CONGRATULATIONS! You passed the CISSP examination. So now what?

As many of us know, there is a process called endorsement that must happen before that precious credential is issued. I know that this seems like a painful requirement but it is a step designed to ensure that only those who deserve the credential are properly screened and obtain it. To do otherwise would be a lack of diligence on the part of the ISC² – and they don’t take this lightly.

In fact – the ISC² does an audit on a percentage of the applications – so be sure that your input is absolutely correct in every way.

This sounds odd. As the candidate – you notice that the ISC² is telling the person doing the endorsement what to do. Well, who wants the credential? If it is the case that you want to be certified – then what stops you from understanding how to do the endorsement?

By formatting the resume in a way such that it reads precisely as needed for the endorsement – then what stops you from understanding how to do the endorsement? By formatting the resume in a way such that it reads precisely as needed for the endorsement – then what stops you from understanding how to do the endorsement?

The (ISC)² certified professional is anyone who:

- Is able to attest to the candidate’s professional experience (Does your endorser know your work? If not – think again – get someone who does.)
- Is an active (ISC)² credential holder in good standing (Prospective endorsers: do you know the status of your annual maintenance fee?)

The endorser will attest that the candidate’s assertions regarding professional experience are true to the best of the endorser’s knowledge. 

Here is what the ISC² says and one way to interpret what is said:

ENDORSEMENT

A candidate applying for certification must be endorsed by another (ISC)² certified professional in good standing before the credential can be awarded. (This is a non-negotiable.)

A candidate receiving a pass letter informing the candidate that he or she has passed the certification examination will also receive a blank endorsement form. The form must be completed and signed by an (ISC)² certified professional. (I was so happy to have passed I wasn’t thinking about another step. Don’t get caught off-guard. While waiting for your results you can go ahead and download the endorsement form and go ahead and read everything.)

The (ISC)² certified professional is anyone who:

- Is able to attest to the candidate’s professional experience (Does your endorser know your work? If not – think again – get someone who does.)
- Is an active (ISC)² credential holder in good standing (Prospective endorsers: do you know the status of your annual maintenance fee?)

The endorser will attest that the candidate’s assertions regarding professional experience are true to the best of the endorser’s knowledge.
Can we expect a cyber attack on the smart grid?

13 April 2012

The vulnerability of the energy industry’s new wireless smart grid will inevitably lead to lights out for everyone, according to leading cyber expert David Chalk. In an online interview for an upcoming documentary film entitled ‘Take Back Your Power’, Chalk says the entire power grid will be at risk to being taken down by cyber attack, and if installations continue it’s only a matter of time.

“We're in a state of crisis,” said Chalk. “The front door is open and there is no lock to be had. There is not a power meter or device on the grid that is protected from hacking - if not already infected - with some sort of trojan horse that can cause the grid to be shut down or completely annihilated.”

“One of the most amazing things that has happened to mankind in the last 100 years is the Internet. It’s given us possibility beyond our wildest imagination. But we also know the vulnerabilities that exist inside of it. And then we have the backbone, the power grid that powers our nations. Those two are coming together. And it's the smart meter on your home or business that's now allowing that connectivity.”

Chalk also issued a challenge to governments, media and technology producers to show him one piece of digital technology that is hack-proof.

“The computer companies that are involved, the manufacturers that are involved, bring forward a technology and I will show you that it’s penetrable,” said Chalk. “I’ll do it on national TV, I'll do it anywhere. But I can guarantee you 100% that there is nothing out there today – nothing – that can't be penetrated.”

Chalk’s strong words come amidst increasing reports of the smart grid’s fatal insecurities, even from the governments and energy companies who are forcing their hand with the smart program. “Every endpoint [meter] is a new potential threat vector,” according to Doug Powell, manager, SMI Security, Privacy & Safety, for Canadian utility BC Hydro.

And in an interview with Energy Now, former CIA Director James Woolsey was also highly critical of energy policy makers, whose plans received multi-billion dollar funding as part of the Economic Stimulus Act of 2008. “The so-called 'smart grid' that is as vulnerable as what we’ve got now is not smart at all,” said Woolsey. “It’s a really, really stupid grid.”

But there’s more. In an audit released in January, the US Inspector General Gregory Friedman was also highly critical. “Without a formal risk assessment and associated mitigation strategy, threats and weaknesses may go unidentified and expose the ... systems to an unacceptable level of risk,” Friedman wrote.

Energy officials knew of these weaknesses but approved plans for the projects anyway, auditors said. “The initial weaknesses had not always been fully addressed, and did not include a number of security practices commonly recommended for federal government and industry systems.”

Keeping the customer satisfied: cybercriminals focus on service

28 March 2012

Cybercriminals are shifting to a business model known as malware-as-a-service (Maas), where authors of exploit kits offer extra services to customers in addition to the exploit kit itself. It was just one of the observations in Verisign’s ‘2012 iDefense Cyber Threats and Trends’ report.

The Maas trend will probably continue as other developers adopt the same business model, the report predicted.

“The bad guys out there are trying to make a buck, and the way to distinguish themselves from their malware competitors is to layer on additional services”, said Rick Howard, general manager of Verisign iDefense. Cybercriminals want to “keep the customer happy”, he told Infosecurity.

“The bad guys out there are trying to make a buck, and the way to distinguish themselves from their malware competitors is to layer on additional services”, said Rick Howard, general manager of Verisign iDefense. Cybercriminals want to “keep the customer happy”, he told Infosecurity.

Read more here: http://www.infosecurity-magazine.com/view/24792/

Cyberattack cripples government agency network 12 weeks and counting

Federal law makers are currently considering multiple cybersecurity bills, but are still incapable of adequately protecting their own networks.

The Washington Post reported Monday that 80 days ago, an email virus struck the Economic Development Administration (EDA) — a small bureau within the Department of Commerce. The virus threatened the entire department’s network, and in order to prevent it from inflicting further damage, the agency’s IT staff was forced to bring the network offline.

The EDA — staffed by 215 employees — gives grants to “distressed” communities. The ability to email or do a Google search has been paralyzed, forcing employees to respond to grant applicants via fax. Agency employees are, however, admitting that the upside to being blown back to the Dark Ages is the return to human contact, the Post reported.

The number of government network intrusions reported to the Department of Homeland Security’s U.S. Computer Emergency Readiness Team is up from 5,500 in 2007 to a staggering 44,000 in 2011, the Post continued. The attack against the EDA is currently the longest intrusion in federal history.

Source: http://dailycaller.com/2012/04/09/cyberattack-cripples-government-agency-network-12-weeks-and-counting/#ixzz1rfVDGdUV

Firm Releases 2011 Report on Russian Cybercrime

Group-IB, a Russian cybercrime investigation and computer forensics company and LETA Group subsidiary, has announced a 28-page report on the Russian cybercrime market in 2011. Analysts from Group-IB’s computer forensics lab and its CERT-GIB unit prepared the report.

The report outlines the main risks associated with various types of hacker activities, analyzes the main trends in the development of the Russian cybercrime market, estimates the shares and the financial performance of the Russian segment of the global cybercrime market, and forecasts market trends for this year.

Full article and additional information here: 


http://group-ib.com/images/media/Group-IB_Cybercrime_Infograph_ENG.jpg

April 9, IDG News Service – (International) **Web attacks use smart redirection to evade URL security scanners.** Antivirus vendor ESET has come across new Web-based malware attacks that try to evade URL security scanners by checking for mouse cursor movement, ESET researchers said in a blog post April 6. The new drive-by download attacks were spotted in the Russian Web space and do not require user interaction to infect computers with malware. Rogue JavaScript code is being added to local JS files that get loaded in the “head” section of every HTML page. The code injected into these JavaScript files loads a different JS file from an external location but only if mouse cursor movement is detected. The purpose of the mouse movement detection is to filter out URL scanners and Web crawlers used by security companies or search engines to detect infected sites. If the check determines the request came from a human, the external JavaScript code injects an iframe into the original HTML page, which then loads attack code from an installation of the Nuclear Pack exploit toolkit. In this case, it attempts to exploit the CVE-2012-0507 Java vulnerability and the CVE-2010-0188 Adobe Reader vulnerability. Source: http://www.computerworld.com/s/article/9225957/Web_attacks_use_smart_redirection_to_evade_URL_security_scanners

April 16, IDG News Service – (International) **Web site vulnerabilities fall, but hackers become more skilled.** The number of coding mistakes on Web sites continues to fall, but companies are slow to fix issues that could be exploited by hackers working with improved attack tools, according to a security expert. The average number of serious vulnerabilities introduced to Web sites by developers in 2011 was 148, down from 230 in 2010, and 480 in 2009, said the chief technology officer (CTO) for WhiteHat Security, which specializes in testing Web sites for security issues. He spoke on the sidelines of the Open Web Application Security Project conference in Sydney, Australia, April 16. The vulnerabilities are contained in custom Web site code and are not issues that can be fixed by applying patches from, for example, Microsoft or Oracle, the CTO said. According to WhiteHat Security statistics, it takes organizations an average of 100 days to fix about half of their vulnerabilities. The risk is that vulnerabilities that have not been speedily remedied could be found by a hacker, resulting in a high-profile data breach. Source: http://www.computerworld.com/s/article/9226259/Website_vulnerabilities_fall_but_hackers_become_more_skilled

April 20, Computerworld – (International) **Flashback botnet not shrinking, huge numbers of Macs still infected.** Contrary to reports by several security companies, the Flashback botnet is not shrinking, according to the antivirus firm that first reported the massive infection 3 weeks ago. Dr. Web, which earlier in April was the first to report the largest-ever successful malware attack against Apple’s OS X, said April 20 the pool of Flashback-infected Macs still hovers around the 650,000 mark, and infections are continuing. Also April 20, the manager of operations at Symantec’s security response center confirmed Dr. Web’s numbers were correct. Dr. Web’s tally and its contention infections are ongoing flew in the face of other antivirus companies’ assertions. Kaspersky Lab and Symantec, which each “sinkholed” select domains — hijacked them before hackers could use them to issue orders to compromised machines — used those domains to count the Macs that try to communicate with the malware’s command-and-control centers. Earlier the week of April 16, Symantec said the botnet shrunk to 142,000 machines. April 19, Kaspersky claimed its count registered only 30,000 infected Macs. Source: http://www.computerworld.com/s/article/9226425/Flashback_botnet_not_shrinking_huge_numbers_of_Macs_still_infected

April 19, Network World – (International) **US-CERT: Social engineers target utilities with fake Microsoft support calls.** The U.S. Cyber Emergency Response Team recently warned that cyber criminals are attempting highly targeted social engineering attacks on operators of industrial control systems. These utility companies are receiving phone calls warning of infected PCs. The utilities receive a call from a representative of a large software company — allegedly, the one that sold them the operating system on their computers — warning them their PCs have viruses and to take a series of steps so the caller can help the operator fix the problem. The calls purport to be from the “Microsoft Server Department” informing the utilities they have a virus. The caller tries to convince the utility operators to start certain services on their computer (likely, those services would allow unauthorized remote access). Source: http://www.networkworld.com/community/node/80337
knowledge, and that the candidate is in good standing within the information security industry.

Download the endorsement form, print it out, have it completed and signed by a proper endorsing party, and return it to: (ISC)² Programs.

Just so we are clear – those two last sentences in the above reference are really key. The last sentence instructs the reader to download the endorsement form. Those instructions are for the CANDIDATE. So if you send your resume to the endorser with the expectation that he/she get that form, read the instructions, and provide you a hearty endorsement – well I suspect that most of you will find something is missing. The disconnect is that you, the CANDIDATE, must be ready and willing to learn the next steps so that you can also perform the endorsement for others when needed. You have entered a world of professional growth and must follow this to the end.

The second to the last sentence is the focal point of the entire process. As the professional who seeks certification – YOU will be making a professional assertion that your experience meets the requirements. You will be stating in exact terms your claim to the credential by asserting your years of specific experience that relate exactly to the domains in the credential.

Let’s first look at a way to format the resume to ensure the endorser has the shortest path to submitting your package as he/she verifies your experience. That’s correct – the endorser must VERIFY your assertions. Knowing this – the candidate will want to get references in order. Take a moment to do a pre-brief with your references by explaining to them that they should expect a phone call from your endorser (INSERT NAME) and that the endorser will only be asking questions that relate to the jobs you’ve done to support you. There is only one way to give your endorser the resume and endorsement form and that is complete and correct. By doing so shows your understanding of the requirements and demonstrates that you have a solid position from which to assert that you meet those CISSP requirements.

RESUME FORMAT TIPS:

1. Make sure your name and applicant number is on every page of your resume (in case the endorsement and resume get separated).
2. Format your resume to flow by the jobs that you have done in reverse chronological order – but only insofar as those jobs relate to the ISC2 domains. The ISC2 wants to see how your work relates to security not how well you learned how to write prose or poetry.
3. Make your assertion in months and map it directly to the domain that is applicable. Make certain that you know what the domains are and what your work maps to. You just spent months and month learning about what is in each domain. Do you really know how your work maps?
4. Your Endorser confirms your assertions. Okay – got it - #3 and #4 look very similar – they are stated this way because if you are unable to convince an endorser that your experience is a direct map – how can that endorser do an ethical endorsement? Moreover, how can ISC2 award the CISSP to someone that doesn’t know how their work experience maps?
5. DO NOT expect the endorser to "figure it out" – have a discussion and give all details. If the ISC2 has to do so – you can expect an audit, which will lengthen the time it takes to get the credential. Based on the high experience requirement of five years in two domains for CISSP – the resume will likely be showing multiple jobs and multiple lines that COULD map to a domain. So - you are likely to have a lot of experience. Keep in mind that ISC2 wants to know HOW that experience relates to security. Is all of the experience you have related to a domain? If not - then take the time to streamline the resume by taking out unrelated content: Map the resume directly to the ISC2 CISSP domains.
6. Your resume format is easiest to verify when it shows the direct mapping - for example:

   Feb 20xx to March 20xx Company XYZ Location, State

   Your Job Title

   Three or maybe four bullets maximum that map directly to the security domain you are asserting. Followed by your assertion -

   *****Domain Name and number of months*****

   Name, phone, email of the person who can verify you did this work.

   One example might be:

   Feb 2000 to March 2012 Internet Service Provider XZY, Denver, CO

   Network Security Architect and Programmer IV

   • Designed infrastructure to consolidate 650 remote locations, DMZ, IDS and SIEM.
- Wrote scripts and drivers to interface with several security systems
- Troubleshooting of all levels of the OSI model in wired and wireless systems

*****Telecommunications and Internet—60 months***** (remember to keep it in months).

*****Security Architecture and Design—60 months***** (overlap is possible because you could be doing both during the same period based on the job requirements but you could not have more months asserted than the actual experience at the job).

- Name, Email and Phone number of the person who can verify that you did this work at that time....

Remember to take out any duplications and ONLY put in the information that directly maps to the domains.

7. Your verifier adds an entry into your softcopy resume after each assertion that looks like this: Verified Experience XX MONTHS followed by his/her name or initials. This is also placed at the end of the resume. Take the time to create a one line entry at the end of the resume to sum it up - it takes 20 seconds and makes it easy for anyone reading through the resume to say... AHA! this candidate meets the requirements.

There is nothing written that precisely says to put that one line entry at the end of the resume to sum up everything but you should use your judgment - if you were screening hundreds of resumes a day - wouldn't you want the candidates to sum up their experience and make the assertion in one place so that it could quickly be verified? Also, who is better at this math - you or the person doing the verification?

If you have 60 months in two domains in the lines directly following your job ... then there is no reason to add the extra line because no total is needed. But - if you have 16 jobs with six months each - that makes it difficult for someone to go through the resume and keep the running total in their head - so it makes sense that the candidate who is making the assert do the math and show the final validator that the requirements are met in a one or two line entry.

8. The person doing the endorsement then sends the resume and endorsement form to the ISC2. STOP and CONSIDER THIS. I favor that the candidate request a copy of the resume be returned to him/her so that you have and keep proof that the endorsement was done and submitted. This ensures nothing slips through the cracks. Most everyone who does endorsements is busy. What if the endorser "forgot" to send your endorsement out? It has happened! So - be clear and discuss this with your endorser and make sure you get a copy.

9. The work requirement is exact: five (5) years (60 months) of professional and relevant work experience in two (2) or more of the ten (10) domains of the CISSP CBK, or four (4) years of work experience with an applicable college degree or another credential from the (ISC)²-approved list. NO SKIMPING - showing more is better and gives the sense that you have been doing this longer than required. Do you want to be the person that just meets the minimum requirement? It is fine if you just meet the requirement – but it is not okay to exaggerate in any way. Anyone caught cheating fails to meet the ethics requirement. Likely to never hold a CISSP.

10. The person doing the endorsement must make the following verifications:

   A) Consistency Evaluation - endorser MUST make sure the candidate maps the jobs to the domains - leave out anything else that does not apply.

   B) Job Verification – the candidate MUST provide name, phone number/email of someone who knew the job and the candidate so that the assertion can be verified.

   C) Determination that the jobs constitute PROFESSIONAL EXPERIENCE - don't leave this to chance - make it clear to the endorser that what you did maps to a security domain and that you were doing PROFESSIONAL level work (management, mentoring etc...). Endorser then verifies that the actual work is professional level work in
the asserted domain. There is no room to fudge on this. If the candidate does not meet the requirement – then a candid discussion is in order:

According to ISC2 - Professional experience includes:

- Work requiring special education or intellectual attainment, usually including a liberal education or a college degree.
- Work requiring habitual memory of a body of knowledge shared with others doing similar work.
- Management. Supervision of the work of others while working with a minimum of supervision one’s self.
- Work requiring the exercise of judgment, management decision making, and discretion.
- Requires the exercise of ethical judgment (as opposed to ethical behavior).
- Creative writing and oral communication.
- Teaching, instructing, training, and mentoring of others.
- Research and development.
- The specification and selection of controls and mechanisms (rather than the mere operation of those controls) (e.g., identification and authentication technology), but not when the basis is that of established standards or procedures.

I’ve recommended that each candidate obtain and read the entire endorsement form for understanding. Please take the time to get really familiar with the form as you will be asked to perform the verification and endorsement for others.

Also - make sure you are discussing your timeline with the endorser. He/she can get busy and you want this done in the shortest possible time, right?

Once this is all in the mail (with delivery confirmation) you can expect to see your wall certificate and wallet card in about 8 weeks. Again, CONGRATULATIONS!

Timothy Hoffman
ISSA-COS
Executive Vice President

Tim is a well-known consultant, trainer, former radio show host, and co-author of four technical books published by Prentice Hall PTR. He has extensive experience with security of wired and wireless networks, and computers and telecommunications that dates from 1969. He has worked with Fortune 1000 to small businesses, helped start small businesses of his own, and is currently the President and Owner of the Alida Connection, a VA Approved Veteran Owned Small Business that provides computer security consulting and technical training. Tim holds an MS, CISSP, GCIH, ISP, C|EH, Expert Rating PmP, CTT+, Security+ and Network+ and a range of other certifications. He consults, teaches and writes about computer and network security, TCP/IP, CISCO and most other vendor BackOffice technologies.
The Top 9 Most Costly Financial Services Data Breaches

By Greg MacSweeney, 02 April 2012

The MasterCard and Visa breach is only the latest in a string of hacks and data thefts that have cost financial institutions millions of dollars. Here are the nine biggest recent breaches.

Data breaches are no joke. Just ask any chief security officer. In addition to the bad headlines, customer churn and regulatory headaches associated with data breaches, the monetary costs can add up quickly. Until the Mastercard and Visa hack, the most recent high-profile data breaches have hit largely outside of the financial services industry, with Sony, Michael’s Stores and RSA (which cost parent company EMC close to $66 million) grabbing most of the headlines.

Despite the focus on other industries, though, financial services continues to be a top target for data breaches, caused by hacks, card scams, insider data theft, and the loss of a portable device that contains financial or private information.

And the details of the data breaches are downright scary, or ingenious, depending on your point of view. Here are 9 of the largest most recent financial services data breaches:

http://www.wallstreetandtech.com/slideshows/articles/232800079

Hack Attacks
Warning On Medical Implants

Insulin pumps and pacemakers can be turned off by radio control warn researchers

April 10, 2012 by Peter Judge

Security firms have warned hackers could use radio signals to attack pacemakers and other medical implants, potentially killing people.

Researchers from McAfee have shown they can take control of insulin pumps implanted inside diabetes patients, while scientists at the University of Massachusetts have shown they can use radio attacks to turn off defibrillators inside heart patients.

Implants such as pacemakers and insulin pumps, sit within patients and keep them alive. They are increasingly being given radio communications so they can be remotely controlled and updated, minimising the number of times they need to be accessed through surgery, and allowing information to be sent and received.

The problem is that the security on the radio link is breakable, and the implants’ operation can be remotely over-ridden.

Barnaby Jack, of Intel security subsidiary McAfee, has shown he can interfere with insulin pumps, by overriding their radio control. The pumps hold 300 units of insulin, enough for about 45 days, and are refilled by a syringe. Jack showed he could get the pumps to empty their reservoir completely in one go—which would cause very severe hypoglycaemia (low blood sugar level). The pump has a vibrating alert when it is delivering insulin, and Jack managed to override this also, making the attack potentially deadly.

“We can influence any pump within a 300ft [91m] range,” Jack told the BBC. McAfee has previously announced products to secure embedded devices, which could include implants.

Read the rest:
http://www.theregister.co.uk/2012/04/24/crackers_tools/

Hackers now pick tools from script kiddies’ toybox

April 24, The Register – (IDG News Service). Hackers are increasingly turning to automated software tools to launch attacks. According to research from Imperva, more than 60 percent of SQL injection attacks and as many as 70 percent of Remote File Inclusion attacks (the two most common attack types) are automated. Remote File Inclusion attacks allows hackers to plant back doors on PHP-based Web sites.

Tools like Havij and SQLMap are used by miscreants to probe for vulnerabilities and execute SQL injection attacks. These tools also employ techniques to evade detection, such as periodically changing headers or splitting attacks through controlled hosts to avoid black-listing.

In the past, using attack tools was purely for novices but these attitudes are changing, said Imperva’s director of security strategy. Automatic attack tools can be used to attack more applications and exploit more vulnerabilities than any manual method, making them a useful adjunct for skilled attackers. Source:

http://www.theregister.co.uk/2012/04/24/crackers_tools/
Cyber Warfare: The next Cold War

Stephen Lawton, April 02, 2012, SC Magazine

Instead of military assaults, today’s adversaries hire coders to create attacks that can run autonomously for years, says Stephen Lawton.

History books tell us that the Cold War ended in roughly 1991 after the dissolution of the Soviet Union. But, today’s security practitioners say the Cold War has simply morphed from a threat of armed conflict among major world powers into a battle of computer-savvy “troops” fighting from the comfort of offices.

Instead of countries spending billions of dollars to create new weapons, supply massive armies and spend millions of dollars (or rubles, francs or yuan) fighting conventional attacks against political, economic, religious or commercial foes, today’s adversaries hire code-writers to create attacks that can run autonomously for years with little or no human intervention. By repurposing code to spawn new attacks, the cost of cyber warfare can be a fraction of the cost of a conventional war.

While China and Russia generally are considered by industry experts to be the leaders in state-sponsored cyber attacks against the United States, they are not the only countries to have sophisticated espionage infrastructures in place, says Richard Bejtlich, chief security officer at Alexandria, Va.-based Mandiant. Other nations with sophisticated capabilities include North Korea, Iran, France, Israel and, of course, the United States.

North Korea, Bejtlich says, uses technology against its neighbor, South Korea, and to make political statements against the West, generally resulting in attacks against the United States, he says. Iran primarily uses its cyber weaponry to suppress internal dissidents.

In the past, he says, U.S. politicians spoke in general terms about cyber attacks, choosing not to name those believed to be responsible. That all changed late last year when the Office of the National Counter Intelligence Executive released a report, “Foreign Spies Stealing U.S. Economic Secrets in Cyber space,” which specifically identified China and Russia as key participants. However, the report also said U.S. allies are actively involved.

“Certain allies and other countries that enjoy broad access to U.S. government agencies and the private sector conduct economic espionage to acquire sensitive U.S. information and technologies,” the report states. “Some of these states have advanced cyber capabilities.”

It cited four factors that will shape the cyber environment over the next three to five years. These are: A technological shift, including the use of smartphones, laptops and other internet-connected devices; an economic shift that changes the way corporations, government agencies and other organizations share storage, computing, networking and application resources; a cultural shift in the U.S. workforce, where younger employees mix personal and professional activities; and a geopolitical shift as globalization of the supply chain and worker access increase the ability for malicious individuals to compromise the integrity and security of computing devices.

Jared Carstensen, manager of enterprise risk services at Deloitte in Dublin, Ireland, likes to differentiate between cyber crime and cyber espionage because the end goals differ significantly. For an attack to be considered a cyber crime, he says, the adversary does so for financial gain. This typically includes attacks designed to obtain credit card or bank data. Cyber espionage, on the other hand, is designed to steal intellectual property, and/or disable or attack critical infrastructure. It often is performed for political purposes.

Spying has been around since the dawn of man, Carstensen says. Early tribes snooped on other tribes to learn where they found food. Today’s sleuths also are looking for the same competitive advantage over their enemies – and even their allies.

In some countries, such as North Korea, students believed to have a propensity for math or technology are trained at an early age as cyber warriors. These academies provide the students with respectability and good pay. In China, for example, the Communist Party codified cyber warfare in 2010, and President Hu Jintao deemed cyber war a priority. Author and retired U.S. Marine Corps Lt. Col. William Hagestad says in an upcoming book that China bases its policies on the Art of War, Sun Tzu’s doctrine written around 500 B.C., one of whose tenets is: Keep your friends close, but keep your enemies closer. Chinese officials, however, regularly deny they are involved in any cyber spying efforts.

Read the rest here:
http://www.scmagazine.com/cyber-warfare-the-next-cold-war/article/232568/
Chapter Meetings

**Note the change in time for the May meeting! Now it’s at lunch.**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 23</td>
<td><strong>11:00 to 1:00</strong></td>
<td>Bambino’s Italian Eatery and Sports Bar, 2849 East Platte</td>
</tr>
<tr>
<td>Jun 20</td>
<td>11:00 to 1:00</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Jul 18</td>
<td>11:00 to 1:00</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Aug 15</td>
<td>5:30 to 7:30</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Sep 19</td>
<td>11:00 to 1:00</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Oct 17</td>
<td>5:30 to 7:30</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino’s</td>
</tr>
<tr>
<td>Dec TBD</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>

Training

**DISA/Navy security tools class... 5 May**

**Security+... June 9, and September 8**

**CISSP... June 2, 16, and 30; July 14 and 28**

**(ISC)2 Exam... 18 August**

**Learning Strategies Course (Tentative)...**

April/May timeframe; details being worked out

Upcoming ISSA Events

**May 16-17, Wednesday and Thursday, CISO Conference (Denver)**

**Aug 1-2, Wednesday and Thursday, Crowne Plaza Hotel (CSTC)**

**Oct 24-26, Wednesday through Friday, Disney Hotel, Anaheim, ISSA Annual Conference**

**Nov Conference, Friday, Nov 16, Crowne Plaza Hotel, 7:30 – 5:00**
ISSA International Has a New Logo & Tagline

As security professionals, we live in an ever-evolving world. Our field is growing while gaining visibility and stature. Our career paths have been guided through our affiliation with ISSA. We have developed our expertise and become leaders in our specialties. As a result, last week the International Board of Directors approved a new logo that reflects our current forward-looking security community and complements the recently-adopted tagline “Developing and Connecting Cybersecurity Leaders Globally.”

The new visual identity retains the familiarity that many associate with ISSA International. The new tagline and logo are our way of evolving with you, the information security expert, and those flocking to our profession.

Watch for the fresh look in next week’s issue of the ISSA Journal. New membership pins are coming soon!

March Conference Results

- 170 Signed up to attend, but...
  - Only 132 Showed up
  - $66.50 per person cost to the Chapter.
- Most speakers were good
  - Unfortunately, some gave a product pitch
- Not enough sponsors to cover costs
- Lessons Learned
  - 25% no-shows without attendance fees
  - 10% non-registered attendees
  - Try to saturate sponsor involvement
  - Qualify presentations better
  - Arrange for registration table to be manned early
  - Request conference speaker and sponsor critiques
- Conference Direction
  - How do we attract a larger attendance?
  - Should we focus on a theme?
  - Is a single track satisfactory?
  - Are there specific sponsors you want to be there?
  - Should we schedule product pitches in a separate area?
  - Any other ideas?

TECHNOLOGY EXPO
Open to all personnel!
Wednesday, 16 May 2012
From 10 a.m. until 2 p.m.
Elkhorn Catering and Conference Center
Fort Carson, Colorado
- Interact with industry partners
- Assess technology capabilities from leading industry experts
- Experience hands-on demonstrations of the latest cutting edge technologies

www.FederalEvents.com
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...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? 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@q.com or william.creamer.ctr@us.af.mil

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

This Skimmer Is Why You Should Be Nervous at ATMs

There have been plenty of attempts to make ATM skimmers look realistic—including 3D printing—but this is perhaps the best yet. Reported by Krebs on Security, you would have to be an expert to spot it. The device was discovered in a bank in San Fernando Valley earlier this year. From the front, it is almost perfect. The only giveaway? A tiny, tiny pinhole on the right hand side of the device (see the close-up), through which a small camera can capture PIN as skimming victims type them in. Flip the innocuous-looking device over, and it becomes clear that its intentions are underhand. The all-in-one device records card details and PIN, and is powered by what looks like a phone battery. Police still haven’t worked out who placed this device—which is believed to be one of many—on the ATM where it was found. Read more here:

http://gizmodo.com/5904949/this-skimmer-is-why-you-should-be-nervous-at-atms/gallery/1