The Colorado Springs Chapter of the Information System Security Association is hosting its Annual November Event on the 14th of November at the Clarion Hotel and Conference Center.

The doors will open at 7:15 a.m., and the first speaker will begin at 8 a.m. with the day ending at 5 p.m.

Many of the subjects to be covered are:

- “Building Security In” or “Learning the Unlearned Lessons of the Past”
- “Awareness Doesn’t Matter- A Behavior Design Approach to Securing Users”
- “Network Access Control”
- “The Evolution of Hacking… All Your Data Still Belongs to Us.”
- “How to Keep NSA Overseas and Out of Your System” or “A Primer on How to Setup Secure E-mail and Web Services”
- …and more!

The registration fee is only $25, and that includes both a continental breakfast and lunch. A number of door prizes will also be given out to some lucky attendees.

Advance registration is available online at: http://www.eventbrite.com/event/1364656725

We hope to see you there. We believe that you will find this well worth your time.

This event does qualify for CPE’s should your certification require them.
You May Want to Password-Protect Your Body

By Laura Hood, Slate, October 7, 2013

If you think it’s enough of a chore trying to stop thieves stealing your credit card details and hacking your Facebook, imagine trying to stop them getting into your pancreas.

Advances in health care mean that in-body devices to treat chronic conditions or even just make you perform better as a human being are not as far away as you might imagine. Some of these innovations already exist. The pacemaker has been around for years, and drug delivery implants are already quite advanced. Some are controlled remotely and many more will be in the future, significantly raising the stakes in the battle to protect ourselves from cybercrime.

When TV series Homeland featured a storyline in which terrorists hacked the vice president’s pacemaker, causing him to have a heart attack, it brought this issue into the public consciousness. But the scenario has been possible for some time, says Sadie Creese, Director of the Global Centre for Cyber Security Capacity at the Oxford Martin School, University of Oxford, and more people will be vulnerable in the future.

“I think the future of chronic disease control will be implanted devices,” she said, speaking after a talk at FutureFest, an event held in London recently. “They will be measuring vital signs, reaching back to the health care providers, whoever that might be and wherever they’re based. So you can imagine consultants and doctors around the world, or your local doctor, firing up a single app and being able to receive alerts on a patient.”

Demonstrating this future phenomenon in action during FutureFest, social psychologist Bertolt Meyer allowed a fellow speaker to control his bionic hand using an iPhone app connected via Bluetooth.

“My hand comes with an iPhone app. There is an app for that. This gives the word hacking an entirely new dimension because if someone hacked my phone they could hack my hand. There’s a trickle-down effect of things we are able to do,” he said.

While many people won’t have to worry about having their limbs controlled remotely like Meyer, in-body devices are not as far away as we might imagine. Meyer noted that it is already possible to hack into delivery systems for diabetics, meaning that criminals could remotely deliver fatal doses of insulin.

As devices like bionic arms become more advanced, it is not inconceivable that people might choose to replace functioning body parts with high-performance models. Meyer’s state-of-art hand can rotate a full 360 degrees. How many of us can say that?

Add to this a number of people who will choose to have voluntary surgery or have devices implanted in order to improve their basic health or appearance, and the implications are even more serious. “The truth of the matter is, it’s kind of already here but mainly for significant conditions. Give it five to ten years and we’ll all be wandering around with devices,” adds Creese.

Creese believes the general public needs to start engaging with the debate about their information now rather than leaving it until the technology develops further.

“When we think about cyborg futures, be that health care or play, we need to get on top of how we make this citizen centric and how we achieve a fair relationship between people and commerce. In understanding that relationship we’ll understand cybersecurity.”

Read the rest here: http://www.slate.com/blogs/future_tense/2013/10/07/bodyhacking_the_next_frontier_in_cybercrime.html
Elections for Your Board of Directors

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

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

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

The following offices (with job descriptions) are up for election this year:

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

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

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

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

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

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

Elections will occur at the December luncheon meeting and assumption of office will occur at the end of the December meeting.
Let’s Hear it for the Ladies:
Women in Information Security

Several of the interviewees agree that many women consider information security – and technology generally – to be an “unattractive career choice” and are keen to articulate that this mindset is self-imposed.

By Eleanor Dallaway, InfoSecurity, October 17, 2013

The latest (ISC)² workforce study, (http://www.infosecurity-magazine.com/view/30888/latest-isc2-workforce-study-shows-lack-of-skilled-infosec-professionals-and-developers-) published in spring 2013, declares that only 10% of the information security industry’s professionals are female. Attendance at industry events and feedback from hiring managers all contribute to this consensus. Although 76% of those interviewed for this article say that they believe more women are entering the field, all agree this is happening “very slowly”.

There are some initiatives – both internally in the industry and externally through government – intent on increasing and supporting women entering the profession. A recent spike in industry events and seminars focused on women in security – including the upcoming Bletchley Park Women Codebreakers of WII event organized by the Cyber Security Challenge and Women’s Security Society – are testament to the increased awareness about the lack of women in the industry and a desire to honor those who are and encourage new (female) blood. But the first question is whether this is something felt necessary by the industry at whole.

More than half of those Infosecurity interviewed for this article do see this deficiency as problematic and disappointing and are eager for more industry action to change this balance. “More needs to be done. There are only a few organizations out there offering women’s scholarships in information security – the (ISC)² Foundation is one of them. Across the board, this issue has been widely ignored but it can’t stay this way forever”, says Michelle Schafer, vice president of the security practice at Merritt Group, a PR firm.

Konstantinia Charitoudi, part-time lecturer and security consultant at the University of South Wales, and PhD research in information security, is also calling for more to be done. “It’s important that women in the field encourage other women, but it would also be nice if more men were involved in this encouragement, to make women feel welcomed in a field that is supposed to be ‘man’s world’”. She declares stereotypes, culture and lack of encouragement “to blame”.

At the other end of the spectrum you have people like Caitlin Rose Johanson, Sheena Wallace, and Anne Wood. “Gender isn’t important here”, answers Wood when asked whether the government and industry are doing enough to encourage women into the sector. “Skills should be the consideration, irrespective of gender”. Anne Wood is a senior consultant at Sysnet Global Solutions.

Sheena Wallace, lead security consultant at Context Information Security, agrees with Wood. “I’m not sure that there should be a requirement for external bodies to encourage or influence in either direction. As long as there is not active discouragement – which I have never observed – then women [should be] left to make their own minds up as to which industry would best suit them.”

“It doesn’t matter either way as long as we are advancing our security practices”, agrees Caitlin Rose Johanson, senior solutions architect at Veracode, when asked the same question.

Seeking a Sexy Career

Several of the interviewees agree that many women consider information security – and technology generally – to be an “unattractive career choice” and are keen to articulate that this mindset is self-imposed. “I think [the low numbers of women in information security] is more a lack of interest in the part of women than exclusion by men”, says Birgit Thorup Mullen, senior security associate at Bishop Fox. “The motivation to enter an industry has to come from the people who want to be in it”, she argues.

“It’s not a terribly glamorous job”, admits Patricia Titus, former CISO at Symantec, Unisys, and the US Transportation Security Administration (TSA). “We have to deal with some of the scum of cyber space, so you have to have a strong stomach and a lot of intestinal fortitude.”

Bridget Burke, vice president, CIO and CSO at HID Global, points to another possible factor that puts women off. “Women are often collaborators not isolationists, so the field may not seem attractive to them. It is also a risk based-discipline, which women may not see as creative or interesting as other fields of study.”

Read the rest here: http://www.infosecurity-magazine.com/view/35127/lets-hear-it-for-the-ladies-women-in-information-security-
Are You Missing Your Coin?

Here is the list of current and former ISSA members that Deborah Johnson has at least one coin for. Please take a look at the list to see if you know any of these folks. The coins can be picked up in person, by proxy, or she can mail them to folks if they can be located. Deborah’s email address is djohnson@swcp.com and her telephone number is 719-329-4495 (voicemail) if folks want to contact her directly. Thank you!

A
Adams, Tim
Aguryanov, Sergey
Alexeev, Eugene
Anders, Christopher
Anderson, Richard
Andress, Jason
Andrus, Thip
Archer, Cliona

B
Bailey, Craig
Beasley, Marke
Bernard, Denny
Bilyeu, Raymond
Birkeland, Rolf
Bond, David
Bone, Regina
Borer, Arthur
Bowers, Mark
Brown, Clark
Brown, Josh
Buckley, Lisa
Buehler, Scott
Bull, Justin
Burns, R.
Burton, James

C
Caldwell, Deborah
Callaghan, John
Calloway, Ernest
Campeau, Ronald
Carlson, George
Chisesi, Dan
Collins, David
Copenhagen, Brian
Corlew, Michael
Coultrap, Michael

D
Dailey, Shane
de la Garza, Enrique
Donjon, Dan
Dgert, Dan
Elmstedt, Matt
Fanberg, Kevin
Farrar, Nathan
Farrow, Chris
Fermanis, Timothy
Fernandez, Damian
Frankovich, Dawn
Freeman, James
Fry, Josh
Garate, Reynaldo
Gates, Ryan
Gearheart, Frank
Gobeo, Michael
Gonzales, Mark
Guzman, Henry
Hair, Christopher
Halloran, David
Hardin, David
Harper, Brian
Henneging, Fred
Herod, Dan
Hill, Butch
Hinze, Kevin
Hjelmstad, Eric
Hoefelmeyer, Ralph
Hooper, William
Hughes, Jeff
Hughes, Paul
Hurley, John

I
Ingram, Louis
J
Jensen, Al
Jones, Bryant
Jordan, Erin
Kidder, Peter
Kieffer, Steven
Koch, Chriss
Kolb, Garrett
Krzywonski, Branden

L
Laborwit, Al
Lanham, Michael
LeFebvere, Brad
Levesque, Robert
Loehndorf, Jon
Lorenc, Chad
Lund, Tim
Malone, David
Mance, Howard
Mann, John
Manous, Carey
Marchand, Hummer
Martin, Jeremy
Martinez, Mitch
Masincupp, Danny
Matthews, Clint
Menkhuis, Mark
Mercer, Samuel
Modissette, Mark
Mohl, Derrick
Moll, Joseph
Mondello, Mark
Moore, Kathryn

M
Morrison, Richard
Myers, Ryan
Nieman, Joann
Norquist, Bruce
Oliphant, Thomas
O’Neill, Michael
Orban, Michael
Palmer, Scott
Paynter, Stephen
Peralta, Rex
Perry, Adam
Peterson, Jeff
Plattenberger, Playle, Greg
Powers, Steve
Ray, Lori
Riggs, Michael
Rodrigues, Rory
Rogelio, Raymond
Roth, Lee
Saporito, Tia
Sawyer, Jim
Schierholz, Andrew
Schooley, Christopher
Schwoerer, Ralf
Shaffer, Tim
Shepherd, Stephen
Slavick, Mike
Smith, Harry
Spencer, Dawn
Spinney, Byron
Staggs, Michael
Stoddard, Lewis
Swinnich, David
T
Tang, Freddy
Taylor, Jeremy
Tesch, John
Thomas, Christopher
Tracy, John
Trussell, Terry
Tugade, Medario
Tyree, George
Underwood, Ralph
Van Cura, Robert
Vulcan, Leland
Wahl, Sarah
Walker, Todd
Walls, Todd
Weiss, Brian
White, Russell
White, Steve
Wiedmann, Lee
Williams, Jarold
Williams, Melanie
Wilmet, Eric
Wilson, Arthur
Wonders, Donald
Wright, Christopher
Growing backlash to government surveillance

By Martha Mendoza, Associated Press, October 12, 2013

From Silicon Valley to the South Pacific, counterattacks to revelations of widespread National Security Agency surveillance are taking shape, from a surge of new encrypted email programs to technology that sprinkles the Internet with red flag terms to confuse would-be snoops.

Policy makers, privacy advocates and political leaders around the world have been outraged at the near weekly disclosures from former intelligence contractor Edward Snowden that expose sweeping U.S. government surveillance programs.

"Until this summer, people didn't know anything about the NSA," said Center for International Security and Cooperation at Stanford University co-director Amy Zegart. "Their own secrecy has come back to bite them."

Activists are fighting back with high-tech civil disobedience, entrepreneurs want to cash in on privacy concerns, Internet users want to keep snoops out of their computers and lawmakers want to establish stricter parameters.

Some of the tactics are more effective than others. For example, Flagger, a program that adds words like "blow up" and "pressure cooker" to web addresses that users visit, is probably more of a political statement than actually confounding intelligence agents.

Developer Jeff Lyon in Santa Clara, Calif., said he's delighted if it generates social awareness, and that 2,000 users have installed it to date. He said, "The goal here is to get a critical mass of people flooding the Internet with noise and make a statement of civil disobedience."

University of Auckland associate professor Gehan Gunasekara said he's received "overwhelming support" for his proposal to "lead the spooks in a merry dance," visiting radical websites, setting up multiple online identities and making up hypothetical "friends."

And "pretty soon everyone in New Zealand will have to be snoops."

Electronic Frontier Foundation activist Parker Higgins in San Francisco has a more direct strategy: by using encrypted email and browsers, he creates more smoke screens for the NSA. "Encryption loses its' value as an indicator of possible malfeasance if everyone is using it," he said.

And there are now plenty of encryption programs, many new, and of varying quality.

Read the rest here:
Researchers split over NSA hacking

Cryptographers condemn US National Security Agency’s tapping and tampering, but mathematicians shrug.

By Ann Finkbeiner, Nature, October 8, 2013

The US National Security Agency (NSA) has upset a great many people this year. Since June, newspapers have been using documents leaked by former intelligence worker Edward Snowden to show how the secretive but powerful agency has spied on the communications of US citizens and foreign governments. Last month, the media reported that the NSA, which is based in Fort Meade, Maryland, had undermined Internet security standards. The revelations have sparked international outrage at the highest levels — even the president of Brazil cancelled a visit to the United States because of the spying.

Yet amid the uproar, NSA-supported mathematicians and computer scientists have remained mostly quiet, to the growing frustration of others in similar fields. “Most have never met a funding source they do not like,” says Phillip Rogaway, a computer scientist at the University of California, Davis, who has sworn not to accept NSA funding and is critical of other researchers’ silence. “And most of us have little sense of social responsibility.”

Mathematicians and the NSA are certainly interdependent. The agency declares that it is the United States’ largest maths employer, and Samuel Rankin, director of the Washington DC office of the American Mathematical Society, estimates that the agency hires 30–40 mathematicians every year. The NSA routinely holds job fairs on university campuses, and academic researchers can work at the agency on sabbaticals. In 2013, the agency’s mathematical sciences programme offered more than US$3.3 million in research grants.

Furthermore, the NSA has designated more than 150 colleges and universities as centres of excellence, which qualifies students and faculty members for extra support. It can also fund research indirectly through other agencies, and so the total amount of support may be much higher. A leaked budget document says that the NSA spends more than $400 million a year on research and technology — although only a fraction of this money might go to research outside the agency itself.

Many US researchers, especially those towards the basic-research end of the spectrum, are comfortable with the NSA’s need for their expertise. Christopher Monroe, a physicist at the University of Maryland in College Park, is among them. He previously had an NSA grant for basic research on controlling cold atoms, which can form the basis of the qubits of information in quantum computers. He notes that he is free to publish in the open literature, and he has no problems with the NSA research facilities in physical sciences, telecommunications and languages that sit on his campus. Monroe is sympathetic to the NSA’s need to track the development of quantum computers that could one day be used to crack codes beyond the ability of conventional machines. “I understand what’s in the newspapers,” he says, “but the NSA is funding serious long-term fundamental research and I’m happy they’re doing it.”

Dena Tsamitis, director of education, outreach and training at Carnegie Mellon University’s cybersecurity research centre in Pittsburgh, Pennsylvania, also wants to maintain the relationship. She oversees visitors and recruiters from the NSA but her centre gets no direct funding. She says that her graduate students understand the NSA’s public surveillance to be “a policy decision, not a technology decision. Our students are most interested in the technology.” And the NSA, she says — echoing many other researchers — “has very interesting technology problems”.

Read the rest here:
http://www.nature.com/news/researchers-split-over-nsa-hacking-1.13911
A pair of researchers have uncovered more than two dozen vulnerabilities in products used in critical infrastructure systems that would allow attackers to crash or hijack the servers controlling electric substations and water systems.

The vulnerabilities include some that would allow an attacker to crash or send a master server into an infinite loop, preventing operators from monitoring or controlling operations. Others would allow remote code-injection into a server, providing an opportunity for an attacker to open and close breakers at substations and cause power outages.

"Every substation is controlled by the master, which is controlled by the operator," says researcher Chris Sistrunk who, along with Adam Crain, found vulnerabilities in the products of more than 20 vendors. "If you have control of the master, you have control of the whole system, and you can turn on and off power at will."

The vulnerabilities are found in devices that are used for serial and network communications between servers and substations. These products have been largely overlooked as hacking risks because the security of power systems has focused only on IP communication, and hasn’t considered serial communication an important or viable attack vector, Crain says. But the researchers say that breaching a power system through serial communication devices can actually be easier than attacking through the IP network since it doesn’t require bypassing layers of firewalls.

An intruder could exploit the vulnerabilities by gaining physical access to a substation — which generally are secured only with a fence and a webcam or motion-detection sensors — or by breaching the wireless radio network over which the communication passes to the server.

"If someone tries to breach the control center through the internet, they have to bypass layers of firewalls," Crain said. "But someone could go out to a remote substation that has very little physical security and get on the network and take out hundreds of substations potentially. And they don’t necessarily have to get into the substation either."

He points to a recent presentation at the Black Hat security conference that discussed methods for hacking wireless radio networks, which a lot of utility control systems use, including ways to crack the encryption.

"There are quite a few ways onto these networks, and utilities have to worry about this new attack vector," Crain said.

Once in the network, an intruder can send a malformed message to the server to exploit the weakness.

"The device is supposed to throw that [malformed] message away," says Sistrunk, "and in these cases it’s not and is causing issues."

Neither Crain nor Sistrunk is a security researcher. Sistrunk is an electrical engineer at a major utility, but conducted the research independently of his employer and therefore asked that it not be identified. Crain recently launched a consulting firm called Automatak that focuses on industrial control systems. They began to examine the systems last April using a fuzzer that Crain created, and submitted their findings to the Department of Homeland Security’s Industrial Control System-CERT, which helped them notify the vendors.

"We found vulnerabilities in virtually all implementations [of the protocol]," Sistrunk said. "Some of them are worse than others."

Since then, ICS-CERT has published a number of advisories about the vulnerabilities, and vendors have distributed patches for nine of them, but the rest remain unpatched so far. Despite the distribution of patches, Crain and Sistrunk say that many utilities have not applied them because they’re unaware of the serious nature of the vulnerabilities.

The systems use DNP3, a protocol for serial communications that is used in almost all electrical utilities in the U.S. and Canada to transmit communication between servers located in data centers and field devices. Electric utilities generally have a data center with two or three servers that can each monitor and communicate with a hundred or more substations, depending on the size of the utility.

The servers communicate with programmable logic controllers and remote-terminal units in the field to collect status data from them in order to allow operators to monitor conditions and to allow them to trip breakers as needed or to increase or decrease the voltage.

A lot of utilities also use the master servers for security purposes to control alarm systems, so crashing them would potentially disable alarms as well.

Read the rest here: http://www.wired.com/threatlevel/2013/10/ics/
'Project SHINE' Illuminates Sad State Of SCADA/ICS Security On The Net

By Kelly Jackson Higgins, Dark Reading, October 16, 2013

A global Internet-scanning project focused on finding SCADA/ICS equipment and systems accessible via the public Internet is discovering some 2,000 to 8,000 new exposed devices each day.

Project SHINE, which has been gathering data on SCADA/ICS devices from SHODAN for a year-and-a-half, has identified more than 1 million unique IP addresses thus far, according to Bob Radvanovsky, one of the researchers behind it. "I would say one-fourth or one-third of them are devices that could be vulnerable to malware attacks ... and buffer overflows, cross-site scripting, things of that nature," he says. "[And] we feel the majority are misconfigured or improperly configured."

This has been a common theme among other global scanning projects searching for exposed devices on the Internet. Many of these devices discovered -- everything from home routers to servers -- contain default backdoor-type access by their vendors for internal ease of use and access, including default passwords or major security holes. And the sites running these products typically are unaware of these holes or the potential dangers associated with these devices sitting exposed on the Net. They often don't even know the devices are Internet-accessible.

But locking down or securing these vulnerable devices on the Internet has been much harder than finding them. The well-publicized scanning projects by renowned researcher HD Moore (http://www.darkreading.com/vulnerability/millions-of-networked-devices-in-harms-w/240147276?itc=edit_in_body_cross) haven't yielded the expected fixes. Moore says Universal Plug and Play (UPnP) devices, for example, still remain exposed on the Net despite his discovery and disclosure of some 40 to 50 million networked devices in harm's way via flaws in the pervasive UPnP protocol, which is enabled by default in most printers, routers, network-attached storage, IP cameras, media players, smart TVs, and even video game consoles.

Moore is one of the pioneers of this practice and, most recently, led his company, Rapid7, in forming a community Internet-scanning initiative called Project Sonar. The goal is to provide a way for researchers to share their data as well as to educate vendors whose products are discovered via scans -- and to raise public awareness of the vulnerability of this Internet-facing equipment.

Project SHINE has no plans to join up with Project Sonar, says Radvanovsky, who has found via the scans both traditional SCADA/ICS devices and software such as programmable logic controllers (PLCs), remote terminal units (RTUs), sensors, SCADA human machine interface (HMI) servers, and DCS, as well as relative outliers such as medi-cal devices, traffic management systems, automotive control systems, traffic light control systems, HVAC systems, power regulators, CCTV and webcams, serial port servers, and data radios.

Radvanovsky runs the project out of his basement, and he and colleague Jake Brodsky use the online search engine SHODAN combined with their own tools to identify SCADA-specific equipment. The researchers crafted their own search terms to find those types of devices among the devices mapped in the SHODAN database. "We created our own search terms to find those types of devices among the devices mapped in the SHODAN database. "We created our custom app that harvests data from the [SHODAN] search engine," he says. "They are all flat files right now, but we are going to need to convert to a SQL database -- there's that much data."

Much of the equipment Project SHINE has found are embedded devices, as well as Web interfaces for managing devices, for instance. "We've had some oddball scans...[control systems for] mining trucks, for example, which aren't your typical SCADA systems," Radvanovsky says.

In one case, Radvanovsky says he found an HVAC system in a building in Florida and discovered that the exposed interface could actually let someone alter the temperature settings of the system remotely via the Internet. "It was 92 degrees outside, and it was a comfortable 78 inside, and we could change the temperature through the management interface, he says.

Rapid7's Moore, who is also the creator of Metasploit, says the SHINE Project can help determine the state of SCADA equipment on the Internet. "The SHINE project can definitely improve our understanding of vulnerabilities in Internet-facing SCADA equipment. At the moment, it isn't clear what type industries are most exposed, what vendors are better or worse than others, and or whether there are classes of vulnerabilities that span a large portion of SCADA infrastructure," Moore says. "We are seeing security researchers continue to focus on embedded systems, both SCADA and otherwise, and so far, the results have been frightening. The security of your average smartphone is decades ahead of the embedded platforms used by ICS and SCADA equipment."

Read the rest here: http://www.darkreading.com/vulnerability/project-shine-illuminates-sad-state-of-s/240162739
Cyber Resilience:
Building a Defense Strategy that Works

By Steve Durbin, Information Security Forum (ISF), September 26, 2013

Cyberspace is continuously evolving as its potential and threats, vulnerabilities, complexity and interconnectivity are in a constant state of change. As activists, cybercriminals and nation-states disproportionately increase traditional information risks, it’s becoming clear that the business risks associated with operating in cyberspace should be moving quickly to the top of most chief executives’ agendas.

Today, chief information security officers (CISOs) and other information practitioners are required to provide more accountability and considered opinion about the commercial, reputational and financial risks that go with cyberspace. Highly publicized breaches in the media, and more stringent regulation, have put the spotlight on information security in most organizations around the world. This has resulted in unprecedented pressure to assure stakeholders that sensitive information is secure.

The big question for governments, enterprises and individuals alike is how can these growing cyber threats be countered without losing the benefits of internet-based trade, commerce and communication? That’s a tall order given that cyberspace is constantly changing and has become an increasingly attractive hunting ground for criminals, activists and terrorists.

A Security-conscious World

There have been a number of initiatives proposed by governments around the world for tackling cyber threats. These range from allocating funds and creating legislation to protect critical infrastructure, to programs that mandate cooperation and collaboration between the government, enterprise and academia. Many of these are still unclear and under development. What is achievable, however, is to prepare an effective response to the inevitable attacks so that their consequences are minimized.

With cyberspace so critical to everything from supply chain management to customer engagement, holding back adoption, or disconnecting from cyberspace altogether, is simply not feasible. All this makes it imperative for governments and enterprises to build up cyber resilience. This can be achieved through a proportional approach that balances the need to protect organizations and individuals with the need to enable free, legitimate trade and communications.

But the commercial, reputational and financial risks that go with cyberspace are real and growing. In the drive to become cyber resilient, organizations need to extend their risk management focus from pure information confidentiality, integrity and availability (CIA) to include other risks, such as those to reputation and customer channels, and recognize the unintended business consequences from activity in cyberspace.

Managing Information Risk with Resilience

Establishing cybersecurity alone is no longer enough. Today, risk management largely focuses on achieving security through the management and control of known risks. The rapid evolution of opportunities and risks in cyberspace is outpacing this approach, and it no longer provides the required protection. Cyber resilience requires recognition that organizations must prepare now to deal with severe impacts from cyber threats that are impossible to predict. Organizations must extend risk management to include risk resilience, in order to manage, respond and mitigate any negative impacts of cyberspace activity.

As I mentioned earlier, cyber threats are not just an issue for the information security function; they require the involvement of every discipline within an organization and its partners and stakeholders. A coordinated, collaborative approach is needed, led by senior business leaders – preferably the chief executive or chief operating officer, certainly a board member. In order to be successful, organizations need to coordinate with customers, suppliers, investors, the media and other stakeholders.

Cyber resilience also requires that organizations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences. This means assembling multidisciplinary teams from businesses and functions across the organization, and beyond, to develop and test plans for when breaches occur. This team should be able to respond quickly to an incident by communicating with all parts of the organization, individuals who might have been compromised, shareholders, regulators and other stakeholders who might be affected.

Cyber Governance and Partnering

One key element of building cyber resilience is to establish a governance framework with board-level buy-in for monitoring online activities – including partner collaboration, and the risks and obligations associated with operating in cyberspace. Organizations should have a process for analyzing, gathering and sharing cyber intelligence with stakeholders. They also need a process for assessing and adjusting their resilience to the impacts from past, present and future cyberspace activity.

Read the rest here:
The Cybersecurity Pipeline

When it comes to educating the current and future information security workforce, the (ISC)² US Government Advisory Board Executive Writers Bureau asks:

Where are universities in the flow?

By InfoSecurity, October 15, 2013

The explosive growth in the number, complexity, and impact of cyber threats in recent years has greatly increased the demand for highly skilled cybersecurity professionals to protect sensitive information and defend public and private information systems and networks. The 2013 (ISC)² Global Information Security Workforce Study (http://www.infosecurity-magazine.com/view/30888/latest-isc2-workforce-study-shows-lack-of-skilled-infosec-professionals-and-developers-) projects there will be 4.2 million information security professionals by 2017, representing a compounded annual growth rate of 13.2%.

It’s encouraging that so many professionals are entering the market, but to overcome the global cybersecurity skills shortage and ensure a healthy future workforce, universities will need to scale their capabilities to meet the growing demand.

In response, academia has dramatically increased the number of centers and courses that focus on cybersecurity. For example, in the US, the NSA/DHS-sponsored National Centers of Academic Excellence alone have grown to over 160 institutions since their inception just over a decade ago. While some of these institutions have developed comprehensive academic programs around cybersecurity, others have merely added minor overlays that only touch on cybersecurity within their current curriculum. Ultimately, there remains a gap in helping prospective professionals move from their educational path into the workforce, with the instincts and skills that the market demands.

Keeping Pace

The reason for the imbalance between what traditional academic programs are able to deliver and what the current hiring needs of organizations call for is multifaceted and complex. “We feel that the real cause of any shortfall in supply of cybersecurity trainees is the fact that cybersecurity is not well understood as a career option among younger people seeking university degrees”, says Chez Ciechanowicz, course director for the Information Security Group at Royal Holloway, University of London. Along with an awareness problem, there are several additional challenges that hinder colleges and universities from playing a larger role in meeting today’s demand for cybersecurity expertise.

First, college and university degree programs are not inherently structured in such a way to provide graduates with current expertise rapidly enough and with content that is fresh enough to meet today’s demand. “What tends to happen is that industry looks very short-term and looks for specific ‘training’ rather than a good ‘education’, and this is particularly true in a fast-changing subject”, observes Kevin Jones, head of Computer Science and deputy dean for the School of Informatics at City University London.

The current cyber environment is more dynamic than traditional programs can accommodate, such that the pace of curricula updates for formal bachelor and master degree programs cannot keep up with the rapidly evolving cybersecurity requirements of public and private organizations. In some cases, there is a tension between long-term educational goals and short-term industry training needs.

Second, the design of cybersecurity degree programs is built on the foundation of computer science or information technology expertise to which cybersecurity skills and knowledge are then added. This generally results in cybersecurity degrees at the graduate level and increases the time required to attain recognized academic competence.

Finally, universities are torn by occasional conflicting signals of demand. On the one hand, government and industry regularly call for an increasingly skilled cybersecurity workforce. However, many of the students entering universities are wholly unaware of the opportunities in the field. This confusion can cause an imbalance between supply of courses and, ultimately, graduates that are in demand by industry.

Simple Solutions

Given the situation just described, what can institutions of higher learning do today to increase their contribution to the cybersecurity pipeline? They can begin by recognizing there is a major need for cybersecurity expertise today and that they play a vital role in filling this need.

One of the first ideas to consider is offering cybersecurity courses as part of undergraduate degree programs. Specifically, there should be increased course offerings for both associate and bachelor degree programs. These programs should be cutting-edge and used to recruit bright students graduating from secondary schools that are interested in pursuing technical career paths.

Read the rest here: http://www.infosecurity-magazine.com/view/35051/the-cybersecurity-pipeline/
Comment:
Beware the Nascent Cyber Insurance Market

As security incidents grow in number and severity, organizations are not only relying on their own defenses to guard against losses, but are increasingly looking to insure themselves against those losses. However, all should be aware that the cyber insurance market is still in relative infancy, as Colin Tankard outlines.

By Colin Tankard, Digital Pathways, October 10, 2013

Security breaches are mainstream occurrences, and every organization should assume that they are a victim. According to recent research published in conjunction with Infosecurity Europe in April, 93% of large organizations state that they experienced at least one breach in the previous year. They also reported that the number of breaches is growing rapidly as organizations experienced, on average, 50% more breaches than in the previous year.

As firms grapple with security breaches and incidents, and the associated losses, there is a growing trend being seen in the number of organizations looking to take out specific insurance to protect themselves since those losses are unlikely to be covered by the existing insurance policies. According to research published by insurance broker Marsh, demand for cyber insurance among its customers rose by a third during 2012 compared to a year earlier.

In response to such growing demand, the range of cyber insurance offered has been expanding. According to Airmic, the Association of Insurance and Risk Managers in Industry and Commerce, insurance coverage is now commonly available for first-party risk exposure, such as loss or damage to digital assets, business disruption, cyber extortion, reputational damage, and theft, as well as third-party risks such as investigation costs, customer notification costs and compensation paid to customers. According to research conducted in 2012 by RIMS, the Risk Management Society, 38% of respondents claim to have a cyber insurance policy. However, while it found that there were lots of figures concerning payouts for automotive, aviation, fiduciary, marine, malpractice, worker’s compensation and other types of insurance, there was little mentioned in the way of payouts for cyber insurance.

Although there are thousands of insurers offering more general policies, it is estimated that there are only about 40 or so firms offering specific cyber insurance. In common with many other emerging markets, it is also a brave new world, with policies varying widely in coverage and details on actual payouts scarce. Generally, such insurance is based on some common factors, such as the size of the company, the amount of data to be protected, past losses and previous claims, and the number of individuals granted privileged user access.

However, one further factor that insurers are basing insurance levels on is ‘standard of care’ requirements, which refers to the policies, procedures and safeguards that organizations need to have in place in order to qualify. Such requirements range from having a security plan in place and raising security awareness among employees, to specific technology safeguards, such as firewalls, access controls and real-time constant monitoring for vulnerabilities.

According to Marsh, insurance firms are showing much greater interest in the information security practices and procedures that their customers have in place as demand for cyber insurance grows. And there is the rub – organizations wishing to take out such insurance must be able to prove that they have the required standard of care requirements covered, which could mean opening up their systems to the scrutiny of the insurers, and therefore potentially providing them with access to confidential information contained within their systems.

It cautions that this could also oblige firms to invest in security controls that are way beyond the traditional demands of auditors, placing further pressure on financially strapped organizations that are looking to balance their budgets.

Read the rest here: http://www.infosecurity-magazine.com/view/34993/comment-beware-the-nascent-cyber-insurance-market/
The practicality of the Cyber Kill Chain approach

By Lysa Myers, CSO Online, October 4, 2013

If you're one of those folks who read a lot of InfoSec news, you've no doubt heard a lot of mention of the effectiveness of a Cyber Kill Chain approach to security. If you managed to miss the hubbub, you may be wondering if that's the latest sci-fi movie starring the usual muscle-bound action hero. In this article we'll talk about what a Cyber Kill Chain approach is, and whether it might be a good fit for your organization.

In military parlance, a "Kill Chain" is a phase-based model to describe the stages of an attack, which also helps inform ways to prevent such attacks. These stages are referred to as:

- Find
- Fix
- Track
- Target
- Engage
- Assess

Ideally, the further towards the beginning of the Kill Chain an attack can be stopped, the better. The less information an attacker has, for instance, the less likely someone else can use that information to complete the attack at a later date.

The Cyber Kill Chain is a similar idea, which was put forth by Lockheed Martin, where the phases of a targeted attack are described. And likewise, they can be used for protection of an organization's network. The stages are:

- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Installation
- Command & Control
- Actions

In essence, it's a lot like a stereotypical burglary — the thief will perform reconnaissance on a building before trying to infiltrate it, and then go through several more steps before actually making off with the loot. Using the Cyber Kill Chain to keep attackers from stealthily entering your network requires quite a bit of intelligence and visibility into what's happening in your network. You need to know when something is there that shouldn't be, so you can set the alarms to thwart the attack.

Another thing to keep in mind is the closer to the beginning of the chain you can stop an attack, the less costly and time-consuming the cleanup will be. If you don't stop the attack until it's already in your network, you'll have to fix those machines and do a whole lot of forensics work to find out what information they've made off with.

Lockheed Martin recently released details of its own success using a kill chain tactic to stop someone who had intruded on its network. It's not just something that applies to government contractors or giant corporations, though it does take quite a bit of work if you're not already set up to gather a whole lot of data about your digital resources.

Let's look at the various stages to determine what questions you should be asking yourself to decide whether it's feasible for your organization.

Reconnaissance: Viewing Your Network From the Outside

This is the stage where the criminals are trying to decide what are (and are not) good targets. From the outside, they try to find out what they can about your resources and your network to determine whether it is worth the effort. Ideally, they would like a target that is relatively unguarded and with valuable data. What information the criminals can find about your company, and how it might be used, could surprise you.

Companies often have more information available than they realize. Are names and contact details of your employees online? (Are you sure? Think social networks too, not just your own corporate website.) These could be used for social engineering purposes, say, for getting people to divulge usernames or passwords. Are there details about your web servers or physical locations online? These could be used for social engineering too, or to narrow down a list of possible exploits that would be useful to break into your environment.

This is a very tricky layer to try to control, particularly with the popularity of social networking, but it's also a fairly low-cost layer. Hiding sensitive information tends to be a fairly inexpensive change, though being thorough about finding the information can be time-intensive.

Weaponization, Delivery, Exploit, Installation: Attempting to Enter

These stages are where the criminals craft a tool to attack their chosen target, using the information they have gathered, and put it to malicious use. The more information they can use, the more compelling a social engineering attack can be. They could use spear-phishing to gain access to internal corporate resources with the information they found on your employee's LinkedIn page. Or they could put a remote access Trojan into a file that appears to be a realistic email from someone unexpected and with valuable data. What information the criminals can use to entice its recipient into running it. If they know what software your users or servers run, including OS version and type, they can increase the likelihood of being able to exploit and install something within your network.

Read the rest here:
Scam artists who deploy credit and debit card skimmers most often target ATMs, yet thieves can also use inexpensive, store-bought skimming devices to compromise modern-day cash registers. Just this past weekend, for instance, department store chain Nordstrom said it found a half-dozen of these skimmers affixed to registers at a store in Florida.

The fraud devices in this case resemble small keyloggers that are sold by dozens of stores for approximately $30 to $40 apiece. These hardware keyloggers are essentially PS/2 connectors that are about an inch in length. The tiny data storage devices are usually purple in color to match the color-coded standard for keyboards, and are made to be inserted between the male end of a PS/2 keyboard connector and the female receptor on a computer.

According to an alert circulated by the police department in Aventura, Florida, on the afternoon of Saturday, Oct. 5, 2013, three male subjects were captured on closed-circuit cameras at Nordstrom tampering with registers in the store. Authorities there say the footage showed two of the men worked to distract sales staff, while the third took pictures of the register and removed the rear access panel to the register and took additional photographs.

Several hours later, three different males returned to the store and performed the same routine: Two of them again distracted sales staff while the third male removed the back panel to the register and installed the above pictured device. The Aventura Police Department said Nordstrom located a total of six devices attached to their registers.

“The subjects then return at a later date to recover the devices and create fake credit cards for fraud,” the Aventura PD stated in a memo describing how the thieves would complete their scam. “The connector was made to match the connections on the back of the register to include color match. Therefore, no one would have detected it unless there was a problem with the register.”

The Aventura PD did not return calls seeking comment. Nordstrom spokeswoman Kara Darrow said the company believes the skimmer incident is limited to one store location. She said it’s not clear yet if any of the men caught on camera were arrested, or if they tried to return to the store to retrieve the devices.

Read the rest here:
http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/#more-23023

By Brian Krebs, Krebs on Security October 13, 2013

Cost of cyber crime increases 78 percent in four years

By Ian Barker, betanews, October 9, 2013

HP has released the results of a global study conducted with the Ponemon Institute indicating that the cost, frequency and time taken to resolve cyber attacks has risen for the fourth consecutive year.

The 2013 Cost of Cyber Crime Study found that the average annualized cost of cyber crime incurred by a benchmark sample of US organizations was $11.56 million, representing a 78 percent increase since the initial study was conducted four years ago and 26 percent up on the figure reported in 2012. The results also show that the time it takes to resolve a cyber attack has increased by nearly 130 percent during this same period, with the average cost incurred to resolve a single attack totaling more than $1 million.

The number of attacks have increased too with organizations experiencing an average of 122 successful attacks per week, up from 102 attacks per week in 2012. The average time to resolve a cyber attack was 32 days, with an average cost incurred during this period of $1,035,769, or $32,469 per day -- a 55 percent increase over last year's estimated average cost of $591,780 for a 24-day period.

“The threat landscape continues to evolve as cyber attacks grow in sophistication, frequency and financial impact,” says Frank Mong, vice president and general manager, Solutions, Enterprise Security Products, HP. "For the fourth consecutive year, we have seen the cost savings that intelligent security tools and governance practices can bring to organizations, and as HP, we are committed to continuing to deliver both industry-leading solutions and research to further disrupt the threat life cycle of the adversary”.

When it comes to the cost of attacks, the report reveals that the most costly cyber crimes are caused by denial-of-service, malicious-insider and web-based attacks, together accounting for more than 55 percent of all cyber crime costs per organization. Information loss accounts for 43 percent of total external costs, down 2 percent from 2012. Business disruption or lost productivity accounts for 36 percent of external costs, an increase of 18 percent over 2012. Recovery and detection account for 49 percent of internal costs.

Cybercrime cost varies by company size, but smaller organizations incur a significantly higher per-capita cost. Organizations in financial services, defense, and energy and utilities experience substantially higher cyber crime costs than those in other sectors.

Read the rest here:
Amid NSA Outrage, Big Tech Companies Plan to Track You Even More Aggressively

By Ryan Tate, Wired, October 11, 2013

Thanks to former NSA man Edward Snowden, we now know a fair amount about the NSA’s ability to collect data about what people do online, and it’s all rather disturbing.

But the future looks even more worrisome. Some of the biggest companies in tech are assembling new forms of online tracking that would follow users more aggressively than the open technologies used today. Just this week, word arrived that Microsoft is developing such a system, following, apparently, in the footsteps of Google.

The new data troves are to be used for advertising, not government surveillance, and only made available to authorized third parties. Yet the NSA has proven adept at co-opting large pools of data for its own ends.

“Users did not have much control in the cookie era,” says Marc Rotenberg, executive director of the Electronic Privacy Information Center, a nonprofit advocacy group in Washington. “But the problem is about to get much worse — tracking techniques will become more deeply embedded and a much smaller number of companies will control advertising data.”

Rotenberg says potential NSA use of the next-generation tracking data is all the more reason to move away from behavioral tracking. And he points out that there’s already evidence that ad data could have been used by government spies. NSA documents published by the Guardian earlier this month appear to postulate that cookies set by the pervasive Google-owned ad network DoubleClick could be used to spot internet users who also use the Tor anonymity system.

The NSA Tor attack could only work on people who made mistakes using what is otherwise a strong system. But yesterday, Ad Age reported that Microsoft is developing a system that has intimate tracking at its core, following people as they hop from the web to apps and from PCs to tablets to phones to videogame consoles. By shoving aside cookies for an unspecified new identification technology built into devices at a lower level, Microsoft and its authorized partners would gain detailed tracking ability — though the report also says that the system could lock out non-authorized parties, who are harder to exclude from the data flow in cookie-based tracking.

That may sound like a good thing, but keep in mind that Snowden’s documents indicate that the NSA has previously helped itself to big company data, with authorization or without.

Read the rest here:
http://www.wired.com/business/2013/10/private-tracking-arms-race/

Cybersecurity Career Doesn't Interest Most Young People

By Raytheon Company, October 24, 2013

While U.S. government officials find the current pipeline for cybersecurity talent to be lacking, 82 percent of U.S. millennials say no high school teacher or guidance counselor ever mentioned to them the idea of a career in cybersecurity, according to a new survey commissioned by Raytheon and conducted by Zogby Analytics. The survey also found less than one-quarter of young adults aged 18 to 26 believed the career is interesting at all.

Young men (35 percent) are far more interested than young women (14 percent) in a career in cybersecurity, according to the survey, which was released as the U.S. marks the 10th anniversary of National Cyber Security Awareness Month, sponsored by the Department of Homeland Security and the National Cyber Security Alliance.

The survey found many young adults raised on social networking trust technology and are not overly concerned about the threat of online identity theft or of their personal data being stolen. Seventy-five percent of survey respondents said they were confident their friends would only post information about them on the Internet that they are comfortable with and 26 percent said they had never changed their mobile banking password.

The Facebook Generation, sometimes referred to as "Generation F," includes millennials who have grown up using social networking tools such as Twitter, Facebook, LinkedIn and Pinterest. The Raytheon Millennial Cybersecurity Survey found that despite their risky online behavior, many millennials are becoming aware of Internet risks and are taking steps to protect themselves. Eighty-two percent of millennials password-protect their laptop or desktop computer, the survey found, while 61 percent password-protect their mobile phone. Thirty-seven percent of millennials said they had backed up the data on their laptop or desktop in the last month.

Key survey findings include:

Read the rest here:


**October 8, V3.co.uk** – (International) **Microsoft awards UK security researcher $100,000 bounty for finding major flaw.** A researcher at Context Information Security was awarded a bug bounty by Microsoft for uncovering a new type of mitigation bypass technique that could have represented a major vulnerability. Source: [http://www.v3.co.uk/v3-uk/news/2299402/microsoft-awards-uk-security-researcher-usd100-000-bounty-for-finding-major-flaw](http://www.v3.co.uk/v3-uk/news/2299402/microsoft-awards-uk-security-researcher-usd100-000-bounty-for-finding-major-flaw)

**October 16, CNET** – (International) **Microsoft-DS no longer hackers’ top target.** Akamai stated in their “State of the Internet” report that Microsoft-DS, also known as Port 445, was no longer the primary path of attack for attackers, for the first time since Akamai began gathering data on attack vectors in 2008. Cybercriminals have instead changed to targeting users through HTTP Port 80 and SSL Port 443. Source: [http://news.cnet.com/8301-1009_3-57607722-83/microsoft-ds-no-longer-hackers-top-target/](http://news.cnet.com/8301-1009_3-57607722-83/microsoft-ds-no-longer-hackers-top-target/)

**October 22, CNET News** – (National) **Aaron’s computer rental chain settles FTC spying charges.** Rent-to-own computer chain Aaron’s agreed to settle Federal Trade Commission charges that the company installed spyware on customers’ computers that took photos and used keyloggers to steal login credentials. Under the agreement, the company is prohibited from using monitoring programs and must obtain customer consent to use location-tracking software on its rental computers. Source: [http://news.cnet.com/8301-1009_3-57608838-83/aarons-computer-rental-chain-settles-ftc-spying-charges/](http://news.cnet.com/8301-1009_3-57608838-83/aarons-computer-rental-chain-settles-ftc-spying-charges/)

**October 24, Help Net Security** – (International) **Attackers use smaller botnets to launch high-bandwidth attacks.** Prolexic’s third quarter 2013 report on distributed denial of service (DDoS) attacks found that attackers have often shifted to using smaller botnets for distributed reflection denial of service (DrDoS) attacks that allow attackers to obfuscate the source of the attack and to use the bandwidth of intermediary victims, among other findings. Source: [http://www.net-security.org/secworld.php?id=15812](http://www.net-security.org/secworld.php?id=15812)

**October 25, Softpedia** – (International) **7 fugitives charged in the U.S. for role in multimillion dollar cyber fraud scheme.** The U.S. Department of Justice charged six Romanians and one Albanian for allegedly running a multimillion dollar online fraud operation where they used forged documents to open U.S. bank accounts, post fictitious ads, and then instructed buyers to transfer payment for nonexistent vehicles using fraudulent invoices. All of the accused are currently fugitives, and the FBI and Interpol issued notices to facilitate their arrests. Source: [http://news.softpedia.com/news/7-Fugitives-Charged-in-the-US-for-Role-in-Multimillion-Dollar-Cyber-Fraud-Scheme-394331.shtml](http://news.softpedia.com/news/7-Fugitives-Charged-in-the-US-for-Role-in-Multimillion-Dollar-Cyber-Fraud-Scheme-394331.shtml)
Challenges of Cloud Forensics in Litigation

By Stephanie Koons, Pennsylvania State Univ., October 28, 2013

Cloud computing — an emerging model that enables convenient, on-demand access to computing resources, applications, storage, and services — has become increasingly widespread in recent years. According to John Bagby, a professor at Penn State’s College of Information Sciences and Technology (IST), while the cloud offers information technology (IT) savings and offers numerous advantages to organizations and individuals, the increasing adoption of cloud services imposes vast new challenges to criminal law enforcement, regulatory enforcement and civil litigation.

“The cloud presents a durable and seemingly irreconcilable conundrum for many constituencies, including the digital forensics communities,” Bagby says.

Bagby’s paper, “On Resolving the Cloud Forensics Conundrum,” was presented in June at the Conference on Digital Forensics Security & Law in Richmond, Va. The article, Bagby wrote, “explores how law and economics, regulation and other public policy forces are likely to coalesce as the challenges of cloud security and forensics emerge in the near to medium term.”

Cloud forensics, Bagby says, is a cross discipline of cloud computing and digital forensics. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a legal or regulatory forum. Cloud forensics is a subset of network forensics, which deals with forensic investigations of networks. Cloud computing is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet.

“Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing environments,” Bagby wrote in the article.

For Bagby, who joined the College of IST after 18 years with Penn State’s Smeal College of Business Administration, where he was a professor of business law, his interests in cyberforensics started in the mid-1970s when he was a clerk for a national oil company and with a Wall Street law firm. In those days, he said, nearly all records were on paper and stored in file cabinets. Currently, more than 90 percent of all archived documents are electronic. The period between 1995 and 2003 was a “transition era in litigation,” as litigators moved from paper-based searching and making photocopies to provide to the opposing side to exchanging thumb drives to access cloud repositories of discovery data.

“Starting around ’02 or ’03, this revolution really came home to a lot of people, particularly to those working in litigation,” Bagby says.

Bagby, who has an master of business administration degree from the Univ. of Kansas and a juris doctorate from the Univ. of Tulsa, has compiled a substantial body of research in the area of cloud forensics. He has given 10 presentations and has completed 10 to 15 publications on the topic. He co-authored a chapter, “United States of America,” for an edition of Butterworth’s Electronic Evidence, a British comparative law treatise, which came out in January. Bagby also published “International Aspects of Migrating Digital Forensics in the Cloud,” co-authored with Joseph Schwerha in Volume 10 of the Digital Evidence and Electronic Signature Law Review.

According to Bagby, many individuals and institutions tout the numerous transformative benefits of the cloud, including economies of scale, reliability, scalability, ubiquitous accessibility and collaboration enablement. Many of the cloud’s advantages, Bagby says, directly translate into the forensics realm. The cloud can be used to lower costs and enhance effectiveness of the marshaling activities in collecting electronically stored information (ESI) for review, analysis and use as forensic quality evidence. The cloud could enable crowd sourcing of investigatory data, thereby vastly lowering costs of dispute resolution. For example, he says, cloud-based litigation war rooms — document depositories using electronic media — may reduce electronic discovery costs substantially.

Despite the numerous ways in which the cloud can aid the legal process, Bagby says, the current architecture of many cloud services arguably undermines justice. Two major factors contribute to the unreliability of the cloud as an evidentiary preservation medium: unstable system states and unstable cloud system architectures.

“By nature, the cloud is in an unstable environment,” Bagby wrote in the article. “Such instability is generally inconsistent with evidentiary safeguards.”

Read the rest here:
By Webster University and 21st Space Wing Public Affairs, October 22, 2013

With the assistance of the Peterson Force Development Flight, specifically Susan Wilson and Blaine Hales, Webster University has been approved to offer a new Master of Science degree in Cybersecurity. This program is targeted to meet the needs of all service members seeking continued professional career development in cybersecurity, or those cybersecurity careers.

The 39 graduate credit-hour program was designed to meet the increasing demand for cybersecurity education. Classes will meet from 5:30-9:30 p.m. one night per week, for nine weeks each term. There are five terms a year and most students who can take two classes a term could complete their degree in approximately 20 months. Webster does not require a graduate management admission test, and students with an undergraduate degree from an accredited institution can apply for admission.

“The growing global cyber threat requires individuals supporting sensitive space, communications and information fields to be aware of Cybersecurity threats and have the skills to implement appropriate methods of protection, including public and private cooperation, and an in-depth understanding of U.S. and International Cyber Law,” said Thomas Johnson, associate vice president at Webster.

“This program meets the Cybersecurity needs of local Army and Air Force officers and enlisted seeking individualized professional development to enhance their career advancement and future civilian career opportunities,” said Margaret Reed, senior site director for Webster University in Colorado Springs.

Information sessions will be held at the Webster Metro Campus, 5475 Tech Center Dr., Suite 110, every hour from 11 a.m. until 6 p.m. Oct. 31; call the metro campus to reserve a time slot.

Detailed information about this cybersecurity professional development program is available by calling Webster University at 590-7340 (metro campus) or 574-7562 (Peterson campus).

The Cybersecurity courses will initially be offered at the Webster metro campus beginning this spring, and will be offered at the Peterson campus as soon as a facility is available.

Webster University is an American non-profit private university with its main campus in Webster Groves, Missouri, United States. Webster University is accredited by The Higher Learning Commission and is a member of the North Central Association of Colleges and Schools. Webster University is ranked 21st among regional universities (Midwest), according to college and university rankings in US News (http://colleges.usnews.rankingsandreviews.com/best-colleges/webster-university-2521).
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: doncreamér-issa@q.com
Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Capella University - CISSP towards Degree

If you are considering completing your Bachelors or Masters degree and would like to learn how your CISSP, other certifications and your professional experiences could result in college credit, let me know.

If you possess a valid professional certification – including CISM, CISA, CISSP, PMP, and many others – you may be able to earn credits that count towards the completion of your Bachelors or Masters Degree.

Click on the links below to find your certifications and see how much time and money you can save:

http://www.capella.edu/partners/7133_BS_IT_PLA.pdf
http://www.capella.edu/online-degrees/bachelors-information-assurance-security/
http://www.capella.edu/partners/7093_MS_ISTM_PLA.pdf
http://www.capella.edu/online-degrees/masters-information-assurance-security/

Capella is one of the select four-year colleges and graduate-level universities designated as a National Center of Academic Excellence in Information Assurance Education (CAEIAE) by the National Security Agency and the U.S. Department of Homeland Security.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, (719) 630-8121</td>
</tr>
<tr>
<td>Dec 6</td>
<td>11:00 to 1:00</td>
<td><strong>Carrabba's North</strong>&lt;br&gt;7120 Campus Dr. Colorado Springs, (719) 264-0401</td>
</tr>
</tbody>
</table>
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.

The World’s First Computer Programmer Was a Victorian Mother-of-Three

By Gerald Lynch, Gizmodo UK, October 15, 2013

Does the name Ada Lovelace ring any bells? No? Seeing as you’re reading this on a computer, tablet or smartphone, it should. The Victorian mother-of-three, born 1815, was the world’s first ever computer programmer.

A close friend of Charles Babbage, inventor of the Difference Engine (considered the first ever computer), Lovelace was tasked with translating notes from Italian mathematician Luigi Menabrea on Babbage’s second mathematical machine, the Analytical Engine. Lovelace went one better, using her own formidable mathematical knowledge to expand upon Menabrea’s notes, leading to her describing an algorithm that could compute a recognised series of numbers, effectively the first act of computer programming.

Read the rest here: http://gizmodo.com/the-world-s-first-computer-programmer-was-a-victorian-m-1445503663