ISSA
Information Systems Security Association
Colorado Springs Chapter
WWW.ISSA-COS.ORG

ISSA-COS NEWSLETTER
VOLUME 9 NUMBER 2
FEBUARY 2020

Colorado Springs, Colorado

A Busy Month!

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

Welcome to February! Having closed the door on the month of January, we can already measure success for our chapter in several areas. It is fair to say we are off to a great start, and we will have many wonderful events to look forward to this year. We have a full complement of principal board members, new event gear prestaged at all our primary venues, and a revised ISSA-COS Catalog of Events outlining all off our regularly scheduled events along with the who, what, where, when, why, and how for actually producing our events – a well-documented guide designed to assist any volunteer. We also invested in new indoor and outdoor signage for all our venues to reduce confusion and guide attendees away from areas off limits to our events. Last of all, we published a new 2020 Chapter Brochure which will prove beneficial to our internal chapter members and external non-members. What a busy first month we have had!!

In terms of our January meetings, new this year, we elevated our Saturday Mini Seminars to the same level as our dinner and lunch meetings. This means, we will now provide a short presentation of chapter business for those members who are unable to attend either the dinner or lunch meetings. This way, no one misses out on important information. Also new this year, is the hosting of the Mini Seminars at Pikes Peak Community College – Rampart Range. This facility is a perfect venue, well suited for our needs. It accommodates all our basic requirements and includes extra services such as an integrated A/V system, a bank of training laptops pre-loaded with Kali Linux, and a coffee bar whereby, ISSA-COS will be serving FREE coffee to ALL attendees. Yes, being new to this venue, we do have some kinks to work out but, once we do, we will be soaring!

During all our chapter meetings in held in January, we profiled two important messages and we were revisited by a past favorite. First, we profiled the President's Annual Address in which I briefed attendees on the State of Cybersecurity as it affects our nation, state, city, and chapter. I also discussed some of our new community programs and strategic partnerships which launched in January. Programs such as our support for the upcoming Women in Cybersecurity conference March 12-16, and our

(Continued on page 4)

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters .

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.

Neo-Nazi Swatting Ring’s Alleged ‘Cybersecurity’ Guru Arrested Thanks to… Terrible Cybersecurity

By Kelly Weill, Daily Beast, January 15, 2020

He called himself the “BotGod.” But the cybersecurity student was so bad at, well, cybersecurity, that he allegedly exposed a neo-Nazi swatting ring that counted him as a member.

John William Kirby Kelley, 19, is accused of leading a notorious troll team loosely affiliated with the neo-Nazi group Atomwaffen Division. Through 2018, Kelley’s online chat group allegedly compiled personal information and led swatting attacks (hoaxes in which trolls try to trick an armed police force into showing up at an innocent person’s house) against politicians, businesses, journalists, and historically black churches.

Kelley and his circle, who convened on a series of online chat rooms, “all appeared to share racist views, with particular disdain for African Americans and Jewish people,” according to a probable-cause statement from an FBI agent involved in his arrest last week.

Although Kelley was majoring in cybersecurity and allegedly acted as the group’s tech support, he left a wide internet trail that could send him and alleged associates to prison. The case suggested that even as far-right groups have shown a disturbing ability to organize online, hangers-on may be just as likely to invite the feds to their doorstep. Kelley’s lawyers declined to comment for this story.

> *“It was an infosec error he’d inadvertently predicted when he got into ODU in early 2018.”*

A violent extremist group, Atomwaffen members have been suspects in at least five killings since 2017. Although the group has a real-world paramilitary presence, it also has a larger and more nebulous online footprint. Multiple men affiliated with the group’s online outposts and spinoff groups have recently been arrested, including one who allegedly planned a violent attack on Jewish sites in Las Vegas.

Kelley, who was arrested on Jan. 10, was allegedly fueled by the same prejudices. Feds say his phone contained pictures of him with Atomwaffen recruiting materials. Meanwhile, he and his online circle allegedly livestreamed swatting campaigns, and even ran a publicly viewable list of future targets’ addresses, earning them notoriety online.

But the group’s apparent quest for infamy left them exposed—especially when Kelley allegedly tried calling in a bomb threat to his own school, Old Dominion University (ODU) in Norfolk, Virginia.

In November 2018, Kelley allegedly posted in a chat room asking the group to swat his college. “norfolk next,” he wrote, according to chat logs included in the probable-cause statement. “I dont want to goto class on wed.”

Later that month, ODU received a phone call from a blocked number. The person on the other end of the line claimed to have an AR-15 rifle, and said he’d placed bombs in campus buildings, according to the FBI. But three hours later, the person called back and apologized for making what he described as an accidental call. This time, the person forgot to block the number. The caller in question was Kelley, the feds have alleged. And not only did Kelley call from his own phone number, but he’d previously listed it as his contact with ODU, they said. When campus police looked up the number, they found it in Kelley’s school records.

With Kelley’s name associated with the crank calls, police started looking into a spate of other bomb threats across the U.S. and Canada, from California to Quebec. They soon found him associated with email addresses and Google Voice numbers that they said had been used in other swatting attempts.

Despite studying cybersecurity and allegedly acting as tech support for the neo-Nazi-affiliated group when it struggled to livestream, Kelley wasn’t exactly difficult to find online. Although he went by “carl” in the alleged swatting group, he reused the moniker across other social media, where he shared links to the chat rooms he is said to have administered. A Twitter account, identified as Kelley’s by the Anti-Defamation League’s Center on Extremism, contained a link to group on the Nazi-beloved chat platform Discord, where a user named “carl” listed himself as “BotGod.” (The FBI also listed “BotGod” as one of Kelley’s aliases.)

Read the rest here:

https://www.thedailybeast.com/neo-nazi-swatting-rings-alleged-cybersecurity-guru-arrested-thanks-to-terrible-

Membership Corner

Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on the “Manage Profile” link under My Profile on the right top of the page. Once there you will see the “Edit Bio” link where you can make your updates. Thank you for your support.

New Members January
Rodney Gullatte Jr.
Julia Johnson
Kelli Blanchard
Michael McFadden
Cameron Landreth
Rachel Green
Michael Quinlan
Eric Crump
Scott Walker
Casey McClure
Nick Williams
Heather Lawrence
Deon Ware
Justin Holmstrom

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

Our membership is at ~400 members as of the end of January!

Please watch the Newsletter, communications and eVites to ensure you stay aware of what’s going on in the chapter. As always, if you have any membership questions don’t hesitate to contact me.

Thanks,

Steven Mulig

Membership Committee Chairman

membership@issa-cos.org

Top Conflicts to Watch in 2020: A Cyberattack on U.S. Critical Infrastructure

By Robert K. Knack, Council on Foreign Relations, January 17, 2020

In this year’s Preventive Priorities Survey, a cyberattack on U.S. critical infrastructure was ranked as the number one threat. Given heightened tensions with Iran following the death of Qasem Soleimani, ongoing Russian election interference, and the ever-present prospect that tensions with China could boil over, the likelihood of a significant cyberattack on the United States in the next year is high.

Whether the target will be the electoral system or the electrical system will depend on which actor is carrying out the attack and for what reason. The most recent Worldwide Threat Assessment [PDF] concluded that Iran has the capability to conduct disruptive attacks against corporate networks, China could disrupt natural gas pipelines, and Russia could do the same for the electric grid. All three countries—and North Korea—have already begun operations to influence the 2020 election.

While Russia was not explicitly identified as the leading source of concern, the U.S. intelligence community has unequivocally stated that Russia used cyber means to influence the outcome of the 2016 presidential election. Russia has now twice tested its capability to use cyber means to shut down the power grid in Ukraine. These outages, which were of limited duration and scope, were likely trial runs for a larger attack against an adversary, such as the United States, with which it does not enjoy the same overwhelming conventional dominance as it does against Ukraine.

Read the rest here:

https://www.cfr.org/blog/top-conflicts-watch-2020-cyberattack-us-critical-infrastructure

A Note From Our President

(Continued from page 1)

development of a Cyber Badge Camp for a local Girl Scout troop. Following my remarks, we then welcomed the National Cyber Exchange (NCX) as they educated us on the details and offerings associated with the NCX/ISSA-COS CyberAlliance+ agreement. This agreement was many months in the making, and one our Board of Directors (BoD) are quite proud of securing. Last of all, we welcomed Justin Whitehead back to our Mini Seminars. Justin launch a new four-part series of hands-on Do-It-Yourself (DIY) training sessions. He was well received by all the attendees, and we are happy to have him back.

As we look forward to February, our guest speak for our dinner and lunch meeting will be Mr. William (Bill) Vivian, Cybersecurity Leadership Coach. In January, Bill provided our BoD with a private training session to help start our new year right. He was so well received, we eagerly invited him to return to address our whole general membership. I'm sure everyone will enjoy his upcoming message and will walk away better prepared to tackle the next stage of their careers.

As you read this, our chapter will be packing up from another successful year attending the AFCEA-RMC Cyberspace Symposium. Each year, AFCEA-RMC donates a FREE booth to our chapter. It is an honor to receive this gift, and it pays huge dividends towards helping our chapter gain sponsors to support our own calendar of events. Thank you AFCEA!!

Last of all, in February we will turn the spotlight towards educating our members on programs offered by ISSA International. These programs include the "ISSA Fellows Program" and the "ISSA Awards Program." Both programs are profiled on pages 8 and 9 of this month's newsletter. Please review them before the upcoming chapter meetings and be prepared to answer and ask questions.

In closing, I encourage all of you to respond to some upcoming volunteer opportunities. Soon, we will release signups to support the Women in Cybersecurity conference and the Girl Scouts Cyber Badge Camp. We hope to have strong representation from our chapter at each event and we need you to make that happen. As always, on behalf or our BoD, we thank you for your continued support, membership referrals (keep 'em coming!), and active participation. With out the combined efforts of all our general members, we would not have become such a strong anchor of Cybersecurity in our community.

Sincerely,

Ernest

Hackers Brought Down A U.S. F-15, Is Americas Air Force At Risk?

By David Axe, National Interest, January 28, 2020

A team of hackers in early August 2019 gained access to an F-15 fighter in an eye-opening U.S. military test. The successful hack underscores U.S. forces' vulnerability to electronic intrusion.

"It was the first time outside researchers were allowed physical access to the critical F-15 system to search for weaknesses," reporter Joseph Marks wrote for *The Washington Post*.

From the article:

And after two long days, the seven hackers found a mother lode of vulnerabilities that — if exploited in real life — could have completely shut down the Trusted Aircraft Information Download Station, which collects reams of data from video cameras and sensors while the jet is in flight.

They even found bugs that the Air Force had tried but failed to fix after the same group of hackers performed similar tests in November [2018] without actually touching the device. …

The hackers lobbed a variety of attacks — including injecting the system with malware and even going at it with pliers and screwdrivers. When I saw it, the metal box that's usually secure on the aircraft had wires hanging out the front.

Read the rest here:

https://nationalinterest.org/blog/buzz/hackers-brought-down-us-f-15-americas-air-force-risk-117801

Read the Washington Post article here:

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/08/14/the-cybersecurity-202-hackers-just-found-serious-vulnerabilities-in-a-u-s-military-fighter-jet/5d53111988e0fa79e5481f68/?noredirect=on

Final DOD Cybersecurity Certification Model Due Friday

By Mariam Baksh, NextGov, January 28, 2020

The Defense Department official leading the development of an ambitious plan to independently certify military contractors' cybersecurity practices will review a final version of the plan Friday and shared key details for its implementation.

Stipulations of the Cybersecurity Maturity Model Certification will be written into the Defense Federal Acquisition Regulation Supplement as an update to rule 252.204.7012, which currently requires contractors handling information of certain sensitivity to implement security practices spelled out in National Institute of Standards and Technology Special Publication 800-171 and to report cyber incidents within 72 hours.

The major change in the updated rule—which is expected to be open for comment in the spring—will be that contractors will no longer be permitted to self-attest their adherence to the NIST-described practices, as they are now.

The new program will also introduce five levels of tiered requirements for defense contractors. Contractors dealing with information that is not as sensitive would have to meet the "basic cyber hygiene" of level 1, versus the "good cyber hygiene" that implies compliance with the NIST 800-171 controls, or the "advanced" practices that would be required at level 5.

That risk-based approach has gotten the coming CMMC some praise, but the contracting community is on high alert with concerns ranging from the cost of certification to the details of how the audits will function through a nonprofit accreditation body.

Katie Arrington, chief information security officer for the Office of the Assistant Secretary of Defense for Acquisition, answered stakeholders' many questions during an event hosted by the law firm Holland & Knight today, and delivered some tough love for naysayers.

"For those of you who are attesting that you're doing the 171, and you say it's too high of a barrier to get compliant to level 3, I ask why," Arrington said. "If you're already attesting on your contracts that you're doing it, and I'm just saying I need you to prove that you're doing it, and you're telling me that's too much of a burden to bear, I struggle with that."

Details of the cybersecurity practices—in addition to the NIST controls they include practices outlined by other bodies such as the International Organization for Standardization—required for each level are described in draft 0.7 of the model.

Arrington said version 1.0, the final version to be rolled into regulation, will be delivered to her Friday Morning, and hinted it may be the subject of a Pentagon press conference that day. Arrington stressed the intent is to have the model be updated at least every year, as "electronic warfare is not static."

"When the model releases this week or next, it will have user guides," Arrington said, noting it will then be turned over to the accreditation body along with a memorandum of understanding spelling out how the new certification process will work with existing requirements.

"When we hand them the MOU, there will be caveats in it that say we need you to work through your assessors to create reciprocity for government work already done," she said. "So if your company has been through a [Defense Industrial Base Cybersecurity Assessment Center] audit, there's going to be reciprocity for that. If you have paid—your company—for an ISO 27001, we will give you credit for those controls that were made."

Arrington said language for that specification will also be included in the updated rule.

The accreditation body will require a "crown jewel" database, which the government is building. Arrington said she herself wrote the "pretty stringent" requirements for the database into a request for information from commercial vendors.

She said the RFI will be released at the end of this week or next, and that the database will be cloud-based and that the CMMC will be "portaled into your [System for Award Management] ID."

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/01/final-dod-cybersecurity-certification-model-due-friday/162713/

NCX | ISSA-COS CyberAlliance+

Contact:

Darla Lindt, CyRM, Executive Director
National Cyber Exchange
darla.lindt@nationalcyber.org
(719) 660-6427

Ernest Campos, President
ISSA-COS
president@issa-cos.org
(703) 850-7157

Mike Schmidt, Managing Director
mike.schmidt@nationalcyber.org
(719) 247-3468

FOR IMMEDIATE RELEASE

National Cyber Exchange and ISSA-COS Chapter

Announce CyberAlliance+ Partnership

COLORADO SPRINGS – January 20, 2020 – National Cyber Exchange (NCX) and Information Systems Security Association Colorado Springs (ISSA-COS) Chapter announce a CyberAlliance+ Partnership to benefit members. With growing cybersecurity threats to our nation that target citizens, businesses and institutions of government, the alliance between NCX and ISSA-COS holds the promise of developing a new type of local, regional and national collaboration. This alliance will enable the sharing of membership resources, education, awareness and cyber threat sharing not only to benefit the ISSA-COS professionals, but C-Suite executives, small businesses and individuals.

"ISSA-COS is thrilled to partner with NCX. The services and support we offer one another will mutually strengthen our organizations for years to come. More importantly, the sharing of collateral information between our organizations will significantly increase the value and benefits for our members. Together, we will become stronger than we would otherwise be apart," explains Ernest Campos, President ISSA-COS.

"Two are better than one ...this principle rings true in this alliance with NCX and ISSA-COS. We have many hopes for the year ahead as these two great organizations collaborate to provide resources, threat sharing and solutions to the ever-increasing cybersecurity threat," states Darla Lindt, CyRM (Cyber Risk Manager) and Executive Director of NCX and lead cyber risk/ insurance professional.

ISSA-COS supports approximately 500 active members and meets monthly with presentations and information of interest to security professionals throughout the Pikes Peak region. In addition to monthly meetings and mini seminars, the chapter hosts two major annual conferences in Colorado Springs – the Cyber Focus Day (CFD) Symposium and the Peak Cyber Symposium. ISSA COS also offers CompTIA Security+ exam prep sessions and an (ISC2) (CISSP) exam prep session each year for IT industry professionals.

With active participation from individuals and chapters all over the world, ISSA is the largest international, not-for-profit association specifically for security professionals. 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. There are currently over 179 chapters in more than 79 countries around the world with more than 10,000 total members. For more information, visit www.issa-cos.org.

The National Cyber Exchange is a nonprofit member organization based in Colorado Springs, Colorado. NCX is dedicated to improving cybersecurity by sharing cyber threat information, providing cyber education to citizens, increasing awareness, engaging in secure network and cyber best practices for businesses and executives, supporting member training, and protecting critical infrastructure and IT operational needs through advanced technology development. NCX participates in the Cyber Information Sharing and Collaboration Program (CISCP) with the Department of Homeland Security (DHS) and acts as an Information Sharing and Analysis Organization (ISAO). The organization offers a suite of cybersecurity membership programs for the CyberCitizen, CyberExecutive and CyberISPro. In addition, NCX provides the first ever cybersecurity alert notifications for

(Continued on page 7)

(Continued from page 6)

iPhone and Android devices via the NCX mobile app.

The roots of NCX were originally established in 2011 as the Western Cyber Exchange (WCX), offering various levels of information sharing, training, cyber exercises and technology development. WCX established the first Cyber Analysis Center in 2012 using MITRE Corporation's Collaborative Research into Threats (CRITs) program. WCX also announced the first successful exchange of a cyber threat data report with the Advanced Cyber Security Center (ACSC) in Boston in August 2014. In 2015 WCX and the DHS established a Cooperative Research and Development Agreement (CRADA) with the Office of Cybersecurity and Communications. In October 2016 WCX announced its name change to the National Cyber Exchange to better support members nationwide. For more information, visit www.nationalcyber.org.

ISSA-COS and the Girl Scouts

Our Chapter has been asked by some local Girl Scout troops to help with the Cyber Badges. Similar to the Merit Badges of the Boy Scouts, the Girl Scout badges are acquired through studying, learning, and doing to demonstrate mastery in some area. The Board unanimously approved the request and several Board members took on roles to make this effort a success. Anna Parrish is working with the leaders to produce materials, along with Phebe Swope (Deputy VP of Training), and interns from PPCC.

The materials will be suitable for each of the six levels of Girl Scouting: Daisies (Grades K–1), Brownies (Grades 2–3), Juniors (Grades 4–5), Cadettes (Grades 6–8), Seniors (Grades 9–10), and Ambassadors (Grades 11–12). Each level will cover things like technology, self protection, and social impacts. This represents a significant amount of material, and we hope that our members will help keep it up-to-date as time goes by.

The current effort is considered a pilot project and will support just a few of the troops in Colorado Springs. If the local Girl Scout leadership considers it a success, we will consider working to make it a much larger program.

As a side note, the Girl Scout leaders originally approached the city's Economic Development Council for advise on who could help them. Because of our chapter's reputation and activity, the EDC immediately referred the leaders to us. I hope you are all feeling proud!

Mark Heinrich

VP Training

ISSA Fellow Program

2020 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the Fellow Program, once the 2020 award criteria is made available please contact Colleen Murphy at past-president@issa-cos.org to help you through the steps. Below are some details on the ISSA Fellow Program. Qualification information is also presented below:

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

Nominations and applications are accepted on an annual cycle. Applications will be accepted in the near future, and details will be provided in a future newsletter. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2020 ISSA International Conference.

To Become a Senior Member

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

Senior Member Qualifications

- 5 years of ISSA membership
- 10 years relevant professional experience
- For your convenience, we will have available the Senior Member Application Check-list to confirm eligibility and completion of application

All Senior Member applications require an endorsement from their home chapter to qualify.

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow.

Fellow Qualifications

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

All Fellow applications require a nomination to qualify.

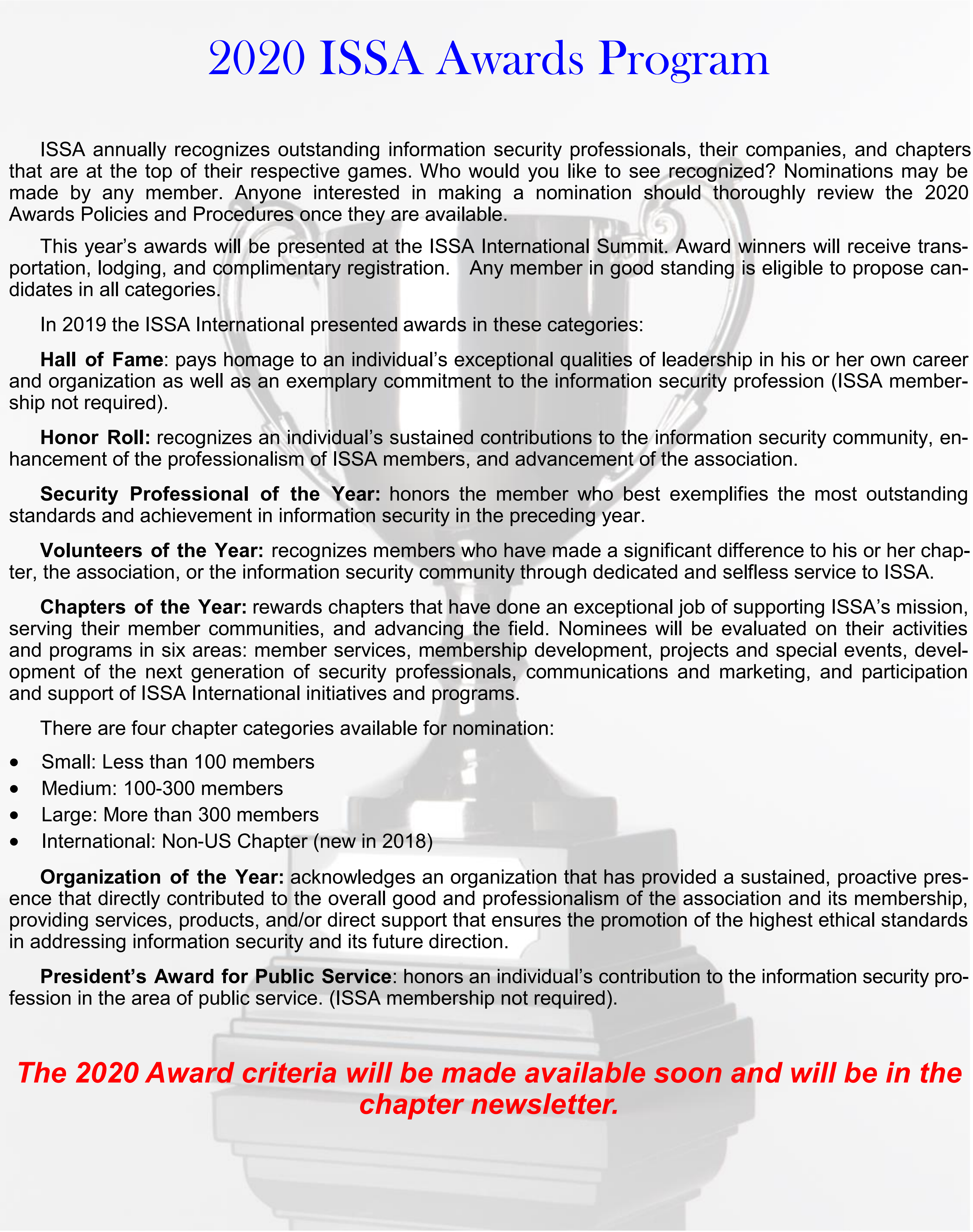
Distinguished Fellow Qualifications

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

All Distinguished Fellow applications require a nomination to qualify.

Additional details will follow as they become available.

2020 ISSA Awards Program



ISSA annually recognizes outstanding information security professionals, their companies, and chapters that are at the top of their respective games. Who would you like to see recognized? Nominations may be made by any member. Anyone interested in making a nomination should thoroughly review the 2020 Awards Policies and Procedures once they are available.

This year's awards will be presented at the ISSA International Summit. Award winners will receive transportation, lodging, and complimentary registration. Any member in good standing is eligible to propose candidates in all categories.

In 2019 the ISSA International presented awards in these categories:

Hall of Fame: pays homage to an individual's exceptional qualities of leadership in his or her own career and organization as well as an exemplary commitment to the information security profession (ISSA membership not required).

Honor Roll: recognizes an individual's sustained contributions to the information security community, enhancement of the professionalism of ISSA members, and advancement of the association.

Security Professional of the Year: honors the member who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

Volunteers of the Year: recognizes members who have made a significant difference to his or her chapter, the association, or the information security community through dedicated and selfless service to ISSA.

Chapters of the Year: rewards chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities, and advancing the field. Nominees will be evaluated on their activities and programs in six areas: member services, membership development, projects and special events, development of the next generation of security professionals, communications and marketing, and participation and support of ISSA International initiatives and programs.

There are four chapter categories available for nomination:

- Small: Less than 100 members
- Medium: 100-300 members
- Large: More than 300 members
- International: Non-US Chapter (new in 2018)

Organization of the Year: acknowledges an organization that has provided a sustained, proactive presence that directly contributed to the overall good and professionalism of the association and its membership, providing services, products, and/or direct support that ensures the promotion of the highest ethical standards in addressing information security and its future direction.

President's Award for Public Service: honors an individual's contribution to the information security profession in the area of public service. (ISSA membership not required).

The 2020 Award criteria will be made available soon and will be in the chapter newsletter.

The hack back bill legitimizes a messy game of revenge for businesses

By Betsy Atkins, Quartz, January 15, 2020

Often, when new regulations are introduced in an industry, they can bear unintended consequences for the future.

Since this past summer, legislatures have been contemplating a law relating to cyber defense called the Active Cyber Defense Certainty Act, or ACDC. The bill is intended to limit the negative consequences for parties that engage in computer fraud and abuse when responding to or defending themselves against cyber intrusions.

It may seem like a straight-forward act of protection at first appearance, but the bill has evoked a lot of big questions as it's worked its way through the government—especially from the business vantage point.

Cyber cons/cyber pros

And with good reason. If or when the act becomes law, one concern is that boards and executives will be asked to make decisions on "hacking back"—meaning using a protocol of active cyber defense—when they really are not in the best position to do so.

Given the way cyber attacks operate, i.e. off-grid in the unregulated dark web, any counter action, even by a government entity, runs the risk of being founded on incomplete and/or misleading information in the first place.

These decisions could potentially have disastrous consequences not just for companies, but for the global economy as a whole.

Proponents of the ACDC bill argue that defenders would benefit from tools and rights, as long as they observe a version of the following protocol:

1. Establish attribution of an attack.
2. Disrupt the cyberattack without damaging another party's computers or other property.
3. Retrieve and destroy stolen or compromised files.
4. Monitor the behavior of an attacker.
5. Utilize beaconing technology

The justification we've heard most loudly from legislatures is that a very small number of cybercrimes are prosecuted, leaving criminals to face no consequences for their illegal behavior. And that hacking back guidelines, listed above, can provide that deterrence.

Mal-attribution

For the most part hacking back leads to a slew of unintended harmful consequences for whoever owns a system or company proactively trying to protect itself. But let's examine what we see as perhaps the biggest reason why prosecution of cybercrimes is so rare: Attribution is *difficult*. Nearly impossible, in many cases. The anonymity that the internet provides, and the ability to be located almost anywhere in the world, contributes to this challenge. That it is easy for bad actors to falsify evidence and make an attack look like it originated from someone or somewhere when it didn't makes matters all the more complicated.

An example of a so-called "false flag" operation was the hacking of the French TV network TV5Monde. The attack was made to look like it was perpetrated by an ISIS-affiliated group. But as it turned out, the attackers were in fact tied to the Russian government.

The reality is that even governments and agencies with ample enough resources to invest in a defensive strategy struggle with attribution. How then can we expect private enterprises with more meager intelligence resources to accomplish this effectively and with minimal errors?

Read the rest here:

https://finance.yahoo.com/news/hack-back-bill-legitimizes-messy-171008949.html?guccounter=2

Design Weaknesses Expose Industrial Systems to Damaging Attacks

By Eduard Kovacs, SecurityWeek, January 21, 2020

An analysis of industrial control systems (ICS) has shown that many products contain features and functions that have been designed with no security in mind, allowing malicious hackers to abuse them and potentially cause serious damage.

PAS, which provides industrial cybersecurity and operations management solutions, has analyzed data collected over the past year from over 10,000 industrial endpoints housed by organizations in the oil and gas, refining and chemicals, power generation, pulp and paper, and mining sectors.

The company's researchers discovered that many of the industrial control systems used by these organizations are affected by design flaws and weaknesses that could be leveraged by malicious actors for a wide range of purposes, including to cause disruption and physical damage.

On the 10,000 industrial endpoints it has analyzed, PAS discovered a total of more than 380,000 known vulnerabilities, a majority impacting software made by Microsoft. However, the company found not only typical vulnerabilities that can be patched with a software or firmware update, but also weaknesses introduced by the existence of legitimate features and functionality that can be abused for malicious purposes.

These issues can impact various types of ICS, including human-machine interfaces (HMIs), programmable logic controllers (PLCs) and distributed control systems (DCS), and exploitation in most cases only requires network access or low/basic privileges.

An attacker does need to have an understanding of how the targeted system works in order to exploit these weaknesses. However, if they do know how a feature or function works, abusing it is an easy task, Mark Carrigan, chief operating officer at PAS, told *SecurityWeek* in an interview.

PAS has identified two types of issues: ubiquitous weaknesses, which affect a wide range of products, and unique weaknesses, which are specific to one product.

One example of a ubiquitous issue provided by Carrigan is related to a control function parameter, known as the output characteristic, that is present in a wide range of control systems. This parameter, whose name is unique to each product, has a binary setting that determines whether a control system is direct acting (i.e. the controller output rises if the measurement increases) or reverse acting (i.e. the controller output drops when the measurement rises).

If the system controls a valve, for instance, and the operator wants to increase the flow from 80% to 100%, they will open the valve to reach the desired flow. However, if the aforementioned setting is flipped, the valve will actually close, and if that controller is part of a safety function it could have serious consequences.

Modifying the binary setting is easy for someone who has knowledge of these types of systems, and an attacker could target multiple devices at the same time, Carrigan said.

Read the rest here:

https://www.securityweek.com/hackers-can-cause-damage-industrial-systems-abusing-design-weaknesses

ISSA Nametags

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

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

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

2020 Schedule of Events

Chapter Meetings – Dinner (5:30 – 7:30 PM)

Tuesday, February 18, 2020
Tuesday, April 21, 2020
Tuesday, May 19, 2020
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

Mini-Seminars – Breakfast (8:30 – 12:00 PM)

Saturday, February 22, 2020
Saturday, April 25, 2020
Saturday, May 16, 2020
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

Security + CE Reviews

Saturday, March 7, 2020
Saturday, March 14, 2020
Saturday, March 21, 2020

Saturday, September 12, 2020
Saturday, September 19, 2020
Saturday, September 26, 2020

Chapter Meetings – Lunch (11:00 – 1:00 PM)

Wednesday, February 19, 2020
Wednesday, April 22, 2020
Wednesday, May 20, 2020
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

ISSA-COS Conferences

Cyber Focus Day (CFD) Symposium

Wednesday, March 25, 2020
Thursday, March 26, 2020

Peak Cyber (PC) Symposium

Wednesday, September 16, 2020
Thursday, September 17, 2020
Friday, September 18, 2020

CISSP Review

Friday, June 5, 2020
Saturday, June 6, 2020
Saturday, June 13, 2020
Friday, June 19, 2020
Saturday, June 20, 2020
Saturday, June 27, 2020

CyberVIEW Hiring & Networking Fairs (1:00 – 6:00 PM)

Wednesday, March 11, 2020
Wednesday, June 10, 2020
Wednesday, September 9, 2020
Wednesday, December 9, 2020

CyberVIEW hiring and networking events connect Cybersecurity professionals searching for employment with companies looking to fill current or upcoming positions. Soft-skill coaches and resume reviewers will be on hand. This event concludes with a social hour for exhibitors, ISSA-COS members, and guests.

Annual Chapter Celebration (11:00 – 1:00 PM)

Thursday, December 3, 2020

Take time with ISSA-COS to reflect and celebrate the many accomplishments of our chapter from throughout the year. During this event, we will present specific honors, introduce the newly elected board members, and recognize specific professional accomplishments of our general members.

For additional information, contact info@issa-cos.org or visit www.issa-cos.org.

Special Interest Groups (SIGS)

Special Interest Groups (SIGs) are groups comprised of Cybersecurity professionals who gather together to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: Affinity Groups and Industry Groups. On a quarterly basis, ISSA-COS brings together both groups to participate in formally structured events. During these gatherings, participants have an opportunity to first attend one of four (4) Affinity Groups then, one of four (4) Industry Groups. CPEs/CPUs are awarded for attend these events.

In-between formal gatherings, the SIG Leaders for each individual SIG are encouraged to coordinate informal gatherings. ISSA-COS encourages SIG leaders to consider hosting informal gatherings at social venues such as sporting events, restaurants, bars, or breweries. Informal gatherings may also include participating in a community improvement project, a group walk or hike, or a picnic/BBQ.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups gather to share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

- Women in Security – **W**[omen]**IS (WIS)**
- Young Professional in Security – **Y**[oung Professionals]**IS (YIS)**
- Educators in Security – **E**[ducators]**IS (EduIS)**
- Executives in Security – **E**[xecutives]**IS (EIS)**

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups gather together to discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

- Finance in Security – **F**[inance]**IS (FIS)**
- Healthcare in Security – **H**[ealthcare]**IS (HIS)**
- Retail in Security – **R**[etail]**IS (RIS)**
- DoD in Security – **D**[oD]**IS (DodIS)**

ISSA-COS invites you to join us at our next SIG gathering or any one of our many other events.

For additional information, contact: info@issa-cos.org or visit www.issa-cos.org.

Platinum Sponsor—Murray Security Services—
https://www.murraysecurityservices.com/

Murray

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

ISSA-COS Scholarship Fund Sponsor—ASPG
https://aspg.com/

ASPG
Advanced Software Products Group, Inc.

Update Your Profile!

Don't forget to periodically logon to *www.issa.org* and update your personal information.

Cyberattackers lurking longer inside computers, report finds

By Gopal Ratnam, Roll Call, January 14, 2020

Online attackers are becoming so good at hiding themselves that they can remain undetected in victims' computers for months before being found, potentially giving these criminals more time to inflict greater damage than if they were detected earlier, according to cybersecurity research firm CrowdStrike.

Cyberattackers remained undetected for an average of 95 days before discovery last year, compared with an average of 85 days in 2018, CrowdStrike said in a report made public Monday.

The sharp increase in dwell time "is not a metric that we want to see go up," Tom Etheridge, CrowdStrike vice president of services, told CQ Roll Call. Deploying so-called living-off-the-land techniques, "where an attacker can masquerade as a legitimate user in a client environment and remain stealthy provides an opportunity to get a full spectrum lay of the land" of the computer system, thus making their moves more impactful.

The increase in dwell time last year seen by CrowdStrike may have been partly because it took on a larger number of international clients with weaker technological means to find attackers than their American counterparts, Etheridge said.

To avoid detection, sophisticated nation-state attackers tend to operate with speed once they have broken into a victim's computer. But criminals may move slowly, hoping to cause bigger disruptions and collect larger ransoms, CrowdStrike found in a report published in 2019.

Russian intelligence agency operators code-named Fancy Bear and Cozy Bear were eight times as fast as their nearest North Korean attackers, according to CrowdStrike. The Fancy Bear group has been linked to a large number of global attacks, including on the Democratic National Committee in 2016 as well as several Eastern European governments and militaries.

Criminals seeking to get higher ransoms could use their extra time inside a computer system to encrypt not only active data in use by a victim but backups as well, causing greater damage, Etheridge said.

Weakness in the supply chain

As large companies get better at finding and stopping attackers, cyber thieves are turning to smaller suppliers and software service providers for their targets, CrowdStrike found.

About 6 percent of incidents investigated by CrowdStrike in 2019 were the result of a compromise on a contractor or subcontractor to a larger company, the company said. Although these supply chain compromises are a small proportion of attacks, "third-party compromises have the potential to be more impactful or far-reaching than attacks originating" from other sources, the report said.

Third-party providers also include cloud service companies and internet service providers, and any compromises of their networks could allow attackers to penetrate many of the providers' client computers as well, Etheridge said.

Lawmakers, intelligence agencies and the National Institute of Standards and Technology have been warning U.S. companies about supply chain cybersecurity risks for more than two years.

A variety of vendors, from janitors to software suppliers, with physical or virtual access to a company's computer network could inflict damage, NIST has said. The agency has advised companies to undertake a variety of best practices, including better screening of their employees and of vendors' cybersecurity routines.

The Office of the Director of National Intelligence also has prepared a series of presentations advising federal agencies and U.S. companies on cybersecurity risks posed by suppliers and vendors. The agency and others have also warned about the risks of software backdoors that would allow hackers and spies to gain access to networks.

In one example of widespread concern over far-flung networks of suppliers potentially undermining U.S. security, the top three makers of voting machines told lawmakers last week that many of their electronic components, including capacitors and chips, were sourced from China, but executives said they had no idea what proportion came from there.

Companies that engage in large mergers and acquisitions also are starting to examine the cybersecurity practices of their potential takeover targets, Etheridge said. Due diligence assessments are starting to examine the target company's networks either before closing a deal or before the acquired company is integrated into the buyer's computer networks, he said.

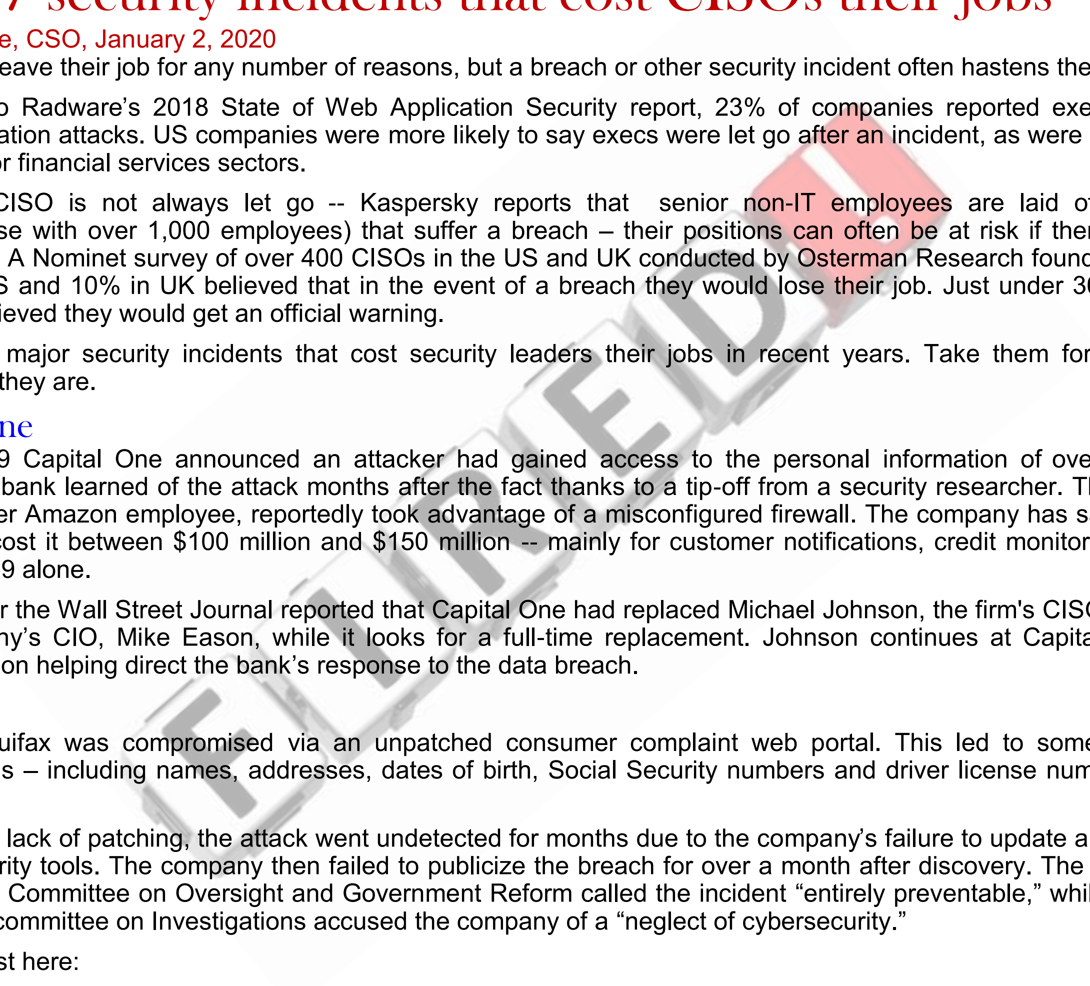
Detection improving

Read the rest here:

https://www.rollcall.com/news/congress/cyber-hackers-lurking-longer-inside-computers-report-finds

7 security incidents that cost CISOs their jobs

By Gary Swinhoe, CSO, January 2, 2020



CISOs can leave their job for any number of reasons, but a breach or other security incident often hastens their departure.

According to Radware's 2018 State of Web Application Security report, 23% of companies reported executive firings related to application attacks. US companies were more likely to say execs were let go after an incident, as were companies in the technology or financial services sectors.

While the CISO is not always let go -- Kaspersky reports that senior non-IT employees are laid off at 27% of enterprises (those with over 1,000 employees) that suffer a breach – their positions can often be at risk if there were clear security failures. A Nominet survey of over 400 CISOs in the US and UK conducted by Osterman Research found that 6.8% of CISOs in the US and 10% in UK believed that in the event of a breach they would lose their job. Just under 30% of survey respondents believed they would get an official warning.

Here are 7 major security incidents that cost security leaders their jobs in recent years. Take them for the learning opportunity that they are.

1. Capital One

In July 2019 Capital One announced an attacker had gained access to the personal information of over 100 million customers. The bank learned of the attack months after the fact thanks to a tip-off from a security researcher. The suspected attacker, a former Amazon employee, reportedly took advantage of a misconfigured firewall. The company has said it expects the incident to cost it between $100 million and $150 million -- mainly for customer notifications, credit monitoring and legal support -- in 2019 alone.

In November the Wall Street Journal reported that Capital One had replaced Michael Johnson, the firm's CISO since 2017, with the company's CIO, Mike Eason, while it looks for a full-time replacement. Johnson continues at Capital One as an advisor focused on helping direct the bank's response to the data breach.

2. Equifax

In 2017 Equifax was compromised via an unpatched consumer complaint web portal. This led to some 143 million customer records – including names, addresses, dates of birth, Social Security numbers and driver license numbers – being stolen.

As well as a lack of patching, the attack went undetected for months due to the company's failure to update a certificate on an internal security tools. The company then failed to publicize the breach for over a month after discovery. The US House of Representatives Committee on Oversight and Government Reform called the incident "entirely preventable," while US Senate Permanent Subcommittee on Investigations accused the company of a "neglect of cybersecurity."

Read the rest here:

https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html

From the Mentorship Team

ISSA-COS Mentorship is available as an embedded feature/service which is matrixed through each SIG. This custom-tailors ISSA-COS Mentorship so that it tailor-fits each career lifecycle stage and special interest. ISSA Mentors and Proteges aren't enrolled into a mentorship program; rather, the process is that of an intake in which a need is assessed with the goal of the need being met. The need is taken in and evaluated and an action plan is created to meet the need. (As an additional need arises, an additional intake is created.)

ISSA Mentorship is an exchange in which both parties are protected and respected. Healthy boundaries are maintained and proprietary knowledge is protected. ISSA Mentorship is designed to be a win-win situation in which both parties are enriched.

ISSA Mentorship is goal/need-driven. The ISSA-COS Mentorship Intake Form serves as a guide regarding the length of the mentorship session as the goal/need of the mentor or protege will determine parameters. The carefully-crafted intake form provides ISSA-COS leadership with metrics so that ISSA Mentorship is treated as a service with KPIs (Key Performance Indicators) and next step suggestions. If ISSA-COS Mentorship can *measurably* boost the careers of its membership, ISSA will, in turn, be boosted as we become known for building each other.

Mentorship Intake Form

email completed form to: mentorship@issa-cos.org

ISSA
Information Systems Security Association
Colorado Springs Chapter

I seek to:

- ❏ mentor
- ❏ protégé
- ❏ peer-to-peer

I aim to meet:

- ❏ in person
- ❏ by phone
- ❏ via email
- ❏ via Skype

What drives you to invest in mentorship now? Please state two goals:_______

____

____

____

____

____

Name:______________

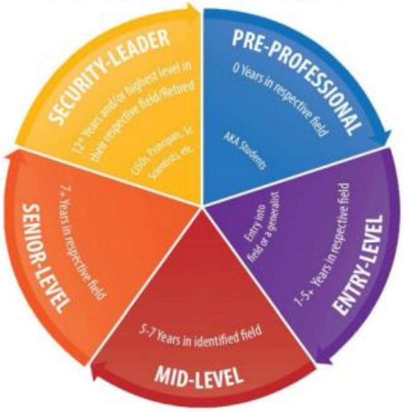
Phone:______________

Email:

____

____

Checkmark your current status in the ISSA Cyber Security Career Lifecycle:



SECURITY-LEADER
12+ Years and/or highest level in their respective field/Retired
CISOs, Principals, Sr. Scientists, etc.
PRE-PROFESSIONAL
0 Years in respective field
AKA Students
ENTRY-LEVEL
1-5+ Years in respective field
Entry into field or a generalist
MID-LEVEL
5-7 Years in identified field
SENIOR-LEVEL
7+ Years in respective field

Are you on LinkedIn? Y / N
Are you on Skype? Y / N

Have you visited the ISSA-COS website? Y / N

Which ISSA committees or special interest groups align with your interests?

- ❏ Speakers Bureau
- ❏ Friends of Authors
- ❏ Women in Security
- ❏ Healthcare in Security
- ❏ Finance in Security
- ❏ Retail in Security
- ❏ DoD in Security
- ❏ Executives in Security
- ❏ Young Professionals in Security
- ❏ certification prep
- ❏ continuing education
- ❏ other: ___________

My mentorship goals align most closely with:

- ❏ career advice
- ❏ building an alliance
- ❏ seeking opportunity
- ❏ technical training
- ❏ practice leadership
- ❏ practice speaking
- ❏ practice authoring for publications
- ❏ solving a specific technical challenge
- ❏ finding my place in our ISSA chapter
- ❏ other ___________

MENTOR USE ONLY

Feedback / Recommendations

Time invested:____ mins / hrs

Were goals met? Y / N

Is additional mentorship requested at this time? Y / N

Additional notes:

OFFICE USE ONLY

Follow-up Plan

- ❏ *time recorded*
- ❏ *goals recorded*
- ❏ *resources provided*

____

- ❏ *referred to SIG:*

____

Next steps:

email completed form to: mentorship@issa-cos.org

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce

Additional photographs are available on the ISSA-COS.ORG website.

Colorado Springs Chapter

WWW.ISSA-COS.ORG

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Dennis Schorn
- Deputy: **Vacant**

Recorder/Historian: Andrea Heinz
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig
- Deputy: Melissa Absher

Vice President of Training: Mark Heinrich
- Deputy: Phebe Swope

Member at Large: Art Cooper
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

Committee Chairs:

Training: Mark Heinrich
Hospitality: **Vacant**
Mentorship Committee Chair: Carissa Nichols
Ethics: **Vacant**
Recognition: **Vacant**
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

Executive Assistant: Andrea Heinz

** Executive Board Members*

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?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Past Senior Leadership

President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy

These subject lines are the most clicked for phishing

By N.F. Mendoza, Tech Republic, January 16, 2020

The most successful email lures don't promise riches, but issue imminent cybersecurity warnings or urgent office messages, a report reveals.

By now, even the least-seasoned email user knows not to open messages from Nigerian princes or vacationing "friends" desperate for an emergency loan.

But bad actors have become increasingly clever in phishing attempts. KnowBe4, which provides security awareness training, revealed the most clicked subject line in a fourth-quarter report.

Read the rest here:

https://www.techrepublic.com/article/these-subject-lines-are-the-most-clicked-for-phishing/

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