hackers into honeypots before they make headlines

By Peter Bright, ArsTechnica, May 27, 2015

South African security firm Thinkst is hoping to give new life to an old idea—the honeypot—in a bid to help organizations detect security breaches and intruders in their private networks. Thinkst's Canary is a simple network appliance and corresponding online monitoring service that makes it easy to set up juicy-looking targets on the corporate LAN that will sound the alarm if any attempt is made to access them.

One of the consistent features of large hacks, such as the late 2013 Target breach, is that attackers have been able to move around their victims' networks to find systems with interesting or valuable data without being detected. From one point of entry—a compromised Web server, say—the hackers perform what's called "lateral movement;" accessing other systems and computers on the same network, discovering new sets of user credentials to gain further access to their victims, and finding valuable information to steal.

This behavior appears to go undetected, giving the attackers weeks or months to learn about their victims and steal vast quantities of sensitive data. It's this lateral movement that Canary is designed to detect by presenting the hackers with a juicy target that will ring the alarm bell whenever they access it.

Security honeypots—systems that look like they contain valuable data and are ripe targets for attack, but which are really traps—are a well-known technique for detecting intrusions. Hackers will inevitably discover and explore the honeypot systems, unwittingly alerting their victims to their intrusion. However, they're not commonly used. Creating and maintaining a honeypot that looks authentic, but is reliably able to report intrusion attempts, isn't easy, and most organizations don't bother.

Which is not to say that they do not look for intrusions at all; intrusion detection systems that heuristically monitor network traffic and use big data mining techniques to discover anomalies are common, and typically expensive. But these systems tend to be noisy, inundating administrators with alerts, many of which are spurious or incorrect.

Target appears to fall into this very category: it had malware and intrusion detection systems from FireEye, but according to a report by Bloomberg some alerts that would have detected the hack were disabled. Reuters reported that these alerts were often disabled, because they produced so much noise.

A honeypot system should be much less susceptible to false alerts, since almost any access to a honeypot system should, by definition, be suspicious.

The Canary box aims to tackle this problem, offering the reliable reporting of a honeypot, but without the complex configuration. In fact, Thinkst says that configuring Canary should only take a few minutes. A hardware button is used to put the Canary into "configuration" mode. An administrator then connects to the Canary with Bluetooth and chooses the personality it should use: it can masquerade as, for example, Windows Server 2008, Linux, and ReadyNAS—and the services it offers.

Read the rest here:
http://arstechnica.com/security/2015/05/canary-box-aims-to-lure-hackers-into-honeypots-before-they-make-headlines/?
The 10 Worst States for Cybercrime

Which states do you want to avoid if you’re worried about cybercrime?

Every year, the FBI and its partners in the Internet Crime Complaint Center (IC3) publish a report detailing the number and type of complaints the center receives. The list includes everything from non-delivered merchandise to bank account-clearing fraud.

The most recent report was based on complaints in the year 2013. That year, there were 262,813 consumer complaints to IC3. More than 45% of these complaints involved financial loss, adding up to $781,841,611. That’s 48.8% higher than the amount of loss reported in 2012, $581,441,110.

What follows is a list, in reverse-countdown format of course, of the 10 states with the most complaints documented by IC3.

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Complaints % of All</th>
<th>Average Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Georgia</td>
<td>2.58%</td>
<td>$3,039</td>
</tr>
<tr>
<td>9</td>
<td>Ohio</td>
<td>2.75%</td>
<td>$1,888</td>
</tr>
<tr>
<td>8</td>
<td>Virginia</td>
<td>2.84%</td>
<td>$3,004</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>2.95%</td>
<td>$2,265</td>
</tr>
<tr>
<td>6</td>
<td>New Jersey</td>
<td>3.21%</td>
<td>$1,753</td>
</tr>
<tr>
<td>5</td>
<td>Pennsylvania</td>
<td>3.32%</td>
<td>$1,819</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>5.29%</td>
<td>$3,015</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>6.74%</td>
<td>$3,521</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>7.45%</td>
<td>$2,750</td>
</tr>
<tr>
<td>1</td>
<td>California</td>
<td>12.13%</td>
<td>$3,639</td>
</tr>
</tbody>
</table>

National Security Institute, Inc. www.nsi.org
Training Team Update

CISSP

Development of the new CISSP Exam Prep Seminar Review material, to incorporate the new format and content per the 2015 (ISC)2 CBK, is progressing well. Draft slides should be ready for initial review by early June. The CISSP Exam Prep Review Seminar is tentatively scheduled to take place over five alternating Saturdays in August and September (1, 15, 29 August and 12, 26 September). If you are a CISSP and would like to teach one of the new CISSP domains, or if you have questions, please contact our Chapter Training leads at: Training@issa-cos.org. If you are interested in attending the CISSP Exam Prep Review Seminar, watch for a Chapter email with the EventBrite link to register, or send an email to our Chapter Training leads at: Training@issa-cos.org.

Security+

The next Security+ Exam Prep Review Seminar is scheduled for 11 July, at Colorado Technical University (CTU). If you’re interested in attending, watch for a Chapter email with the EventBrite link to register, or send an email to our Chapter Training leads at: Training@issa-cos.org.

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs? We’re always looking for members to teach one or more of the Security+ 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 criteria. If you would like to volunteer to teach one of the Security+ domains, or if you have questions, please contact our Chapter Training leads at: Training@issa-cos.org.

Study Groups

Organized study groups are in progress for the CISSP concentration, Information Systems Security Architecture Professional (ISSAP), and for the Certified Authorization Professional (CAP) certification.

Per Kurt Danis, the ISSAP Study Group Organizer: the ISSAP study group will be meeting in Conference Room II at the East Library on 5550 N. Union Blvd on Thursday, June 4th at 5:30 pm. The agenda for this meeting will be focused on Domain 3 Cryptography. Domain 3 in the ISSAP book is about 100 pages long. In support of this topic, a quick review of one of the ISSAP reference books will be provided. The reference book is called, Cryptography Engineering: Design Principles and Practical Applications.

NOTE FOR MEMBERS: The ISC2 website typically publishes a 50% discount for official ISC2 books. Once you acquire the current discount code, visit the publisher here:

https://www.crcpress.com/browse/series/CRCISC2PRESS/1/?order=pubdate&size=10

Per Luke Ingerman, the CAP Study Group Organizer: The CAP Study Group is going well. We had a successful group kick-off meeting and now have four sessions under our belt. We are moving a bit slower than anticipated, but we are also having some good discussions. The group is gelling together pretty well, and we are sharing experiences which are helping to solidify the concepts. So far, we have spent four two hour sessions in Domain 1, Security Authorization of Information Systems, and we will be continuing Domain 1 into June. The first domain is the largest and is fundamental in establishing the overall Security Authorization program. I want to give a shout out to Frank Gerheart for establishing the Wiggio.com site for the CISSP Training Team members to collaborate on the slides. I decided to use Wiggio.com to form an online presence for the CAP Study Group which allows me to more easily communicate with the group and distribute information.

A few members have expressed interest in participating in a study group for the Certified Information Systems Manager (CISM) certification but we still need someone to organize and facilitate this study group. If you hold the CISM certification, please consider volunteering your time and knowledge by organizing and guiding a CISM study group. Additional study groups can be organized for other certifications if there are enough members interested and if someone is willing to take on the role of organizing the group and scheduling the meetings.

Contact our Chapter Training leads at: Training@issa-cos.org if you’re interested in organizing a study group, want to participate in a study group, or if you have any questions.

We have a lot planned for this year, so stay tuned for updates.
EFF Asks Court To Reconsider Ruling That Would Make Violating Work Computer Policies A Criminal Act

By Tim Cushing, TechDirt, May 20th 2015

The EFF is asking the Oregon Supreme Court to take a look at a disturbing opinion issued by the state's appeals court -- one that could see employees face fines and prison time simply for violating company policies.

The case prompting the filing of an amicus brief on behalf of Caryn Nascimento worked as a cashier at the deli counter of a convenience store. As part of her job, she was authorized to access a lottery terminal in the store to sell and validate lottery tickets for paying customers. Store policy prohibited employees from purchasing lottery tickets for themselves or validating their own lottery tickets while on duty. After a store manager noticed a discrepancy in the receipts from the lottery terminal, it was discovered that Nascimento had printed lottery tickets for herself without paying for them. She was ultimately convicted not only of first-degree theft, but also of computer crime on the ground that she accessed the lottery terminal “without authorization.”

Nascimento appealed the computer crime conviction. She argued that because she had permission to access the lottery terminal as part of her work duties, she did not access the terminal without authorization—as required under the Oregon’s computer crime statute. Unfortunately, the Oregon Court of Appeals affirmed Nascimento’s conviction, finding she had only “limited authorization” to access the lottery terminal for purposes of printing and validating lottery tickets for paying customers, and acted without authorization when she printed them for herself.

At first glance, it almost seems like a reasonable application of the law simply because the end result was theft. But it's the specifics that make it troublesome. "Without authorization" is far too broad a term to be used in this context. With this reading of Oregon's law, the appeals court has basically criminalized a wide variety of corporate computer-related policy violations. Actions that would normally be met (in a corporate setting) with warnings and reprimands could now be viewed as criminal acts.

[The Court of Appeals’ decision transforms millions of unsuspecting individuals into criminals on the basis of innocuous, everyday behavior—such as checking personal email or playing solitaire on a work computer. Such restrictions, frequently included in employers’ computer policies, are no different than the restriction imposed on Nascimento. They’re ultimately all computer use, not access, restrictions. Upholding Nascimento’s conviction on the basis of a violation of a computer use restriction expands Oregon’s computer crime statute to criminalize violations of any computer use restriction.

The broad reading of Oregon's criminal statute also poses potential problems outside of the work environment.

The court’s holding that a person acts “without authorization” if she violates a policy regarding the use of a computer that she is otherwise authorized to access could be extended to an Internet user who accesses a website in violation of a written terms of service. For example, Facebook’s terms of use provide that “[y]ou will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.” But as the Ninth Circuit noted en banc, “[l]ying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight.” Under the Court of Appeals’ expansive reading of ORS 164.377, if a user shaves a few years off her age in her profile information, asserts that she is single when she is in fact married, or seeks to obfuscate her current physical location, hometown or educational history for any number of legitimate reasons, she violates the computer crime law. The court’s decision thus opens the door to turning millions of individual Internet users—not just millions of individual employees—into criminals for typical and routine Internet activity.

The EFF points out that rolling back this "unconstitutionally vague" reading of Oregon's computer crime law doesn't leave the state without options to punish Nascimento for her actions. She still faces one count of aggravated first-degree theft -- a charge the EFF is not disputing. Pointing to previous decisions by the Fourth and Ninth Circuit courts, the EFF states that similarly broad readings of the rightfully-maligned CFAA (Computer Fraud and Abuse Act) have been rejected for potentially criminalizing violations of workplace computer use policies.

Read the rest here:
Talking Insider Data Theft With Jonathan Grier

By Ernie Austin, DFI News, May 21, 2015

If a thief tries to break into a house he’s going to leave broken windows, explains digital forensic expert Jonathan Grier. But someone on the inside doesn’t leave broken glass; he’s already in.

The same goes with insider theft in digital forensics. And research shows that the data that insiders steal is usually the data they are working on. The data stolen is no different from the data a thief uses every day, making it impossible to detect.

DFI News spoke with Jonathan Grier, principal of Grier Forensic, before he left Las Vegas after attending this year’s Computer and Enterprise Investigations Conference (CEIC). Although, due to a scheduling conflict, he was not able to give his presentation “How to Catch an Insider Data Thief,” Grier gave DFI News an exclusive look into the world of insider theft and his thoughts on CEIC this year. Grier said many conference attendees were looking forward to his talk (we believe him), but they will have to see the online version available in the near future.

Grier said that insider theft is much less common than outside attacks, but they are far more damaging. One only needs to think of Edward Snowden and the effect his actions have had.

Grier mentioned that when forensic expert Harlan Carvey is asked, “Are you able to forensically identify when people copy data?” Carvey responds that there are no artifacts, and thus identification isn’t possible. If someone copies data there are no footprints of their actions beyond copying the data, Grier explained.

DFI News also asked Grier his thoughts on CEIC this year and in general. We think of CEIC as a conference for digital forensics practitioners, not just another cybersecurity conference.

“You’re hitting the nail on the head,” Grier answered. “There are a lot of cybersecurity conferences out there, and there are a lot of research conferences for forensics. This is the conference for digital forensic practitioners.”

“You get a conference full of people who do the in-the-trenches, day-to-day forensic operations,” Grier added. “Most people there aren’t even interested in security.”

He pointed out the hands-on, practical nature of the conference. One presentation took apart USB flash drives. Another took apart the Apple Watch and the latest Apple Macbooks. Since Apple now makes its own flash drives getting into them is a forensic nightmare, Grier explained.

This year, vendors emphasized speeding up forensic acquisition, Grier said. He also mentioned how many of the digital forensic vendors are trying to get into cybersecurity.

Read the rest here:

Cyber-Attack Warning: Could Hackers Bring Down a Plane?

By Marcel Rosenbach and Gerald Traufetter, Der Spiegel, May 22, 2015

The officials from the European Aviation Safety Agency (EASA) were not at all happy about what they were hearing. An unshaven 32-year-old from Spain, his hair pulled back in a ponytail, was talking about cockpit computers and their weaknesses and security loopholes. Specifically, he was telling the EASA officials how he had managed to buy original parts from aviation suppliers on Ebay for just a few hundred dollars. His goal was to simulate the data exchange between current passenger-jet models and air-traffic controllers on the ground in order to search for possible backdoors. His search was successful. Very successful.

The Spaniard’s presentation took place two years ago in an EADS conference room looking over the rooftops of Cologne. He had been invited after, in accordance with the hacker ethic, he had notified the agency that he was planning to release the results of his years-long study at a hacker conference. Engineers from airlines and airplane manufacturers were also following the Spaniard’s presentation via video. After he had finished, he recalls, they all wanted to know the same thing: “You aren’t really planning on making all of that public, are you?”

Their concern focused on his central finding, which he continues to repeat to this day. "In modern airplanes, there are a whole series of backdoors, through which hackers can gain access to a variety of aircraft systems."

Read the rest here:
Every 4 Seconds
New Malware Is Born

By Ericka Chickowski, Dark Reading, May 18, 2015

New research data out today shows that the rate of new malware variants released by malicious attackers continues to break records. According to the G DATA SecurityLabs Malware Report (https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H2_2014_EN_v1.pdf), new malware types were discovered less than every four seconds and 4.1 million new strains were found in the second half of 2014, an increase of close to 125 percent over the first half. Over the course of the entire year, nearly 6 million new malware strains were discovered. This is a 77 percent increase over 2013.

The data shows that in the second half of 2014, Trojans still remained atop the categories tracked by G DATA researchers, but could be on pace to be supplanted by adware. Adware showed the highest rate of growth among all of the malware categories, at a rate of 31.4 percent. While the number of new downloaders was on the rise during the second half, adware's growth rate outpaced that rise to take over the number two spot on the malware category chart. Meanwhile, spyware increased in prevalence while backdoors decreased, putting them in the number four and five spot, respectively.

Interestingly, while rootkits ranked ninth in the categories list, the second half of the year saw a huge spike in their prevalence. The report showed that there were 18 times more new variants than in the first half of 2014.

Specifically within the Trojan market, researchers reported that the second half of the year was novel in that there were no significant innovations compared to previous years.

"In the past, more and more new Trojans have been appearing very quickly in this sector over the years, with new groups in the background using new attack methods. However, in recent months there have been few changes to report," the study said, explaining that in spite of this the volume of attacks is still rising. According to G DATA, the number of banking Trojan attacks rose by 44.5 percent.

The authors speculated that the banking Trojan market seems to have consolidated due to a number of reasons.

"Improved security measures by banks are making it more and more difficult for online bank robbers to get money from bank customers," explains Ralf Benzmüller, head of G DATA SecurityLabs.

Read the rest here:
http://www.darkreading.com/vulnerabilities---threats/every-4-seconds-new-malware-is-born/d/d-id/1320474?&

Cyber extortionists are hitting hedge funds

By Ziljka Zorz, Help Net Security, May 12, 2015

Hedge funds are increasingly targeted by cyber extortionists, John Carlin, US Assistant Attorney General for National Security, has warned the audience at the SALT hedge fund conference held last week in Las Vegas.

Encrypting a user's or an organization's important files via crypto ransomware then asking for money to decrypt them has proved very lucrative for cyber crooks.

Not only do many individual users fall for the scheme and ultimately pay the ransom, but so do businesses and organizations that should have their files regularly backed up and that you would not expect to comply with the crooks' demands (e.g. police departments).

According to Carlin, the US Department of Justice is currently working with several hedge funds that have become victims of cyber blackmail, and he encouraged others who are in the same predicament to ask for their help.

"We are seeing nation-state action - from Russian, China, Iran and North Korea - target your companies and what you have, day in and day out, to use your information against you."

He told the crowd that it's not only Russian, Chinese, Iranian and North Korean state-backed attackers that have US companies and hedge funds in their sights, but "jihadist" terrorists and criminal organizations as well.

The ransom asked in these situation is much, much higher than the usual one demanded from individual users and organizations that are not in the financial industry. While the former can expect a ransom that rarely passes $1,000, hedge funds and other financial organizations and investment firms will be asked to pay millions of dollars in order to get their information back.

Carlin also tried to reassure the crowd that collaborating with the FBI and prosecutors will not result in the government misusing access to the companies' corporate secrets, Kaja Whitehouse reports.

Read the rest here:
http://www.net-security.org/secworld.php?id=18374&
Request for Chapter Presenters

We are looking for members to present at both the lunch and dinner meeting. The presenter has about 40 minutes to give the presentation and answer questions. This could be one slide with a situation identified and audience will then discuss possible solutions or a how-to presentation with a demonstration afterwards. The below listed are topics that have been suggested as areas of interest from our members. Please send an email to either, Pat Laverty (plaverty1961@gmail.com) and/or myself, Cindy Thornburg (thornbuc@aol.com) with topic to be presented, and we will connect with you for your availability. We would like the topic to be presented at both meetings however we do understand that may be difficult to accomplish.

- Cyber Security Laws in Colorado
- Interior Protection
- Building in Resiliency
- Ethics
- Intrusion Detection/Prevention Systems – configuration and how to review
- Making the Business Case for Security – how to
- Hacking – how to
- Application Security Scanning
- COMPTIA CE Cycles & Fee Structure
- A Summary and Rating of available Certifications
- A Survey of current IA Incidents We Should Know About (heartbleed) and What They Mean for the State of Our Industry
- Latest Innovations in Network Management Systems
- Real World Case Studies
- Threat Overview – Real World
- Legal Issues in Information Systems
- Asymmetric Warfare – what is it
- Spear Phishing – what is it and demonstration
- Prevention of Cyber Bullying
- Best Practices for Backing Up & Archiving Corporate Data
- When to Maximize or Minimize Your Cyber Footprint/Persona
- Threat Structuring
- Security Modeling – how to
- Data Flow Control
- Trusted Software Development – how to
- Risk Management Framework and what does it mean
- Case Study of Breaches – how they happen and how to prevent
- Security Architecture Development – ‘Building it In’
- ‘Mobile’ Security Management
- Bring Your Own Device (BYOD)
- Biometric Security and Privacy
- Hacking Back

Thank you!

Cindy
There has been an increase in the reporting of elicitation attempts of cleared defense contractors.

By Unattributed, Undated

There has been an increase in the reporting of elicitation attempts of cleared defense contractors.

Elicitation Defined

Elicitation attempts can be simple, and sometimes are obvious. If they are obvious, it is easier to detect and deflect. On the other hand, elicitation may be imaginative, persistent, involve extensive planning, and may employ a co-conspirator. Elicitors may use a cover story to account for the conversation topic and why they ask certain questions.

Elicitation can occur anywhere—at social gatherings, at conferences, over the phone, on the street, on the Internet, or in someone’s home.

Elicitation is Not Rare

It is not uncommon for people to discover information about a person without letting on the purpose. For example, have you ever planned a surprise party for someone and needed to know their schedule, wish list, food likes and dislikes or other information without that person finding out you were collecting the information or for what purpose?

Why Elicitation Works

A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit those. Natural tendencies an elicitor may try to exploit include:

- A desire to be polite and helpful, even to strangers or new acquaintances
- A desire to appear well informed, especially about our profession
- A desire to feel appreciated and believe we are contributing to something important
- A tendency to expand on a topic when given praise or encouragement; to show off
- A tendency to correct others
- A tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used
- A tendency to believe others are honest; a disinclination to be suspicious of others
- A tendency to answer truthfully when asked an “honest” question

For example, you meet someone at a public function and the natural getting-to-know-you questions eventually turn to your work. You never mention the name of your organization. The new person asks questions about job satisfaction at your company, perhaps while complaining about his job. You may think, “He has no idea where I work or what I really do. He’s just making idle chat. There’s no harm in answering.” However, he may know exactly what you do but he relies on his anonymity, your desire to be honest and appear knowledgeable, and your disinclination to be suspicious to get the information he wants. He may be hunting for a disgruntled employee who he can entice to give him insider information.

Techniques

There are many elicitation techniques, and multiple techniques may be used in an elicitation attempt. The following are descriptions of some of those techniques.

Assumed Knowledge: Pretend to have knowledge or associations in common with a person. “According to the computer network guys I used to work with…"

Bracketing: Provide a high and low estimate in order to entice a more specific number. “I assume rates will have to go up soon. I’d guess between five and 15 dollars.” Response: “Probably around seven dollars.”

Can you top this? Tell an extreme story in hopes the person will want to top it. “I heard Company M is developing an amazing new product that is capable of …”

Confidential Bait: Pretend to divulge confidential information in hopes of receiving confidential information in return. “Just between you and me….” “Off the record…”

Criticism: Criticize an individual or organization in which the person has an interest in hopes the person will disclose information during a defense. “How did your company get that contract? Everybody knows Company B has better engineers for that type of work.”

Deliberate False Statements / Denial of the Obvious: Say something wrong in the hopes that the person will

(Continued on page 13)
correct your statement with true information. “Everybody knows that process won’t work—it’s just a DARPA dream project that will never get off the ground.”

Feigned Ignorance: Pretend to be ignorant of a topic in order to exploit the person’s tendency to educate. “I’m new to this field and could use all the help I can get.” “How does this thing work?”

Flattery: Use praise to coax a person into providing information. “I bet you were the key person in designing this new product.”

Good Listener: Exploit the instinct to complain or brag, by listening patiently and validating the person’s feelings (whether positive or negative). If a person feels they have someone to confide in, he/she may share more information.

The Leading Question: Ask a question to which the answer is “yes” or “no,” but which contains at least one presumption. “Did you work with integrated systems testing before you left that company?” (As opposed to: “What were your responsibilities at your prior job?”)

Macro to Micro: Start a conversation on the macro level, and then gradually guide the person toward the topic of actual interest. Start talking about the economy, then government spending, then potential defense budget cuts, then “what will happen to your X program if there are budget cuts?” A good elicitor will then reverse the process taking the conversation back to macro topics.

Mutual Interest: Suggest you are similar to a person based on shared interests, hobbies, or experiences, as a way to obtain information or build a rapport before soliciting information. “Your brother served in the Iraq war? So did mine. Which unit was your brother with?”

Oblique Reference: Discuss one topic that may provide insight into a different topic. A question about the catering of a work party may actually be an attempt to understand the type of access outside vendors have to the facility.

Opposition/Feigned Incredulity: Indicate disbelief or opposition in order to prompt a person to offer information in defense of their position. “There’s no way you could design and produce this that fast!” “That’s good in theory, but…”

Provocative Statement: Entice the person to direct a question toward you, in order to set up the rest of the conversation. “I could kick myself for not taking that job offer.” Response: “Why didn’t you?” Since the other person is asking the question, it makes your part in the subsequent conversation more innocuous.

Questionnaires and Surveys: State a benign purpose for the survey. Surround a few questions you want answered with other logical questions. Or use a survey merely to get people to agree to talk with you.

Quote Reported Facts: Reference real or false information so the person believes that bit of information is in the public domain. “Will you comment on reports that your company is laying off employees?” “Did you read how analysts predict…”

Ruse Interviews: Someone pretending to be a headhunter calls and asks about your experience, qualifications, and recent projects.

Target the Outsider: Ask about an organization that the person does not belong to. Often friends, family, vendors, subsidiaries, or competitors know information but may not be sensitized about what not to share.

Volunteering Information / Quid Pro Quo: Give information in hopes that the person will reciprocate. “Our company’s infrared sensors are only accurate 80% of the time at that distance. Are yours any better?”

Word Repetition: Repeat core words or concepts to encourage a person to expand on what he/she already said. “3,000 meter range, huh? Interesting.”

Deflecting Elicitation Attempts

Know what information should not be shared, and be suspicious of people who seek such information. Do not tell people any information they are not authorized to know, to include personal information about you, your family, or your colleagues.

You can politely discourage conversation topics and deflect possible elicitations by:
- Referring them to public sources (websites, press releases)
- Ignoring any question or statement you think is improper and changing the topic
- Deflecting a question with one of your own
- Responding with “Why do you ask?”
- Giving a nondescript answer
- Stating that you do not know
- Stating that you would have to clear such discussions with your security office Stating that you cannot discuss the matter

If you believe someone has tried to elicit information from you, especially about your work, report it to your security officer.
Intelligence officers given immunity from hacking laws, tribunal told


GCHQ staff, intelligence officers and police have been given immunity from prosecution for hacking into computers, laptops and mobile phones under legislative changes that were never fully debated by parliament, a tribunal has been told.

The unnoticed rewriting of a key clause of the Computer Misuse Act has exempted law enforcement officials from the prohibition on breaking into other people’s laptops, databases, mobile phones or digital systems. It came into force in May.

The amended clause 10, entitled somewhat misleadingly “Savings”, is designed to prevent officers from committing a crime when they remotely access computers of suspected criminals. It is not known what category of offences are covered.

The act is primarily deployed to provide legal cover for domestic investigations. It is thought that individual warrants are not being obtained to justify each inquiry. Different legislation – section 7 of the Intelligence Services Act, nicknamed the “James Bond clause” – is believed to permit activities abroad that would otherwise be illegal.

Addressing the Investigatory Powers Tribunal, which deals with complaints about the intelligence services and surveillance, lawyers for Privacy International said they had only been informed of the alteration earlier this week.

“We had previously thought [hacking] in this country to be unlawful,” said Ben Jaffey, a lawyer representing Privacy International. “The effect of this amendment has passed everyone by. Attention was not called to it during the parliamentary process, which may not have been accidental. It was hidden in plain sight.”

Hacking is more damaging than mere interception of messages, Jaffey told the tribunal, because it involves unlocking a backdoor into someone else’s computer system which was meant to be secure. It is not clear whether the damage done is always made good following a hacking attack.

Hacking into someone’s computer appears to take place under a general class permission for such activity, Jaffey said. “There’s something profoundly objectionable in bugging and burglary of computers without any [individual] authorisation from the secretary of state,” he told the IPT.

Changes to the Computer Misuse Act were introduced by the Serious Crime Act 2015 which received royal assent on 3 March 2015. No reference to the true impact of the changes was made in the parliamentary explanatory notes that accompanied the bill, according to Privacy International.

Nor was there any public debate, the organisation claimed. “No NGOs, regulators, RIPA commissioners, the Information Commissioners Office, industry, or the public were notified or consulted about the proposed legislative changes,” it added.

“The underhand and undemocratic manner in which the government is seeking to make lawful GCHQ’s hacking operations is disgraceful,” Eric King, the organisation’s deputy director said after the hearing. “Hacking is one of the most intrusive surveillance capabilities available to any intelligence agency, and its use and safeguards surrounding it should be the subject of proper debate.”

“Instead, the government is continuing to neither confirm nor deny the existence of a capability it is clear they have, while changing the law under the radar, without proper parliamentary debate.”

Professor Peter Sommer, one of the UK’s leading experts in the Computer Misuse Act, said he had also only belatedly discovered the changes to the legislation. Altering the law without proper public debate, he said, risked “building up unnecessary mistrust”.

“I wasn’t aware of it until recently,” he said. The previous clause dated from a time when police officers physically seized computers and examined them in a police station.

“Now if you have remote access,” he said, “you can hack into a computer and put in a Trojan horse program. I have looked at the government notes covering the changes and it was extremely obscure guidance. But they are giving highly intrusive powers to go into someone else’s computer.

“If this had been done properly, people would have said we want a principled debate about this. There’s a danger now that [lawyers] will say that the police or spooks have put things into their clients’ computers.”

Read the rest here:
http://www.theguardian.com/uk-news/2015/may/15/intelligence-officers-have-immunity-from-hacking-laws-tribunal-told?
Islamic terrorists are stoking alarm with threats of an all-out cyber crusade against the United States, and experts say the warnings should be taken seriously.

Hackers claiming affiliation with the Islamic State in Iraq and Syria (ISIS) released a video Monday vowing an “electronic war” against the United States and Europe and claiming access to “American leadership” online.

“Praise to Allah, today we extend on the land and in the Internet,” a faceless, hooded figure said in Arabic. “We send this message to America and Europe: We are the hackers of the Islamic State and the electronic war has not yet begun.”

The video received ridicule online for its poor phrasing and the group’s apparent inability to make good on its cyber threat this week. But as hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends, experts said.

“It’s only really a matter of time till we start seeing terrorist organizations using cyberattack techniques in a more expanded way,” said John Cohen, a former counterterrorism coordinator at the Department of Homeland Security.

“The concern is that, as an organization like ISIS acquires more resources financially, they will be able to hire the talent they need or outsource to criminal organizations,” Cohen added. “I think they’re probably moving in that direction anyway.”

Military officials agree. NSA Director Adm. Michael Rogers this week called the pending shift “a great concern and something that we pay lots of attention to.”

“At what point do they decide they need to move from viewing the Internet as a source of recruitment … [to] viewing it as a potential weapon system?” Rogers asked.

While ISIS has been widely recognized for its social media prowess, the growing computer science talent of its recruits has mostly gone unnoticed.

“A number of individuals that have recently joined the movement of ISIS were folks that studied computer science in British schools and European universities,” said Tom Kellermann, chief cybersecurity officer at security firm Trend Micro, who said ISIS’s cyber capabilities are “advancing dramatically.”

Even the man reportedly responsible for a number of the brutal ISIS beheadings, dubbed “Jihadi John” by his captives, has a computer science degree, Kellermann said.

The burgeoning online threat posed by Islamic extremists was part of the motivation for a new security pact announced Thursday between the White House and Gulf states.

In addition to securing infrastructure and providing cyber training, U.S. officials will also work with partner states to expand joint exercises that involve the potential for cyber warfare.

Part of the danger of the ISIS threat is the group’s ability to marshal attacks from its sympathizers, generating a diffuse and unconnected network that is hard to track.

Kellermann said the video threats this week were “a call to arms more than anything,” meant to incite individuals to act on their own.

“It has actually added a new dimension to the terrorist threat that our counterterrorism approach is not intended or designed to pick up on,” Cohen said.

So far, supporters have focused on distributed denial-of-service attacks, spear phishing campaigns and hijacking legitimate websites to push malware, creating what are known as “watering holes.”

“For example, if you go to an ISIS website and download their videos, you better recognize most of those websites are watering holes,” Kellermann said. “[They are] basically trying to attack you while you’re watching that video.”

Experts think radical hackers are likely to expand this tactic to mainstream websites and powerful companies’ websites as a way to gather information on targets.

“They’re beginning to conduct more and more counterintelligence,” Kellermann said.

The ISIS’s use of the Internet has been described as unprecedented for a terrorist group, and lawmakers are growing increasingly concerned about U.S. attempts to counter its rhetoric online.

Sen. Cory Booker (D-N.J.) recently criticized U.S.-led online campaigns against radicalization as “laughable,” saying he was “stunned” by the efforts’ lack of sophistication.

Jen Weedon, threat intelligence manager at security researcher FireEye, said these concerns are understandable.

“Part of the reason why there’s a belief that these emissaries are so savvy is because there’s a sense of people not feeling that they’re in control of the message,” she said.

Read the rest here: http://thehill.com/policy/cybersecurity/242280-isis-preps-for-cyber-war?
ISSA photos are courtesy of our Chapter Photographer Warren Pearce.

ISSA-COS May Luncheon

Suzanne Chance
What 700 TB of Cyber Threat Data Can Do for You

By Amanda Ziadeh, GCN, May 8, 2015

The value of cyber threat intelligence increases as it’s shared.

That’s the idea behind the X-Force Exchange, a 700-terabyte platform of aggregated cyber threat information IBM has built to foster cybersecurity collaboration. This hoard of cybercrime data features IBM’s security intelligence research, a global network of third-party threat data, expert analyses and real-time insight on live attacks, all on a social sharing site built on IBM’s cloud.

As the sophistication of cybercrime increases, governments and private organizations alike depend on sharing their threat intelligence. “The need for trusted threat intelligence is greater than ever, as 80 percent of cyber attacks are driven by highly organized crime rings in which data, tools and expertise are widely shared,” IBM said, citing a 2013 UNODC Comprehensive Study on Cybercrime.

IBM has described the X-Force Exchange as “one of the largest and most complete catalogs of vulnerabilities in the world.” In detail, the platform will pull from threat data and intelligence based on more than 15 billion security events a day, over 25 billion web pages, more than 8 million spam and phishing attacks, a malware threat intelligence network of 270 million endpoints and reputation stats on a million malicious IP addresses that are categorized by geo-location and severity, the company said.

The cloud will continuously be updated -- it can add 1,000 malicious indicators each hour -- and as the third-party user base grows, so too will the depth of information, IBM said. Users can work with industry peers, analysts, researchers and trusted technology on a social interface with clearly organized tools, annotated findings and prioritized information. A library of application programming interfaces even works as an open forum for programmatic queries between businesses, machines and applications for further threat-fighting support.

In some ways, the platform looks like any other community social sharing site. Logged-in users can search, comment, collect and share information, while guests can view and search reports.

In the “activity” section, users can access recent vulnerabilities, find links to security intelligence blogs for helpful tips and search through trending topics and recent history of the entire community. In a personalized collections tab, users can add reports and pull in evidence from external resources, made shareable to the community or kept private.

Read the rest here:
http://gcn.com/articles/2015/05/08/x-force-threat-intelligence-exchange.aspx?

US Navy Looks to Dump Lenovo Servers on Security Concerns – Report


The US Navy is reportedly looking for a new server supplier for some of its guided missile cruisers and destroyers due to security concerns around Lenovo’s recent purchase of IBM’s x86 server division.

The Chinese hardware giant acquired IBM’s System x, BladeCenter and Flex System blade servers and switches, and its NeXtScale and iDataPlex servers and software in autumn last year in a $2.1bn deal – propelling it to a position as the third largest x86 server provider globally.

However, that’s not gone down too well with the government, according to USNI News.

“The Department of Homeland Defense [sic] identified security concerns with the IBM Blade Center sale and placed restrictions on federal government procurement of Lenovo Blade Center server products,” Navy spokesman Dale Eng told the site.

The decision will affect the Navy’s Aegis Combat System – an integrated naval weapons system developed by Lockheed Martin which includes ballistic guided missile destroyers and cruisers.

According to the report, IBM x86 BladeCenter HT servers were included in “Aegis Technical Insertion (TI) 12” hardware upgrades for the combat system.

The Integrated Warfare Systems’ Aegis program office is apparently working with the Department of Defense Committee on Foreign Investment in the United States Mitigation Development and Compliance Monitoring Team, in order to find an alternative supplier.

Lenovo has been called out for national security concerns in the past, when an Australian Financial Review (AFR) article claimed two years ago that ‘Five Eyes’ intelligence agencies had banned Lenovo PCs after finding backdoor vulnerabilities.

The Australian Department of Defence subsequently claimed it had not instituted a ban but that Lenovo had not requested to be accredited for Top Secret and Secret Networks.

Read the rest here:
Harvard Uses Forensics to Save Obsolete Digital Records

By Kate Kondayen, Harvard Library Communications, May 8, 2015

When digital becomes dinosaur, most people simply get inconvenienced. But librarians and archivists get seriously concerned.

Ensuring that digital content — whether it’s a short story by John Updike or a very rare audio recording of a vanished Native American language — lives on past its initial platform is one of the most pressing issues in preservation science. Harvard is one of a handful of cultural institutions in the first wave of adopting a technology and process to preserve its digital content.

Libraries and archives at Harvard hold thousands of unique items across hundreds of digital formats, including aging technology such as CDs, floppy disks, tapes, and cassettes. To retrieve content prior to total obsolescence or decay of digital formats, librarians are using digital forensic software commonly employed by the police or the FBI to solve crimes, which enables them to identify content noninvasively and migrate it to a more stable platform.

Digital forensics was developed to create authentic, unimpeachable source data suitable as evidence in criminal trials. Library staff members hold themselves to the same high standards and model some of their workflow on law-enforcement practices. After all, altering a document literally rewrites history.

But librarians and archivists face mounting urgency in this task. For centuries, data meant print. Paper was far and away the best medium to record and preserve information, and for good reason. It is relatively affordable, easy to make, and stands up well to benign neglect. Open a book that was placed on a shelf 200 years ago, and its pages will still provide the same information, tell the same stories.

With the comparatively quick shift to digital content delivery, and the even faster evolution of digital hardware from Mark III-era behemoths to today’s sleek iPhones, an increasing amount of content is born digital, created, disseminated, and accessed completely on computers, existing as 1s and 0s instead of printed type, engraved texture, or magnetic coding — all of which are more robust than more modern technologies.

Now, collections might come in with digital material that is already on the brink of decline. Digital degradation doesn’t follow a steady curve like books. Items can be fine for decades, and then quickly decline from perfectly accessible to completely useless. For some formats, experts don’t know what that plateau and drop-off might be, and it can even vary among individual items kept in the same condition. The situation poses problems for preservation, access, and collection development.

“People outside of the field hadn’t anticipated how quickly this would become such a pressing issue,” said Megan Sniffin-Marinoff, University archivist. “It happened practically overnight.”

The presence of digital materials in incoming collections has risen exponentially over the past decade or so as professionals who started their careers on paper and migrated to digital hand over their work to the library to preserve. All-paper collections are becoming rare.

When the first hybrid hard-copy and born-digital collections came into the library in the 1980s, the digital formats were treated as objects or artifacts instead of content. A disk might have been noted but was not accessed, and was tucked back in with the papers it arrived alongside.

“We certainly have that issue of these hidden problems riddled throughout the collections,” Sniffin-Marinoff said. “I don’t think people were imagining the extent of the implications. It’s added a layer of complexity to our work that’s pretty unbelievable.”

Archivists are now much savvier when assessing incoming collections. They try to uncover these issues in a collection as soon as it comes in — sometimes even before it arrives at the door. University archives staff members take a mobile forensics kit to the offices, basements, attics, and studies of donors and are equipped to survey materials onsite, like members of a forensics SWAT team.

Harvard’s first collection to be preserved via digital forensics was at the Business School’s Baker Library. One recent acquisition left librarians pondering how to capture the significant portion of born-digital information and integrate it with the print items in the collection.

Read the rest here:
http://news.harvard.edu/gazette/story/2015/05/saving-the-digital-record/?
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.

Chapter Officers:
President: Dr. Patrick J. Laverty
President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Executive Vice President: Tim Hoffman
Vice President: Cindy Thornburg
Vice President of Training: Colleen Murphy
Treasurer: Melody Wilson
Communications Officer: Jeff Pettorino
Recorder: Matt Everlove
Member at Large: Russ Weeks
Member at Large: James Asimah
Director of Membership: David Reed
Director of Professional Outreach: Chuck Forth

Committee Chairs:
Don Creamer—Newsletter
Tim Westland—Ethics
Suzanne Chance—Marketing
Mentoring—Melissa Absher

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

Are you a budding journalist? 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-issa@q.com

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

If you have a security job to share with ISSA-COS members please go to http://cyberjoblist.com and click on "Post a Job." It is FREE and easy to fill out the form. You can cut and paste into the job description block. (It is polite to check with the company offering the job before posting.) Most employers will appreciate your efforts.

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