

ISSUE 6

VOL. 22

SEPTEMBER-OCTOBER

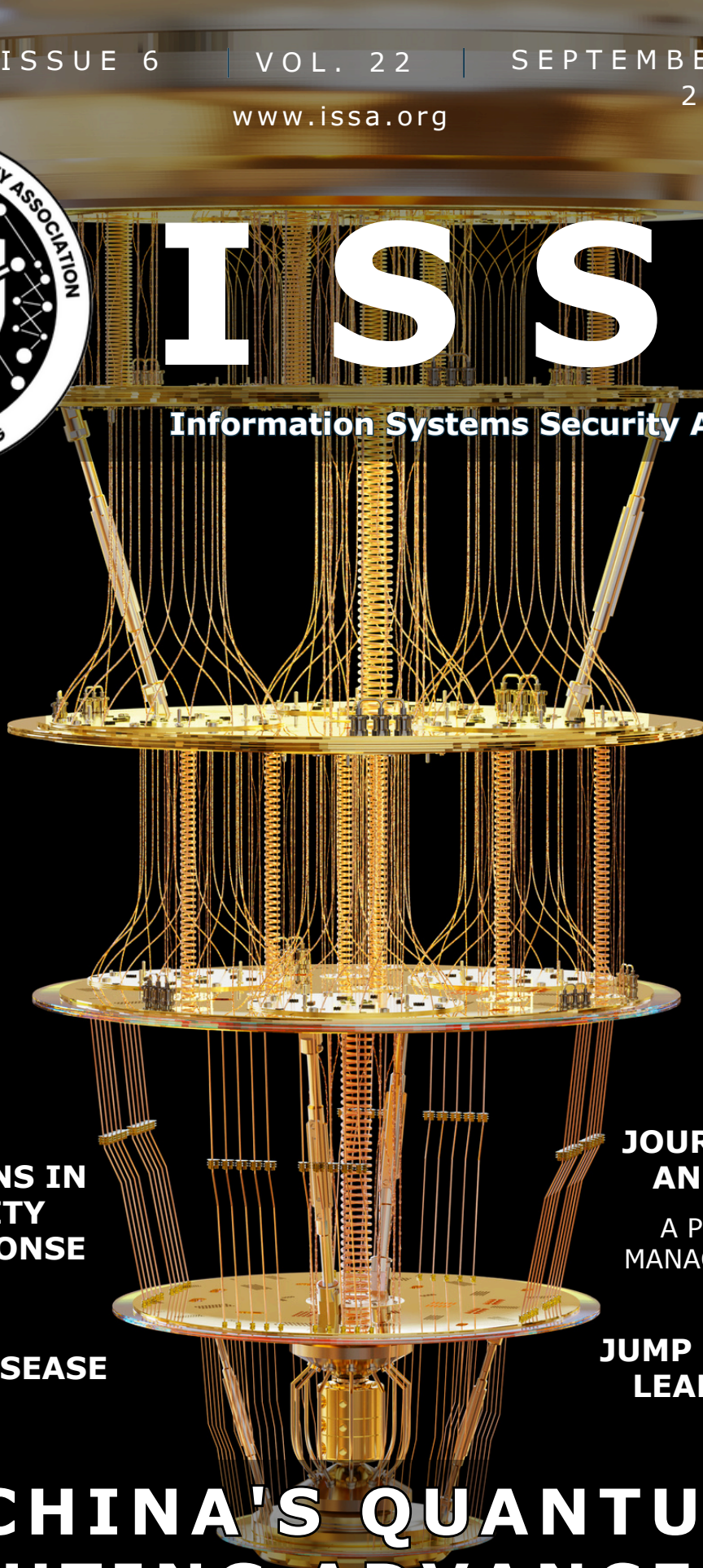
2024

www.issa.org



ISSA

Information Systems Security Association



**ETHICAL
CONSIDERATIONS IN
CYBERSECURITY
INCIDENT RESPONSE**

**JOURNEY OF PRIVACY
AND PROTECTION**

**A PRIVILEGED ACCESS
MANAGEMENT PERSPECTIVE**

AI AND COST DISEASE

**JUMP START A CHAPTER
LEADERSHIP BOARD**

CHINA'S QUANTUM COMPUTING ADVANCEMENTS AND ECONOMIC IMPACT

Advancing Information Security, Empowering Professionals



ISSA
40 YEARS STRONG

Follow Us On:



The Information Systems Security Association (ISSA)® is a non-profit, global community of information security professionals and practitioners. With a mission to foster the exchange of best practices in information security management, ISSA facilitates educational events, publications and networking platforms for security experts worldwide.

Serving as a vital resource, ISSA supports professionals at every career stage, offering resources to enrich their knowledge, skills, and professional development. As the preferred community for information security professionals, ISSA is committed to fostering individual growth, mitigating technology risks, and safeguarding vital information and infrastructure.

ISSA opens doors to network with industry leaders, dedicated professionals, and top minds in the field. **Membership provides access to:**

- A global network of chapters for forging lasting connections with like-minded professionals and addressing common business concerns.
- Opportunities to boost professional stature by speaking at events or contributing to the ISSA Journal.
- Access to information via the ISSA website, online e-newsletters, and the bi-monthly ISSA Journal.
- Exclusive event rates for members and discounts on various security resources and events.
- CPE credits through chapter meetings, ISSA Web Conferences and Journal subscriptions
- Leadership roles within chapters and international councils and Special Interest groups and work groups.

www.issa.org

CONTENTS

VOLUME 22 - ISSUE 6

FEATURE FOCUS

07 China's Quantum Computing Advancements and Economic Impact

An Assessment of the Chinese Communist Party's "Made in China 2025" Initiative on Technological Advancement and Economic Development in the area of Quantum Computing.

SUPPLEMENTARY SEGMENTS

18 Straining Our Security

Straining our security: Shifting the security, developer, and developmental practitioner professions towards building an understanding of technology component security and cybersecurity practitioner roles.

25 Ethical Considerations in Cybersecurity Incident Response

This study explores ethical considerations in cybersecurity incident response, focusing on protecting digital identities, balancing privacy and security, ensuring regulatory compliance, and promoting fairness and transparency. It emphasizes the importance of ethical practices in maintaining cybersecurity and stakeholder trust in the digital age.

28 Journey of Privacy and Protection: A Privileged Access Management Perspective

This article explores the critical role of Privileged Access Management (PAM) in addressing privacy challenges in cybersecurity. As a Security Engineer Lead, I discuss navigating complexities such as cloud adoption and regulatory demands (GDPR, CCPA). Key strategies like zero trust, least privilege, and robust monitoring are pivotal in mitigating risks and ensuring compliance. Lessons emphasize adaptability, collaboration, and transparency to enhance privacy protections.

DEPARTMENTS

05 PRESIDENTS LETTER

Welcome letter from ISSA International's new Board President Jimmy Sanders, including plans and strategies to grow ISSA!

06 EDITORS CORNER

31 EVENTS: ISSA, INDUSTRY & CHAPTER

Global Chapter & Meeting Events and ISSA Specific Events

SPOTLIGHT

11 Chapter Spotlight

Jump Start a Chapter Leadership Board

VOICES

14 CRYPTO CORNER

AI and Cost Disease

15 CRYPTIC CURMUDGEON

Generative/LLM Bio

16 THE CYBER LIBRARY

William J. (Jay) Carson shares his reviews on the workings of Damien Van Puyvelde and Aaron F. Brantly's "Cybersecurity: Politics, Governance and Conflict in Cyberspace" and Dr. Chase Cunningham's "Cyber Warfare - Truth, Tactics, and Strategies: Strategic Concepts and Truths to Help You and Your Organization Survive on the Battleground of Cyber Warfare".

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.

➔ International Board of Directors

President

Jimmy Sanders

Vice President

Deb Peinert

Secretary/Chief of Operations

Lee Neely

Treasurer/Chief Financial Officer

David Vaughn

Board of Directors

Dr. Curtis Campbell

Mary Ann Davidson

Laura Harder

Stefano Zanero

Connie Matthews

Gene McGowan

John Johnson

➔ Service Directory

Website

Blair Patterson

blair.patterson@issa.org

Chapter Relations

Shaif Salehin

shaif.salehin@issa.org

Member Relations

Carolina Anota

carolina.anota@issa.org

Executive Director

Anne Rogers

anne.rogers@issa.org

Sponsorships & Journal Advertising

Roxanne Pirooz

roxanne.pirooz@issa.org

➔ Advertiser Index

ISSA Socials 06

ISSA Online Webinars 24

ISSA Chapter List 13

ISSA Board 32

ISSA Mission Statement



ISSA is a nonprofit organization for the information security profession committed to promoting effective cyber security on a global basis.

- Being a respected forum for networking and collaboration.
- Providing education and knowledge sharing at all career lifecycle stages.
- Being a highly regarded voice of information security that influences public opinion, government legislation, education and technology with objective expertise that supports sound decision-making.

Want to Become an ISSA AIM Partner?



What is AIM Program?

Building a Cybersecurity Workforce Through Industry Alliances for Apprenticeships, Internships, and Mentorships (AIM)

The purpose of the ISSA International Apprenticeship, Externship, Internships, Mentorships (AIM) Program is to be an influential force that positively contributes to the Cybersecurity Workforce profession.

To find out more and become a partner, visit:
<https://www.issa.org/what-is-aim-program/>



To the Valued ISSA Member!

The ISSA International Board and I are excited to share our vision of the future of ISSA at our 2024 ISSA Annual Membership Meeting on September 26, 2024. There will be many announcements, new initiatives, and ideas that ISSA International has been working on. Vice President Deb Peinert has been working on ISSA chapter policies and outreach. David Vaughn, our CFO, has been working with the finance team to ensure we align fiscal discipline with the goals of ISSA. Lee Neely, the ISSA COO, has been working with our IT Team and coordinating with our Executive Program Director, Anne Rogers, to advance our technology infrastructure and modernize technological resources for our members. In addition, they have been working to resolve some of the information technology issues that have been affecting our members.

As the president of ISSA International, I pledged to be a person of action and community. Currently, local chapters provide a great sense of community and value to local members. I am excited to announce an amazing lineup of ISSA International initiatives.

ISSA will kick off October 2024 with discounts for all members, new and existing. We want everyone to become new and returning members. Starting October 1, 2024, the details for the discounts will be sent via newsletters, LinkedIn, and other social media outlets.

I have had the opportunity to talk to many members, chapter leaders, and various security professionals globally. Furthermore, I have been working with the ISSA International Board on engaging initiatives at the regional and chapter levels. In addition to the terrific board of directors and Executive Program Director, I am excited to announce the formation of the ISSA International Presidential Council Advisors. This group is comprised of Dutch Schwartz, Olivia Rose, Dorin Baniel, Aaron Rinehart, Terence Jackson, Nathan Hamiel, Cailin Sullivan, Olivia Herriford, Todd Thiel, Kendrick Trotter, Isiah Walters, and Jamal Mayo. This dynamic group will be essential in providing unfiltered advice and knowledge.

ISSA International is an organization that strives to be a leader in the ever-changing information technology landscape. I am excited to announce the formation of the Emerging Technology Special Interest Group. An amazing group of technology leaders spearheads this group: Dutch Schwarz, Aaron Rinehart, Terrence Jackson, Nathan Hamiel, and Todd Thiel. This group is committed to pushing technological and thought-provoking conversations via webinars, journals, and web articles.

Our community has a vast group of amazing members and professionals. We will now have a central location to share our journey and vast knowledge within our career. This central location is titled "Experiences". I am excited to announce the initial creation of two experiences with more coming, "World of Cyber Venture Capital" and "The ATLAS" (All Together Learning and Sharing).

Dorin Baniel will be moderating and coordinating the World of Cyber Venture Capital experience. In the experience, "World of Cyber Venture Capital," she has gathered an amazing array of articles, journals, and webinars with leaders within the Cyber Community to share with ISSA members.

Cailin Sullivan and Olivia Herriford will be the moderators and contributors for "The ATLAS." This will be the opportunity for members to share their experiences as they traverse their careers, whether you are new to information security or a practitioner with several years of experience.

Lastly, the president of a community needs to be transparent and available to our ISSA community consistently. In addition, I want to be able to involve other security leaders and ISSA members. There will now be a new initiative titled "Third Thursday" to further these ideas. This will be an open online "Office Hours" for Technology Leaders to answer audience questions from 11 am-1 pm Eastern on the Third Thursday of the month, holidays permitting. ISSA will provide a link to these meetings via our website, newsletter, and LinkedIn. The first "Third Thursday" will be on September 19, 2024. I will be joined by Miki Bellon and Dr. Keith Clement, two amazing community activists involved in improving the technology curriculum and exposure for post-college, college, and high-school students.

These announcements are only the prelude. I am excited to share these exciting announcements and several other ISSA International Board initiatives, programs, and collaborations.

Jimmy Sanders, President
ISSA International Board of Directors



president's open office

The ISSA International president believes that a president of a community needs to consistently be transparent and available to our ISSA community. In addition, the president should be willing to involve other security leaders and ISSA members. To further these ideas, there will now be a new initiative titled President's Open Office. This will be an open Zoom "Office Hours" for the President of ISSA International and Technology Leaders to answer audience questions 11am-1pm Eastern. ISSA will be providing a link to these meetings via our website, newsletter, and via LinkedIn a week before each session.

To be held the 3rd or 4th Thursday monthly.

Editors Corner



Jack Freund

Editor, ISSA Journal
NC Charlotte Metro Chapter

As we move through the latter half of the year, it's always a good time to reflect on the fast-evolving nature of the cybersecurity landscape. The challenges we face continue to grow in complexity as threat actors advance in sophistication and technology evolves rapidly. However, the resilience and innovation shown by cybersecurity professionals around the globe give us confidence that we can continue to rise to meet these demands. The importance of security is not only a matter of protecting data but also safeguarding the very infrastructure that fuels global economies and everyday life. Our role in this critical endeavor has never been more vital.

This issue brings an array of insightful articles that highlight current industry challenges and advancements. Our feature article, "An Assessment of the Chinese Communist Party's 'Made in China 2025' Initiative on Technological Advancement and Economic Development in the area of Quantum Computing," authored by Celeste Clarke, Hanh Nguyen, Sahrash Tanveer, Zachary S. Risseuw, and Brian K. Ngac, all from George Mason University, provides an in-depth look into China's ambitious plans for technological leadership. This analysis delves into how the "Made in China 2025" initiative is impacting quantum computing, a critical area with far-reaching implications for both national security and global economic competition.

In addition to this comprehensive study, we also present several thought-provoking articles. "Straining Our Security" explores the importance of cross-discipline collaboration between security professionals, developers, and practitioners to enhance technology component security and to better define roles within the cybersecurity domain. We also take a closer look at ethical decision-making in the article, "Ethical Considerations in Cybersecurity Incident Response," which discusses how ethics play a pivotal role in guiding incident response actions. Finally, "Journey of Privacy and Protection: A Privileged Access Management Perspective" gives us valuable insight into how privacy and privileged access intertwine in the effort to safeguard sensitive data.

As always, this issue also includes our regular columns and book reviews, which offer practical tips, expert analysis, and valuable recommendations to keep you informed and engaged.

Thank you for your ongoing support of the ISSA and this Journal. We encourage you to consider submitting your own articles for future editions—if you need assistance with developing an idea or article, please don't hesitate to reach out to us. We look forward to seeing you again in our November/December issue.

Warm regards,

Jack Freund, Ph.D.
ISSA Distinguished Fellow
Board Director, ISSA Education Foundation
Editor, ISSA Journal

➔ Editorial Advisory Board

Garrett Felix, ISSA Fellow

Jack Freund, PhD, Distinguished
Fellow - Chairman

Michael Grimala, PhD, Fellow

John Jordan, Senior Member

Enoch Anbu Arasu Ponnuswamy

Kris Tanaka

Disclaimer:

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.

Follow ISSA on Social Media



Information Systems
Security Association
(ISSA)



@ISSAINTL

FOLLOW

AN ASSESSMENT OF THE CHINESE COMMUNIST PARTY'S "MADE IN CHINA 2025" INITIATIVE ON TECHNOLOGICAL ADVANCEMENT AND ECONOMIC DEVELOPMENT IN THE AREA OF QUANTUM COMPUTING

**By: Celeste Clarke, Hanh Nguyen, Sahrash Tanveer, Zachary Risseuw, and
Brian K. Ngac, Costello College of Business, George Mason University**

Unlike in Western countries where bipartisan concept exists in the government, the governments in China, Vietnam, and North Korea follow only one Communist party. The Communist government holds the highest power where they issue laws, collect taxes, and control most of the major industries of the country such as mineral mining, oil drilling, banking, export, and import. Each Communist government often launches 5-year or 10-year initiatives to boost different sectors during a certain period of time. The "Made in China 2025 (MIC 2025) Initiative" is one of China's planned initiatives to help boost their economy and defense system. According to McBride and Chatzky, "Made in China 2025 is the government's ten-year plan to update China's manufacturing base by rapidly developing ten high-tech industries. Chief among these are electric cars and other new energy vehicles, next-generation information technology (IT) and telecommunications, and advanced robotics and artificial intelligence" [1]. This state-led 10-year plan aims to develop the country's industrial base by advancing high-technology production and implementation while strengthening and protecting its economy. While the MIC 2025 focuses on ten key high-tech sectors ranging from bioengineering to maritime engineering, the focus in this paper will be on quantum computing. We have conducted our research, analysis, and completed our writing in collaboration with the U.S. Cyber Command and thus, we will analyze this sector from a cyber environment perspective. The Office of the Director of National Intelligence (ODNI), in its 2024 Annual Threat Assessment, asserts that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks" [2]. With this in mind, we seek to evaluate the pertinent topic of China's cyber advancement via MIC 2025 on the global geopolitical landscape with the focus on quantum computing capabilities.

Quantum computing is known as supercomputing and are also understood "as specialized computers that can solve specialized problems set at an extremely fast rate such as complex optimization problems or molecular modeling, that current computers cannot" [3]. It uses qubit instead of bit which is used in traditional computing. Even though quantum computing is not fully developed yet, many nations have entered the race to develop their own quantum computing capabilities which can serve in many sectors from medicine, business, science, computing, and communication to national defense systems. According to Penney, "Quantum computers may also be more efficient and faster at highly complex artificial intelligence/machine learning algorithms, but there are also many use cases where classical (or traditional) binary computing delivers faster and more accurate solutions" [3].

Investment and achievements

China has invested billions of dollars in Quantum computing in recent years. They have attracted many physicists and scientists around the world to help them build complete made-in-China quantum computers by heavily funding quantum computing sector. For example, the United States committed to fund an additional \$1.8B in quantum computing while China also announced that it would invest \$15.3B [4]; however, according to Freedberg, maybe China only invested about \$4B [5]. China's actual investment in quantum computing remains unclear until today.

Quantum computing is a new technology race for many nations. Thus, many startups to giant tech firm have entered this field. According to Dargan, there are 9 major quantum computing companies in China such as Baidu Research, Ciqtek, Huawei Cloud, Origin Quantum, Qasky, Quantumtek, Qudoor, Tencent Quantum Lab, ZTE. They focus on applying quantum computing in "search engines, cloud computing, online business platforms, software solutions, network security, quantum cryptography communications, quantum AI, quantum algorithms and quantum architecture" [6].

The U.S. surpass China in both the number of quantum computing companies and patents: "12 public and 78 private start-up quantum computing companies with over 1086 patents" versus "a dozen companies and 384 patents in China;" and the U.S. has closed 110 quantum computing deals while China only has closed 30 deals [7]. Giant technology firms such as Google, Microsoft, Intel, and IBM have invested dramatically in this field. According to Pichai, the CEO of Google, Google was "the first company" to launch a strong complete quantum computer in 2019 after "13 years of research and development" [8]. For example, "Google recently achieved quantum supremacy by solving a problem in 200 seconds that would take a classical computer 10,000 years to solve" [9]. In response to this event, China claimed that they have successfully built two complete quantum computers which is much stronger than the one Google built; however, China did not provide any evidence to support their claim.

Quantum computing potential application

Quantum computing has vast promising future applications varying from medical field, business services to national defense system. According to Amerongen, a co-author of NATO's White Paper on Quantum Technologies, the focus of quantum computing will be on "quantum sensing, quantum communication, quantum computing, implications for defense and security" [10].

First, quantum sensing can increase the precision of medical imaging and diagnosis which helps detect any ailment in the early stage, so medical physicians deliver more accurate treatment schedules and medication to shorten the treatment time and save more lives. For instance, "... quantum sensors can detect subtle brain activity changes, aiding in the diagnosis and monitoring of neurological disorders [20]. Similarly, in cardiology and oncology, quantum-enhanced imaging techniques provide valuable insights into heart conditions and cancer detection" [11].

Second, quantum communication used qubit which is more secure than bit in optical fiber cables in traditional internet. According to Amerongen, when hackers try to steal data by interrupting data during its transmission, quantum communication channel will collapse which means hackers cannot steal data since "quantum computing is extremely sensitive to external disturbances" [10]. Quantum communication opens the door for ultra-secure data transmission via the internet since data becomes un-hackable in quantum communication which creates a much safer channel for transferring data in the future.

Third, quantum computing can simulate drug discovery and new materials, solve complicated optimal solutions in logistics and finance. Additionally, it combines artificial intelligence for advanced machine learning and applies to asymmetric encryption algorithm for secure data transmission. "Big technology companies like IBM, Google and Microsoft are racing for 'quantum supremacy', which is the point where a quantum computer succeeds in solving a problem that no classical computer could solve in any feasible amount of time" [10].

Fourth, implications of quantum computing for defense and security are extremely important in any defense system. For instance, according to Smith-Goodson, "Once fully developed, quantum radar could threaten the US lead in stealth technology. That translates into the increased vulnerability of US stealth aircraft such as the B-2 Spirit, F-22 Raptor, F-35 Lightning II, and allied stealth aircraft. Quantum radar might also be able to determine the type of aircraft or the weapons the plane is carrying. It could also compromise US domination over the electromagnetic domain in combat environments" [9].

However, during the 118th Congress Hearing on Current and Emerging Technologies in U.S.-China Economic and National Security Competition, Thursday, February 1, 2024, Freedberg Jr. stated that the U.S. ruled out quantum radar and quantum key distribution (QKD) technologies while China has invested heavily on them. Experts predicts that this could be bad bets for China since "the U.S. military has publicly identified quantum radar as impractical" [5]. He wrote "My own assessment largely agrees with the U.S. DoD's position that QKD and quantum radar are unlikely to deliver significant military operational advantage" [5].

Quantum computing technologies help increase the security and ability of detecting objects in air, land, and water. These technologies will have a huge impact on future economy and defense systems for any nation.

Current Challenges

Quantum computing chips get very hot during their operations. Chinese companies have successfully developed a device called EZ-Q Fridge, which "is designed to provide an ultra-low temperature environment, nearing absolute zero Celsius, crucial for the optimal performance of quantum computing chips" [12]. Chinese companies enjoyed the success of their research and development as it performed well in testing and those companies

have begun deliveries of this refrigerators to their customers starting in the second quarter of 2023; however, there is no evidence about how effective the EZ-Q Fridge are yet.

The U.S. researchers are in testing phase for a new cooling technology for quantum computing. According to Toon, "A new cooling technique that utilizes a single species of trapped ion for both computing and cooling could simplify the use of quantum charge-coupled devices (QCCDs), potentially moving quantum computing closer to practical applications" [13]. This promising technology can be used to produce a cooling system for any device or system that uses quantum chips.

Economic and technology prediction

Although quantum computing is still in its infancy stage, investors around the world have already started investing in quantum computing companies varying from start-ups to giant tech firms. According to Williams, the investment in this market was nearly \$500M in 2021 but it is expected to reach nearly \$1.7B by the end of 2026 [14]. Quantum computing seems to set the run for the fifth industrial revolution. In addition, Bogobowicz et al. predicted that "... the four industries likely to see the earliest economic impact from quantum computing—automotive, chemicals, financial services, and life sciences—stand to potentially gain up to \$1.3T in value by 2035" [4].

Quantum computing application in medical field may lead to advance technologies in treatment and medicine which would draw people to the U.S. for medical tourism. According to Precedence Research, the global medical tourism market is predicted to grow very fast from about \$116B in 2022 to more than \$346B in 2032 [15]. It triples this market value within a 10-year period. Medical tourism has become very popular in the last decade since wealthy people still want to get advanced medical care such as high technology, advanced medicine, and better services. It is one of the most attractive markets that contributes a good revenue to a nation's economy which helps boost other sectors of the economy such as retail, other services, hospitality, and tourism industry.

According to Liu, "In 2022, GlobalData said the U.S. was about five years ahead of China in the quantum computing race. Now, in 2024, the firm considers the two countries as "nearly equal" in the arena" [16]. The quantum computing race is now nearly tied between the U.S. and China; however, the U.S. is behind with around 45 thousand versus China with nearly 58 thousand when it comes to the number of quantum computing talents [4]. Still, we are not sure about the quality of Chinese quantum talents yet.

The post-quantum cryptography (PQC) algorithms standard may be released in 2024. The National Institute of Standards and Technology (NIST) is in its final process to finalize a new standard for PQC communication encryption which cyber experts believe would provide long-term security for cyberspace communication. According to NIST, "The agency has begun the process of standardizing these algorithms — the final step before making these mathematical tools available so that organizations around the world can integrate them into their encryption infrastructure" [17].

Quantum computing threatens our nation's safety. The ability of combining two quantum computers to increase their power imposes a threat to our national defense system. According to Sanzeri, China has proven the "ability of entanglement sub-atomic particles and maintain them over twelve kilometers" which also means that quantum power can be used as a threat to crack standard encryption that our current defense system uses [18].

Recommendations

As mentioned, China surpasses the U.S. in the number of quantum computing talents which means China has more scientists and physicists than the U.S. Therefore, the U.S. should attract more quantum talents starting with nurturing the next generation. For instance, we should distribute more funding to high schools, colleges, and universities by providing excellent mathematics and science education programs to attract more students in this field.

In addition, we should facilitate visa program for quantum talents around the world who are currently studying in the U.S. or planning to come to the U.S. for studying and research in this field. Work permits should be granted to quantum talents so they can stay in the U.S. for work after their graduation.

According to Kitchen and Drexel, the U.S. should establish “stricter patent protections and more aggressive repercussions for domestic and international offenses in IP theft” [19]. The U.S. Department of Defense should maintain partnerships with private sectors as they have been doing in the last decade along with collaboration with our allies around the world in quantum computing research and development.

The U.S. should monitor the supply chain of exporting critical components and materials of quantum computers and also create an ecosystem where the government pays attention to the financial health of small, specialized quantum computing firms.

In conclusion, the U.S. should closely monitor quantum computing sector which means they have to set quantum computing standards and create an ecosystem where the government supports both public and private quantum computing companies. This will help the United States stay ahead in quantum computing race which support both the country’s future economy and national defense system.

About the Authors



Celeste Clarke is a senior student and a member of Honors Program at George Mason University and pursuing a bachelor’s degree in management information system. She has been an independent investor for 19 years. Celeste is interested in French, network security, and cloud computing.

Hanh Nguyen is pursuing an undergraduate degree at George Mason University in Business with concentration in Management Information System and is a member of Honors Program. She is interested in programming.



Sahrash Tanveer is an undergraduate student at George Mason University, pursuing a degree in Business Administration with a concentration in Management Information Systems. She is a member of the Honors Program and is interested in data analytics and cloud computing.



Zachary S. Risseuw is a Business Technology Solutions Analyst at Deloitte Consulting within its Government & Public Services practice. Zach received his Bachelor of Science summa cum laude from George Mason University with a major in Business Analytics and a minor in Legal Studies. Prior to graduating, he interned at the U.S. Department of the Navy’s Office of the Assistant Secretary.

Brian K. Ngac, PhD is an Instructional Faculty Member and Dean’s Teaching Fellow at George Mason University’s Costello College of Business. He’s the Founding Director of the Professional Readiness Experiential Program (PREP) where Honors and High-Performing Students work on real projects with real industry participants to gain hands-on experience prior to their graduation. Any interested organizations that would like to be an industry participant are encouraged to contact Brian at bngac@gmu.edu



References

- [1] McBride, J., & Chatzky, A. (2019, May 13). Is "Made in China 2025" a Threat to Global Trade? Council on Foreign Relations. <https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade>
- [2] ODNI. (2024, February 5). 2024 Annual Threat Assessment of The U.S. Intelligence Community. Office of the Director of National Intelligence; DNI. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community>
- [3] Penney, H. R. (2024, March 22). The Quantum Advantage: Why It Matters and Essential Next Steps. Mitchell Institute for Aerospace Studies. <https://mitchellaerospacepower.org/the-quantum-advantage-why-it-matters-and-essential-next-steps/>
- [4] Bogobowicz, M., Gao, S., Masiowski, M., Mohr, N., Soller, H., Zimmel, R., & Zesko, M. (2023, April 24). Quantum Technology sees record investments, progress on talent gap. McKinsey & Company. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap>
- [5] Freedberg, S. J. (2024, March 4). China's investing billions in quantum R&D, but is Beijing making some bad bets? Breaking Defense. <https://breakingdefense.com/2024/02/chinas-investing-billions-in-quantum-rd-but-is-beijing-making-some-bad-bets/>
- [6] Dargan, J. (2021, April 20). 9 Chinese Quantum Computing Companies Leading the National Race. The Quantum Insider. <https://thequantuminsider.com/2021/04/20/9-companies-leading-the-quantum-technologies-race-in-china/>
- [7] Klebanov, S. (2022b, February 23). Who's winning the quantum computing race? China and the U.S. are neck and neck. The Business of Business. <https://www.businessofbusiness.com/articles/whos-winning-the-quantum-computing-race-china-and-the-us-are-neck-and-neck/>
- [8] Pichai, S. (2019, October 23). What our quantum computing milestone means. Google. <https://blog.google/technology/ai/what-our-quantum-computing-milestone-means/>
- [9] Smith-Goodson, P. (2019, October 11). Quantum USA vs. Quantum China: The world's most important technology race. Forbes. <https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=37cd43fd72de>
- [10] Amerongen, M. van. (2021, June 3). Quantum Technologies in Defence & Security. NATO Review. <https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>
- [11] Shams, M., Choudhari, J., Reyes, K., Prentzas, S., Gapizov, A., Shehryar, A., Affaf, M., Grezenko, H., Gasim, R. W., Mohsin, S. N., Rehman, A., & Rehman, S. (2023). The Quantum-Medical Nexus: Understanding the Impact of Quantum Technologies on Healthcare. Cureus, 15(10), e48077. <https://doi.org/10.7759/cureus.48077>
- [12] Swayne, M. (2024, February 28). Reports: China mass producing dilution refrigerator critical to superconducting quantum computing. The Quantum Insider. <https://thequantuminsider.com/2024/02/28/reports-china-mass-producing-dilution-refrigerator-critical-to-superconducting-quantum-computing/#:~:text=REQUEST%20ACCESS-,QUANTUM%20TECHNOLOGY%20IN%20CHINA,-Our%20Quantum%20Technology>
- [13] Toon, J., (2024, February 6). New ion cooling technique could simplify quantum computing devices. Phys.org <https://phys.org/news/2024-02-ion-cooling-technique-quantum-devices.html#:~:text=Using%20a%20technique%20called%20rapid%20ion%20exchange%20cooling%2C>
- [14] Williams, L. (2021, November 9). The world's top five quantum computing hubs. Investment Monitor. <https://www.investmentmonitor.ai/tech/the-worlds-top-five-quantum-computing-hubs/?cf-view&cf-closed>
- [15] Precedence Research. (2023, January 30). Medical Tourism Market Size to Surpass USD 286.1 Bn by 2030. www.precedenceresearch.com. <https://www.precedenceresearch.com/medical-tourism-market>
- [16] Liu, N. (2024, February 16). China invests billions in quantum computing, race with US now neck-and-neck. SDxCentral. <https://www.sdxcentral.com/articles/analysis/china-invests-billions-in-quantum-computing-race-with-us-now-neck-and-neck/2024/02>
- [17] NIST. (2023, August 24). NIST to standardize encryption algorithms that can resist attack by quantum computers. The National Institute of Standards and Technology. <https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers>
- [18] Sanzeri, S. (2023, February 6). The quantum threat: Our government knows more than you do - cyber ... Cyber Defense Magazine. <https://www.cyberdefensemagazine.com/the-quantum-threat-our-government-knows-more-than-you-do/>
- [19] Kitchen, K., & Drexel, B. (2021, April 22). Quantum Computing: A National Security Primer. American Enterprise Institute - AEI. <https://www.aei.org/research-products/report/quantum-computing-a-national-security-primer/>



Jump Start a Chapter Leadership Board - **START NOW!**

Power up your career, business, life through chapter leadership

By: Debra Christofferson

If you changed jobs, moved to new location, were downsized or outsized, or you seek diversity in job roles, and growth options that are absent in your current role, this is for you. Newcomers listen up!

Would you like to stand out in your career, business and life, while you learn “on the job”? Join an ISSA chapter leadership board!

You can form a start-up chapter, restart a stalled or dormant chapter, or enhance a current board that needs your passion, skills or time. You will meet new people, upgrade your skills, and make a difference.

ISSA Chapter leaders create active events, that educate, engage and grow the ISSA cybersecurity community and outreach across organizations and individuals. Your community needs you!

Chapters are:

- Led by volunteer leaders and board members across industry verticals and roles
- Managed autonomously with ISSA International Board oversight
- Populated by members of ISSA and our local security community
- Operate as not-for-profit, formed legally or not, based on the chapter or region
- Non-member guests are welcomed
- Resident in digital and in-person communities within ISSA's chapter membership, LinkedIn and Meetup groups, web sites and through chapter subscriber databases and events.

What's in it for you?

WIIFM—Benefits of Chapter Leadership

When I departed long-time corporate employment, to make my own way, my network evaporated. You can only meet up over lunch, for so many days until you run out of time and money. Meanwhile, your former colleagues, good friends and all, are busy chatting over lunch, about the trials and tribulations of the workplace—what they can share, and which you are no longer a part.

Without the corporate name and role--and implied competency, it became clear, that the market based my value on my employer and job title. This forced me to build and articulate a renewed identity, network and value. Board leadership helped me do this, plus build many long-standing relationships.

Why should you lead a chapter?

To actively engage and develop your local security community and build a powerful network—fast. You will grow professionally far more than you anticipate and open up visibility and opportunities not visible otherwise. These include:

- Creating thought leadership
- Growing management, influence and communication skills, while becoming a more effective spokesperson and speaker
- Developing professional relationships and partnerships
- Expanding your career to new directions or heights

It's all in your hands, and presents a huge career enabler for newcomers, and to any of us.

Portrait of a Chapter Leader

Chapter leaders represent a broad group of professionals in their own roles, across a large spectrum of business and organizations. No better way exists, to engage in the field, and build relationships with people who would not be in your trajectory otherwise.

Leadership roles are not meant to build LinkedIn profile filler (although they do!). Passion and commitment are prerequisites to success, and an ability to interact successfully with talented volunteers who work with you, not for you. They hold full time jobs and lives outside the Chapter. However, if you have passion, some bandwidth, plus commitment, you can thrive and launch a strong security community through your ISSA Chapter.

Chapter leaders support and activity drive cybersecurity community events for members and friends.

Any current member is eligible to join a leadership team, or run for an open board position in elections. You must be an ISSA member in good standing, and a member of the local chapter whose board you seek to serve. At startup, elections may be run, or a board installed based on volunteers, passion, skills and a desire to serve the community. Some roles require expertise or skills, but those often can be developed.

Starting, Reviving or Joining a Chapter Leadership Board

Starting from scratch requires a good network, or people on the board leadership who have strong networks. To lead the chapter requires skills to attract and motivate and hold accountable a performing volunteer leadership team. It's a team sport, a fun enriching experience, but one that requires good relationship, influence, and leadership skills. The team must deliver and be accountable to their commitment.

Taking over a failing chapter that requires a restart, also presents challenges, and usually means building a new board, or replacing dormant and non-committed or burnt-out folks who aren't up to the challenge. Sometime the Board's leader needs to step aside and be nudged to do so by team members.

If you sign up for the commitment, expect to live up to it, or step aside or down. Our work and life commitments evolve over time, and it's ok to depart. Help someone else take the reins. Help bring others in with the skills and passion the group needs. Or just ask to be replaced—“man up”, or “put your big girl pants on”.

It can help to partner on events with other local groups, such as chapters for ISC2, ISACA, IAPP (Privacy), Infragard, OWASP, ASIS, ACP, CFE, DAMA, ARMA, WICys, and conferences that come to town.

Joining a functioning board allows you to create an impact and bring new ideas, programs and passion to the members.

Board Roles Typically at Play

Boards evolve too, and chapter needs differ across sites. Fill the board roles you need as the chapter and need evolve. Non-profits in the US typically require a President, Secretary and Treasurer. If you initially have no money, no Treasurer is needed, but the role can assume other responsibilities interim. Other roles will manage speakers, venues, sponsors, insurance, membership, social media including LinkedIn, partnerships, etc. Match people for their desires, not just the position you want filled.

Speaker role presents the best networking opportunity, but needs someone with a network, who is comfortable interacting for speaker sourcing and interaction, and keeping the board current. It's a critical role. Build your network fastest right here.

Membership role is also critical, with responsibility for member communication on chapter activities and events. The role owns management of the member and subscriber lists, email communication to both, creation and management of event registrations online and onsite, and answering member queries. Sometimes you start from scratch.

For a new board, do not fill a Vice President role initially, not until you place critical roles and get the chapter going. You do not want filler people—each role needs explicit responsibilities—no bystanders. Remove the role interim, if you are reforming a board. Yes, the President needs backup, but with other professional peers in place, factor in bench strength when you staff the Board.

All board members own responsibility to actively educate their community, colleagues and managers, about the chapter and its events, plus develop and grow membership. Good leadership shows up quickly.

Successful boards need diversity in their make-up, across sectors, companies, roles and people. They cannot originate from just one or two organizations, nor made up entirely of consultants, vendors and service providers. Else you will repel sponsors, speakers and members. Seek a mix of skill sets, perspective and outreach beyond your own back yard.

Where to Find Chapter Members

If you lack a chapter base, you must build a member community. You can do this with an event launch, starting small with 20-50 invited folks. But I would target two, three or four times that number to really launch successfully, based on your market size. Expect only half to show.

You'll need a venue, catering sponsor and a strong keynote. A standing event schedule and venues should be lined up as soon as you can. See why you need help from a good network and committed board members?

Otherwise, you have a chapter member community with ISSA International, and possibly a local subscriber base too. But outreach will be similar for a chapter revival or to grow the chapter.

Conclusion

All boards need volunteers, and good leadership is always in demand. Has your interest been peaked?

Virtually no job or opportunity I've received, came from outside my network. Since leaving Corporate America, and becoming an un-networked consultant, my network came entirely from board leadership roles, many with ISSA. Many presented substantial opportunities. Other ISSA leaders will agree with me about opportunities and growth potential.

Don't be a popcorn eater on the sidelines! Make a choice and live up to your power.

A startup especially offers pure-play, and you can truly make a difference. But it's work along with love! Reach out today.

For existing leaders, we appreciate you as the heart and soul of ISSA, for giving your time, competency and hearts. You create the underpinning to ISSA.

Help us showcase your chapters. Contact us, to share best practices based on your chapter success, an update on your new or restarting chapter, or a current healthy or growing chapter. Photos welcome!

Resources for Getting Help

Reach out to ISSA to form a new chapter or restart one. Contact your local chapter for opportunities within an existing team. Visit chapter web sites for contacts. Attend events to meet and talk to folks.

For more guidance, ask for my "Chapter Start-up Best Practices", which is based on 22 years of chapter leadership in and outside of ISSA. A template is also offered for Chapter Board roles. Do not reinvent the wheel!

- Send to me with subject line Chapter Startup Best practices, at membership@phoenixissa.org.

If you desire mentoring for your chapter startup—or any function within--other chapters boards will happily assist. ISSA has many successful chapters and leaders. Phoenix (my home chapter) reformed after the pandemic, originally founded in 1999, 25 years ago.

- Reach out to Chapter Services at chapter@issa.org or to a friend chapter.

Visit ISSA's web site and go to contacts to reach out for other contacts. A Chapter Leader Committee exists, an online community on ISSA.org, and a newsletter is sent to chapter leaders.



About the Author

Debra Christofferson, CISSP, CISM, CCSK: 30 years security enterprise management. ISSA Distinguished Fellow, ISSA Honor Roll, Volunteer of the Year, Chapter of the Year. Led CISO Advisory Council/Cyber Exec Forums. Leads Women in Security SIG. Published Women in Security book.

CHAPTERS LIST



ISSA
40 YEARS STRONG

Asia Pacific

Chennai
India
Philippines

Canada

Ottawa
Quebec City

Europe

Brussels European
France
Germany
Italy
Poland
UK

Latin America

Argentina
Barbados
Brasil
British Virgin Islands
Columbia

Middle East

Egypt
Israel
Kuwait
Qatar
Saudi Arabia

Alamo San Antonio
Austin Capitol of Texas
Blue Ridge
Boise

Buffalo Niagara
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
Eastern Idaho
Eugene
Fayetteville/Fort Liberty
Grand Rapids
Grand Traverse

United States

Greater Augusta
Greater Cincinnati
Greater Spokane
Hampton Roads

Hawaii
Inland Empire
Kansas City
Kentuckiana
Kern County

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
Northern 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 Florida
South Texas

Southeast Arizona
Tampa Bay
Tech Valley of New York
Texas Gulf Coast

Triad of NC
Upstate SC
Utah
Ventura County
Wyoming

For Support, contact: Chapter@ISSA.org

AI and Cost Disease

By: Luther Martin, ISSA Member, Silicon Valley Chapter



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.

Will artificial intelligence (AI) cause the end of the world as we know it? Will it create a race of robot overlords that enslave humanity? Will it make people so productive that a three-day work week could soon be a reality? In most cases, it's probably reasonable to assume that the answer to these sorts of questions is "no."

But if we remember what we learned in ECON 101, some of the consequences of the use of AI aren't too hard to understand and anticipate. Baumol's cost disease, which tells us that things that don't get more efficient with better technology tend to get more expensive relative to other things, might be one of these.

Why? Suppose Alice and Bob work at different companies, and both make \$50 per hour. Now suppose that better technology at Alice's company increases her productivity and thus her wage to \$60 per hour. Bob might want to go work for Alice's company for the higher wage, so to keep him, his company will also need to increase his wage to \$60 per hour. But because this wage wasn't justified by higher productivity, Bob's company will need to raise prices to pay the higher wage while Alice's won't.

Research suggests that cost disease is one of the big reasons that both higher education and health care tend to get more expensive faster than the overall rate of inflation. Both of them are examples of industries where better technology doesn't necessarily increase productivity. Better technology doesn't necessarily let professors teach more students or let doctors see more patients. The result is that healthcare and higher education tend to get more expensive over time relative to other goods and services, and we probably can't do much about that. The best that we can probably do is decide as a society how much we're willing to pay for these things and then live with that constraint.

Now suppose that some of the predictions about AI are right, or at least not too wrong. In particular, some people have suggested that AI will let some people realize a three-day or four-day work week. Working fewer days per week while (presumably) keeping the same salary suggests that the people enjoying those three- or four-day weeks are productive enough in those three or four days to justify them being paid for what once took five days to accomplish, leaving jobs that don't get a productivity boost from AI susceptible to cost disease.

Being in an industry susceptible to the effects of cost disease may be a bad thing. After cost disease dramatically increased the cost of higher education for so many years, we may now be at the point where many high-school graduates don't see the value in higher education and forgo it entirely, leading to decreased demand for it, and thus fewer jobs in the field.

Cost disease may be impossible to avoid in parts of the information security industry. Expect AI to increase the cost of security consultants, for example, who will find their cost increasing for the same reason that the cost of healthcare and education increases. And if the value provided by security products and services doesn't increase as the adoption of AI spreads, we should expect those things to get more and more expensive relative to other things and eventually become unattractive to customers when their price exceeds the value that they provide.

Some effects of AI may be hard to predict, but cost disease probably isn't one of them, and we should plan for the future accordingly. Forewarned is forearmed.



Generative/LLM Bio

By: Robert Slade

The bloom seems to be coming off the AI rose. So, for quite a while, my take on the large language models has been that they are a solution in search of a problem.

Recently I was given a date for a presentation (on AI) to a group that I knew would want a bio.

I hate writing bios. So, I thought it would be amusing to have ChatGPT write a bio of me. And Claude, the tool from Anthropic. And, today, Meta announced Llama 3.1.

Well, It was somewhat amusing. But it has also become part of my presentation. The bios that all three systems produced point out, in large measure, the problems associated with the large language models of artificial intelligence.

Rob Slade was born, variously, in 1948, 1952, and "the 1950's." So, some of the material is purely in error. (Claude ***did*** manage to figure out that I am Canadian.) There is no particular secret about any of this.

I gave them a three hundred word limit, and, somewhat to my surprise, given the weird and wonderful errors that LLMs seem to be capable of making, all three did come in "under budget," at 246, 268, and 279 words. All three systems wasted an awful lot of their word count on what could primarily be called promotional or sales material.

ChatGPT found three of my books, Claude two, and Meta one. Nobody found all five. There are other Robert Slades on the Internet. Over thirty years ago we had the "Robert Slade Internet Club," with a membership of about a dozen. There is a Robert Slade who publishes on Greek pottery and inscriptions, another who publishes on fishing lures, another who teaches mathematics, and another who is a DJ for events and parties. In order to give AI the best chance, I specified that I wanted a biography of the Robert Slade who was an information security expert. To their credit, none of the models came up with specific references to the publications of these other Robert Slades.

However, I have been credited with degrees from a number of universities which I did not attend, so their backgrounds may be the explanation. But that doesn't explain my "memberships" in a number of tech associations to which I don't, and have never, belonged, and the failure to list the ***one*** organization to which I did, for some time.

Claude says that I developed an early interest in computers and technology during my university years, which is pretty much false. Both Claude and Meta insist that I started with mainframes, again, pretty much completely false. (Meta insists that I started with computers at age twelve: I was almost thirty before I really got interested.) Claude managed to figure out that it was my reviews of antivirus software that first got me any attention. (Overall, I'd say Claude definitely gets top marks for accuracy. But being the best of a bad lot is not exactly a stunning accolade.)

Yes, it has been somewhat amusing to have the LLMs write my bio. But that's because I hate writing bios anyways. If this bio were, in fact, important to me - if it were some type of resume - I would not be able to accept the errors that have been made. Granted, it has automated the task of generating marketing and promotional fluff; with claims that are both unverifiable, but unchallengeable. But do we want to produce this kind of material, for any reason? Is this not the slippery slope to the post-truth world in which we live, where major figures are able to lie, blatantly, provably, without regard or interest in whether or not people are going to be able to say that is a complete and utter lie? I have, in another piece, commented that the large language models could not be better at producing disinformation than if they had been designed that way.

Have they?



About the Author

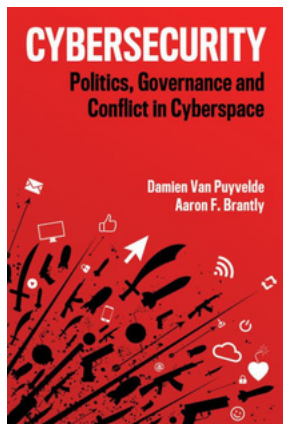
Robert Slade is renowned, with a career spanning several decades, has made significant contributions to the field of cybersecurity, authoring numerous books and papers, with a solid foundation for his expertise, is influential and his publications have served as essential resources for both novices and seasoned professionals, gives engaging presentations with an ability to demystify complex security concepts making him a sought-after speaker and educator, with a career marked by significant achievements and a commitment to advancing the field of information security, his work has been instrumental in shaping the understanding of digital threats and has left an indelible mark on the information security landscape. His legacy serves as a testament to the importance of dedication, expertise, and innovation in the ever-evolving landscape of information security. You will note that none of these claims are really verifiable, and so they are also basically unchallengeable. 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



The Cyber Library

Reviewing the Works of Damien Van Puyvelde, Aaron F. Brantly, and Chase Cunningham

By: William J. (Jay) Carson, ISSA Member Colorado Springs



Cybersecurity: Politics, Governance and Conflict in Cyberspace.

by Van Puyvelde, Damien, and Aaron F. Brantly. Policy Press, (2019).

Sound Bite: Good stratospheric perspective of cyber, with many fitting example stories.

Opinion on Primary Audience: More for world decision-makers, but plenty of information to interest the cyber-adept. I recommend you read this book thoroughly, then put it on your professional bookshelf for a bibliographical reference for your own future writings.

The Authors:

Dr. Damien Van Puyvelde is now an associate professor at Leiden University. Formerly he was a reader/director/lecturer at the University of Glasgow. He is a PhD from Aberystwyth University. He has been around the international security arena in academics for the last 10-15 years.

Dr. Aaron F. Brantly has been an assistant professor at VA Tech for the last seven years. Before that, he was an assistant professor and Cyber Policy Fellow at West Point. His PhD in International Relations is from the University of Georgia.

The Metadata:

A 2019 publishing date! The online ordering cost including shipping is about \$20. The paperback is about 200 pages. There are no copies in my local public library system.

This book is quite readable. I took a one-page sample of the text to analyze. Using a Wikipedia article about the Flesch-Kincaid Readability Test, the readability is upper college level. The sample had 5% passive voice. This article is under 2% passive voice.

Table of Contents: [Including Reviewer notes]

Chapter 1: The Expanding Scope of Cybersecurity [Reviewer note: History]

Chapter 2: What is Cyberspace? [Reviewer note: OSI Model, DoD Model, and Heartbleed]

Chapter 3: Governing Cyberspace

Chapter 4: Cyber Capabilities and Insecurity [Reviewer note: Polymorphic Malware & Cyber Kill Chain]

Chapter 5: National Cybersecurity and Strategy [Reviewer note: China/Russia/US]

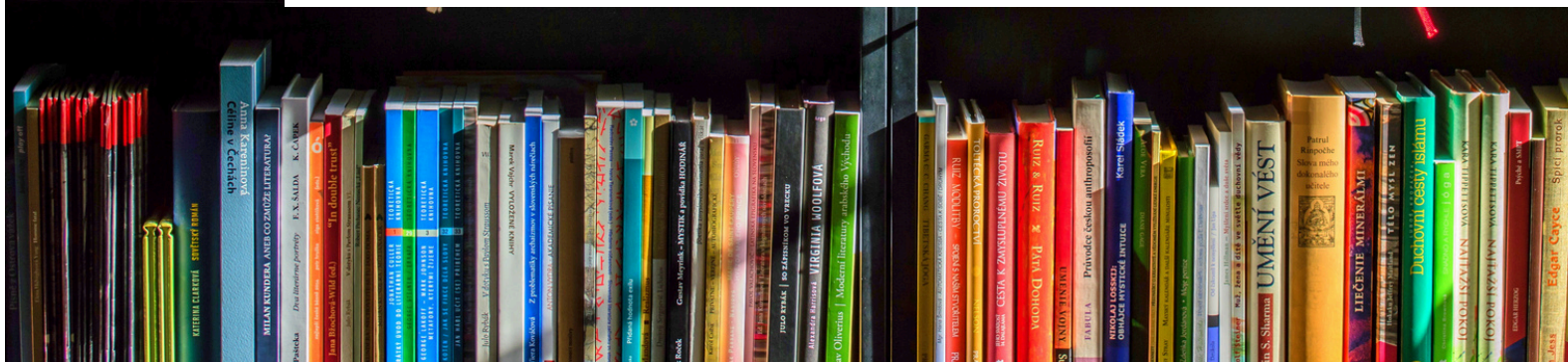
Chapter 6: Cyber War

Chapter 7: Non-state Threats: From Cybercrime to Terrorism [Reviewer note: Hacktivists & Cyberterrorists]

Chapter 8: Organizing Deterrence and Defense in Cyberspace

Chapter 9: Cybersecurity and Democracy [Reviewer note: Liberation Technology Yes/No]

Chapter 10: The Futures of Cybersecurity [Reviewer note: IoT & AI]



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.

by Dr. Chase Cunningham. Packet Publishing, (2020).

Opinion on Primary Audience: The cyber-adept, but anyone would find it worthwhile.

Positives/Negatives: The book's Forward by Brig. Gen (USAF ret.) Gregory J. Touhill, impressed me. However, under the topic of weak passwords, there is a tangential reference to Dr. Bruce Blair's report on nuclear command and control procedures. In my opinion, this is too tangential for the topic.

The Metadata: A 2020 publishing date! You can get a copy by online ordering for a little over \$30, including shipping. The paperback copy is about 300 pages. There are no copies in my local public library. Again with a one-page sample of the text to analyze, it is college-level, about 33% passive voice. This article is under 2% passive voice for comparison.

Chapter 1: A Brief History of Cyber Threats and the Emergence of the APT Designator

Chapter 3: Emerging Tactics and Trends - What is Coming?

Chapter 5: DeepFakes and AI/ML in Cyber Security [Reviewer note: Lyrebird AI, etc.]

Chapter 7: Strategic Planning for Future Cyber Warfare

Chapter 9: Bracing for Impact

Happy Reading!

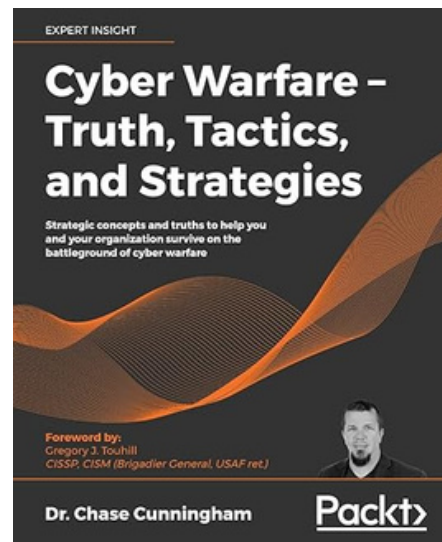
Next Month:

Additional sources used in the article:

- 

William J. (Jay) Carson, ISSA Senior Member, ISSA 2020 Volunteer of the Year, and past ISSA-Colorado Springs Executive Vice President. He is the 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. Reach him at Runningjay51@gmail.com.

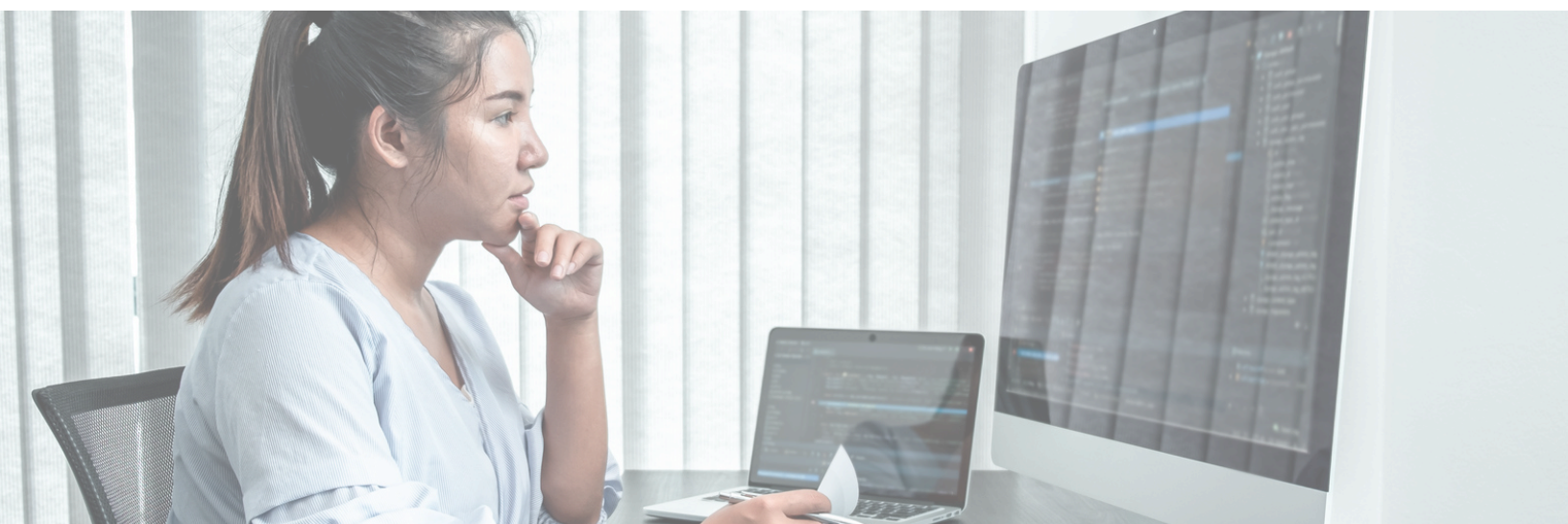
ISSA JOURNAL SEPTEMBER-OCTOBER 2024



Supplementary Segment

Straining our Security

Shifting the security, developer, and developmental practitioner professions towards building an understanding of technology component security and cybersecurity practitioner roles.



By: Ervin H. Frenzel, University of North Texas, Professional Associate Professor; **Richard W. Lightcap, Bilal Abu Bak**, University of North Texas, Clinical Associate Professor

Abstract

This article introduces a holistic definition for cybersecurity; enabling our organizational end-users to safely, securely, and efficiently engage our organizational technology. We formed this definition through critical deconstructive analysis of roles within the various countermeasure component level securities, then organizing them in a way designed to assist the lay people with identifying the key differences between technology security versus cybersecurity roles. We aim to link commonly recognized security practitioner classifications, like the information security color wheel, into academically taught concepts to train the base of required technicians.

Keywords: technology component security practitioners, holistically defining cybersecurity practitioners, information security color wheel, deconstruction of technology security roles

Introduction

In 2019 the United States lost \$6.7 trillion, with \$5.7 trillion of the total attributed to losses associated with the people specifically the end-user countermeasures (Ponemon Institute, 2019). Human Resources (HR) staff often simply purchase a video to conduct training, seldom based security requirements rather the training is often based upon compliance requirements, as most users have experienced in the workplace. This may in part be due to not having sufficient security technicians in place to properly train end-users. These training roles are currently being filled by HR staff with little or no security training experience in the field of security. Per CompTIA, 75% of infrastructure and up to 98% of security technicians are missing from roles in securing infrastructure and technology within organizations (CompTIA, 2015). Infrastructure is the term used to describe the internal equipment used to carry information within an organization, while cybersecurity (or Information Assurance) involves enabling people or end-users to safely operate technology within the context of their organization (Information Technology, 2020; Kissel, 2013; Frenzel & McAndrew, 2023; Frenzel & McAndrew, 2022a; Frenzel & McAndrew, 2022b). It is unlikely the current training models have capacity to alleviate the pressures caused by missing technicians, as the field continues

to expand to cover even more singular component security fields, yet still denying the existing requirement for a holistic field of study (Frenzel & McAndrew, 2023; Frenzel & McAndrew, 2022a; Frenzel & McAndrew, 2022b).

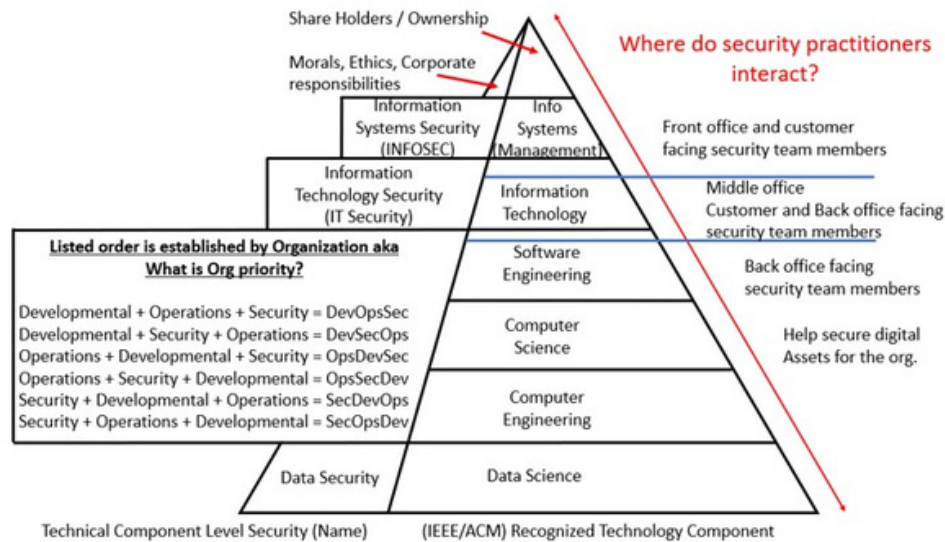
Method

Research was performed via an integrative literature review to identify methods of classification for technology component security countermeasures versus holistic cybersecurity. Through an analysis of existing literature, leveraging a varied sampling frame, resulting in an in-depth portrayal of the concepts of technology component security countermeasures and holistic cybersecurity (Whittemore & Knafl, 2005). Different academic groups identify cybersecurity as technical component security as a means of selling academic programs and technological concepts as it seems to be more mainstream.

Discussion

Security technicians go missing for various reasons, in this case there was a lack of concerted efforts to train these security experts in lieu of training infrastructure technicians. The State of Texas uses the Workforce Enhancement Course Manual or *WECM* to categorize security as related to Infrastructure or Information Technology or *IT* hence the overall rubric of Information Technology Security or *ITSY* (THECB, 2021). Many academic instructors define cybersecurity within the scope of information technology thus information technology security, not the other technology domains addressed by IEEE or ACM (CC 2020 Task Force, 2020; Cyber2yr2020 Task Group, 2020; Joint Task Force on Cybersecurity Education, 2018; Patnayakuni & Patnayakuni, 2020; The Joint ACM/AIS MSIS 2016 Task Force, 2016). Currently there are 16 active courses that fall within the *ITSY* Rubric in *WECM* (THECB, 2021). In comparison there are 361 active courses that address configuration of specific IT equipment in different environments either as *ITXX* excluding *ITSY*, *HITT*, or *CPMT* (THECB, 2021). From this perspective, IT security is being overtrained while cybersecurity is rarely touched, essentially 4% of all IT courses relate to security.

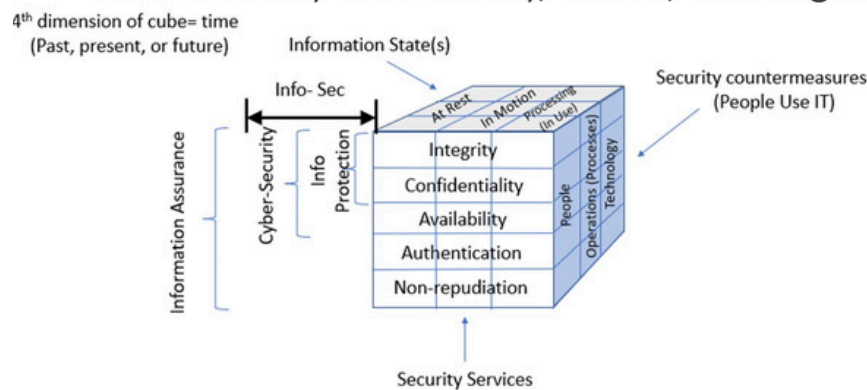
Cybersecurity encompasses three countermeasures; people, processes, and technology but there is a need to further identify where the organizational security team members sit, for instance will the security practitioner interact with organizational end-users or will they interact with the back-end developers (Sosin, 2018; Maconachy et al, 2001). Once it has been determined that a specific type of security practitioner is needed, further detail is needed to determine which priority will be given to development, operations, and finally security. The order of which these priorities are listed by the organization is what the organizational leadership see as priority for activity.



Each recognized component has a specific component level security associated with it as explained in figure 1, such as IT security. Each component security is associated with a technology present in the organization. End users interact with component level technologies and therefore must interact with component level security specialists who must be able to adequately engage the organizational end users.

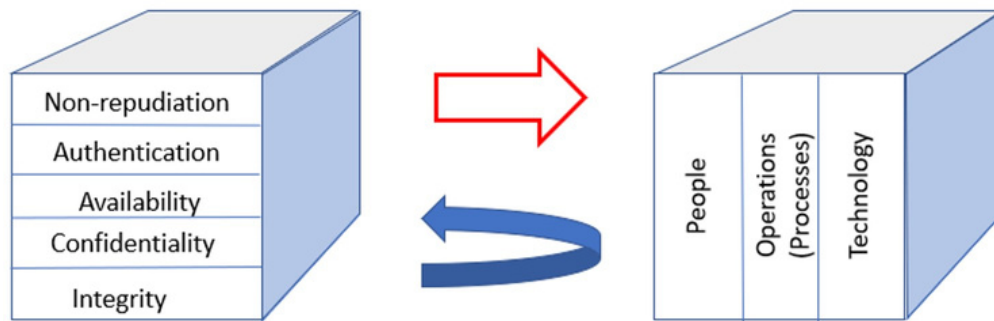
Cybersecurity is a subset of Information Assurance (IA), not technology, and according to IBM and the Ponemon Institute, both of which study root causality for data breaches, fewer than 5% of data breaches are caused by a failure of IT equipment, with 15% caused by process failures and 80% caused by people intentionally bypassing security protocols (IBM Security, 2020; Ponemon Institute, 2019). IA is composed of five key components; integrity, confidentiality, availability, authentication, and non-repudiation and is interrelated as shown in figure 2 (Sosin, 2018; Maconachy et al, 2001).

Sosin Cube explaining Information Assurance
as created by Maconachy, Schou, and Ragsdale



A banner for the 2024 ISSA International Awards Program. The banner features a light blue background with a subtle geometric pattern. On the left and right sides, there are vertical panels with a white marble texture and gold borders. The central text reads "2024 ISSA International Awards Program" in a large, bold, dark blue font. Below this, there are two gold laurel wreaths. The left wreath contains the text "Volunteer of the Year" and the right wreath contains "Chapter of the Year". Both wreaths have a gold ribbon at the bottom with the year "2024". Above each wreath is the ISSA logo, which consists of a globe icon and the text "ISSA Information Systems Security Association". At the bottom center, the text "Nominations Accepted until November 20" is displayed in a bold, dark blue font. In the bottom right corner, there is a circular seal for the "46th ANNUAL MEETING" with the text "PROTECTING OUR COUNTRY" and "46 YEARS STRONG".

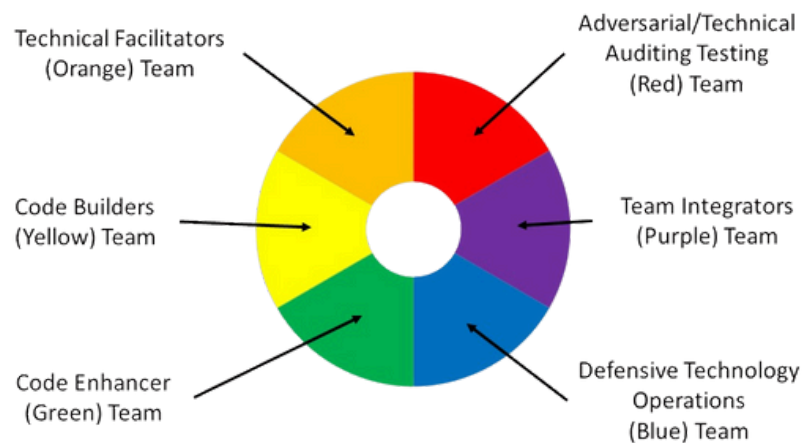
More emphasis should be directed toward identifying potential failures within people or processes rather than solely focusing on technology. The arrangement and coordination of these components dictate the specific subset of IA being addressed. For instance, information defense involves integrity and confidentiality, information security (infosec) pertains to data, and cybersecurity encompasses integrity, confidentiality, and availability. (Sosin, 2018; Maconachy et al, 2001). By rotating the cube 90 degrees, we identify a completely different focus and more importantly identify a possible way to focus our security practitioners (Frenzel & McAndrew, 2023). This rotation is visualized in figure 3.



Cybersecurity technicians are trained in the key tenants of confidentiality, integrity, and availability and are cursorily trained in IT operations to know how to navigate the organizational network. Cybersecurity is defined as all actions taken to protect organizational cyber assets, which can include administrative policies (such as sign in sheets at a data center or actively monitoring a network), physical controls, and even posted security guards (Kissel, 2013). This limited amount of training somehow justifies IT managers, hiring these technicians as infrastructure technicians, while truly trained infrastructure technicians are told that they will need to undergo cyber training to compete in the organization.

This “repurposing of the worker” is a direct challenge to the identity of the worker who has spent several years training for a career which is often tied directly to their own personal identity, this tying of a profession to an identity is often referred to as **workism**, (Thompson, 2021). This research exposes placement of IA/Cyber technicians in Infrastructure roles tends to lead to IA/Cyber technicians leaving the career field, further compounding the worker shortage. The toll demanded of IA technicians when placed in an information technology role is an emotional demand most IA technicians are unwilling to pay, therefore, they leave the field never to return, believing all IA work is akin to IT work (Tsai and Cheng, 2012).

Recently, there has been a growth within the developer community where once again developers who specialize in security are considered as cybersecurity technicians. This is consistent with what occurred originally with IT Security practitioners, in fact per CSEC 2017 we can again expect this to occur as once Data Science begins to formalize security within its ranks (Joint Task Force on Cybersecurity Education, 2018; Cyber2yr2020 Task Group, 2020; Frenzel and McAndrew, 2023). This was best drawn by Stacy Wright at Blackhat 2017, who introduced the information security color wheel as depicted below (Wright, 2017). The infosec color wheel has been rearranged and labeled with developmental teams on the left-hand side and operational teams on the right-hand side in figure 4.



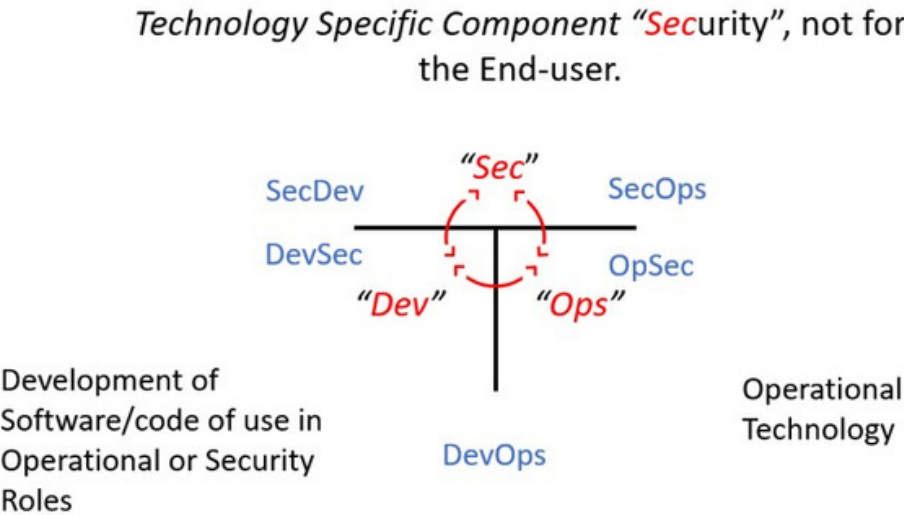
Gartner Information Technology is a global consulting organization that has a reputation built on delivering guidance and knowledge about services and products within the technology space for over 40 years (Gartner, 2024a). This market presence provides a basis for their understanding of Security, Operations, and IT Operations. These definitions are commonly used and understood by businesses around the world as core functions.

IT Operations - Gartner defines IT operations as the people and management processes associated with IT service management to deliver the right set of services at the right quality and at competitive costs for customers (Gartner, 2024d).

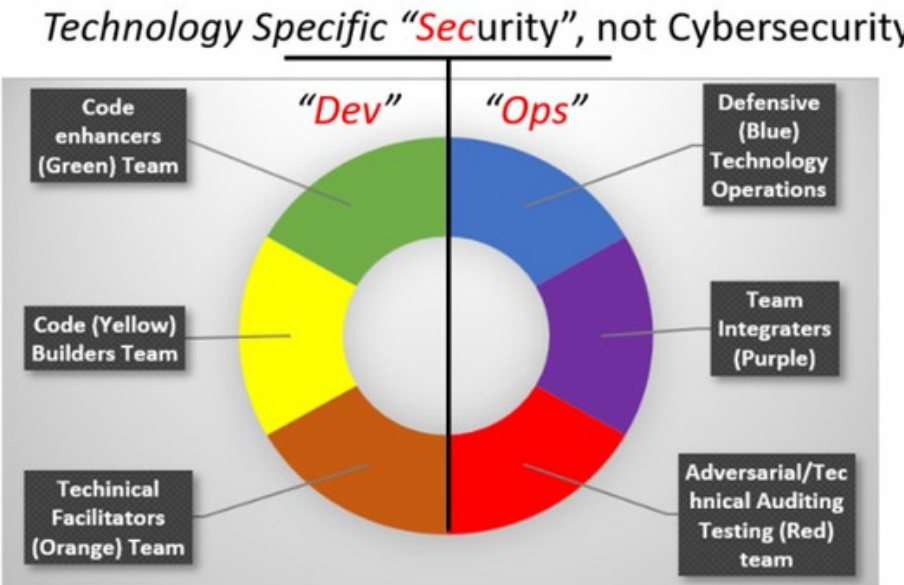
Software Development - Project management, specifications, design, programming, testing, installation and training associated with a specific application development project of any size (Gartner, 2024f).

Security - Security is the combination of people, policies, processes, and technologies employed by an enterprise to protect its cyber and physical assets. Security is optimized to levels that business leaders define, balancing the resources required with usability/manageability and the amount of risk offset (Gartner, 2024e).

More importantly, the interrelationship between the operational, technology and security components can be visualized as a “T” overlay which can be visually represented as in figure 5.



This can then be applied to the Infosec Color wheel so that a direct relationship or correlation is visualized as in figure 6.



A primary function may be combined with a secondary function to further expand upon an organization’s role. This leads to roles such as DevSec, SecDev, DevOps, SecOps OpsDev, or OpSec; depending upon how an organization sees its own role within the marketplace, as seen in table 1.

Listed order is established by Organization aka		
What is Organizational Developer to Operational technology priority?		
Primary Focus	Secondary Focus	Is Called (Known as)
Development	Security	DevSec
Development	Operations	DevOps
Operations	Development	OpsDev
Operations	Security	OpSec
Security	Operations	SecOps
Security	Development	SecDev

This primary and secondary combination creates a new form of technical role focused on a modified understanding of the terminology. For instance, Gartner (2024b) defines DevOps as:

“DevOps represents a change in IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture), and it seeks to improve collaboration between operations and development teams. DevOps implementations utilize technology — especially automation tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective.”

This binary combination does not include all possibilities within the Technological Security, Operational, and Developmental worlds. As is clearly shown, combining the three elements together forms a completely new developmental, operational, and technology specific security, that is still not quite the sought holistic cybersecurity, as this typically addresses specializations within technology, as demonstrated in table 2.

Listed order is established by Organization aka			
What is Organizational Developer to Operational technology priority?			
Primary Focus	Secondary Focus	Tertiary Focus	Is Called (known as)
Development	Security	Operations	DevSecOps
Development	Operations	Security	DevOpsSec
Operations	Development	Security	OpsDevSec
Operations	Security	Development	OpsSecDev
Security	Operations	Development	SecOpsDev
Security	Development	Operations	SecDevOps

In this case, Gartner (2024c) has already defined DevSecOps as:

“DevSecOps is the integration of security into emerging agile IT and DevOps development as seamlessly and as transparently as possible. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment.”

Conclusion

The misidentification of security technicians within the technology component as cybersecurity professionals persists and will likely persist as long as the definition of cybersecurity remains strictly confined to technology without addressing more challenging questions. Rather than solely focusing on technology, the pertinent inquiries should center on the organizational necessity for security technicians. Technicians and technical component security practitioners avoid interfacing with the single largest source of security failure – the user. This is not blaming the user, but rather the security practitioners who avoid interacting and building an emotionally safe space for users to engage the security team without embarrassment.

To fully be a cybersecurity technician, the end-user of the technology must be integrated in a safe manner with our organizational technology. Effectively, a better understandable definition for cybersecurity is “enabling our organizational end-users to efficiently, safely, and securely engage our organizational technology”. As an educational structure, most schools or even regions claim to provide cybersecurity training, though they are often providing specific component security training programs. Each cybersecurity programs focus on specific countermeasures, but these programs often fail to provide the entire socio-technical system encompassing the entire set of people, processes, and technology security countermeasures or provide a minimalistic level of holistic training.

Suggestions

To better address this, call a technical component security technician a security technician, as identified by the organizational direction. Do not lump all security technicians together as a single set of cybersecurity technicians, instead call them as Stacy Wright so eloquently stated a team member based upon their functionality (Wright, 2017). More importantly, recognize these specialists are now hybrid specialists, they are better than a generalist in their fields. Much as a heart surgeon is better at heart surgery than a general practitioner.

References

[1] CC 2020 Task Force. (2020). Computing curricula 2020: Paradigms for global computing education. Association for Computing Machinery, New York, NY, USA. 2020. pp. 50. doi: <https://doi.org/10.1145/3467967>

[2] CompTIA. (2015). Trends in information security study. <https://www.comptia.org/content/research/trends-in-information-security-study>

[3] Cyber2yr2020 Task Group. (2020). Cybersecurity curricular guidance for associate-degree programs. Association for Computing Machinery, New York, NY, USA. doi: <http://dx.doi.org/10.1145/3381686>

[4] Frenzel, E. and McAndrew, I. (2023). Component Security vs. Cybersecurity: Defining next generation Cybersecurity. International Journal of Applied Technology and Leadership, 2(1)

[5] Frenzel, E. and McAndrew, I. (2022a). Identifying and training adjoining career fields for life in cybersecurity. International Journal of Applied Technology and Leadership, 2(1)

[6] Frenzel, E. and McAndrew, I. (2022b). Cybersecurity: Revealing the legalized profession. International Journal of Applied Technology and Leadership, 2(1)

[7] Gartner. (2024a) About us. <https://www.gartner.com/en/about>

[8] Gartner. (2024b). DevOps. <https://www.gartner.com/en/information-technology/glossary/devops>

[9] Gartner. (2024c). DevSecOps. <https://www.gartner.com/en/information-technology/glossary/devsecops>

[10] Gartner. (2024d). IT Operations. <https://www.gartner.com/en/information-technology/glossary/it-operations>

References continued:

- [11] Gartner. (2024e). Security. <https://www.gartner.com/en/information-technology/glossary/security>
- [12] Gartner. (2024f). Software Development. <https://www.gartner.com/en/information-technology/glossary/software-development>
- IBM Security. (2020). Cost of insider threats global report 2020. <https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats>
- [13] Information Technology. (2020). In Merriam-Webster's online dictionary. Retrieved May 31, 2020 from <https://www.merriam-webster.com/dictionary/information%20technology>
- [14] Kissel, R. (2013). Glossary of Key Information Security Terms (NISTIR 7298 Revision 3) Retrieved from <https://doi.org/10.6028/NIST.IR.7298r3>
- [15] Joint Task Force. (2020). NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations). <https://doi.org/10.6028/NIST.SP.800-53r5>
- [16] Joint Task Force. (2018). NIST Special Publication 800-37 Revision 2 (Risk Management Framework for Information Systems and Organizations [A System Life Cycle Approach for Security and Privacy]). <https://doi.org/10.6028/NIST.SP.800-37r2>
- [17] Joint Task Force on Cybersecurity Education. (2018). Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity. Association for Computing Machinery, New York, NY, USA. 2018. doi: <https://doi.org/10.1145/3184594>
- [18] Maconachy, W.V., Schou, C.D., Ragsdale, D., & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach.
- [19] Patnayakuni, N. and Patnayakuni, R. (2020). Does cybersecurity education focus on the right things? A professions-based approach to cybersecurity education and the nice framework. NICE Framework Special Issue: Investigating Framework Adoption, Adaptation, or Extension. pp. 82-87.
- [20] Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. Retrieved 23 May 2020 from <https://databreachcalculator.mybluemix.net/executive-summary>
- [21] Sosin, A. (2018). How to increase the information assurance in the information age. Journal of Defense Resources Management, 04/2018, Volume 9, Issue 1, 45-57. <https://doaj.org/article/2dbbd0cb37444c0fb51d3df6d5c24cf5>
- [22] Texas Higher Education Coordinating Board (THECB). (2021). WECM - Regular Course Search Report. http://reports.thecb.state.tx.us/ibi_apps/WFServlet.ibfs
- [23] The Joint ACM/AIS MSIS 2016 Task Force. (2016). Msis 2016 global competency model for graduate degree programs in information systems. Association for Computing Machinery, New York, NY, USA. doi: <https://doi.org/10.1145/3127597>
- [24] Thompson, D. (2021). Workism Is Making Americans Miserable. <https://www.theatlantic.com/ideas/archive/2019/02/religion-workism-making-americans-miserable/583441/>
- [25] Tsai, M.-T., & Cheng, N.-C. (2012). Understanding knowledge sharing between IT professionals – an integration of social cognitive and social exchange theory. Behaviour & Information Technology, 31(11), 1069–1080. <https://doi.org/10.1080/0144929X.2010.550320>
- [26] Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. Journal of Advance Nursing, 52(5), 546–553. <https://doi.org/10.1111/j1365-2648.2005.03621.x>
- [27] Wright, A. C. (2017). Orange is the new purple. BlackHat USA 2017. Las Vegas, Nevada, United States. <https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf>

About the Authors



Ervin Frenzel is a Clinical Associate Professor at the University of North Texas and serves as the Program Coordinator for the Undergraduate Cybersecurity program. He has worked in many different cybersecurity and technical capacities in the past 35 years, including roles varying from bench technician, SOC technician and manager, Security Manager, Chief Information Security Officer, and academic instructor. Ervin maintains certifications through ISC2, EC-Council, and CompTIA. He currently works within the cybersecurity industry as an academic instructor and consultant, and he seeks to reduce breaches through better integration of the end-user into the overall security processes within the organization. He holds multiple Master Degrees, a PhD (Cybersecurity Leadership) is currently pursuing an MBA (Strategic Leadership) and a Doctorate in Cyberpsychology.

Bilal Abu Bakr is a distinguished academic and researcher with a rich background in computer science, focusing on cybersecurity and wireless sensor networks. He is currently a Clinical Associate Professor at the University of North Texas and a Professor in the Department of Cybersecurity at Collin College. His extensive cybersecurity and wireless sensor network work demonstrate his commitment to research. He holds multiple advanced degrees, including two Master's degrees in Mathematics, an MS in Computer Science, an MS in Cybersecurity, and a Ph.D. in Computer Science.



Richard Lightcap is an Associate Professor and Program Chair at Brazosport College, and an Associate Director of Cybersecurity & Compliance at Raytheon Company. He has worked in varied capacities over the past 25 years holding roles within higher education, defense, and financial sectors. Richard serves as a dissertation chair for Capitol Technology University and maintains affiliations within the Cybersecurity field with ISC2, ISACA, and EC-Council. Richard's research interests surround the application of social cognitive career theory to technology and cybersecurity, securing smart grid technologies, and consumer privacy. He holds multiple master's degrees and a PhD in Cybersecurity Leadership and a Doctor of Education degree, with current pursuits of a Master of Science in Computer Science, and a Doctor of Science in Cybersecurity.

LIVE! & On-Demand Web Conferences

Every month ISSA International hosts educational live webinars focused on key issues and technologies for cyber security professionals. Access the Events page of [ISSA.org](https://www.issa.org) or visit the ISSA International BrightTalk channel at: <https://www.brighttalk.com/channel/16125/>

Upcoming Web Conferences

COMMUNITY SPONSOR SERIES

Unlocking Zero Trust:
A Blueprint for
Secure
Operations

November 13, 2024
1:00 PM ET

netwrix



Privacy is About More Than
Just Regulation

November 19, 2024
1:00 PM ET

Recent On-Demand Web Conferences

Cyber Resilience Awareness Day Virtual Summit

15 Sessions to
Choose From!



CYBER RESILIENCE SIG

COMMUNITY SPONSOR SERIES

PAM Roadmap: Key Strategies for
Effective Deployment and Team
Engagement

netwrix

COMMUNITY SPONSOR SERIES

Data Security Posture
Management (DSPM)



BigID



snowflake

COMMUNITY SPONSOR SERIES

When and Why to Reevaluate Your SIEM

sumo logic

Supplementary Segment

Ethical Considerations in Cybersecurity Incident Response



By: Emmanuel Enietan, Security Engineer at Amazon Web Services

Introduction

The digital age has profoundly transformed our thinking, living, and working paradigms. Consequently, a significant portion of our activities have transitioned to the online sphere. The intricacies, advantages, possible risks, and threats related to these activities are all growing as they become more widespread. Thus, cybersecurity has emerged as a paramount concern for individuals, businesses, governments, and society at large [1].

Cybersecurity threats are categorized as high, medium, or low. Regardless of their severity, there is an intensified focus on developing practical solutions to prevent and eliminate these threats. Cyberattacks are evolving at an alarming pace, ranging from sophisticated ransomware assaults that disrupt critical systems to data breaches compromising personal information [2]. Therefore, to counter these threats, and effectively respond to incidents, cybersecurity defenses must advance even more rapidly.

Why is Incident Response Important?

Incident response has long been a crucial component of Information Security due to various cybersecurity needs. It is essential because users access networks and resources through digital identities such as usernames, passwords or PINs, digital certificates, or biometric features as used across multiple platforms and applications. Whether these identities reside on company workstations, home computers, or mobile devices like phones or PDAs, they leave behind significant traces of preferences, habits, and personal information [6].

Incidence response plays a critical role in safeguarding organizational assets and data. Most large organizations invest in a dedicated information security management (ISM) function to ensure that digital assets are protected [7]. A cyberattack or security breach can result in substantial costs to individuals, businesses, or government agencies, including financial losses, reputational damage, and loss of clients. These detrimental effects can be mitigated with an effective incident response system in place [8].

Cybersecurity Incident Response Life Cycle

The Information Technology Laboratory under the National Institute of Standards and Technology (NIST) has established that performing incident response effectively is a complex undertaking. Its life cycle encompasses preparing and maintaining an incident response plan (prevention), identifying a threat, assessing the risk, curbing or eradicating the attack (defense), the recovery process, and post-incident activities.

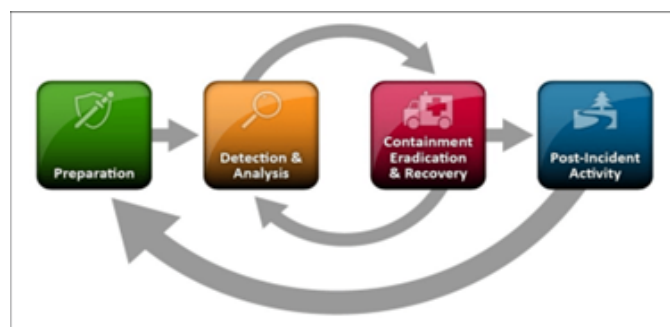


Figure 1: Cybersecurity Incidence Response Life cycle, Cichonski et al (2012)

The first phase involves assembling and equipping an emergency response team, as well as obtaining the required equipment and supplies. Based on the findings of risk assessments, the organization selects and implements a set of controls to reduce the likelihood of events [9]. Detection is always necessary to discover security breaches and alert the organization for subsequent steps of containment, eradication, and recovery to occur. Once the incident has been appropriately addressed, the organization publishes a report outlining the incident's cause, cost, and

recommended preventative measures. It is crucial to note that under each of these phases, the bulk of activities that need to be carried out involve both technical aspects and ethical considerations.

Ethical Considerations in Cybersecurity Incident Response

Venmuri et al. [10] highlighted that an important aspect of incident response is maintaining ethical standards in the incident response process, in addition to its technical requirements and aspects. According to Shaw [11], it is critical to incorporate moral considerations into all aspects of corporate decision-making, including incident response.

Since cyber ethics deals with the nexus of ethics, technology, and human conduct, it is distinct from other fields of ethics. Professionals in this field must negotiate difficult ethical dilemmas in a rapidly changing digital environment where decisions can have a profound impact on society. Some of the core ethical considerations occasioned by incident response are discussed below.

Privacy and Data Protection of Digital Identities

Users create digital identities by assembling different components to verify themselves on several platforms. Typically, these elements consist of digital certificates, PINs, usernames, passwords, and biometric information like fingerprints or facial recognition [12]. All these components act as distinct identifiers that people can use to safely confirm their identity and gain access to the required resources, be they personal or professional.

To detect incidents, professionals must gather and process data. A major challenge here is that these data include digital identities, which are also vulnerable to attacks. Therefore, in a bid to act against cyber threats, professionals must first understand and then protect the privacy of these identities [13].

Compliance with Regulatory Requirements

Throughout the entire life cycle of the cybersecurity incident response, professionals must consider and obey legal requirements on data breach notifications and privacy, among others. These requirements may sometimes hinder identifying and dealing comprehensively with cyberattacks [14]. The situation is further complicated by the jurisdictional nature of data protection regulations and the fact that cyberspace is inherently international, encompassing a vast, interconnected digital landscape that transcends national borders. For instance, numerous laws, like the EU's General Data Protection Regulation (GDPR), require timely notification, frequently within a certain amount of time (e.g., 72 hours under GDPR). Organizations need to be ready to report on breaches promptly to determine their extent and consequences. Professionals must stay abreast of legal requirements and comply with them to ensure ethical incident response.

Transparency

This ethical consideration entails the dilemma of candidly discussing the details, extent, and consequences of an incident with relevant parties. It has been argued that reputation risk management, trust-building, and regulatory compliance all depend on effective transparency. Therefore, crisis communication during cyber incidents should be concurrent with incident response activities [15]. To ensure this, identifying all the relevant parties/stakeholders is the first crucial step. Sometimes, professionals may face the dilemma of not being entirely transparent with the relevant parties where the incident is far-reaching, such that the time used to identify and communicate with all stakeholders involved might slow the incident response process down.

Fairness

In a broader sense, fairness entails looking at the moral standards and values that guide the company's activities in making decisions. Shaw and Miller [16] expressed that business ethics includes analyzing the effects of a company's decisions on different stakeholders, including shareholders, customers, employees, and society at large. In this context, it entails the considerations professionals must have to ensure balanced interest by considering how cybersecurity incident actions affect different stakeholders and strive to balance the impacts as ensuring that all actions taken during incident response are just and equitable [17].

Assessment of Related Ethical Theories

The utilitarian theory, as articulated by Shaw [18], promotes the maximization of happiness as a determinant of what is just and fair. In the context of cybersecurity incident response, utilitarianism emphasizes balancing the need to respond effectively to incidents while minimizing harm to the greatest number of stakeholders.

John Rawls' Fairness Theory underscores the importance of equality and fairness. This theory reaffirms that all actions taken during incident response should be non-discriminatory, just, and fair for all relevant parties.

Best Practices to Promote Ethical Cybersecurity Incident Response

To incorporate ethical considerations and adopt best practices, organizations should address the following questions at each phase of incident response:

1. How do we ensure that the rights and privacy of all parties involved in the incident are respected by our incident response policies?
2. Are we being transparent about the detection of the incident and its potential impact on all relevant parties?
3. How are we controlling the situation while reducing impact and preventing additional harm to people and systems?
4. Are we addressing the incident's underlying causes in a way that prevents recurrence without violating stakeholders' rights or privacy?
5. How can we ensure that our recovery efforts restore normal operations to stakeholders in an ethical manner without placing them at unnecessary risk or burden?
6. Are we adhering to all applicable laws and regulations in their entirety?

Conclusion

This study has detailed the importance of ethics in handling cybersecurity incident response. It has been demonstrated that upholding ethical standards is crucial for preserving confidence and ensuring data security as organizations confront increasing cyber threats. This research has addressed significant ethical issues in cybersecurity incident response, including compliance with regulatory requirements, transparency, fairness, and privacy and data protection of digital identities. Through the evaluation of these concerns, the study proposes practical guidelines for organizations to adopt ethical practices in incident response.



Emmanuel Enietan is a Security Engineer with over 5 years of experience in IT infrastructure, cloud administration, and incident response. Holding a Master's degree in Cybersecurity and a Bachelor's in Industrial Mathematics, his educational background provides a strong foundation for his professional expertise. Emmanuel is a member of the [ISSA Central Maryland Chapter](#).

Editors Note: Article References next page.

References:

- [1] SpremiÄ, M., & Å imunic, M., "Cybersecurity in the Digital Age," 2018.
- [2] Shinde, A., & Kulkarni, P., "The Evolution of Cyberattacks," 2021.
- [3] Craigen, D., Diakun-Thibault, N., & Purse, R., Defining Cybersecurity, 2014.
- [4] Naseer, S., et al., Strategies for Effective Cybersecurity Incident Response, 2021.
- [5] Riebe, D., et al., Role of CERTs in Cybersecurity, 2021.
- [6] Mitropoulos, F., et al., Digital Identities in Cybersecurity, 2006.
- [7] Ahmad, A., et al., Information Security Management and Incident Response, 2020.
- [8] The Importance of Efficient Incident Response Systems, 2020.
- [9] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Revision 2, 2012.
- [10] P. Venmuri, T. Johnson, and R. Lopez, "Ethical Implications of Cybersecurity Incident Response," Journal of Cyber Ethics, vol. 15, no. 3, pp. 245-267, 2023.
- [11] J. Shaw, "Corporate Moral Responsibility in Cybersecurity," Business Ethics Quarterly, vol. 27, no. 2, pp. 123-141, 2017.
- [12] M. Mitropoulos, E. Stavrou, and J. Samaras, "Digital Identity Verification in Cybersecurity," Cybersecurity Journal, vol. 9, no. 4, pp. 101-119, 2006.
- [13] R. Cormack, "Privacy Concerns in Incident Response," Journal of Information Security, vol. 18, no. 2, pp. 221-237, 2016.
- [14] D. Tutton, "Legal Challenges in Cyber Incident Management," Information Law Review, vol. 22, no. 1, pp. 56-74, 2010.
- [15] S. Aoyama, K. Tanaka, and L. Nishimura, "Transparency in Cyber Incident Response," International Journal of Cyber Crisis Management, vol. 5, no. 1, pp. 34-48, 2020.
- [16] J. Shaw and M. Miller, "Ethical Decision-Making in Cybersecurity," Business Ethics Review, vol. 30, no. 1, pp. 88-102, 2025.
- [17] K. Riebe, L. Hartmann, and P. Klein, "Fairness in Cybersecurity Incident Response," Journal of Ethical Hacking, vol. 12, no. 3, pp. 199-212, 2023.
- [18] J. Shaw, "Corporate Moral Responsibility in Cybersecurity," Business Ethics Quarterly, vol. 27, no. 2, pp. 123-141, 2017.



Member Benefits!



Certificate of Cloud Security Knowledge (CCSK)

Training Offer Exclusively For ISSA Members

The Certificate of Cloud Security Knowledge (CCSK) is widely recognized as the standard of expertise for cloud security and provides you with the foundations you need to secure data in the cloud. The newly updated course covers CSA's Security Guidance v.5 and provides an in-depth understanding of the full capabilities of cloud computing, and enables you to prove your skills in Zero Trust, DevSecOps, Cloud Telemetry and Security Analytics, Artificial Intelligence, and more. Choose from self-paced online, instructor-led online, in-person or self-study trainings to gain the knowledge you need.

CSA and ISSA have partnered to provide an **exclusive 20% ISSA member discount.**



MindEdge is a premier developer of online learning solutions, including certificate and professional development courses.

Cybersecurity Awareness Month Special!
Promo Code: ISSACYBERMONTH
20% off all courses

Courses Include:

[Real-World Cloud Cybersecurity Scenarios](#)
[Security Architecture and Engineering](#)
[Networking for Success](#)

And many others to choose from in the ISSA catalog.

Join Today:

www.issa.org/membership



Journey of Privacy and Protection: A Privileged Access Management Perspective



By: Anderson Viotti, Security Engineering Lead at Mars

1. Introduction

In today's interconnected digital landscape, the protection of personal information has become a paramount concern. Despite advancements in cybersecurity, the frequency and sophistication of privacy breaches continue to escalate. Privileged Access Management (PAM) is critical in safeguarding sensitive data and infrastructure. Organizations can mitigate risks associated with unauthorized access and data breaches, when they manage and monitor privileged accounts. This article explores practical use cases, and best practices for effectively implementing PAM. It also examines how PAM aligns with the Zero Trust security model, emphasizing its importance, common breaches related to privilege abuse, and key features essential for robust security measures.

2. Privacy Challenges in Today's Cybersecurity Environment: The Role of Privileged Access Management (PAM)

The rapid adoption of cloud services and the proliferation of Internet of Things (IoT) devices have significantly expanded the attack surface for cyber threats, highlighting critical privacy challenges that organizations must address, particularly in the context of Privileged Access Management (PAM). Cloud services provide scalability and operational efficiency but introduce complexities in managing access to sensitive data stored off-premises. Improperly configured cloud environments or mismanaged privileged credentials can lead to unauthorized access, compromising data privacy and regulatory compliance.

Similarly, IoT devices are integral to modern business operations but often lack robust security protocols, making them susceptible to exploitation by malicious actors. Compromised IoT devices can serve as entry points for unauthorized access to critical systems and data, posing significant privacy risks. Regulatory frameworks such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) impose strict requirements on organizations to protect consumer data privacy. Effective PAM strategies are essential for ensuring compliance by

securing privileged accounts, monitoring access activities, and promptly detecting and responding to potential breaches. Implementing PAM solutions involves deploying privileged session management, least privilege access controls, and comprehensive auditing capabilities. These measures help mitigate risks associated with privileged accounts, ensuring that only authorized personnel have access to sensitive data and systems.

3. Understanding Privileged Access Management

Privileged Access Management (PAM) encompasses the processes and technologies designed to control and monitor access to critical systems and data within an organization by privileged users. These users typically possess elevated rights that, if exploited or misused, could result in severe security breaches. Effective PAM solutions incorporate several key components, including credential vaulting to securely store and manage privileged credentials, credential rotation to regularly update passwords and access keys, session isolation and monitoring to oversee and record privileged sessions in real-time, and privileged threat and user behavior analytics to detect anomalies and potential threats promptly. PAM plays a crucial role in enhancing cybersecurity posture by enforcing the principle of least privilege, ensuring that privileged access is granted only when necessary and for authorized tasks. By implementing robust PAM frameworks, organizations can mitigate the risks associated with insider threats, external cyber attacks, and inadvertent misuse of privileged credentials, thereby safeguarding sensitive data and maintaining regulatory compliance.

4. Critical Role of PAM in Zero Trust Security Frameworks

The Zero Trust model is a security framework that assumes no implicit trust, regardless of whether the access request originates from inside or outside the network. In this model, every access request is verified, authenticated, and authorized, ensuring the principle of "never trust, always verify." PAM plays a crucial role in Zero Trust by controlling and monitoring privileged access, ensuring that elevated permissions are only granted when absolutely necessary and continuously verified.

Furthermore, navigating the complex regulatory landscape adds another layer of challenge. Regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States impose strict requirements on how organizations collect, process, and protect personal data. Failure to comply can lead to severe financial penalties and reputational damage.

5. Uncovering Cybersecurity Vulnerabilities: The Impact of Insufficient Privileged Access Management (PAM)

Many high-profile cybersecurity breaches have been attributed to the misuse or compromise of privileged accounts. Without PAM, organizations are at risk of attackers gaining elevated access to critical systems, leading to data breaches, financial losses, and reputational damage. Some notable examples include:

The Target Breach (2013):

Attackers gained access through compromised vendor credentials and moved laterally within the network, leading to the exposure of 40 million credit card numbers. The attackers initially accessed Target's network via stolen credentials from a third-party Heating, Ventilating and Air Conditioning (HVAC) vendor. Once inside, they leveraged the lack of PAM to escalate privileges and gain deeper access to Target's systems, eventually exfiltrating vast amounts of sensitive data.

Target faced over \$200 million in costs related to the breach, including settlements and legal fees. The breach also caused significant reputational damage, impacting customer trust.

The Uber Breach (2016):

Hackers accessed privileged credentials stored in a public repository, resulting in the theft of sensitive user and driver data.

Uber's developers had inadvertently posted privileged access credentials to GitHub, which attackers discovered and used to access Uber's data stored on AWS. The absence of PAM controls allowed the attackers to use these credentials to navigate Uber's systems unchecked.

The breach affected 57 million users and drivers, leading to a \$148 million settlement and severe criticism for Uber's delayed disclosure of the breach.

The SolarWinds Attack (2020):

Compromised privileged accounts were used to infiltrate multiple government and private sector networks.

Attackers inserted malicious code into SolarWinds' Orion software update, which was subsequently distributed to thousands of customers. Once installed, the attackers used privileged accounts to move laterally within affected networks, remaining undetected for months due to insufficient PAM controls.

The attack compromised numerous high-profile organizations, including U.S. government agencies, leading to widespread data breaches and significant security concerns.

Robust PAM practices, such as managing privileged accounts and protecting credentials, continuous monitoring and anomaly detection, could have identified suspicious privileged account activities early, potentially limiting the extent of the breach.

6. Unlocking Protection and Threat Mitigation: 4 Key Features Every PAM Solution Must Have

Credential Vaulting and Password Manager:

- Securely stores and manages privileged credentials, enforcing strong password policies, rotation schedules, and encryption standards to centralize password management.
- Prevents unauthorized access by securing credentials in non-accessible locations, enhancing security against credential theft and ensuring compliance with regulations. These features minimize human error and strengthen overall protection against unauthorized access and cyber threats.

Session Isolation and Monitoring:

- This feature ensures that each privileged session is isolated from other network traffic and sessions, reducing the risk of lateral movement and unauthorized access.
- Includes real-time monitoring of privileged sessions, capturing and logging all activities such as keystrokes and commands executed. Detailed logs provide an audit trail essential for compliance and incident response purposes.

Just-in-Time Access:

- Enhances security by granting temporary privileged access only when necessary, whether for internal staff or third-party vendors, thereby mitigating the risk of persistent exploitation of privileged accounts. Access privileges are granted and revoked promptly as needed.
- Enforces strict access controls to minimize vulnerabilities, thereby strengthening overall security posture and safeguarding critical infrastructure from unauthorized access and potential breaches.

Behavioral Analytics:

- Provides advanced protection by analyzing user behavior to detect anomalies.
- Identifies deviations that may indicate potential insider threats or compromised accounts. Early detection enables swift mitigation measures, such as account lockdowns or additional authentication requirements, enhancing overall security and minimizing the impact of unauthorized access and malicious activities.

7. Identifying Potential Gaps in PAM Implementation: Overlooked Accounts, Administrative Oversight, and Other Critical Areas

While Privileged Access Management (PAM) solutions are critical for securing sensitive assets, several key areas often present gaps that can undermine their effectiveness. One significant issue is the oversight of accounts that are not properly managed within the PAM system. This includes accounts, like domain administrators, that are not assigned to PAM policies or are inadvertently excluded from regular audits, leaving them vulnerable to exploitation.

Another critical gap lies in administrative oversight. In some cases, administrators may not have comprehensive visibility or control over all privileged accounts and activities. This lack of oversight can lead to gaps in monitoring and enforcing security policies, potentially exposing the organization to security risks.

Furthermore, the integration of PAM across all IT infrastructure components is essential but often challenging. Incomplete integration or misconfigurations can create gaps where certain systems or endpoints are not adequately protected by PAM measures.

Addressing these gaps requires a holistic approach that includes regular audits, comprehensive training for administrators, and thorough integration testing. By identifying and rectifying these potential vulnerabilities, organizations can strengthen their overall security posture and ensure that their PAM solutions provide robust protection against unauthorized access and threats.

8. Future Directions and Emerging Trends in Cybersecurity

Looking ahead, the future of privacy protection will likely be shaped by advancements in technologies such as artificial intelligence (AI) and machine learning (ML), which can enhance PAM capabilities by enabling predictive analytics and proactive threat detection. Additionally, regulatory frameworks are expected to evolve further, with new laws and regulations addressing emerging privacy concerns in areas like biometric data and digital identities.

9. Conclusion

In conclusion, Privileged Access Management (PAM) plays a critical role in mitigating privacy risks and enhancing data protection within organizational cybersecurity frameworks. By implementing strategies such as Zero Trust Architecture, Least Privilege Principle, and Continuous Monitoring, organizations can strengthen their defenses against privacy breaches and regulatory non-compliance.

Moving forward, adapting to evolving cybersecurity threats, fostering collaboration across teams, and maintaining transparency will be essential for organizations seeking to uphold privacy rights and maintain trust in the digital age.

References:

- [1] National Cybersecurity Center of Excellence. (n.d.). Privileged Account Management. <https://www.nccoe.nist.gov/financial-services/privileged-account-management>
- [2] Gartner. (n.d.). Zero Trust. Gartner. <https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust>
- [3] National Association of Corporate Directors. (2024, April 09). Privileged Access Management: A Vital Strategy for Combating Identity-Centric Threats. Directorship Magazine. <https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/online-exclusives/2024/april/privileged-access-management-vital-strategy-combating-identity-centric-threats/>
- [4] The New York Times. (2022, September 20). Uber Investigating Breach of Its Computer Systems. <https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html>
- [5] Fortinet. (n.d.). What is Privileged Access Management. Fortinet. <https://www.fortinet.com/br/resources/cyberglossary/privileged-access-management>
- [6] Uber Data Breach (2016): Source: BBC News. "Uber Data Breach: Ex-boss Kalanick 'knew About Hack.'" <https://www.bbc.com/news/technology-42190990>
- [7] SolarWinds Supply Chain Attack (2020): Source: Reuters. "Exclusive: Suspected Russian Hackers Spied on U.S. Treasury Emails - Sources." <https://www.reuters.com/article/us-global-cyber-solarwinds-idUSKBN28Q2A1>
- [8] Target Data Breach (2013): Source: CNBC. "How Target's 2013 Data Breach Compromised 40 Million Credit and Debit Cards." <https://www.cnbc.com/2020/05/06/how-targets-2013-data-breach-affected-the-retail-industry-7-years-later.html>



Anderson Viotti is a cybersecurity professional with over 8 years of experience, specializing in Privileged Access Management (PAM). He designs and implements strategies that safeguard critical systems around the world. Passionate about driving innovation in cybersecurity and exploring creative solutions to keep our digital world safe. Anderson is a member of the [ISSA Brasil Chapter](#).



General Membership Benefits

Here are just a few of the many reasons why ISSA is the association of choice for cyber security specialists around the world:



Local Chapters



Professional Networking



Learning and Development



Career Advancement



Leadership Opportunities



Recognition



The ISSA Journal



Exclusive Savings



Earn CPE/CPU Credits



Access to a Global Network

ISSA 40th Anniversary Special Membership Offer

Join or Renew with ISSA Today!

In celebration of ISSA's 40th Anniversary we would like to say thank you for your dedication and support through the years.

\$40 off ISSA General Membership 2 Year during October 2024*
Use Promo Code: 2YEAR-OCT2024

\$15 off ISSA General Membership 1 year during October 2024*
Use Promo Code: 1YEAR-OCT2024



Events: ISSA, Industry & Chapter



GLOBAL CHAPTER & MEETING EVENTS

Alamo San Antonio Chapter

- Quarterly Meeting & Chapter Elections, November 19, 12:00 PM - 4:30 PM CT, Maggiano's Little Italy - The Rim, 17603 I-10, San Antonio, TX 78257.

Central Maryland Chapter

- ISSA Central MD Meeting, November 20, 5:00 PM - 7:00 PM ET, Leidos Franklin Building, 6841 Benjamin Franklin Drive, Georgia Conference Room, Columbia, MD 21046.

Central Ohio

- Toastmaster, November 13, 6:00 PM - 8:00 PM ET, 4675 Lakehurst Court, Dublin, OH, 43016.
- Monthly Meeting, November 20, 7:45 AM - 11:30 AM ET, Upper Arlington CoHatch, 1733 West Lane Avenue, Upper Arlington, OH 43221.

Chicago Chapter

- Chapter Meeting, November 7, 3:00 PM - 5:00 PM CT, Carlucci's, 6111 N River Road, Rosemont, IL 60018.

Denver Chapter

- Chapter Meeting (Afternoon), November 13, 11:00 AM - 1:30 PM MT, Trace3, 4601 DTC Boulevard #400, Denver, CO 80237.
- Chapter Meeting (Evening), November 13, 5:00 PM - 7:30 PM MT, Gensler Denver Office, 1225 17th Suite #150, Denver, CO 80202.
- ISSA Women in Security, November 20, 5:30 PM - 7:30 PM MT, Trace3, 4601 DTC Boulevard #400, Denver, CO 80237.

Hawaii Chapter

- End-of-Year Luncheon Meeting, November 15, 11:30 AM - 1:00 PM HST, Dave and Buster's, Hale Paina Room, 1030 Auahi Street, Honolulu, HI 96814.

Kansas City Chapter

- Chapter Meeting & Happy Hour, November 7, 5:00 PM - 7:00 PM CT, Seasons 52, 340 Ward Pkwy, Kansas City, MO 64112.

Kentuckiana Chapter

- Monthly Meeting, November 1, 11:30 AM - 1:00 PM ET, Farm Credit Mid-America Building, 12501 Lakefront Place, Louisville, KY 40299.

Los Angeles Chapter

- Dinner Meeting, November 20, 5:30 PM - 9:00 PM PT, Accenture, 1003 E 4th Pl 8th floor, Los Angeles, CA 90013.

North Alabama Chapter

- November Chapter Lunch, November 19, 11:30 AM - 12:30 PM CT, Auburn University Research and Innovation Campus, 345 Voyager Way NW, Huntsville, AL 35806.

Poland Chapter

- Advanced Threat Summit, November 13-15, Onsite & Online: www.atsummit.pl.

Silicon Valley Chapter

- November 2024 Event, November 19, 5:30 pm - 8:30 PM PT, Fortinet Inc., 909 Kifer Rd, Sunnyvale, CA 94086.

South Texas Chapter

- South Texas ISSA & ISACA GHC: CISA Prep Review Course, November 4-8, 8:00 AM - 4:30 PM CT, Microsoft Corporation, 750 Town and County Blvd., Suite 1000, Houston, TX 77024.
- ISSA South Texas Chapter Meeting: Emeritus Panel, November 14, 11:30 AM - 1:30 PM CT, The Ballroom at Tanglewood, 5430 Westheimer Ct., Houston, TX 77056.



ISSA EVENTS

November 13 - Webinar: Unlocking Zero Trust: A Blueprint for Secure Operations (1:00 PM - 2:00 PM ET)

Join us for an enlightening webinar as we explore the intricacies of embracing the Zero Trust Model, from theory to practice. Whether you're a novice or seasoned professional, this session will equip you with expert insights and actionable strategies for implementing Zero Trust principles effectively. Dive deep into understanding the Zero Trust Model and discover how it can revolutionize your cybersecurity approach.

November 19 - Webinar: Privacy is About More Than Just Regulation (1:00 PM - 2:00 PM ET)

In recent years privacy regulation has taken over the globe. Many companies have made changes to their websites and applications in order to comply with these laws, while at the same time neglecting the changing technical infrastructure upon which those systems are built. In this session Cory Underwood will review the slate of changes imposed by browsers and operating systems in recent years which continue to impact existing architectures, and how those changes impact existing business processes.

Your ISSA International Board



Jimmy Sanders
President



Deb Peinert
Vice President



David Vaughn
CFO/Treasurer



Lee Neely
COO/Secretary



Dr. Curtis Campbell
Director



Laura Harder
Director



Stefano Zanero
Director



Mary Ann Davidson
Director



Connie Matthews
Director



Gene McGowan
Director



John Johnson
Director