ISSA JOURNAL

December 2023
Volume 21 Issue 12
Hiring Your Next (or First) CISO

Hiring Your Next (or First) CISO

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

18 **Hiring Your Next (or First) CISO**
John C. Checco (President, ISSA NY Metro Chapter) and Steven Kolombaris (CISO, Sotheby's)
This article provides an overview of points to consider when hiring your first CISO.

Also in this Issue

3 **From the President**
Dr. Shawn P. Murray, International President
December is Here!

4 **Editor's Corner**
Season's Greetings
Jack Freund – Editor, ISSA Journal

5 **The Cryptic Curmudgeon**
Secrets, Lies, Discord, and Humility
By Robert Slade

6 **Crypto Corner**
Fads: Good and Bad
By Luther Martin – ISSA Member, Silicon Valley Chapter

8 **Women in Cybersecurity**
What Attracts Women to Cybersecurity?
By Dr. Curtis Campbell, ISSA Fellow, ISSA International Director

10 **From the Cyber Library**
Book Reviews
By William J. (Jay) Carson

12 **Open Forum**
Improving Cybersecurity for SAP: A Quick Guide to Adopting the NIST Cybersecurity Framework
By Christoph Nagy, SecurityBridge

14 **Cloud Security Corner**
Is Securing Generative AI Just Securing the Cloud?
By John Yeoh - Global VP of Research, CSA

16 **Association News**
News from the Foundation
ISSA Community Corner
Corporate Member Spotlight
Chapter News

©2023 Information Systems Security Association, Inc. (ISSA)

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association
1964 Gallows Road, Suite 210, Vienna, VA 22182
+1 (866) 349-5818 (local/international)

Greetings ISSA Members

Dr. Shawn P. Murray, International President

December is Here!

December is here and a time to focus on friends, family, and holiday activities! It is a time to reflect on accomplishments over the year and celebrate our successes. We will develop strategies to tackle unfinished obligations and look at new and innovative approaches to address challenges. Networking and collaborating are significant parts of the journey, and your association has many resources to assist you, so be sure to reach out to our team!

November was another busy month!

Your ISSA International Board of Directors began transitioning with a new management company to refresh our services, streamline our processes, and organize our membership and chapter portfolios. Some people have transitioned already, and some familiar faces remain. Look for new team members to reach out over the next month or so as we complete the transition by the end of the year!

We approved two new working groups. One to focus on member growth in Central and South Americas and another to refresh and update our bylaws. There are opportunities to participate in these working groups and to provide input. Please reach out to our team to inquire if you are interested!

Our chapters and members continue to make contributions to our industry! In correspondence with our Italian chapter president, Marco R.A. Bozzetti, he informed me of the release of the latest publication of the Observatory of Digital Attacks (OAD) report, which is now in its 16th year and focuses on international attacks on the Italian public and private companies. Reach out to our team to gain more information!

We held our Cyber Executive Forum (CEF) in Dallas last month. We saw a significant focus on privacy and cyber legislation, AI complexities, and a further discussion on the growing concerns with Deep Fakes. Our next CEF is scheduled for February near Tampa, Florida. We hope to see you there if you are a CEF Member!

As a continued reminder, help others outside our industry be aware of the scams and social engineering attacks that come this time of year. Younger children and our senior population are more targeted during the holidays.

Whatever you and your family and friends celebrate, I wish you a safe and enjoyable holiday season and a prosperous new year!

Holiday Cheers!

Dr. Shawn P. Murray, President

ISSA International Board

ISSA
Information Systems Security Association

International Board Officers

President
Dr. Shawn P. Murray

Vice President
Deb Peinert

Secretary/Chief of Operations
Betty Burke

Treasurer/Chief Financial Officer
Pamela Fusco

Board of Directors
Dr. Curtis Campbell
Debbie Christofferson
Mary Ann Davidson
Alex Grohmann,
Laura Harder
Lee Neely
Jimmy Sanders
David Vaughn
Stefano Zanero

The Information Systems Security Association, Inc. (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, skills, and professional growth of its members.

With active participation from individuals and chapters all over the world, the 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.

The ISSA international board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

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.

Season's Greetings

Jack Freund – Editor, ISSA Journal

As the year draws to a close and the festive season approaches, we find ourselves looking back at the remarkable strides taken in the world of cybersecurity in 2023. This final issue of the year stands as a testament to the profound insights, robust debates, and the endless pursuit of knowledge that has characterized our journey together. I would like to extend my heartfelt season's greetings to all our readers, contributors, and partners who have played an integral role in our shared mission – securing the digital frontier.

This December issue brings forth two trailblazing articles, casting a spotlight on both the vast landscape of cybersecurity infrastructure and how to effectively hire a CISO to oversee all the dynamic attacks and complex control environments.

First, we have "Improving Cybersecurity for SAP: A Quick Guide to Adopting the NIST Cybersecurity Framework" by Christoph Nagy of SecurityBridge. As businesses worldwide increasingly depend on SAP for their critical operations, the need for a robust cybersecurity framework becomes paramount. Christoph Nagy elucidates how the National Institute of Standards and Technology's Cybersecurity Framework can be adeptly adopted to bolster SAP's digital defenses. Through this article, you'll gain insights into the steps and strategies to ensure that your SAP systems are not just compliant but truly resilient against the ever-evolving cyber threats.

Our feature article, "Hiring Your Next (or First) CISO" by John C. Checco and Steven Kolombaris provides a comprehensive guide for organizations on how to effectively recruit a Chief Information Security Officer (CISO). It emphasizes the importance of proper planning and understanding the role's scope, which includes managing cyber security akin to a general contractor overseeing a construction project. The authors advise on thorough role definition, alignment with company needs and regulatory requirements, and understanding the board's expectations. They discuss the significance of fitting the CISO into the correct position within the company's hierarchy and ensuring the compensation reflects the responsibilities and expertise required. The article also touches on the nuances of executive candidate selection, the interview process, diversity and inclusion, and the importance of a well-structured onboarding process.

The realm of cybersecurity is dynamic, with new challenges and solutions emerging every day. As we wrap up another year of diving deep into this fascinating world, I want to express my sincere gratitude to all of you. Your support, whether through contributing articles, engaging in discussions, or simply reading our journal, is the backbone of our endeavor. Together, we foster an environment of knowledge-sharing and continuous learning.

In the spirit of the season, I wish each one of you joy, peace, and prosperity. May the New Year bring with it new horizons, fortified security postures, and an ever-growing community dedicated to safeguarding our digital universe.

Thank you for being a pivotal part of our journey this year. I am looking forward to yet another year of illuminating discoveries and discussions in 2024.

ISSA JOURNAL

Now Indexed with EBSCO

Editor: Jack Freund, PhD

editor@issa.org

Advertising: vendor@issa.org

Editorial Advisory Board

Garrett Felix, ISSA Fellow

Jack Freund, PhD, Distinguished Fellow – Chairman

Michael Grimaila, PhD, Fellow

John Jordan, Senior Member

Enoch Anbu Arasu Ponnuswamy

Kris Tanaka

Services Directory

Website

webmaster@issa.org

Chapter Relations

chapter@issa.org

Member Relations

memberservices@issa.org

Executive Director

execdir@issa.org

Advertising and Sponsorships

vendor@issa.org

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use, and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, are the responsibility of the reader.

Articles and information will be presented as technically correct as possible and to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see www.issa.org.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

Secrets, Lies, Discord, and Humility

By Robert Slade

Bruce Schneider has published, on his blog, some thoughts about a time when he saw the infamous Snowden classified files. He made the point that having access to classified information skews your view of the world, since you know that the media, and politicians, and certainly the coffee klatch that tends to solve all the problems of the world, get things wrong so much of the time. They don't have all the information.

What Schneider doesn't particularly stress is that even those with access to classified information don't have all of the information. They don't necessarily have the truth, even though they may have more indications and inferences, and even know more secrets than we do.

Nobody has ever been foolish enough to give me security clearances. I'm a teacher, and therefore a blabbermouth. It's probably a good thing that I don't have a security clearance, because, although I do practice a lot of self-censorship about what I do know, it avoids any danger of me actually betraying terribly important secrets.

But, because I work in security, I do have friends in the military, and the intelligence, communities. I remember a story that made the news, for quite a few news cycles, a number of years ago. This was about the release of a military budget, and the fact that someone took issue with a line item in one particular project that made reference to hammers costing X hundreds of dollars, and toilet seats costing Y hundreds of dollars. At the time, I assumed that, since these items were part of a project whose very existence had been classified up until a few years before the release of this particular budget, they were specialized tools, or items, or components, and therefore cost a bit more than something that you might pick up at Canadian Tire.

I was wrong.

Recently I obtained information from a friend of a friend of a friend that someone had seen the original of that budget and that 1) they weren't hammers, and 2) they were very necessary to the project, and 3) X hundreds of dollars was a reasonable price to pay for those particular components.

I think the point that I am trying to make here is about humility. We don't have all the information. Sometimes, we don't even have enough information to make a good guess. And trying to account for a seeming price inflation, it didn't occur to me, at the time, that in a classified project, parts of which were still classified back then, and parts of which still are classified, that, while you might want to tell people how much it cost, you might not want to give them all the details about why it cost that much, and that sometimes a flat out lie is reasonable in the circumstances.

We don't have all the information, and, as Donald Rumsfeld famously told us, there are some things that we know we don't know, and some things that we don't even know that we don't know. Any decisions, or conjectures, that we make about something we don't know about, can be flawed, and we have to be humble in the face of that.

I have recently been preparing materials on formal security models. Pretty much all of us who work in information security are familiar with the Bell-LaPadula confidentiality model. However, fewer of us will recall the Biba integrity model. One of the properties of the integrity model is that you do not write up: that is, you do not contaminate information of greater sensitivity, or higher accuracy, for greater integrity, with information that isn't as accurate, or that you don't know fully. A lot of us forget that. Basically, this is the humility part of the integrity model, and, therefore, one of the basic facts of our jobs. We can't contaminate what we do know, and what is accurate, and what is information of high integrity, with our conjectures. We don't know everything.

Part of what we don't know is how much of what we are told is disinformation. And, recently, disinformation has been increasingly turned to a new tactic, that of discord. There are certain adversaries who managed to make us fight ourselves. They feed us lies, based on disagreements that we already have, knowing that some of us are going to believe the lies, because we already are quite willing to think the worst of the people on the other side of the argument. The lies are meant to inflame the argument, and get us to battle with people we disagree with, and therefore fight and injure ourselves, when we should be preparing to fight a true adversary: the people who fed us the lies in the first place.

A little humility in evaluating lies, and determining, when we first hear a bad report about someone who we are quite willing to dislike, would go a long way to preventing us from falling victim to the discord attacks. But only if we are humble about what we think we know.

About the Author

Robert Slade is, IMNSHO, not to be trusted with secrets. If you want, you can (virtually) accompany him on his daily walk (and prep for your CISSP exam) at https://fibrecookery.blogspot.com/2023/02/cissp-seminar-free.html It is next to impossible to get him to take bio-writing seriously, but you can try at the-usual-suspect@outlook.com

Fads: Good and Bad

By Luther Martin – ISSA Member, Silicon Valley Chapter

I was recently reminded of the old saying, "Fool me once, shame on you. Fool me twice, shame on me." I was talking about the future of quantum computing (QC) when this happened.

I don't remember technology fads like QC when I was younger. Instead, we seemed to have management fads. This might have peaked in the days of Total Quality Management (TQM), which, its supporters told us, could end global warming, feed the hungry, and bring back the cancelled TV show Firefly. Sadly, this turned out to not be true (possibly hindered by the fact that Firefly wasn't around back then).

Management fads didn't seem to improve management, but they got some people excited about thinking of new ways to make their organizations run better, and that really seemed enough to justify their existence. Is there similar value in technology fads?

I'm going to tentatively say that there isn't, at least not with QC.

I've seen technology fads come and go. The first one that I was aware of was the dot-com-era hype of public key infrastructure (PKI). I was suckered into believing in this one, and was genuinely surprised when PKI wasn't able to deliver on the promises its fans made.

That was the one time that I was fooled by a technology fad, and I try to stay skeptical of the newer ones because of that experience. Even "crackpot" columnists for the ISSA Journal can be wrong from time to time. But we're in good company. In the imagined dialog between Pope Benedict XIV and Voltaire in Durant's *The Age of Voltaire*, Benedict notes to Voltaire, "Well, you see that you too can make mistakes, just like a pope." So here are my thoughts about quantum computing, possibly setting up the scenario where people will one day be able to say "Well, you see that you too can make mistakes, just like an ISSA Journal columnist."

I don't believe almost any of the hype around QC. Some QC claims are so wrong that they deserve to be called "not even wrong," as physicist Wolfgang Pauli is thought to have first said. Others are probably just wishful thinking or justifications for getting funding for research.

I'd love to see what the National Security Agency (NSA) calls "cryptographically relevant quantum computers," but I don't expect to see those in my lifetime. I simply don't believe the many claims that quantum computers will be able to crack existing cryptographic algorithms any day now. Without getting into too many details about quantum mechanics, like Hamiltonians of superconducting qubits and coherence times, it's hard to accurately summarize why I believe this, but saying that quantum systems are just too delicate and finicky to easily scale well might be a good attempt at this.

As far as I can tell, the biggest impact of quantum computing is that people seem to want to hear me talk about quantum mechanics these days, or at least they pretend to. Pretty much no one cared about it several years ago, and any discussion of it back then seemed to remind people that they needed to do important things, like going back to their desk to check their email or filling in that HR form that describes their goals for the next year.

Now, people seem to like to hear about this stuff, even when it involves lots of math, although I'm pretty sure that they listen just as carefully to the math now as they did before quantum computing was popular. And I'm pretty sure that absolutely nobody has really followed my discussion of Hamiltonians of superconducting qubits or quantum coherence. But they now seem to prefer hearing about it to doing HR paperwork, so that's something.

So there's definitely a similarity between what I saw with management fads and what I see now with the hype around quantum computing (as well as artificial intelligence, but that's a topic for another column). But while fads like TQM seemed to have the good side-effect of getting people excited about improving their organizations, it's not clear to me that we get a similar benefit from quantum computing. Maybe that's because it's very easy to understand the details of TQM while it's very hard to understand the details of QC, possibly because there's essentially no math involved in TQM. This means that lots of wishful thinking is easily passed off as fact in QC, making it, as far as I can tell, a bad fad.

About the Author

Luther Martin has survived over 30 years in the information security industry, during which time he has probably been responsible for most of the failed attempts at humor in the ISSA Journal. You can reach him at lwmarti@gmail.com.

– SPONSORED CONTENT –

Controls-Based Versus Risk-Based Cybersecurity Programs

In the face of an escalating regulatory burden and increasingly common data breaches, many teams are being pushed to mature from a controls-based to a risk-based approach to cybersecurity. While this pressure presents new opportunities for teams to more directly address risk and prove their value to executive leadership, it is also a significant demand: not only must cybersecurity professionals make major changes to their risk management methodology, they must also learn and adopt a new way of looking at cybersecurity. This blog will cover the difference between controls-based versus risk-based cybersecurity approaches and the benefits of making the transition.

The controls-based approach is a common starting point for developing teams because the wide field of available control frameworks provide a strong backbone for a new program. Teams that choose this methodology review the available frameworks until they've found the one that's right for their organization and its regulatory requirements then implement the appropriate controls until they've come into compliance. This methodology is popular because it allows less mature teams to achieve a baseline "best practice" program without escalating their project to the point that it becomes unwieldy. Still, this approach has considerable limitations: because your team is checking the box on a premade framework, there's the possibility that you'll miss key risks that are specific to your organization.

Key features of controls-based cybersecurity:

- Program started recently
- Uses cybersecurity frameworks as foundation
- Helps achieve "best practices"
- Collects risk data in an ad-hoc fashion

By contrast, the risk-based approach takes a more active role in identifying the risks that would most likely disrupt critical business processes and planning actions to mitigate that possibility. Where a controls-based approach depends on a given framework to cover all your risk areas, teams that take the risk-based approach act directly to more effectively reduce the risks your organization faces. This has the added benefit of making it easier to defend your program to executive leadership: it's good to argue that your team has maintained compliance using a well-chosen cybersecurity framework, but it's exceptionally convincing to call out the specific risks you've prevented and the potential cost of letting them go unaddressed.

Key features of risk-based:

- Program has had time to mature
- Addresses risk directly
- Justifies itself to leadership using metrics
- Collects risk data programmatically

Making the transition from the controls-based to the risk-based approach can be a daunting task, but a strong cybersecurity platform can make it much easier. With its configurable reporting functionality and risk register, ProcessUnity for Cybersecurity Risk Management empowers your team to track the risks facing your organization, plan mitigation efforts according to a color-coded heatmap and communicate your posture to the board. To learn more about risk-based cybersecurity, read our new white paper, "Mature Your Cybersecurity Program from a Controls-Based to a Risk-Based Approach."

CONTROLS-BASED

- Less mature program
- Uses framework as foundation
- Ad-hoc collection of risk data

RISK-BASED

- More mature program
- Addresses risk directly
- Programmatic collection of risk data

To learn more about Cybersecurity Risk Management, visit www.processunity.com

ProcessUnity

What Attracts Women to Cybersecurity?

By Dr. Curtis Campbell, ISSA Fellow, ISSA International Director

This article looks at one woman's journey from Chemical Engineering, working as a global process engineer, to re-engineering her passion and skills to Cybersecurity. What attracted Catie to Cybersecurity was the way to blend her talents for building relationships and trust around the framework of problem solving.

Want to know a smart, capable woman who has found just the right combination for a career and work-life balance to have it all? Meet Catie Bush, ISSA Chapter leader, female executive, wife, mother, outdoor enthusiast, account manager, and president's club achiever. Catie represents an inspiring, dynamic example of how to channel your passion for work and creating community while carving out family time. I recently sat down with Catie to ask for her secret sauce and recipe for success.

Eight years ago, Catie Bush made the transition from Chemical Engineering to Cybersecurity, an "aha moment" she recalls vividly. When I asked Catie why she was attracted to the field of Cybersecurity, she told a story that started a decade ago. The short answer, she explained, is that Cybersecurity is the perfect blend of analyzing and solving complex problems and building relationships. The long answer started right after college graduation when she realized she enjoyed connecting people and processes and was good at it!

What follows is a glimpse inside the busy world of a female executive achieving her passion and satisfaction of navigating her career and raising a family.

Early Years

Q: What is your educational background?

A: I took the traditional path of a four-year university degree program where I graduated with a Bachelor of Science in Chemical Engineering and a minor in Business Management.

Q: What were your early roles?

A: Right out of college, I accepted a process engineering role with Shaw Industries, one of the world's largest carpet manufacturers. Shaw is a huge, global company, and I worked at the company's headquarters in Georgia. After my tenure with Shaw, I moved to Tennessee to take on a role as a Global Process Engineer for Alstom Power with their global power and grid division which was later acquired by General Electric. While at Alstom, I designed cleaning solutions for coal-fired power plants. In that role, I traveled frequently and went onsite to plants, meeting with technical folks as well as executives. It was then that I realized that I had the ability to speak the technical talk when needed but also the business talk with the leadership at the facilities. The icing on the cake was that I enjoyed building those relationships.

Q: How did you make the transition into Cybersecurity?

A: When working with all levels of employees in the plants, I realized I was good at building relationships and could talk with diverse groups on several levels. When more of a customer-facing position piqued my interest, I accepted the opportunity. Later, when approached for a position with Avertium, an Information Security company focused on a cyber fusion approach and not just one product or service, I saw a way to utilize my analytical process for solving problems with developing relationships with companies. This is when my "aha moment" told me to make the switch. Information Security was very interesting to me, and I felt that I could grow in this field.

Q: What are you doing now?

A: I am a Senior Account Manager with Avertium. It is a great role to satisfy my passion of analyzing problems and designing solutions with a customer-centric approach. That was 8 years ago, and I have loved every moment.

Q: Now that you have almost a decade of information security experience, how have you seen educational paths evolve in this industry? In other words, do you see multiple paths for Cybersecurity education?

A: The demand for talent in Cybersecurity has increased tremendously. We have definitely seen an increased focus on Cybersecurity education and certifications out there to gain knowledge and experience in different areas of cyber. The shortage of jobs and unfilled roles remains, and I have seen a lot of progress over the years. In addition to the traditional four-year university-based degree programs, there are now Cybersecurity apprenticeship programs, internships, certification and specialization opportunities, and job-embedded programs. When you think about it, the types of training that include cybersecurity sales, client success, consulting, technical, customer-facing technical, and project management, etc. are all needed for working in Cyber companies.

Obstacles, Challenges, and a Work-Life Balance

Catie and I talked about challenges- from first jobs until now, the after-effects of the pandemic, and the remote working environment that has remained. I asked Catie to share her secret sauce regarding the flexibility of work and time management needed for working mothers.

Q: From your education path and first jobs until now, did you experience any challenges along the way?

A: Absolutely. In those early years, I was trying to figure out what I was passionate about, and I spent some years going through a few positions that didn't ignite that for me.

Q: What is the most difficult obstacle you've had to overcome in your professional life?

A: In previous years, balancing work and family was a real struggle for me. I loved my time with my kids, but I realized I needed my career to make me feel whole. Until I went into Cybersecurity, I felt torn and somewhat unfulfilled, and the two constantly pulled at each other. Having a career that I'm passionate about now is very fulfilling and confirms I can achieve a nice balance of applying my skills and talents in the workplace and then spending time with my family and enjoying raising my kids.

Q: Work-life balance is top of mind these days. How do you achieve it?

A: I've always had a work hard, play hard mentality. I LOVE to travel and fortunately get to do it quite often since my husband homeschools our kids, and I can work remotely at times. I truly believe it's very important to figure out what your own work-life balance is that makes you happy and keeps your work and life goals achievable. That balance is a personal journey and is something you have to pay attention to.

Q: What would your children be most proud of with you as a working Mom?

A: Balancing work and family. We figured it out and are blessed to have this balance. With our kids homeschooling under the charge of my husband and me working from home quite a bit more now, we get a lot of random chats and hugs throughout the day. It's not a mad rush out the door in the morning and back again for only a few hours of together time at night. I'm very thankful for that opportunity.

Q: Do you have a mentor? Or are you in a mentoring role?

A: Not formally as defined mentor/mentee roles, but I definitely lean on my past and present managers as mentors. I've been very fortunate to work for some amazing people that do their best to help me succeed in whatever I'm trying to accomplish.

Q: Being Director of Programs for your ISSA chapter must take a lot of coordination and planning. What are some tips you would pass along to other chapter leaders?

A: I feel the key is understanding your audience- knowing what they need and how we can bring it to them. During the pandemic, it became very difficult to maintain our community as our chapter had previously enjoyed large half-day events on a regular basis with educational programs, networking, great food, and fellowship.

As we were forced to return home to work, it became a time of isolation and restrictions. Now that we are "open" again, there are still some limitations in event spaces. Not all of them are available so we are rebuilding and revising as needed. Members want to be connected again. Providing a space to network and socialize is as important as educational programming. I enjoy bringing people together to form a community to collaborate. I would advise other program directors to know your audience and try different approaches. I like to vary my events from fireside chats to panels on a certain topic, to an outdoor restaurant patio setting for food and fellowship. This takes some time and effort but the rewards from the relationships that are formed and sustained make it all worthwhile.

Q: What changes or innovations in the industry are you most excited about?

A: Cybersecurity is evolving all the time so helping my customers stay as secure as possible with whatever services or tools they need excites me. Staying current on changes and innovations helps me help them.

Encouraging Advice

In wrapping up our interview, I asked Catie to shed some light on helping other women climb the ladder. As women are still underrepresented, starting out in the field and climbing the ladder may seem intimidating so I asked Catie to weigh in.

Q: For women aspiring for participation at a leadership level, what steps should they take?

A: Find a mentor and ask about their journey. Network with like-minded peers. Gain hands-on experience so you can understand the tasks of the people you could be leading one day. Make it known that is your goal and work hard until you achieve it.

What does AI Think?

After talking with Catie, I turned to Microsoft Bing for AI's opinion on what attracts women to Cybersecurity. Bing's AI Chat returned an interesting response which made me reflect on Catie's journey.

Q: What attracts women to Cybersecurity?

A (Bing's AI): "Women are underrepresented in cybersecurity, and there are several initiatives to attract more women to the field. According to a report by DiversityQ, some of the best ways to attract and retain more women in cybersecurity include building inclusive environments, having strong female role models, addressing the gender pay gap, offering flexible working practices, promoting diverse skill sets, promoting STEM interests early on, understanding the problem, learning to communicate cybersecurity, using gender-sensitive language, ensuring women visibility, ensuring equal pay for equal work, empowering women and promoting network, and creating initiatives with the goal of attracting and retaining more women in cybersecurity."

"Women possess a wide range of skills that are highly relevant to cybersecurity, including strong communication skills, attention to detail, and analytical thinking. These skills are crucial for tasks such as threat analysis, risk assessment, and communicating security issues to non-technical stakeholders".

Conclusion

With two answers to the question, there is a lot to reflect upon. My thoughts are that it is well answered by AI, but better said by a human. Catie's story is heartwarming and illustrates that passion drives intentional effort and determination toward satisfaction. AI's response is a great reminder of just how many opportunities await women wanting to work in Cybersecurity. It's a welcoming journey and a lifelong reward.

About the Author

Dr. Curtis C Campbell, VP, Information Security Governance professional, serves as Director on the ISSA International Board, and is a member of Atlanta, Chattanooga, Denver, Los Angeles, Middle TN, Minnesota, and San Francisco ISSA Chapters. Curtis holds a Ph.D. in Information Systems and serves on the advisory board of University of TN-Chattanooga, a national Center for Academic Excellence for Cyberdefense (CAE-CD) studies. She was named ISSA Fellow and holds C|CISO and CIPM certifications. Connect with Curtis via curtis@mprotechnologies.com.

Book Reviews

By William J. (Jay) Carson

Disclaimer: These are the author's subjective opinions, and do not necessarily reflect the opinions of any organization or other individual. A human prepared this article, with assistance from Microsoft Editor and Grammarly.

Some cybersecurity soapbox speakers are saying to focus on your particular area and not worry about other areas. I think to be a cybersecurity professional you need a general awareness of all the profession's areas. Please never stop your professional continuing education/learning program.

Some book review readers may think my "Metadata" statements on readability (passive voice) are pointless. In addition to encouraging your professional reading, my secondary goal is for smart technical people (like you!) to author books that are read. Plenty of excellent writers with limited technical knowledge beat the cybersecurity pros in the publishers' competition! Passive voice percentage is an indicator of how difficult the reader is going to find your book. Sure, they might plow through a classic or a coursebook regardless of difficulty, but if you want to write for the cybersecurity community at large, you need to make it readable.

Book #1 of this review, here we go:

Faux, Zeke. Number Go Up: Inside Crypto's Wild Rise and Staggering Fall. Crown Currency (2023).

Sound Bite: Quos Deus vult perdere, prius dementat (Whom the gods would destroy, they first make mad).

If you are one of the cryptocurrency speculation devotees, and think all regulated financial intuitions are inherently evil, you are going to hate this book! You will also hate human trafficking tied so effectively to cryptocurrency abuses. For me, I am going to be a little more polite on those scamming calls, as they may be human trafficking victims.

Almost 400 years ago financial speculation over tulip bulbs struck the well-established Dutch business community. Although "Tulip Mania" was not actually as bad as its hype, the event does point out how ridiculous people can be. In your mind swap out 'tulip bulb' with 'cryptocurrency,' and you will get my point.

In the case of cryptocurrency, people with exceptional training and experience in science and technology sometimes function as if they do not respect the conventional rules, especially of law and ethical financial management. Are they so smart and paper-rich that they can hire lawyers to get them out of any problem? In the book photo, Sam Bankman-Fried looked unhappy as he was being extradited to the US after Bahamian jail time. Cyber entrepreneurs should take heed before deciding to get 'edgy.'

Another book, Michael Lewis' Going Infinite: The Rise and Fall of a New Tycoon is out, and he has a terrific business writing reputation. I like Number Go Up better. Do not think Number Go Up is a 'rush to press' book to capitalize on the hype. The research and investigative reporting are meticulous. Zeke Faux has extensive footnotes compiled at the end of his book, as he covers the cryptocurrency scene.

The Author

Zeke Faux is a business news reporter with a bachelor's degree from Cornell. He has 13+ years on the business news beat. I have not seen evidence of an IT or cybersecurity background, and it shows in his otherwise excellent writing. In his defense, he did begin explaining cryptocurrency with the mysterious Satoshi Nakamoto, so I think he does know the fundamentals.

The Metadata

A 2023 publishing date! The online ordering cost, including shipping, is under $25. The hardcover version is under 300 pages. You can cut that cost if you use an e-reader. My public library has a copy, so expect it in your library.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style measurement is high school level. There was 0% passive voice in my sample, and please note a low percentage is typical of professional writers. This article is under 5% passive voice, for comparison.

Table of Contents (abbreviated/modified and annotated in bold font in parenthesis by me)

1. "I Am Freaking Nostradamus" **(Protect me from my friends)**
2. Number Go Up Technology **(OK, but limited in tech detail)**
3. Doula for Creation **(Egos!)**
4. The Plastic Surgeon **(These billionaires came to crypto differently)**
5. Getting Hilariously Rich
6. Cat and Mouse Tricks
7. "A Thin Crust of Ice"
8. The Name's Chalopin. Jean Chalopin. **(Inspector Gadget - no, really!)**
9. Crypto Pirates
10. Imagine a Robin Hood Thing
11. "Let's Get Weird"
12. "Click, Click, Click, Make Money Make Money" **(Think Wall Street attitudes before the 1929 crash)**
13. Play to Earn
14. Ponzinomincs **(Yep!)**
15. All My Apes Gone **(You will not believe this! You really will not believe this!)**
16. It's the Community, Bro
17. Blorps and Fleezels
18. Pig Butchering **(The public is the pig, butchering = scam)**
19. "We Have Freedom"

20. No Acceptamos Bitcoin **(What really happened when El Salvador went officially crypto)**
21. Honey is Better **(Arrogance)**
22. Assets Are Not Fine
23. Inside the Orchid

Hill, Kashmir. Your Face Belongs To Us: A Secretive Startup's Quest to End Privacy as We Know It. Random House (2023).

Sound Bite: Halloween may be over, but facial recognition technology is very scary. Do not let technology out of the lab without studying all societal impacts and getting ethical frameworks/public protections in place.

You may hate the idea, on an ethical basis, of artificial intelligence systems using face recognition at all. Lord of the Rings fans may liken it to the "One Ring to Rule Them All"; something to be destroyed. Others may think the concept of "Forbidden Fruit" has not worked since Adam and Eve, so we had better understand it and establish legal safeguards. Regardless of your viewpoint, this book will add value to your decision-making.

This is a book about the birth of a company called Clearview AI, and where commercial face recognition technology was in late 2022 - early 2023. It is the result of years of investigative reporting and detailed research. It will make your mind spin with ethical considerations. Warning - this is not a technical book to tell you how facial recognition can be coded. It is much more about its pervasiveness, power, current limitations, and its dangers.

The Author

Kashmir Hill has been a technology and privacy reporter for the New York Times for over four years. She has a bachelor's degree from Duke and a master's in journalism from NYU. She has been reporting for over 15 years. She has reported for Gizmodo and Forbes.

The Metadata

A 2023 publishing date! The online ordering cost, including shipping, is under $30, again half with an e-reader. The hardcover book is over 300 pages, including extensive notes pages. My local public library system has a couple of copies, so I expect yours will as well.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style measurement is high school level. There was around 4% passive voice in my sample, and it reads well. Again this article is about 5% passive voice, for comparison.

Table of Contents (abbreviated/modified and annotated in bold font in parenthesis by me)

Part I The Face Race

1. A Strange Kind of Love **(Introduction of some of the principal players)**
2. The Roots (350 B.C. - 1880s) **(Face reading Pseudoscience)**
3. "Fatface is Real" **(Making cruel assumptions about people based on facial characteristics)**
4. If At First You Don't Succeed (1956-1991)
5. A Disturbing Proposal **(Smartcheckr, predecessor of Clearview AI)**
6. The Snooper Bowl (2001) **(Facial Recognition at the Super Bowl)**
7. The Supercomputer Under the Bed
8. The Only Guy Who Saw It Coming (2006-2008) **(Birth of privacy landmark 2008 Illinois Biometric Information Privacy Act)**
9. Death to Smartcheckr

Part II Technical Sweetness

10. The Line Google Wouldn't Cross (2009-2011) **(Line = Facial recognition)**
11. Finding Mr. Right
12. The Watchdog Barks (2011-2012) **(Watchdog = FTC)**
13. Going Viral
14. "You Know What's Really Creepy?" (2011-2019) **(Al Franken quote)**
15. Caught in a Dragnet
16. Read All About It

Part III Future Shock

17. "Why the (expletive) Am I Here?" (2020) **(The infamous false arrest of Robert Williams)**
18. A Different Reason to Wear a Mask **(COVID time)**
19. I Have a Complaint
20. The Darkest Impulse **(Public shaming enabled by facial recognition)**
21. Code Read **(or Floyd Abrams (representing Clearview) v. the ACLU)**
22. The Future is Unevenly Distributed
23. A Rickety Surveillance State
24. Fighting Back
25. Tech Issues

Happy Reading!

PS – If you have a book you want me to read & review, please use the email address in my bio to let me know! Thank you to ISSA's co-chair of the Privacy Special Interest Group, Janelle Hsia, for recommending next month's selections.

Up next month:

- Hoepman, Jaap-Henk. Privacy Is Hard and Seven Other Myths: Achieving Privacy through Careful Design. The MIT Press (2021).
- Buolamwini, Joy. Unmasking AI: My Mission to Protect What Is Human in a World of Machines. Random House (2023).

William J. (Jay) Carson

Aka 'Dad'

The Cyber Librarian

Additional sources used in the article:

1. https://en.wikipedia.org/wiki/Whom_the_gods_would_destroy,_they_first_make_mad
2. https://en.wikipedia.org/wiki/Tulip_mania
3. https://en.wikipedia.org/wiki/Ponzi_scheme
4. https://en.wikipedia.org/wiki/Biometric_Information_Privacy_Act
5. https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests
6. LinkedIn profiles for authors listed, where available.

About the Author

William J. (Jay) Carson, ISSA Senior Member, Aka 'Dad' The Cyber Librarian is the ISSA-Colorado Springs Executive Vice President. He is part-time 'Cyber Librarian' of Semper Sec, LLC. Holding Security+ and CIPP/E certifications, he is a former high school math/science teacher, civil servant, contractor, and retired USAF Lieutenant Colonel. He can be reached at Runningjay51@gmail.com

Improving Cybersecurity for SAP: A Quick Guide to Adopting the NIST Cybersecurity Framework

By Christoph Nagy, SecurityBridge

Cybersecurity is more crucial than ever, especially for enterprise applications like those running on the SAP platform. However, ensuring that security measures are sufficient and current can be challenging due to the growing complexity of these applications. To address this challenge, the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) - a set of guidelines and best practices for improving cybersecurity.

While the NIST CSF is a generic framework, it provides a common language for discussing and effectively managing cybersecurity risks. However, it does not offer specific guidance for securing SAP systems. Organizations that use SAP need to manually map and adopt the NIST CSF controls to their specific SAP operations or use specific tools to help them with this process and establish missing controls.

The NIST CSF consists of five core functions that provide a structure for organizing cybersecurity activities—that need to be mapped to SAP operations specifics. The five NIST CSF functions, as related to SAP, are as follows:

Identify

Understanding the organization's cybersecurity risks and creating an inventory of the systems (incl. SAP), assets, data, and capabilities that need protection. This understanding includes identifying and prioritizing assets and data, understanding threats and vulnerabilities, and assessing the potential impact of a cyber-attack.

SAP customers should start by understanding their critical SAP processes, SAP-handled assets, SAP datasets, and enterprise capabilities supported by SAP applications. To achieve this, organizations should leverage SAP Solution Manager (sometimes referred to by admins as "SolMan") as their source for all SAP landscape information and inventory.

SolMan is an application lifecycle management (ALM) platform to implement, maintain, and integrate SAP systems. It also supports troubleshooting issues and keeping things running securely, cleanly, and smoothly. Its numerous applications can be categorized into one or more of the defined Information Technology Infrastructure Library (ITIL) stages of service strategy, service design, service transition, service operation, and continual service improvement.

Understanding the ALM platform and how the applications contribute to ITIL-type processes is essential. Once recognized, IT personnel can pinpoint the related SAP transactions and data, enabling them to determine crucial business information, its application, and its vulnerability. Furthermore, IT personnel should continually assess this part of SAP to evaluate their security standing. This provides clarity about the SAP environment and the associated data security risks.

Protect

Implementing safeguards and controls to ensure that critical systems and data are secure. Safeguarding includes protecting against unauthorized access, implementing security controls, and promoting cybersecurity awareness and training.

SAP customers can receive guidance on implementing the appropriate safeguards and controls described in the NIST Cybersecurity Framework's Subsections,[1] such as "Manage, verify, revoke and audit SAP identities and credentials" and "Implement protection against Data-Leaks."

Protecting SAP landscapes and operations is all about SAP security and compliance, ensuring the application is configured correctly for proper system hardening. Like most applications, SAP is porous and needs authentication and authorization measures, e.g., setting up and maintaining user IDs and passwords and ensuring users can only access the data and functions they need to perform their roles.

However, unlike most applications, SAP environments have unique requirements and characteristics that necessitate particular identity management practices such as:

- Centralized User Administration: SAP offers a centralized user administration tool within the NetWeaver platform, which helps manage users across different SAP systems and components. This centralization simplifies administration efforts, especially in large landscapes.
- Role-based Access Control (RBAC): SAP's authorization concept is primarily based on roles. Properly designing and maintaining these roles is crucial. Each role should provide access to specific transactions, reports, and functions that the role's user requires and nothing more (principle of least privilege).
- Single Sign-On (SSO): SAP supports SSO solutions to simplify user access across various SAP and non-SAP systems. SSO reduces the need for multiple passwords and can improve user experience while maintaining security.

To meet compliance requirements, IT personnel need internal policies and guidelines to adhere to various industry and country-specific regulations, such as the General Data Protection Regulation (GDPR) for data privacy in Europe, Sarbanes-Oxley Act (SOX) for financial accountability in the U.S., and others.

Finally, no protection conversation is complete without a discussion about patch management. Security patches are issued monthly by SAP for system updates, and—speed-to-security is essential for an up-to-date SAP system. Cybercriminals quickly weaponize SAP bugs; businesses must download SAP patches [2] as soon as they become available to prevent breaches. However, determining the relevant SAP patches from dozens or more recommended every month is another tedious process. To prolong the agony, a Windows-like upgrade process to implement SAP patches will not be forthcoming, even though it has been strongly suggested by the German-speaking SAP user group (DSAG). It is also important to note that implementing the necessary patches is not a panacea; real-time monitoring is still an essential defense.

Detect

Implementing processes and tools to detect cybersecurity events and security-critical activities. Detecting includes identifying unusual activity, continuous monitoring, and implementing incident detection and response capabilities.

Since the NIST framework provides only a generic approach to cybersecurity, SAP customers should constantly tailor their detection controls to their specific SAP operations.

Before abnormal user activity can be detected, SAP administrators need to determine what is normal user behavior. Determining a baseline for normal user behavior involves collecting and analyzing user activities over a period of time. Once a clear pattern of typical behavior is established, deviations from this baseline can be considered abnormalities and potentially indicate unauthorized activities, security breaches, or process inefficiencies.

Administrators can move on to User Entity & Behavior Analytics (UEBA) when the normal baseline is established. Simply put: UEBA understands the user's normal role and identifies abnormal activities by analyzing log data, transaction records, authentication logs, and network traffic patterns. By applying UEBA, SAP administrators will notice improved threat detection, reduced false positive alarms, and more effectively spot insider threats. Finally, complementing UEBA services is Violation Management, integrated with SIEM and Incident Management processes. Violation Management streamlines the entire detection lifecycle when integrated with Security Information and Event Management (SIEM) and Incident Management processes. The union of these services will provide holistic visibility of security events and a proactive response through SIEM's real-time monitoring capabilities.

Respond

Developing and implementing an incident response plan to manage cybersecurity events. This plan includes developing procedures for responding to incidents, defining roles and responsibilities, and communicating with stakeholders.

Defining procedures, roles, and responsibilities entails elevating the integration of SIEM and Incident Management deeper into the organizational structure behind it. Essential "guidelines" or "protocols" should dictate the response to an SAP incident, designating responsibility and outlining standard actions during disturbances. Focusing on SAP operations and synchronizing them with other elements and technological frameworks within the broader enterprise, such as Network and Infrastructure Management, is crucial. It's important to note that, even if IT personnel notice unusual activities at the SAP level, the most effective countermeasure might be addressing the network or firewall tier first.

While SAP roles and responsibilities and incident management procedures are well defined within SAP operations, SAP customers should focus on aligning them with the IT organization. Setting up these integrations is challenging due to their cross-departmental nature. Successful incident response involves transcending isolated thinking since threats often span multiple technologies.

Recover

Establishing processes and procedures to restore systems and data after a cybersecurity event within the recovery function. The recovery process includes developing and testing a disaster recovery plan, analyzing lessons learned from incidents, and taking steps to improve resilience. A disaster recovery plan has two essential parts: Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

As the name implies, RTO aims to calculate how much time is required to recover quickly—the lower the time to recover, the higher the cost. RPO represents a point in the past to which a system will be restored. RPO's objective is to ascertain the duration between data backups and gauge the potential volume of data at risk of being lost between those backups should a catastrophe occur.

SAP HANA leverages backup, storage replication, and system replication to perform disaster recovery.

According to SAP's blog: [3]

- Data backup in SAP HANA is written into the disk from memory. It can only be performed when the database is online and supports Data backup (savepoint) and log backup (redo log) methods.
- The storage replication process can be synchronous or asynchronous, depending on the distance between the primary and the standby SAP HANA system. The synchronous transfer is used for shorter distances, whereas the asynchronous method is used for longer distances. SAP suggests you use synchronous replication as it gives more performance, and even the slightest chance of data loss is removed.
- SAP HANA system replicates all data to a secondary system. Once the system replication is enabled, each server process on the secondary system establishes a connection with its primary counterpart and requests a snapshot of the data. SAP HANA system replication has less RTO and is faster than storage replication.

SAP landscapes and the disaster recovery plan are quite complex. Therefore, SAP customers should consider engaging with dedicated experts and consulting firms specializing in this topic.

By following the NIST CSF framework, organizations can better understand their cybersecurity risks, implement controls and best practices, and improve their resilience to cyber-attacks. Fortunately, third-party tools for SAP can significantly reduce this process by providing a faster route to security.

Implementing effective cybersecurity practices and choosing the best tools to support the strategy requires careful planning and execution of the cybersecurity program with the framework as a guideline. By adopting the NIST CSF, SAP customers can improve their cybersecurity posture in a structured and systematic way, ensuring that their security measures are sufficient and current.

Is Securing Generative AI Just Securing the Cloud?

By John Yeoh - Global VP of Research, CSA

Artificial Intelligence (AI) has been a part of business and security applications for years. This past year has seen Generative AI (GenAI), a subfield that uses AI disciplines of machine learning and deep learning techniques, take off as one of the most exciting technologies available to the public in quite some time. GenAI technologies themselves are also not new (see Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs)). However, the use of the cloud has seen an emergence of technologies leveraging the availability, scalability, and computing capabilities of major cloud services. What makes GenAI different from other emerging technologies and trends we've seen lately is the availability and ease of using GenAI tools and integrating GenAI functionality into existing applications. The interactive ability and "co-pilot" functions are changing how we ingest data, utilize business applications, and implement cybersecurity.

An Executive Order (EO) on AI from the President of the United States was issued to help establish standards for AI safety and security, with American privacy and civil rights at the very top of its priorities. In anticipation, industry groups have been working hard to address the key components of the EO, addressing gaps and critical areas of AI and the cloud that the industry is seeing for challenges in the present and future.

Generative AI technologies are built on top of foundational models, such as Large Language Models (LLMs), using intensive data collection, processing, training, and computational resources readily available in cloud services. The leading Frontier GenAI models are hosted in and supported by the major hyperscaling Cloud Service Providers (CSPs). The cloud has become the vehicle for hosting and deploying Generative AI capabilities. Securing cloud operations and platforms becomes foundational in developing, deploying, and running AI services.

While securing GenAI and cloud environments involves unique challenges, the fundamental principles of cybersecurity apply to both. These include ensuring data privacy, managing access control, maintaining compliance, and preparing for threats and disruptions. Cloud access control will involve several layers for GenAI models, including access to raw data sets, training, tuned data, and processing. Operational resilience and business continuity in each layer will allow GenAI models to grow and adjust to new data utilizing the cloud for scalability and flexibility. Biases and privacy corrections must be re-trained within these models, requiring resource-intensive computational power in the cloud. Data privacy and protection will be paramount at each layer in the encryption of data and the authorization of users, systems, and devices accessing them. New compliance and regulatory requirements will add to the complexity of building and operating GenAI systems. Threat detection and response, continuous monitoring, and other cybersecurity practices will play roles in securing GenAI and leveraging GenAI to enhance these areas.

The above is far from an exhaustive list of considerations, as the convergence of AI and the cloud will likely lead to more shared security practices and strategies. Both involve managing and protecting digital technologies and business data in a complex and interconnected environment. As technology advances, GenAI may be just the evolution of the cloud as both integrate seamlessly into business and daily lives.

CSA will play a pivotal role in conducting research and building content such as AI threat modeling, AI governance documentation, and AI security controls mappings. With how quickly the entire realm of AI and underlying models are growing, it is imperative to begin working on realistic approaches to this technology as soon as possible. By bringing volunteers from across the globe, from multiple areas of expertise, CSA aims to lock down concepts and guidelines that everyone can benefit from.

Improving Cybersecurity for SAP: A Quick Guide to Adopting the NIST Cybersecurity Framework (continued)

continued from page 12

Summary

In conclusion, cybersecurity is critical to enterprise applications. The National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) to provide guidelines and best practices for improving cybersecurity. Moreover, as the NIST CSF is a widely recognized and accepted cybersecurity framework, it serves as a benchmark for assessing the effectiveness of cybersecurity programs across many industries. SAP customers can benefit from the NIST CSF by evaluating their cybersecurity posture, identifying gaps, and developing a plan to improve their cybersecurity capabilities. However, as the NIST CSF is a generic framework, it needs to be mapped to the SAP specifics and language to implement cybersecurity measures in SAP operations. Third-party tools for SAP can significantly reduce the process of mapping the necessary controls to existing SAP operations or establishing missing controls, providing a faster route to security. With careful planning and execution of the cybersecurity program with the framework as a guideline, organizations can implement effective cybersecurity practices and choose the best tools to support their strategy.

About the Author

Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at SecurityBridge–a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as a SAP technology consultant at Adidas and Audi.

References

1. Information Technology Laboratory: NIST Cybersecurity Framework, (https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework)
2. SecurityBridge: Patch Systems To Eliminate Known Vulnerabilities, (https://securitybridge.com/patch-management-for-sap/)
3. SAP: How to Plan for Disaster Recovery with SAP HANA by Akash Kumar, (https://blogs.sap.com/2015/11/13/how-to-plan-for-disaster-recovery-with-sap-hana/)

ISSA JOURNAL

Regulation, Public Policy, And Law · Preparing The Next Generation Security Professional · Political Dimensions Of Cybersecurity: Elections, Cyberwarfare · Cryptography/ Quantum Menace · InfoSec Toolbox: Basics To The Bleeding Edge · Security Vs Privacy Tug Of War · Disruptive Technologies · Security Paradigms In The Cloud · The Business Side Of Security · Big Data/Machine Learning/Adaptive Systems · Looking Toward The Future Of InfoSec

Write for your ISSA Journal…

- *Advance your career*
- *Gain chapter, national, and global recognition*
- *Help others benefit from your expertise*
- *Indexed in EBSCO database*

- **Monthly topics**
  Expanded theme descriptions here.
- **Choose your own topic**
  Have a different InfoSec topic in mind? Go ahead and submit it.
- **Mentor program**
  We will pair you up with an experienced writer with Friends of Authors

It's Your Journal – Contribute Your Knowledge & Expertise

News from the Foundation

Year-end 2023 is fast approaching! Don't forget to make your tax-deductible (US) donation to The Foundation. Founded in 2003 by the ISSA International Board as a separate, 501(c)(3), public charity, ISSAEF is qualified to receive tax bequests, devises, transfers or gifts to foster and support education and training in cyber security and related fields. Ending this, our 20th anniversary, year to-date the Foundation has given out 37 scholarships and 31 Chapter-sponsored scholarships. Your donations make a tremendous difference in the lives of future cyber security professionals. Contribute today on our website: www.ISSAEF.org/donate.

Warmest wishes of the season from the ISSAEF Directors, Foundation volunteers and the students, who are grateful to ou and the ISSA for your continued support!

As announced in last month's Journal, this year The Foundation again challenges the chapters to a contest designed to encourage friendly competition between chapters, while raising funds in support of the ISSAEF's mission, e.g. to provide scholarships to those studying cyber security. The contest runs from Giving Tuesday, (November 28, 2023,) until the end of June, 2024. Chapters contributing the most, by chapter size (number of members,) will be announced at the 2024 Awards Gala. For more details about the contest, follow us on Facebook or LinkedIn.

Volunteer Opportunities

The Foundation is seeking a Chairperson for its 2024 Scholarship Selectin committee. Want to make a difference? Join a truly dedicated and enthusiastic group! Please email us @: volunteer@issaef.org 20 CPEs is awarded for this volunteer position.

ISSA Community Corner

Wishing you a wonderful holiday season!

The Sixth Annual Life and Times of the Cybersecurity Professional

On September 6th we launched the latest report on The Life and Times of the Cybersecurity Professional. There is valuable information for you to use as a guide for budget, planning, and next steps in your career.

To see summary and download report:

https://www.issa.org/new-research-from-techtargets-enterprise-strategy-group-and-the-issa-reveals-continuous-struggles-within-cybersecurity-professional-workforce/

Stay tuned for the launch of our seventh annual survey. Please take the time to answer questions. Your thoughts and opinions are important to our organization and the cybersecurity industry.

Cyber Executive Forums

The Hilton Clearwater Resort and Spa. Clearwater, FL. Feb 22 & Feb 23, 2024

To find our more or apply to attend:

https://www.issa.org/event/february-cyber-executive-forum-2024/

Looking for Journal Authors and Contributors

Want to get your thoughts and opinions published? We are looking for you!

- Share your wisdom and expertise through thought leadership articles.
- Gain peer recognition.
- Add to your professional portfolio.
- Possible CPE credits for your cybersecurity certifications.

https://www.members.issa.org/page/journal-contribute

ISSA Chapter Leader Meetings

Mark your calendars for the 2024 Chapter Leader's Meetings

- January 19th , 2024 - 1:00 PM Eastern Time - Register Here
- March 15, 2024 - 1:00 PM Eastern Time - Register Here
- May 17, 2024 - 1:00 PM Eastern Time - Register Here

To learn more about all the exclusive opportunities and offers available to you as a member visit: https://www.members.issa.org/general/custom.asp?page=SpecialOffers

There's always a webinar worth viewing either live or On Demand.

Visit and bookmark our events page to see our latest offerings. https://www.issa.org/events/

Visit our past webinars and view them on demand. https://www.issa.org/past-web-conferences/

Join One of The Special Interest Groups Available Only to ISSA Members

- ISSA Privacy SIG Join here: https://www.members.issa.org/members/member_engagement/groups.aspx?id=229802
- ISSA Women in Security Sig Join here: https://www.members.issa.org/page/WomenInSecurity
- ISSA Cyber Resilience Sig Join here: https://www.members.issa.org/page/CyberResilience

Corporate Member Spotlight

"By joining ISSA we recognize the significance of standing alongside the organization partners in shaping the future of cybersecurity. In this interconnected world it's critical for companies to share its expertise and resources to fight cyber threats and ensure safer and more resilient digital future for all"

– Inesa Dagytė, Information Security Manager at Oxylabs

Resources and tools such as ISSA's allow companies to stay ahead of the latest trends and strategies in the cybersecurity field. These assets can be of utmost importance in assisting Oxylabs' Risk and Information Management team in their day-to-day operations of identifying vulnerabilities, responding to incidents, implementing robust preventative measures, and protecting the company's digital assets and reputation.

Established in 2015, Oxylabs is a web intelligence acquisition solution and premium proxy provider, enabling companies of all sizes to utilize the power of big data. Constant innovation, an extensive patent portfolio, and a focus on ethics have allowed Oxylabs to become a global leader in the web intelligence collection industry and forge close ties with dozens of Fortune Global 500 companies.

Companies use Oxylabs ethical premium proxy network and web scraping solutions for various cases, including cybersecurity, threat intelligence, and anti-phishing. Businesses can monitor various websites on a large scale and access geo-restricted content, gaining insights and making data-backed security decisions.

In addition, as market leaders, Oxylabs feels responsibility for the direction the whole industry is taking. As active advocates of an ethical approach to web scraping, the company was one of the founding members of the Ethical Web Data Collection Initiative (EWDCI), dedicated to promoting best practices for the web intelligence industry.

Chapter News

The Central Florida chapter enjoyed their time at the Women in Cybersecurity conference held at ECPI University. They enjoyed great presentations by subject matter experts such as Taryn S. Sunny Wear, and D.Sc. Debbie Hoffman.

The New Hampshire Chapter welcomed guest speakers Luke Bradley and Scott Reid who delivered their talk Data Protection Unveiled: Beyond Backup to Business Continuity. The insightful and motivating talk was sponsored by 11:11 Systems

continued on page 22

Hiring Your Next (or First) CISO

John C. Checco (President, ISSA NY Metro Chapter) and Steven Kolombaris (CISO, Sotheby's)

This article provides an overview of points to consider when hiring your first CISO.

You are a growing company, and your board (or regulations such as NYS DFS 500) requires you to hire your first CISO. Heed this business management cliché: "Failing to spend time now to do it right will cost you time to do it twice."

A peer who has been a CISO in multiple industries offers the analogy of a landowner who wants a house, so they hire a general contractor. They realize the general contractor is there to achieve that goal by applying knowledge, experience, expertise, capabilities, connections, tools, in-house and external resources. Yet, many organizations hire a CISO without examining either their goals or the CISO's skills but expect to be handed immediately a "Cybersecurity Level Achieved" badge.

CISOs are the general contractors for cybersecurity. They work to achieve an organization's security goals through their own knowledge, experience, expertise, capabilities, connections, tools, in-house and external resources.

Here are our suggestions for doing it right the first time.

Define the CISO Role

Writing and broadly disseminating a job requisition is not your first step. Too often, the job description for the CISO position is left to HR, an external recruiting agency, or written internally by the CTO or other technology-focused executive. This leads to job descriptions that vary wildly from governance, to hands-on firewall maintenance, or reflects a buffet of skills that no one person possesses.

The correct first steps are analysis, comprehension, and reconciliation of the following factors:

1. Board and/or executive committee ask;
2. Regulatory minimum requirements;
3. Needs of the organization;
4. Responsibilities for the CISO;
5. Where the CISO best fits into the reporting structure; and
6. Justifying a compensation package.

Once these six items have been properly vetted and documented, you can work with the executive committee to build the right level of language for the job requisition.

Deconstructing the Board Ask

Although it seems forward-thinking that the board has requested the creation of a CISO role, deeper exploration of the 'ask' is truly needed.

- What factors brought about this request?
    - Internal incident, direct or indirect (with suppliers/partners);
    - Internal risk report;
    - External event or industry tailwind; or
    - Regulatory compliance, recent audits or other examinations.
- What is the board really asking for?
    - Additional business risk governance;
    - Explicit security program; or
    - Other objectives (or checkbox confirmation).
- What is the board expecting to see delivered?
    - Position fulfillment;
    - Regular risk (and risk exception) reporting; or
    - Explicit security initiatives.
- What is the expected reaction if the CISO challenged the board?
    - Board is expecting to be challenged;
    - Board is expecting confirmation, not challenge (narcissism); or
    - Board's security governance committee will work with the CISO through challenges.

Determining Regulatory Scope

Another aspect of the CISO role is the scope of regulatory requirements the organization must comply with regarding information security and data privacy. It is also important to note that regulatory compliance does not make a security program successful.

If your company is a service organization or removed from direct regulatory requirements, understand the impact from your clients' regulatory obligations and align your company's scope using standards such as ISO-2700x and/or SOC2 compliance.

There is a dichotomy where CISOs view that compliance is far below the minimum standard for security, whereas organizations view regulatory compliance as their maximum spend. Deciding what level of control beyond compliance can be afforded to the CISO position is a crucial factor in determining the job's responsibilities.

Organizational Security Roadmap

By the time an organization has decided to engage its first CISO, there may have been an incident or event that triggered this need. This implies that the organization has already gained some realization of its existing security posture.

In developing the CISO role, one must identify and document the status quo, and determine an ideal target state. Given those two endpoints (and assuming your organization could never fully reach this ideal target), the hiring manager should plan alternative paths and first steps needed to bolster the security program.

These paths and steps will define the first two years of the CISO role. Beyond that, we can expect both organizational and environmental changes to mold the CISO role perhaps in a different direction. However, understanding these paths will help vet candidates who understand the roadmap.

Responsibilities of the CISO

Given the detailed nuances of the ask, minimum and maximum requirements (also known as guardrails), and the tentative security roadmap, the hiring manager can define the high-level responsibilities for the newly created CISO position. These can be further broken down into four main buckets:

Governance, Risk and Compliance (GRC)

GRC is the administrative branch of the security team that manages policies and their supporting controls, audits, upward (board) reporting, and maintaining the aggregate risk register.

Security Operations (SecOps)

The Security Operations Team employs security technologies to support the controls, monitor users and networks for anomalous activities, investigates events, and mitigates incidents.

Security Technologies

The Security Technologies Team, which may or may not report to the CISO or CTO, deploys and maintains the tools needed for the other branches to operate effectively.

Business Unit Risk Management (BISO)

The BISO team works with each business unit to assess risks in both operations and development help prioritize security issues with their operational issues, define roadmaps for reducing risk exceptions, work with business leaders to gain budgets for security initiatives, and report on the overall security health of the business unit.

Sanity Check #1: Structuring Exercises

If these structuring exercises–pertaining to scope, roadmap, and responsibilities–do not resonate with your organization, perhaps the role they seek is not that of a CISO. Many times, the title of "*Information Security Officer*" is misused hoping to attract more candidates; but in reality, the organization is looking for skills associated with a *Security Analyst or Policy Manager.*

Aligning the CISO in the organization's structure for success

Defining the material responsibilities of the CISO also means understanding where in the organizational reporting chain those responsibilities will be most successful. Todd Inskeep has analyzed the benefits for each reporting option:

REPORTING	RATIONALE	BENEFITS
CIO	The CIO is responsible for managing and classifying the organization's information.	• Natural tie between security and information. • Peer relationship with CDO (Chief Data Officer)
CTO	The CTO handles the technology infrastructure and operations.	• CISOs get greater exposure to the operations. • Security tooling requires heavy support from the technology team.
CFO	Cyberattacks and data breaches measurably affect the bottom line.	• Provides a fiduciary voice at the leadership table. • CFO better understands the costs of risks.
CRO	Security is an enabler for reducing business risk.	• CRO is already a recognized leader and could help foster security agenda. • Moves security out of CIO/CTO technology-centric organizations, making it clear cyber risk is part of the broader risk management agenda.
GENERAL COUNSEL	GC and CISO have similar incentives to ensure policies enable the company to meet legal obligations.	• General Counsel supports security projects that have a governance/compliance component. • CISO gains exposure to other parts of organization.
CEO / BOARD	The company has a mature security program and security is core to the business.	• Demonstrates management's commitment to the strategic importance of the CISO's role. • Working closely with the CEO ensures alignment of security with strategic business objectives. • Provides CISO positional authority to drive a security agenda. • CISO is positioned equal to other (revenue-generating) parts of the business, increasing ability of prioritizing security in those areas.

REPORTING	RATIONALE	BENEFITS
BELOW C-LEVEL	CISO is an operational role, rather than an executive role.	• Ability to work closely with operational teams to get projects done without layers of overhead.

If the CISO will be the main communicator of incidents to the board, then subsuming them under any other CxO is counter-productive to their ability to enact change. For example, if your most important asset was rendered unusable, would the top-level CxO accept responsibility, or does it fall on the CISO to mitigate? If the audit/regulatory (or even client) confidence does not clearly involve the CISO in the planning stages but is required to deliver, can that CISO effectively manage without authority?

Positioning the CISO for success also means positioning the CISO for authority and responsibility. Unfortunately, many top-level CxOs may feel that giving the CISO equal share in leadership means diluting their own budgets and authorities; political fiefdoms are alive and well in many organizations.

Rightsizing the CISO compensation package

CISO–or any executive–compensation is based on both responsibilities and expertise required to execute those duties. As a hiring manager, do not fall into the falsehood of "aligning compensation with the market" or "restricting compensation based on internal senior management pay ranges." Although both factors play a key role in determining compensation, there are other issues that should allow a candidate to measure above the corporate-defined salary range:

- Experience in executing similar objectives in other industries;
- Demonstrable expertise in your organization's industry;
- Reputation of the candidate amongst their peers;
- Delivery of management business objectives (MBOs) based on knowledge; and
- Ability to lead culturally within the political realm of the organization.

In short, if your organization cannot compete financially, this may show a more systemic problem than cybersecurity.

Sanity Check #2: Positioning Exercises

If these positioning exercises–reporting chain and compensation–are not within your control, the role they seek is not that of a CISO but of a lower role such as security operations manager.

Job Requisition

At this point, one can document a robust job description. This first pass at documenting the role is extremely important but should be kept internally. The externally facing job description needs to be direct, clear, and concise. The elements of an attractive CISO job description include:

- Organization purpose for the position
- Primary responsibilities (abridged)
- Reporting structure (level and reporting purpose)
- Collaboration requirements (upward, downward, and lateral)
- Compensation factors (i.e., executive contract or employee salaried)

Executive Candidate Selection

Unlike other executive roles, the CISO needs to communicate complex concepts and issues tangibly to allow boards, business units, and operational teams to own cybersecurity and make educated decisions. As such, selecting CISO candidates is much more difficult, as AI-based recruiting filters focus on hard skills rather than leadership skills.

To get quality candidates, it is worth the cost to engage an executive search firm that specializes in placing CIOs/CDOs or CSOs/CISOs. Avoid agencies purporting to place technology-focused roles such as CTOs and those focused on sales or marketing.

Your priorities determine which qualities you want to see in the next leader, but other stakeholders in the hiring process may have their own goals. You are likely looking for someone who can cure certain deficits. The hiring manager (or committee) may look for the best skill sets. Fulfilling both these visions requires a balancing act. But by driving the process, you can exercise a greater influence on the final candidate selection.

Candidate Primary Qualities

The primary qualities to consider include:

- Leadership skills — leaders have an ability to listen and be responsive, as well as to inspire and motivate.
- Organizational skills — every organization has some level of politics that the leader needs to navigate and influence.
- Relevant knowledge and experience — the executive needs a certain level of technical prowess and industry background.
- Cultural fit — look for a leader who can either augment your culture or disrupt it, depending on what your organization needs.

Besides these top qualities, consider secondary ones, such as:

- Management skills to oversee projects and programs
- Administrative skills to develop and manage budgets
- Change-management skills to usher the organization through changes
- Outside knowledge and experience to be innovative

Interviewing Candidates

Traditional interview processes include a phased approach: recruiter, HR, hiring manager, and some team members.

For a role such as the CISO where they will interact across departments and teams, it behooves an organization to allow the candidate to interview with cross-functional leaders and even several board members. This will give a more realistic representation of how the candidate will interact at various levels and demonstrate if they can effectively speak the specific dialect needed for each area.

Diversity & Inclusion

Ensuring diversity equality is important, especially at the senior leadership levels. In a large population, such quotas are beneficial to ensure representation across different experiences; but a mandated quota in a small pool of executives may present challenges to the new CISO whose perceived selection criteria outweigh the true value they bring to the organization.

There is a fine balance between hiring a candidate because they are diverse versus hiring a candidate who happens to be diverse. How does one hire for diversity without the new hire feeling devalued because of diversity quotas? A panel titled "Educating Future Leaders" at the 2020 NCSA conference held in NYC at NASDAQ broached this very subject, providing a thoughtful and interesting approach. The quota need not be in the hiring, but in the candidate pool itself. When there are finalists of equivalent capabilities, hiring for diversity then becomes not only defendable, but hugely beneficial to the organization.

Sanity Check #3: Candidate Pool

If the initial candidate pool is too small (< 3), too broad, or lacks in diversity, it is a red flag for a problem in the job requisition or the resource channels being marketed to. It may be time to revisit and reevaluate the steps that define the role.

Leadership Onboarding

Like succession planning, there needs to be an explicit plan to jumpstart the new CISO. The best way to give the new CISO some traction is to help build the initial relationships both internally and externally. This means allowing the new CISO to absorb some of the hiring manager's political capital as their own.

Lean In: Internal Introductions

Introduce the new CISO to the executive staff and collaborate on an overarching objective for the first 90 days.

Assist in creating the new CISO's memo to the board, outlining the objectives and the associated expectations of each group/department/team to meet those objectives.

Co-create a welcome letter to all groups/teams/members, introducing the new CISO leadership and outlining the initial vision of the security program.

Outreach: External Relationship Introductions

Notify clients/customers of the new security leadership and help schedule strategic customer visits within the first 90 days.

Subsequently, encourage the CISO to meet with any critical partner/supplier leadership.

If the new CISO is coming in from another industry, try to have them meet with industry leadership.

The First 90-Days

Before hiring your first CISO, many security functions–whether or not they were viewed as such–were handled by other leaders, business units, or operational teams.

Assignment

It is in these first 90 days where a CISO needs to identify those security functions and categorize them as either "security governance," "security operations," or "security technologies." The CISO must then navigate what can/should be moved into the various security teams, and what can remain with the existing structure.

Assessment

At the conclusion of the first quarter, the new CISO should be able to:

- Engage an external audit and compare against the new CISO's internal assessment.
    - Ideally, the audit should be an annual recurrence to provide consistency in security posture long term.
- Report on existing security posture, key areas of inherent risk, a rolling risk register, and the impact of existing risk exceptions.
- Present a set of recommendations for reducing inherent risks and removing and/or mitigating risk exceptions.
- Garner congruence on what teams/units own each risk–as the security team cannot own a risk created by another team over which they have no control.

Sanity Check #4: The 90-day Review

The first months of assessing the new CISO hire allow the observation of several factors that signify a successful role:

1. Leadership Traction / Cultural Fit
2. Comprehension / Strategic Direction
3. Communication

Unlike traditional hiring, it is acceptable to dismiss a CISO who causes more destructive distraction than constructive disruption. Finding the right senior executive is not always easy when other parts of the organization do not understand cybersecurity. Every setback is an experience to build on, and you may find that parts of the role's responsibilities were not as important as originally expected, whereas other responsibilities bubble up in priority.

Summary

In hiring a CISO for your organization, do your homework to envision what the role would be in three to five years. Do they enhance the organization's resiliency? Do they follow a good decision-making process? Are they respected by the board? Do they work well cross-functionally? Are they sought for advice by business units and other business leaders? Are they part of the corporate family? Will they have a seat at the adult table or be relegated to the kids' table?

The answer to these questions will put you on the path to a successful hire.

About the Authors

John C. Checco

John C. Checco is the president of the ISSA New York Metro chapter. He previously led the financial services practice at Proofpoint and served as a security executive at several large financial institutions.

Follow, connect with, and read more from Checco at https://www.linkedin.com/in/xn--fci/

Steven Kolombaris

Kolombaris is an experienced CISO and Board Member dedicated to information security. A design thinker fostering talent and guiding startups, he is the CISO at Sotheby's. Prior executive roles includes Blue Origin, Bank of America, JP Morgan, and Apple. He is an NYU and Stevens Institute alum, with an executive MBA (PLD) from Harvard Business School.

Follow, connect with, and read more from Kolombaris at https://www.linkedin.com/in/steven-kolombaris.

Chapter News (continued)

continued from page 17

The Puget Sounds chapter welcomed a packed house for dinner and their chapter meeting and enjoyed talks from representatives of Cyversity.

Holiday Party Update - Caroline:

Where: The Golf Club at Newcastle

When: December 14, 2023

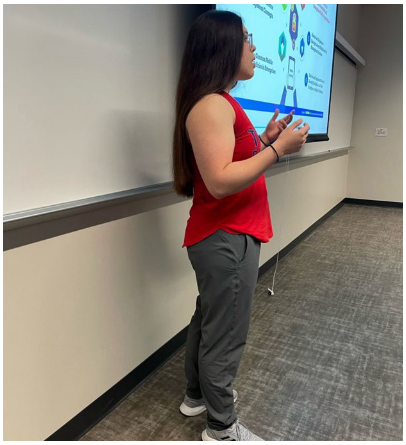
Volunteers: Reach out to Caroline Song if you are interested in volunteering

Sponsorship: Seeking sponsors, please contact Mark Petersen to discuss sponsorship opportunities

Association Collaborators:

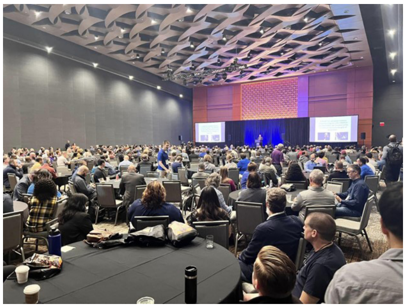
ISSA France published "Snake News" manga to help kids navigate the complex landscape of fake news on the internet and in social media.

North Texas Collin College communication officer Amanda Jordan, spoke to the Cybersecurity Management Practices class at Collin College to spread the word on how much ISSA membership has helped her cybersecurity career.



Association News

The ISSA Raleigh Chapter wrapped up a very successful Triangle InfoSeCon! Guests enjoyed top notch speakers, a Capture the Flag, and a fun AfterDark networking event.



Thales Solutions Engineer, Matthew Olive was the speaker for Boise ISSA Chapter's November luncheon at Cottonwood Grille in Boise. They had an excellent turn out and Matt Olive was terrific in engaging the group in his lively presentation.

The South Texas chapter enjoyed a talk about AI during their monthly lunch.

ISSA
Information Systems Security Association

The Cyber Executive Forum is a peer-to-peer event – Members can feel free to share concerns, successes, and feedback in a peer-only environment.

ISSA Cyber Executive Membership Program

The role of information security executive continues to be defined and redefined as the integration of business and technology as it evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will shape the profession.

The Information Systems Security Association (ISSA) recognizes this need and created the exclusive Cyber Executive Membership program to give executives an environment to achieve mutual success. Connecting professionals to a large network of peers, valuable information, and top industry experts the program is a functional resource for members to advance personal and industry understanding of critical issues in information security.

Membership Benefits

- Free registration at four Cyber Executive Forums per year, including lodging for one night and all meals at each Forum
- You'll be part of an effective forum for understanding and influencing relevant standards and legislation
- Extensive networking opportunities with peers and experts on an ongoing basis
- Direct access to top subject matter experts through educational seminars
- CPE credits you earn will be automatically submitted
- Vendor Influence: A unified voice to influence industry vendors
- Online Community: Privileged access to our online community

Visit Cyber Executive Forum for more information or to register for the Forum.

Asia Pacific

Bangladesh
Chennai
Dehradun
India
Philippines

Canada

Alberta
Ottawa
Quebec City
Vancouver

Europe

Brussels European
France
Germany
Italy
Netherlands
Poland
Romania
Spain
Switzerland
Turkey
UK
Ukraine

Latin America

Argentina
Barbados
Bolivia
Brasil
British Virgin Islands
Chile
Colombia
Ecuador
Peru

Middle East

Bahrain
Egypt
Iran
Israel
Kazakhstan
Kuwait
Qatar
Saudi Arabia

USA

Alamo San Antonio
Blue Ridge
Boise
Buffalo Niagara
Capitol of Texas
Central Alabama
Central Florida
Central Indiana
Central Maryland
Central New York
Central Ohio
Central Plains
Central Texas
Central Virginia
Charleston
Charlotte Metro
Chattanooga
Chicago
Colorado Springs
Columbus
Connecticut
Dayton
Delaware Valley
Denver
Des Moines
East Tennessee
Eastern Idaho
Eugene
Fayetteville/Fort Bragg
Fort Worth
Grand Rapids
Grand Traverse
Greater Augusta
Greater Cincinnati
Greater Spokane
Hampton Roads
Hawaii
Inland Empire
Kansas City
Kentuckiana
Kern County
Lansing
Las Vegas
Los Angeles
Metro Atlanta
Mid-South Tennessee
Middle Tennessee
Milwaukee
Minnesota
Motor City
National Capital
New England
New Hampshire
New Jersey
New York Metro
North Alabama
North Dakota
North Oakland
North Texas
Northeast Florida
Northeast Indiana
Northeast Ohio
Northern Colorado
Northern
Virginia (NOVA)
Northwest Arkansas
Northwest Ohio
Oklahoma
Oklahoma City
Orange County
Phoenix
Pittsburgh
Portland
Puerto Rico
Puget Sound (Seattle)
Quantico
Rainier
Raleigh
Rochester, NY
Sacramento Valley
San Diego
San Francisco
Silicon Valley
South Bend - Michiana
South Florida
South Texas
Southeast Arizona
Tampa Bay
Tech Valley Of New York
Texas Coastal Bend
Texas Gulf Coast
Triad of NC
Upstate SC
Utah
Ventura County
West Texas
Wyoming
Yorktown

ISSA.org => Chapters