



ISSUE 1 | VOL. 23 |
www.issa.org

JANUARY-FEBRUARY
2025

ISSA

Information Systems Security Association

**A CISO'S
GUIDE TO
AI & PRIVACY**

**2024
ARTICLE OF
THE YEAR**

**Is TikTok a
National
Security
Risk?**

**THE PYTHON PROGRAMMING LANGUAGE:
NUMERICAL ANALYSIS/MACHINE LEARNING SERIES**

BRIDGING THE GAP

AN ANALYSIS OF DIGITAL FORENSICS CREDENTIALING

Advancing Information Security, Empowering Professionals



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 23 - ISSUE 1

FEATURE FOCUS

13 Bridging the Gap (Part 1): An Analysis of Digital Forensics Credentialing

This research is aimed at presenting a case for a framework to be developed for credentialing digital forensic professionals. This first part will delve in to the problems caused by lack of such a framework by presenting the literature available in the area and by presenting some case studies. Future parts will present the key findings, outline for such a framework, and next the framework itself.

SUPPLEMENTARY SEGMENTS

21 Training Tomorrow's Security Experts in AI and LLM Application Security

As AI adoption accelerates, security professionals must be equipped to understand and mitigate the risks associated with AI and large language models (LLMs). This article explores key training strategies, including foundational AI knowledge, identifying AI-specific vulnerabilities, regulatory compliance, and hands-on learning to prepare the next generation of security experts for emerging AI threats.

24 The Python Programming Language

Numerical Analysis/Machine Learning Series
This article is part of a series of articles which deal with topics in programming using the Python programming language. In this article we will review the various ML algorithms which have been presented and proceed with an introduction to neural networks and deep learning.

2024 ARTICLE OF THE YEAR

08 Is TikTok a National Security Risk?

An analysis of the popular social media platform among younger Americans, and its potential impact to national security.

DEPARTMENTS

05 EDITORS CORNER

Reviewing the theme of this issue and contributions.

07 PRESIDENTS LETTER

Update from the ISSA International President.

27 NEWS FROM THE FOUNDATION

2024 Scholarship Winners and More News!

30 PRIVACY SIG THOUGHT LEADERSHIP

A CISO's Guide to AI & Privacy

32 COMMITTEE UPDATE

The AIM Committee Leadership team provides an update of what they are up to and how they are planning to support the community.

33 EVENTS: ISSA, INDUSTRY & CHAPTER

Global Chapter & Meeting Events and ISSA Specific Events

VOICES

11 CRYPTO CORNER

It's About Time.

19 CRYPTIC CURMUDGEON

Listening to AI?

28 THE CYBER LIBRARY

Reviewing the Works of Yuval Noah Harari, and Ethan Mollick

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 12

ISSA Chapter List 20

ISSA Board 34

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/>

Editors Corner



Jack Freund

- Charlotte Metro Chapter
- Editor, ISSA Journal
- ISSA Distinguished Fellow
- Vice President, ISSA Education Foundation

Dear ISSA Members,

Welcome to the January/February 2025 issue of the ISSA Journal! As we step into a new year, we find ourselves at the crossroads of relentless technological evolution and the enduring mission to secure our digital world. The rapid adoption of artificial intelligence, the challenges of upskilling our workforce, and the need for robust frameworks in emerging domains like digital forensics and application security continue to shape our landscape.

This issue offers a rich selection of articles and columns that address these critical topics:

- **A CISO's Guide to AI and Privacy:** Maryam Meseha provides practical insights into building ethical and secure AI governance frameworks, equipping CISOs to navigate the complex intersection of innovation, regulation, and organizational risk.
- **Listening to AI?:** In his Cryptic Curmudgeon column, Robert Slade explores the lessons generative AI can teach us about human psychology and listening skills, emphasizing the art of active engagement amidst technological advances.
- **It's About Time:** Luther Martin reflects on the inexorable passage of time and its implications for cybersecurity professionals, stressing the importance of continuous learning and adaptation.
- **Bridging the Gap: Digital Forensics Credentialing:** Zahadat's feature analyzes the urgent need for standardized credentialing in digital forensics, presenting a case for a structured framework to enhance professionalism and trust in the field.
- **The Cyber Library:** William J. (Jay) Carson reviews two thought-provoking books by Yuval Noah Harari and Ethan Mollick, exploring the role of information networks and AI in shaping our future.
- **Python and Machine Learning:** Constantinos Doskas continues his series on Python programming, delving into neural networks and deep learning while offering practical guidance for aspiring data scientists and engineers.
- **Training Tomorrow's Security Experts in AI Application Security:** Shah discusses strategies for equipping security professionals to address vulnerabilities in AI and large language models, integrating frameworks like OWASP and MITRE ATLAS into training.

These contributions exemplify the depth and breadth of expertise within our community. As you read through this issue, we encourage you to engage with the ideas presented, consider how they apply to your work, and contribute to the ongoing conversations shaping our field. Here's to a year of growth, innovation, and strengthened resilience in cybersecurity.

Warm regards,

Jack Freund, Ph.D.

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)

FOLLOW



@ISSA.org

ISSA International Special Events

Cyber Executive Forum In-Person Meeting

Calling all Cyber Executive Forum Members: The first in-person meeting is scheduled for Thursday & Friday, February 27th - February 28th, 2025.

- Thursday, 5-8PM : Cocktail Reception
- Friday, 8AM-5PM : CEF Meeting
- Friday, 5PM-8PM : Dinner Reception

Register today!

<https://www.issa.org/event/february-cyber-executive-forum-2025/>



Thursday, February 27 - Friday, February 28, 2025



Buckhead Club
3344 Peachtree Road NE, Suite 2600
Atlanta, Georgia, 30326 USA

ISSA International 40th Anniversary & Awards Gala

Join us for this three-day in-person event from Wednesday, April 2nd to Friday, April 4th. Meet friends and colleagues, attend meetings, learn new information, and cheer on your Award-winning peers at the Anniversary Gala.



Planned activities currently include:

- Awards Ceremony
- Cyber Executive Forum Meeting
- ISSA Board Meeting
- Chapter Leaders Meeting

Attend to meet leaders and long-time ISSA members in the cyber community!



Wednesday, April 2 - Friday April 4, 2025



The Westin Galleria Dallas
13340 Dallas Parkway
Dallas, Texas, 75240 USA

ISSA Mixer at the 2025 RSA Conference

Join friends and colleagues at the ISSA Mixer at the RSA Conference 2025 in San Francisco! Pencil in time for the mixer while you are attending the Conference, more ISSA Mixer details will be shared as they become available.



ISSA Mixer Date: TBD



Mixer Venue to be Confirmed
San Francisco, California, USA

RSAConferenceTM2025

San Francisco | April 28 - May 1 | Moscone Center

ISSA Emerging Technologies SIG: "Technical Thought"



An upcoming virtual event ALL ISSA members are invited to attend. More information to be shared in upcoming Member eNewsletters, so watch your email! Tentatively planned for Thursday, May 22nd.

CONTACT MEMBERSERVICES@ISSA.ORG WITH QUESTIONS ABOUT ANY SPECIAL EVENTS.

Presidents Letter



Jimmy Sanders

International President



2025 has started off strong and productive. ISSA International has been collaborating with local chapters and universities to launch the ISSA University program, which enables educational institutions to establish formal ISSA student chapters. We've also seen impressive growth in the formation of new ISSA chapters and significant expansion within smaller chapters. The ISSA International Board and I remain committed to supporting our chapters and members, offering logistics, assistance, and whatever resources are necessary to ensure their continued success.

I'm thrilled to share some exciting news! We are officially announcing the date and details of our 40th Anniversary ISSA Celebration. This milestone event will honor our rich history, celebrate our achievements of today, and showcase our vision for the future. The celebration will take place at the Westin Galleria in Dallas, Texas, on April 4th, 2025. We'll also host executive and student events on April 3rd, with additional activities on April 5th. Our incredible planning committee is working tirelessly to ensure the event will be both inspiring and memorable.

The general conference will run from 9am to 5pm Central Time, and the Anniversary Gala and Dinner will begin at 7pm. I'm incredibly excited to be part of this historic occasion and look forward to celebrating with you, the ISSA International Board, our distinguished leaders, and your peers. Don't miss out on this unforgettable event!

Jimmy Sanders, President
ISSA International Board of Directors



El 2025 ha comenzado de manera fuerte y productiva. ISSA International ha estado colaborando con los capítulos locales y universidades para lanzar el programa ISSA University, que permite a las instituciones educativas establecer capítulos formales de estudiantes de ISSA. También hemos visto un impresionante crecimiento en la formación de nuevos capítulos de ISSA y una expansión significativa en los capítulos más pequeños. La Junta Internacional de ISSA y yo seguimos comprometidos en apoyar a nuestros capítulos y miembros, ofreciendo logística, asistencia y los recursos necesarios para garantizar su éxito continuo.

¡Estoy emocionado de compartir algunas noticias increíbles! Anunciamos oficialmente la fecha y los detalles de nuestra Celebración del 40º Aniversario de ISSA. Este evento tan significativo honrará nuestra rica historia, celebrará nuestros logros actuales y mostrará nuestra visión para el futuro. La celebración se llevará a cabo en el Westin Galleria en Dallas, Texas, el 4 de April de 2025. También tendremos eventos para ejecutivos y estudiantes el 3 de April, con actividades adicionales el 5 de April. Nuestro increíble comité de planificación está trabajando incansablemente para asegurarse de que el evento sea tanto inspirador como memorable.

La conferencia general se llevará a cabo de 9 a.m. a 5 p.m., hora central, y la Gala y Cena del Aniversario comenzarán a las 7 p.m. Estoy realmente emocionado de ser parte de esta ocasión histórica y espero poder celebrarlo con ustedes, la Junta Internacional de ISSA, nuestros distinguidos líderes y sus compañeros. ¡No se pierdan este evento inolvidable!

Jimmy Sanders, President
ISSA International Board of Directors

CYBER EXECUTIVE FORUM

FIRST 2025 CYBER EXECUTIVE FORUM In-Person Meeting

Thursday & Friday February 27th - 28th

Buckhead Club
3344 Peachtree Road NE
Atlanta, Georgia 30326 USA

Register Today!
<https://www.issa.org/event/february-cyber-executive-forum-2025/>

INFORMATION SYSTEMS SECURITY ASSOCIATION
40 YEARS STRONG

2024 ARTICLE OF THE YEAR



IS TIKTOK A NATIONAL SECURITY RISK?

By: Paul Frenken, Enterprise Architect
Consultant

Many of us watched the CEO of TikTok, Shou Zi Chew, give testimony to congress a few months ago. The line of questioning only highlighted how much Congress really does not understand technology, at best it made them look naive and at worst, morons. Their main line of questions focused on privacy issues and if the Chinese Government had access to American data. Chew throughout the line of questioning continued to emphasize that data is not hosted in China. He however, never really answered the question if the Chinese government could gain access to the data.

He conveniently left out the fact that under Chinese law TikTok is obligated to allow government access to company data. Currently there are 3 Chinese laws, National Intelligence Law of 2017, Data Security Law of 2020, and the Cryptology Law of 2020 that require a company doing business in China to allow for the Peoples Republic of China, PRC government to have access to any data it deems necessary. These laws require all Chinese or foreign companies doing businesses in or with a Chinese firm or its citizens to support and facilitate China's government access to the collection, transmission, and storage of data.[1] Virtually giving unfettered access to company records and files, to include business contracts, intellectual property, confidential strategies, and employee and customer personal data. So, it really does not matter where the data is hosted, if a company is owned by a Chinese citizen, does business in China or with a Chinese company the PRC can demand access. [2]

The laws focus on data hosted in China, however they also cover equipment or software made by Chinese firms used in data centers around the world. Another reason why western governments have been focusing on removing Huawei equipment from any western data centers due to security issues and built in vulnerabilities. In addition to hardware vulnerabilities the law also incentivizes Chinese software firms to build in backdoors to such mobile device applications as TikTok, fitness wearables, and other devices that can provide data to the Chinese government.

What is it? Why is it a threat?

TikTok is one of these mobile applications that is created and owned by a Chinese company, ByteDance. It is a video sharing app that allows users to create and share short form videos on any topic. Upward of 97% of TikTok users utilize it on their mobile device. At first look this is just another playful app that allows people to share their world with friends and family. It is easy to download and setup on your phone. It allows one to easily use to create content with their device and share it with others. Some creators of content have built up large numbers of followers and have been coined "Influencers" as their content can be watched by millions at any given time. Influencers have made millions through endorsements of products and services by just talking about them with their followers. In a word this application is "Popular", not only in the United States, but with almost 1 billion people around the world.

TikTok's facade is that it is a playful fun application for people to have fun with. However, there is anecdotal evidence that it has a more sinister use. FBI director Christopher Wray told lawmakers in September of 2022 he was extremely concerned that PRC could weaponize the media app TikTok. [1] When a person downloads and

opens TikTok on their device it could open it up to hidden code much like a Trojan Horse. Similar to the famous Trojan Horse of the Stuxnet worm. Developed in 2005, this highly specialized worm floated around the world for almost 5 years before it was discovered in 2010. It went to work in early 2011 when an Iranian engineer had it on his computer and plugged into a network that connected to centrifuges in one of the Iranian Uranium enrichment plants. The virus infected the centrifuges and caused them to spin out of control damaging the internal components of the hardware. The damage to the hardware set back the Iranian enrichment process by 3 to 5 years. A TikTok Trojan Horse could act the same way but with even more impact by damaging American society.

When you download and install TikTok it asks for access to the following items on your phone the camera, microphone, WIFI connection, and your contact list. These items are expected for a video collection and sharing app. However, there are other items that seem to be suspicious for a video recording application such as access to GPS, network, IP addresses, clipboard, photos, calendar, browser cookies and the ability to read, write, and delete contents in your phone's memory. Once installed it can install and remove apps and shortcuts, record your keystrokes, read home screen settings, and reorders running apps. The most concerning requests is that it wants access to other apps on your phone in addition to your biometric data such as your faceprint, voiceprint, or your fingerprint if you use these as a security authentication on your phone. These are items that we know it accesses or utilizes. What about what we don't know. Could the PRC have hidden code buried in the application that sends more information to a state-sponsored agency? Could there be a Trojan Horse concealed within TikTok?

China is notorious for stealing sophisticated military weaponry and intellectual property and now with TikTok it can gain access to over 100 million Americans' personal information. With TikTok on your phone it is now collecting personal information about your usage or even waiting for a more sinister motive.

Think about all that you do on your phone. Many of us shop on our phones through Amazon, Home Depot, Walmart, or purchase groceries from our local supermarket. We have an app for our insurance, health track our blood pressure, sugar, or weight. Purchase airline tickets, Uber/Lyft, Bank, Venmo, or trade stock, or have a digital wallet. We access IoT devices such as our ring, web cameras, or the countless other IoT devices in our homes and businesses. Our phone is the key to our personal, financial, and health information and interaction to the world around us.

Think about if you lost your phone, the mental anguish you would go through, the fear of some bad actor getting into our lives and messing up what we have worked so hard to organize. We simply do not know what is in TikTok's code base as it is proprietary. Unlike China, most of the western world does not require companies to give their governments unfettered access to code base or collected data. No one knows if there is a Trojan Horse built into its code. However, many in the intelligence and security communities believe that it is not if, but how many are hidden within its code. According to the Counterterrorism Group, TikTok is very likely collecting account data such as usernames, passwords, and credit card information on several of your applications on your mobile device and could transfer funds or hold data for ransom to obtain financial profits.[1] This information could be used later to hold you hostage.

What Would Happen If?

What would happen to your personal life if someone got a hold of your phone and was able to log into your bank account and transfer money to an offshore account. Use your digital wallet for cash advances or purchase of services or merchandise. Log into your Amazon account and order hundreds or thousands of dollars' worth of merchandise. Buy airline or cruise tickets using your stored credit card information. Gain access to your retirement or broker's account and sell your portfolio then transfer the funds out of the account. Cancel your insurance, capture your biometric data, create and send inappropriate email to your contact list, damage to your reputation and credit, the list goes on. Visualize the chaos that would occur if all the apps on your phone did the opposite of what you wanted. Think about the work it would require, the dozens of phone calls, emails, and possible lawyer expenses to get some of your life back in order. It could take months or even years of constant effort to try to fix your life. In some cases, it will never be the same.

Imagine the other side of the coin, all the work a business will need to do to try to get your accounts cleaned up, if they can, return the money, restock or write off merchandise that was missed ordered and shipped, cancel and reissue credit cards, close and reopen new bank, brokerage, insurance accounts, etc. Collectively the firms that you do business with could spend several hundred-man hours correcting your accounts. Mind you in some cases they are not legal bound to correct these issues, this work is a direct expense and negatively impacts their bottom line. They do this work out of positive customer service. They could choose not to clear up the issues if it becomes too costly.

Preemptive Strike

Now let's step up this to how it could be a national security issue. Imagine the Chinese want to make a preemptive strike against the United States. As they coordinate an invasion of Taiwan, they activate the Trojan Horse in TikTok that runs through your phone's apps and does the mass bank account clearing, credit card purchasing, appointment canceling, email sending, totally reeking havoc with your personal life. Now multiply it by 100 million users. 100 million users experiencing issues with their life essentials would inflict havoc across our society tying up our financial, retail, and health care infrastructure. This act would pull our attention from the regional conflict in the west Pacific to our homeland. Institutions we take for granted would be in chaos, it would take months or even years to fix the billions of issues and billions of dollars that would be experienced by American society. We would not be able to focus on the matter at hand an ally being invaded with such chaos going on in our society.

Now think about the soldier or sailor stationed overseas in direct conflict with the Chinese. With communication being relatively easy with the home front they may have direct and instant contact with their loved ones at home experiencing this pandemonium. How do you expect them to focus on the task at hand when they are distressing about what their family is dealing with back home trying to fix their lives.



It was recently confirmed in an October 22, 2023 60 Minute story, The Five Eyes, that China is the defining threat to our current era and is using every resource available to gather and/or steal technology and intellectual property.[1]

Given its history and national goals it is hard to believe that PRC would not be using this platform to spy, influence, manipulate, or launch an attack on the western world as they attempt to usurp the United States as the world's preeminent superpower. There is anecdotal evidence that TikTok has hidden code within its codebase.

For this reason, the US government and several state governments have banned TikTok from being on government devices. In April of 2023 Montana lawmakers passed a bill, SB 419[2], making it illegal for app stores to give users the option to download the app and making it illegal for the company to operate within the state. Additionally, several public universities across the country have prohibited the app and other Chinese products from being accessed on campuses. As a push back, TikTok has started a public relations campaign in the past few months airing commercials on television promoting the positives of the TikTok app by users. With the hope of defending their usefulness and down playing the application's threat to the general public. The PRC is a motivated puppet master and has stated in public that its goal is to replace the United States as the sole superpower. There is plenty of evidence that TikTok is a tool they would use to bring the average American to their knees. TikTok is spyware that we need to treat as such and ban it from our society by removing it from our phones and out of our lives. I understand that this stance will impact some people negatively, however leaving it alone will crimp the nation and damage our society beyond repair when the PRC activates the sinister parts of the app.

References:

1. Wiley, "U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data:" <https://www.wiley.law/newsletter-Mar-2021-PIF-US-Businesses-Must-Navigate-Significant-Risk-of-Chinese-Government-Access-to-Their-Data>, Nazak Nikakhtar, March 2021
2. The Hill, "For Chinese firms, theft or your data is now a legal requirement." <https://thehill.com/opinion/cybersecurity/532583-for-chinese-firms-theft-of-your-data-is-now-a-legal-requirement/>, B. Thayer, January 7, 2021
3. Forbes, "Is TikTok Really A National Security Threat?" <https://www.forbes.com/sites/petersuciu/2022/11/18/is-tiktok-really-a-national-security-threat/?sh=79078a2d4ade>, Peter Suci, November 18, 2022
4. The Counterterrorism Group, "TIKTOK'S Data theft and A Trojan Threat to Latin America" <https://www.counterterrorismgroup.com/post/tiktok-s-data-theft-and-a-trojan-threat-to-latin-america>, M. Tovar, R. Flood, August 2022
5. CBS News 60 Minutes, "More from the 'Five Eyes' intelligence chiefs' warning to 60 Minutes - CBS News" <https://www.cbsnews.com/news/more-from-five-eyes-intelligence-chiefs-warning-to-60-minutes/>, B. McCandless Farmer, October 22, 2023
6. Montana Legislative Services, "leg.mt.gov/bills/2023/billhtml/SB0419.htm", April 18, 2023



About the Author

Paul Frenken is an Enterprise Architect consultant focusing on bringing value by implementing emerging technology and best business practices for his clients. He brings more than 25 years of experience in IT infrastructure, development, change management, customer and consulting services.



He is also a member of the Central Ohio ISSA Chapter (<http://centralohioissa.org/>).

2025 ISSA

International Awards

Nomination Window Closes February 10th for All Categories

Nominate Today!





ISSA
Chapter
of the
Year
2025



ISSA
Organization
of the
Year
2025



ISSA
Security
Professional
of the
Year
2025



ISSA
Volunteer
of the
Year
2025



ISSA
President's
Award for
Public Service
2025



ISSA
Hall
of
Fame
2025



ISSA
Honor
Roll
2025

It's About Time

By: Luther Martin, ISSA Member, Silicon Valley Chapter

It's now the beginning of another year. I don't really do New Year's resolutions, but by December, I usually have a plan for what I hope to accomplish over the next 12 months. I'll admit that I probably only accomplish about 75 percent of what I hope to most years, but I've found that I really need concrete, quantifiable goals to shoot for. Without them, I tend to flounder and waste lots of time.

When a new year starts, I often end up thinking a lot about time. Luckily, lots of other people have already done this, and it usually turns out to be more efficient to just revisit their ideas than to try to think of new ones on my own. I'd like to think that I'm clever enough to think of something new and relevant for this, but I'm not. As someone once noted, "A man's got to know his limitations."

The fact that we always lose the battle that we all fight with time seems to be one of the ideas that the really clever people revisit. Robert Oppenheimer didn't quite get the quote from the Bhagavad Gita (11.32) quite right when he said, "I am become death, destroyer of worlds." The actual text notes that Krishna said that he was time, destroyer of worlds, referring to the fact that we always lose our battle with it.

A thousand or so years later, Ovid (Metamorphoses 15, 234) talked about "tempus edax rerum," time, devourer of all things, while Virgil (Georgics 3, 284) noted how "fugit irreparabile tempus," irreplaceable time flees. Fast-forward to Elizabethan times, and Shakespeare's Sonnet 19 talks about what "devouring time" does to the world.

More recently, "time" is the answer to one of the riddles in the contest between Gollum and Bilbo in *The Hobbit*: "This thing all things devours; / Birds, beasts, trees, flowers; / Gnaws iron, bites steel; / Grinds hard stones to meal; / Slays king, ruins town, / And beats mountain down." Even more recently, Delmore Schwartz said that "Time is the school in which we learn, / Time is the fire in which we burn." Pink Floyd might even have had something to say about this.

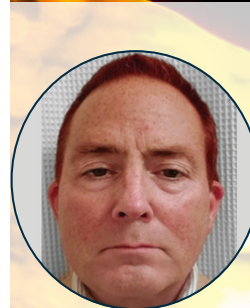
But time can also be your friend. The gains that compound over time can eventually make you a millionaire from only a modest regular contribution to your 401(k), and the same sort of compounding can take you from an entry-level employee to a world-class expert. A one percent improvement per week will add up to over a 1,000 percent improvement over five years! If you're not an expert now, a regular, modest improvement compounded over time can easily make you one.

Benefitting from this sort of compounding is particularly important in the cybersecurity world, where things change very quickly. If you don't keep up with technology, that's just like your knowledge being eroded, much like inflation erodes the value of a dollar or euro. I'd guess that advances and changes in technology are compounding at least 1 percent per month. That's barely noticeable after just a few months, but after 5 years, the usefulness of what you know is roughly only half of what it was 5 years ago. After 10 years, you're down to about 30 percent. You should have been replaced well before then.

I fully understand how hard continuous improvement is to actually do. There were several years when I gave up on shooting for this sort of regular and consistent gain, something that I deeply regret now. That's time that I can never get back, and my lack of motivation led me to accomplish much less than I could have. I first realized how far I had fallen behind when I took a few classes through the (at the time brand-new) on-line education platform Coursera.

In one of the first Coursera classes I took, we learned about research that was fairly recent. The world had changed but I didn't notice because I wasn't paying attention. Instead, I was just focused on the many arcane details that you need to worry about when developing and shipping software. It took more than a year of extremely hard work to recover from my mistake. I eventually took 65 classes through Coursera, and I still felt that there were more things that I should have learned about. This wasn't easy. Instead of just spending 15 minutes a day to stay current, I lost over a year of my free time playing catch-up instead. Stopping the continuous improvement was not one of my better decisions, and it's a mistake that I definitely won't make again.

But enough random thoughts about time. Now it's time to get back to work.



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.

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



Privacy for the People by the People

February 18th
1PM ET



COMMUNITY SPONSOR SERIES

GET OFF THE ASSESSMENT TREADMILL.
TAKE A DATA-FIRST, QUESTIONNAIRE-SECOND APPROACH TO TPRM

March 26th 1PM ET

Recent On-Demand Web Conferences

SPONSORED BY:



CREATING & MANAGING AN EFFECTIVE MENTORSHIP PROGRAM, METHODS & BEST PRACTICES TO CONSIDER



A CISO Guide to AI and Privacy



Privacy & Security: Different But Equal and Why They Need to Work Together



COMMUNITY SPONSOR SERIES

Close the Vulnerability Gap: Using Better Intelligence for Better Prioritization

BRIDGING THE GAP (PART 1): AN ANALYSIS OF DIGITAL FORENSICS CREDENTIALING

By: Dr. Nima Zahadat

In the medical and legal professions, credentialing and accreditation at the state and sometimes national levels are not merely formalities; they are fundamental requirements that ensure the competence and trustworthiness of practitioners. A doctor practicing medicine without a state license or a degree from an accredited institution would almost certainly face severe legal repercussions, including lawsuits and prosecution. Likewise, the public's trust in a lawyer is heavily contingent upon the lawyer holding proper credentials from an accredited university and certification by state or federal authorities. Even the role of a private investigator typically necessitates state licensing in most jurisdictions.

In stark contrast, the field of digital forensic investigation (or for that matter any forensics investigation), despite its critical role within forensic science, lacks such standardized and professional credentialing and accreditation requirements. Digital forensics, which has been evolving since the 1970s, has become increasingly vital as cyber-attacks and computer-related crimes have proliferated (Altheide & Carvey, 2011). This specialized area focuses on analyzing evidence from digital sources such as computers, mobile devices, storage systems, social media platforms, and cloud services, to support legal proceedings and other investigative processes (Mohay, 2005). Core activities in digital forensics include data extraction, collation, carving, and the preparation of detailed forensic expert reports.

However, despite the field's growing importance, there are no universally recognized national or state standards for digital forensic credentialing. While some states have attempted to introduce such standards, these efforts have frequently been inconsistent and disorganized, often leading to more complications than resolutions within the legal system. A common process has been the tendency of states to conflate digital forensic credentialing with private investigator (PI) licensing. This approach is problematic because the skills and expertise required for digital forensics differ significantly from those required for traditional PI work. Such an amalgamation raises concerns about the adequacy and appropriateness of the credentials held by digital forensic investigators.

The absence of standardized credentialing and accreditation in digital forensics poses a significant risk to the field's integrity and the legal processes that rely on it. Without clear and consistent standards, the validity and reliability of digital forensic evidence may be undermined, potentially jeopardizing the outcomes of legal cases. As the reliance on digital forensic evidence continues to grow in addressing cybercrimes and other technology-related offenses, the need for a rigorous and universally recognized system of credentialing and accreditation becomes increasingly urgent. Establishing such a system would not only enhance the professionalism and credibility of digital forensic practitioners but also ensure that the investigations they conduct meet the highest standards of accuracy, impartiality, and technical expertise.

To protect the integrity of the field and the legal outcomes it influences, it is imperative that a robust, nationally recognized framework for digital forensic credentialing be developed and implemented. This framework should be distinct from, yet complementary to, existing licensing requirements for other investigative professions, reflecting the unique challenges and demands of digital forensics.

Here are some examples of how some states and localities have addressed forensic investigation credentialing:

- **Alabama:** The state offers no forensic licensing credentials, but the city of Mobile requires a city-issued PI license for forensic work (Leonardo, White, & Rea, 2012).
- **Colorado:** The state does not mandate digital forensic requirements, and PI licensing is voluntary, allowing individuals to obtain PI licenses even if they have legal issues elsewhere.
- **District of Columbia:** Washington, DC requires a PI license for digital forensic examiners (Leonardo, White, & Rea, 2012).
- **Georgia:** The state requires digital forensic examiners to obtain PI licensing (Leonardo, White, & Rea, 2012).
- **Indiana:** As of 2010, Indiana has no credentialing or licensing requirements for digital forensic examiners (SANS, 2010).
- **Maine:** Similar to Georgia, Maine mandates PI licensing for digital forensic examiners (Leonardo, White, & Rea, 2012).

- **Maryland:** Maryland requires a PI license for private investigations but does not address digital forensic licensing or credentialing.
- **North Carolina:** The state has no licensing requirements for forensic investigators (SANS, 2010).
- **Oklahoma:** Oklahoma permits the use of a PI license from another state for temporary licensing, a practice that can be exploited.
- **Texas:** The state requires digital forensic examiners to be licensed as PIs and even includes computer technicians and repair personnel in this requirement (Leonardo, White, & Rea, 2012).
- **Virginia:** In 2011, Virginia codified that PI licensing requirements do not apply to certified forensic individuals employed as expert witnesses. The state has reciprocity agreements with several others, including Georgia (Leonardo, White, & Rea, 2012).

Many states, including New York, Nevada, North and South Carolina, Washington, and Virginia, are increasingly directing private investigators (PIs) to handle digital forensic investigations. However, none of these states provide a clear pathway for independent digital forensic licensing and credentialing, leaving a critical gap in the standardization and professionalization of this emerging field.

A needs analysis conducted by Rogers & Seigfried (2004) identified training and certification as major obstacles, a sentiment echoed by the National Institute of Justice and other key stakeholders. The discipline remains fragmented, with no national framework for curriculum development or standardized training. Pollitt (2010), drawing on over 20 years of experience as a criminal investigator, highlighted the lack of reliable data and rigorous standards in his paper, "A History of Digital Forensics." He underscores the urgent need for a universally accepted certification standard to ensure consistency, credibility, and professionalism across the field.

The National Institute of Standards and Technology (NIST) addressed some of these challenges by publishing Special Publication 800-181, known as the National Initiative for Cybersecurity Education (NICE). This framework aims to establish a common lexicon, foundational frameworks, workforce categories, specialty areas, roles, and detailed knowledge, skills, and abilities required in cybersecurity work. While NICE provides a valuable foundation for the development of digital forensics frameworks and academic curricula, its focus is predominantly on cybersecurity, leaving gaps in addressing specific needs for forensic training, credentialing, and accreditation.

Furthermore, agencies like the NSA and DHS have developed programs to recognize institutions that meet certain standards. The Centers of Academic Excellence in Cyber Defense (CAE-CD) program, co-developed by the NSA and DHS, allows regionally accredited colleges and universities to apply for designation. While such programs are attractive, they remain voluntary and fragmented solutions. These programs focus primarily on cybersecurity processes, rather than offering a comprehensive framework for digital forensics credentialing and accreditation.

As digital forensic investigations become increasingly central to addressing cybercrime and related offenses, the establishment of a robust, universally recognized credentialing and accreditation system becomes more and more essential. Such a system would not only enhance the credibility of digital forensic professionals but also ensure that investigations are conducted with the highest standards of accuracy, impartiality, and technical expertise.

LITERATURE REVIEW

Numerous studies in the field of digital forensic investigations have highlighted a prevailing bias in research, which tends to focus more on applied aspects of the domain rather than on the development of fundamental theories. This bias, however,

is not without justification, given the practical nature of forensic science and the increasing pressure from external factors such as cyber-terrorism and cyber-crimes, which demand more applied research (Nelson, Phillips & Stuart, 2014). As digital forensic investigations evolve, the issue of credentialing at various levels falls squarely within the realm of applied research, perpetuating this bias. Nevertheless, there is strong evidence to support the claim that the lack of a standardized credentialing process remains one of the primary challenges facing the profession today. For example, a study by Flory (2015) revealed that despite Indiana's law enforcement agencies' deliberate efforts to provide digital forensic training, where half of their staff were trained, their capabilities were still rated from low to mid-range. This underscores the urgent need to establish a standardized and comprehensive framework for identifying experts, developing forensic insights through standard operating procedures, and supporting career advancement in the field. The study also highlights the long-standing challenge of credentialing and locating competent experts in digital forensics, further justifying the focus of research in this direction rather than on fundamental theories.

The challenge of credentialing, while significant, seems to be overshadowed by the even more pressing issue of a lack of consistent curriculum development in digital forensics. Consequently, a substantial amount of research is currently devoted to advancing training and creating a teaching framework that can be widely adopted by universities and colleges. Lang et al. (2014) emphasize that the development of a digital forensics curriculum should result in a comprehensive and self-contained tool for teaching the discipline at the university level, given that many institutions fail to offer such courses due to missing entry requirements. Their proposed curriculum includes introductory and advanced courses, along with hands-on laboratory programs. However, they notably fail to address the critical role of credentialing in the development of digital forensic investigators. This omission is consistent across most curricula and reports on the status of digital forensics and related disciplines. For instance, a report by the West Virginia University Forensic Science Initiative (2007), submitted to the Department of Justice (DoJ) on the training and education of digital forensic investigators, provides detailed qualifications and career paths but omits essential information on credentialing. The report is thorough in its coverage of training and career paths, detailing the qualifications, skills, and knowledge required at the Associate, Baccalaureate, and advanced levels, yet it makes a significant omission by not addressing certifications and credentials. This encapsulates the broader credentialing challenge in existing studies, where the issue is often obscured by the lack of a clear training and education framework for digital forensic investigators.

The literature on establishing accreditation and credentialing in digital forensics is relatively sparse and lacks appeal. This is primarily due to the inherent confusion surrounding the field of digital forensics itself. Losavio et al. (2016) make the bold assertion that digital forensics has not yet achieved the status of a profession, and they attempt to justify this claim on several grounds. According to their paper, a profession requires specialized knowledge, training, highly valuable work, self-regulation, a code of ethics, high levels of autonomy, and other significant elements. Certification and credentialing are the means by which a code of ethics, autonomy of practice, and evidence of specialized training are established elements that are currently lacking in digital forensics, according to Losavio et al. (2016). This deficiency has hindered the development of digital forensics as a recognized profession. Several studies have indeed recommended the establishment of standardized frameworks for credentialing digital forensic investigators. Butler (2015) highlights several such recommendations from the National Academy of Sciences (NAS), which include the creation of a standardized accreditation model to achieve recognition, consistency, and the designation of "expert" status for digital forensic investigators.

From the available literature, it appears that a robust framework exists for providing oversight to various accreditation bodies in digital forensics. This includes organizations such as the National Institute of Standards and Technology (NIST), the Department of Justice (DoJ), and the Organization of Scientific Area Committees (OSAC), which have collaborated to conduct research and establish a framework for operationalizing accreditation bodies. The National Commission on Forensic Science, for its part, acts as an advisory body to the DoJ and plays a critical role in the framework for accreditation, which includes advising on training in science and law, testimony and reporting, providing interim solutions, and overseeing accreditation and proficiency testing (Garfinkel et al., 2009). Although a consistent accreditation framework is lacking, there is a clear structure in place to regulate the bodies that offer credentialing.

The development of accreditation oversight in digital forensics has been reported at the national level, coordinated by the DoJ with the advice of NIST. These frameworks have emerged as a product of OSAC's efforts. According to Butler (2017), OSAC has been instrumental in the development and promulgation of technically appropriate and universally accepted documentary standards used by accrediting bodies to audit forensic laboratories and credential forensic investigators. OSAC has since expanded to include a Forensic Science Standards Board, along with various committees and subcommittees responsible for overseeing the approval process for forensic science standards as developed by different scientific area committees.

There are several credentialing bodies, many of which are international, that operate within the field of digital forensics. Gladyshev, Marrington, & Baggili (2014) note that most of these organizations are either for-profit or privately owned, with the government merely providing the operational framework for these bodies to conduct certification and accreditation. These organizations include companies like Mile2 and ISC2, as well as entities such as the EC-Council, the American Board of Information Security and Computer Forensics (ABISCF), the International Association of Computer Investigative Specialists (IACS), and the International Society of Forensic Computer Examiners (ISFCE) (Freiling & Schwittay, 2007). Some of these bodies, particularly ISC2, utilize the standards and frameworks issued by organizations like NIST to offer certifications such as Certified Information System Security Professional (CISSP), Certified Authorization Professional (CAP), and Certified Cyber Forensics Professional (CCFP). For instance, the CAP certification, which includes Digital Forensics Incident Handling, Risk Management, Continuous Monitoring, Auditing, and Assessment, is based almost entirely on NIST guidelines, specifically the 800 series, including 800-86 (Guide to Integrating Forensic Techniques into Incident Response), 800-37 (Risk Management Framework), 800-30 (Risk Management Guide), 800-39 (Managing Information Security Risks), 800-53 (Security Controls), 800-53A (Security Control Assessments), and 800-137 (Continuous Monitoring), among others. Other organizations, such as the EC-Council, have long offered certifications in the field and continue to update and revise their offerings to appeal to government agencies and private organizations. These certifications are updated every three to five years, with new material added, outdated material removed, and an emphasis on skills sought after by today's forensic and security professionals. The proliferation of private organizations offering a wide range of certifications, many of which focus on digital forensics, underscores the need for a formal credentialing and accreditation process and highlights how these organizations are capitalizing on the opportunity to advance their own, primarily financial, goals, even when labeled as non-profit.

CASE STUDIES

The National Academy of Sciences emphasizes the critical importance of implementing robust quality assurance

procedures in forensic science. These procedures are designed to "identify mistakes, scientific fraud, examiner bias, and to confirm the continued validity and reliability of forensic processes, while also improving processes that require enhancement" (Jordaan, 2012). In the context of digital forensics, a comprehensive quality assurance and management plan is essential to maintaining the credibility of digital forensic laboratories. Both the National Research Council in Washington, DC, and the Association of Chief Police Officers in London recognize quality assurance in digital forensics as a pivotal issue. As recent years have shown, the failure to implement such procedures can lead to grave miscarriages of justice, including the wrongful conviction of innocent individuals (Jordaan, 2012).

A notable case illustrating the dire consequences of inadequate digital forensic practices is that of Connecticut school teacher Julie Amero. In the 2004 case of *State of Connecticut v. Julie Amero*, Amero was wrongfully convicted due to a lack of understanding and proper handling of digital forensic evidence (Alva & Endicott-Popovsky, 2012). Amero, a substitute teacher, was supervising a seventh-grade classroom when students accessed a website that triggered a series of pornographic pop-up advertisements. Unaware of how to stop the pop-ups, Amero followed school instructions not to shut down the computer, inadvertently exposing students to inappropriate content.

During the trial, the prosecution's case hinged on a forensic copy of the computer's hard drive, which was improperly handled and did not adhere to industry standards. The digital forensic investigator failed to use appropriate methods to copy the hard drive, yet the evidence was still admitted in court. The prosecution argued that the computer's Internet history indicated Amero had intentionally accessed pornographic websites, leading to her conviction for "Risk of Injury to a Child" and a potential 50-year prison sentence (Alva & Endicott-Popovsky, 2012).

However, a defense expert, Herb Horner, later discovered that the school's computer was severely compromised due to outdated antivirus software and the lack of antispyware, a firewall, or a content filtering tool. Horner's analysis revealed that spyware on the computer was responsible for the pornographic pop-ups. Despite this critical evidence, the judge refused to allow Horner's full testimony, citing procedural issues during the discovery phase (Alva & Endicott-Popovsky, 2012). Although Amero's conviction was eventually overturned by the State Court of Appeals, and she accepted a plea to a lesser charge to avoid further legal battles, the case caused significant emotional, social, and financial harm to her and her family.

This case starkly demonstrates the fallibility of digital forensics when quality assurance is neglected. However, poorly executed digital forensics does not only risk convicting the innocent; it can also lead to guilty individuals being acquitted. A case in point is that of Aaron Caffrey, who was charged with launching a denial-of-service (DDoS) attack on the Port of Houston, Texas, shortly after the September 11, 2001, terrorist attacks.

During his trial, Caffrey claimed that malicious actors had installed a Trojan horse on his computer, which then carried out the attack without his knowledge. Although the prosecution's expert, Professor Neil Barrett, found tools on Caffrey's computer that could be used to launch such an attack, no evidence of a Trojan horse was detected. Nevertheless, Caffrey was acquitted, largely due to the defense's argument that the Trojan horse, armed with a sophisticated "wiping tool," had erased all traces of its existence from the system logs (Brenner, Carrier, & Henninger, 2004). This case is a classic example of the "Trojan horse defense," a strategy that became increasingly common in the UK during the early 2000s, where defendants claimed their computers were hijacked by malware to carry out criminal activities without their knowledge (George, 2003).

Perhaps the most egregious of these cases is that of Gene Morrison from Manchester, UK. Gene Morrison was a man who managed to deceive the British legal system for nearly three decades, posing as a forensic expert despite having no formal qualifications in forensic science. His story is a startling example of how one individual's deceit can have far-reaching consequences in the justice system, leading to wrongful convictions, miscarriages of justice, and a significant breach of public trust.

Gene Morrison, originally from Hyde, near Manchester, began his fraudulent career in the 1970s. With no formal education or training in forensic science or for that matter in anything else, Morrison nonetheless established himself as a forensic expert, creating a business under the name "Criminal & Forensic Investigations Bureau" (CFIB). He claimed to hold advanced degrees and multiple qualifications in forensic science, psychology, and criminology, all of which he entirely fabricated.

Morrison was a master of deception. He produced impressive-looking reports filled with scientific jargon, which he used to present himself as a credible expert witness in court. His reports and testimonies were accepted in more than 700 cases, including criminal trials, civil disputes, and family court proceedings. Over the years, Morrison's "expertise" was trusted by law enforcement agencies, solicitors, and judges across the UK, as he built a reputation for being a reliable and knowledgeable forensic consultant.

For over 26 years, Gene Morrison's fake credentials went unquestioned, allowing him to operate with impunity. The consequences of his fraud were severe. His testimonies and reports were instrumental in numerous legal decisions, some of which led to wrongful convictions or acquittals. Innocent people were sentenced based on his flawed and often completely fabricated testimonies and/or evidence, while the guilty were sometimes exonerated. The lives of many individuals and families were irreparably damaged by the trust placed in Morrison's false expertise.

One of the most alarming aspects of Morrison's deception was the breadth of cases he influenced. From criminal trials involving serious charges like murder and sexual assault to sensitive family court cases, Morrison's fraudulent testimony factored in a wide array of legal outcomes. His ability to evade detection for so long was a testament to the lack of rigorous vetting of expert witnesses at the time in the United Kingdom.

Gene Morrison's downfall began in 2005 when suspicions arose about the authenticity of his qualifications. Up until then, Morrison had relied primarily on the process of taking court forensics cases and contracting them out to third party professionals. It appears that after such a long streak of good luck, his confidence had gone to his head, and he truly believed that he had been the real investigator. For one of his 2005 cases, he decided to handle the case by himself which arose the suspicion of the police. A police investigation was launched after one of his reports was found to be suspiciously lacking in basic forensic details and professionalism. As investigators delved deeper into Morrison's background, they discovered that he had no legitimate qualifications in forensic science or any related field. His entire career was built on lies and forged documents, including his degrees all of which had been forged.

In 2007, Morrison was brought to trial at Minshull Street Crown Court in Manchester. During the trial, it was revealed that Morrison had never received any formal education beyond basic schooling. He had purchased his fake doctorate from a bogus university in the United States and had been fabricating investigations, evidence, and testimonies for decades. The court heard how Morrison had copied information from textbooks and later, Internet sources to create his reports. It was revealed how Morrison had contracted outside experts, and then presented such works as original forensic analyses of his own doing.

Exclusive ISSA Member Benefits

Education & Training Discounts



Cyber Conferences

RSAConference™2025



<https://www.members.issa.org/page/SpecialOffers>

Join Today:

www.issa.org/membership



Morrison was found guilty of 22 charges, including perjury, obtaining money by deception, and perverting the course of justice. He was sentenced to five years in prison. The case sent shockwaves through the legal community, leading to the reopening of numerous cases in which Morrison had been involved. Many of these cases had to be reviewed, and in some instances, convictions were overturned. It was further found out later that Morrison had been a child molester all these years and many young girls had been sexually molested by him. His sentence was updated to be indefinite.

The exposure of Gene Morrison's fraud highlighted significant flaws in the UK's legal system, particularly in the process of vetting and accrediting expert witnesses. The case underscored the need for more stringent checks on the qualifications and credentials of those who present themselves as experts in court.

In response to the scandal, there were calls for reforms in how forensic experts are vetted and accredited. The case served as a catalyst for discussions about the need for a national registry of accredited forensic experts, as well as the implementation of more rigorous standards for expert testimony in court. Although Morrison's case was particularly egregious, it drew attention to the broader issue of ensuring that forensic science in the UK, the US, and elsewhere to be conducted with integrity, professionalism, and accountability.

Gene Morrison's story is a cautionary tale of how one individual's deceit can infiltrate and corrupt the justice system, leading to profound consequences for countless lives. It is a reminder of the importance of due diligence in the legal process and the need for ongoing vigilance to protect the integrity of forensic science. A documentary was created about Gene Morrison, his rise to fame, his deception, and his eventual downfall. It can be watched online on YouTube.

These cases underscore the profound impact that lack of rigorous quality assurance in digital forensics can have on the judicial process. They highlight the necessity for stringent standards and protocols to ensure that digital forensic evidence is handled, analyzed, and presented with the utmost care and precision. Without such standards, the integrity of the legal system is at risk, as both wrongful convictions and unjust acquittals become more likely. As digital evidence plays an increasingly central role in modern criminal investigations, the establishment and enforcement of comprehensive quality assurance measures in digital forensics are not just advisable, they are essential.

CONCLUSION

The lack of a standardized framework for credentialing digital forensic professionals represents a clear vulnerability in the evolving landscape of cybercrime and digital evidence. As the cases of Julie Amero, Aaron Caffrey, and Gene Morrison starkly illustrate, the stakes are very high: improper handling of digital forensic evidence can lead to wrongful convictions, acquittals of guilty parties, and breaches of public trust. These examples highlight the critical consequences of inadequate practices as well as emphasize the systemic flaws that allow such failures to persist. Without rigorous credentialing and quality assurance measures, the integrity of digital forensics and the justice system itself hangs in the balance.

While existing efforts by organizations like NIST, OSAC, and private credentialing bodies have made strides toward addressing these concerns, their fragmented and often voluntary nature have failed to provide a unified standard. This lack of cohesion leaves room for unqualified practitioners to exploit gaps in the system, eroding the credibility of digital forensics as a profession. Furthermore, the conflation of digital forensic expertise with private investigation licenses in many jurisdictions reflects a fundamental misunderstanding of the specialized skills required for forensic work, underscoring the urgent need for distinct and universally recognized credentials.

The cases discussed in this paper underscore a broader truth: as technology continues to advance, the demands on digital forensic investigators will only increase. This complexity necessitates not just technical proficiency but also a robust framework for ensuring accountability, professionalism, and adherence to ethical standards. A nationally recognized credentialing system, aligned with world-wide best practices and informed by the expertise of seasoned professionals, would bridge the gap between the current ad hoc approaches and a truly professionalized field.

In future follow up articles, the key findings of the research will be presented along with outlines for a credentialing framework and then the framework itself. Those professionals wishing to contribute their time and expertise in this endeavor are respectfully thanked in advance.



About the Author



Dr. Nima Zahadat is a professor of security, digital forensic, and data science. He is also a professional consultant in the IT security industry. He has held positions as Chief Security Officer, Chief Information Officer, Director of security, Director of Training Solutions, Dean of Computer Science, Program Chair of Information Systems, and

Director of Operations. Dr. Zahadat has worked extensively with public and private sectors throughout the years.

Dr. Zahadat has taught at University Systems of the Washington, DC metro area in the fields of forensics, data science, information systems, web development, systems engineering, and security. He has developed and taught over 120 different data science, information systems, security, and forensics courses among others throughout his career. He has a graduate degree in Information Systems and a Ph.D. in Systems Engineering and Engineering Management from the George Washington University. Dr. Zahadat is also a member of the ISSA-NOVA Chapter, in Northern Virginia.



REFERENCES [Bridging the Gap (Part 1): An Analysis of Digital Forensics Credentialing]

- [1] Abdalla, S., Hazem, S., & Hashem S. (2007). Guideline Model for Digital Forensic Investigation. Conference on Digital Forensics, Security and Law, 200
- [2] Alva, A. & Endicott-Popovsky, B. (2012). Digital evidence education in schools of law. The Journal of Digital Forensics, Security, and Law, 7.
- [3] Altheide, C., & Carvey, H. (2011). Digital forensics with open-source tools. Elsevier.
- [4] Beebe, N. & Clark, J. (2004). A hierarchical, objectives-based framework for the digital investigations process, Paper presented at the DFRWS, June 2004, Baltimore, MD.
- [5] Bradshaw, K. & Jordaan, J. (2015). The current state of digital forensic practitioners in South Africa: Examining the qualifications, certifications, training and experience of South African digital forensic practitioners. 2015 Information Security for South Africa (ISSA).
- [6] Brenner, S.W., Carrier, B. & Henninger, J. (2004). The Trojan horse defense in cybercrime cases. Santa Clara High Technology Law Journal 21.
- [7] Butler, J. M. (2015). US initiatives to strengthen forensic science & international standards in forensic DNA. Forensic Science International: Genetics, 18, 4-20.
- [8] Butler, J. M. (2017). Recent activities in the United States involving the National Commission on Forensic Science and the Organization of Scientific Area Committees for Forensic Science. Australian Journal of Forensic Sciences, 49, 526-540.
- [9] Carrier Brian & Spafford (2003). Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Volume 2 (Issue 2):3.
- [10] Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press.
- [11] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
- [12] Flory, T. A. C. (2015). Digital forensics in law enforcement: A need-based analysis of Indiana agencies, (Doctoral dissertation, Purdue University).
- [13] Freiling, F., & Schwittay, B. (2007). A common process model for incident response and digital forensics. Proceedings of the IMF2007.
- [14] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital investigation, 7, S64-S73.
- [15] Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. digital investigation, 6, S2-S11.
- [16] George, E. (2004). UK Computer Misuse Act – the Trojan virus defence: Regina v Aaron Caffrey, Southwark Crown Court. Digital Investigation.
- [17] Gladyshev, P., Marrington, A., & Baggili, I. (Eds.). (2014). Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013, Moscow, Russia, September 26-27, 2013, Revised Selected Papers, (Vol. 132). Springer.
- [18] Jordaan, J. (2012). A sample of digital forensic quality assurance in the South African criminal justice system. Information Security for South Africa (ISSA) 1-9.
- [19] Kessler, G. C. (2007, March). Anti- forensics and the digital investigator. In Australian Digital Forensics Conference, (p. 1).
- [20] Lang, A., Bashir, M., Campbell, R., DeStefano, L. (2014). Developing a new digital forensics curriculum. Digital Investigation, 11, S76-S84.
- [21] Leonardo, Thomas; White, Doug; & Rea, Alan (2012). To License or Not to License Updated: An Examination of State Statutes Regarding Private Investigators and Digital Examiners, Journal of Digital Forensics, Security and Law: Vol. 7: No. 3, Article 5.
- [22] Lillard, T. V. (2010). Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Syngress Publishing.
- [23] Losavio, M., Seigfried-Spellar, K. C., Sloan III, J. J. (2016). Why digital forensics is not a profession and how it can become one. Criminal Justice Studies, 29, 143-162.
- [24] Lundquist, R. (2016). An Examination of Failed Digital Forensics and the Criminal Justice System (Doctoral dissertation, Utica College).
- [25] Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. International Journal of Digital Evidence. 3, 1-11.
- [26] Mohay, G. (2005, November). Technical challenges and directions for digital forensics. In Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on (pp. 155-161). IEEE.
- [27] Nance, K., Hay, B., & Bishop, M. (2009, January). Digital forensics: defining a research agenda. In System Sciences, 2009. HICSS'09.42nd Hawaii International Conference on (pp. 1-6). IEEE.
- [28] Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.
- [29] Pollitt, M. (2010, January). A history of digital forensics. In IFIP International Conference on Digital Forensics (pp. 3-15). Springer, Berlin, Heidelberg.
- [30] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models, International Journal of Digital Evidence, Volume 1(Issue 3):6.
- [31] Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers & Security, 23, 12-16.

Listening to AI?

By: Robert Slade



He kept insisting that he **was** listening, and he **wanted** to hear, and I was finding it very odd that, even in the midst of insisting he was listening, he obviously wasn't.

And in trying to parse out what it was that proved that he wasn't listening, I realized he was like ELIZA. ELIZA is an extremely simplistic attempt at artificial intelligence (more than six decades old, now), which appears to converse by discarding most common words in English, picking up only keywords. So, it discards any detail or nuance.

But, whereas ELIZA uses the keywords to prompt the other side of the conversation to "Tell me more about [keyword]," he uses it as a prompt to his own version of generative AI. Gen/AI uses keywords to generate a stream of text which is glib and plausible, even if it is wrong. It is completely unconcerned with meaning, so it never knows when it is wrong. He, basically, is always confident that he is correct, and it never occurs to him that his (often partial) idea may not be what the other party means. As long as he is able to generate a stream of plausible words (with toxic positivity guardrails), he is doing his job.

It has been said that when we try to teach machines how to learn, it turns out that they don't, and we do. I am aware that some of the pointed failures of large language models and generative AI have prompted those interested in neurology to question the neural network models which have informed both artificial intelligence, and neurobiology, for at least the past four decades. The success of neural networks in some areas has prompted a fairly firm belief in the truth of the model. In fact, there is relatively little actual evidence for the model, other than the fact that the black box that is the brain does seem to operate similarly to the output of neural networks, in very simple cases. Science, however, is in the business of testing a hypothesis against all cases, and even a single failure may indicate that the hypothesis is flawed. Sometimes fatally so.

But there is a possibility that we can learn from even our flawed attempts to understand the human brain, and psychology. The errors and hallucinations that we are now seeing from gen/AI may point out common errors in psychology.

I have studied listening for more than five decades now. I have attempted to put it into practice. I can't say that my early practice and experiments were particularly good, but, even back then, they definitely provided benefits. However, I can say that ELIZA, itself, even in those early days, provided me with some valuable lessons, and tools, in listening. When I realized how very simple ELIZA was, and yet how effective it was, I used the utility of this simple matter of picking out keywords, and encouraging the respondent to tell me more about one or more keywords. I also learned to identify multiple keywords, and to keep some in reserve, when a particular line of prompting remained unfruitful.

But that was early days, and simple stuff. This recent experience, coupled with the enormous interest in generative AI, has provided new opportunities. In the same way that we are trying to debug generative AI models, by identifying and examining the errors that generative AI make, we should be able to identify our own errors in the practice of listening, and other relational and psychological tools. These tools are not yet a science. Or, rather, the use of these tools is not yet a science. It is still very much an art, and there are practitioners who are good at using the tools, such as listening, and those who, despite great professed interest in the tools, such as listening, are still unable to use them effectively. If I had a nickel for every person who told me that they were a good listener, and then, immediately and very profoundly, demonstrated that they had no skill in listening at all, I would be an extremely rich man.

So it may possibly be that, probably much to the dismay of the individuals, venture capitalists, and corporations who are pouring billions of dollars into generative AI, that this is, once again a matter of finding out that the machines don't, and we do. It may be that the greatest benefit of generative AI is in teaching us where some of our models of psychology are incorrect, and in prompting other, more useful tools, or instructions on the use of existing tools, such as listening and active listening.



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



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

Supplementary Segment

Training Tomorrow's Security Experts in AI and LLM Application Security

By: Parth Shah, CISSP

Artificial intelligence leads in the technology trend, with 2025 Top Strategic Technology Trends from Gartner detailing a number of areas in the advancement of AI that are key focus areas [1]. Of these, Agentic AI and AI governance platforms are featured as the essential parts of technology landscapes of the future as organizations scale out the use of AI technology for decision-making. As great as this rapid adoption may be, it also means a lot of security challenges come along with it. With AI-driven tools becoming key to enterprise operations, understanding and mitigation of AI-related risks are very important among security experts.

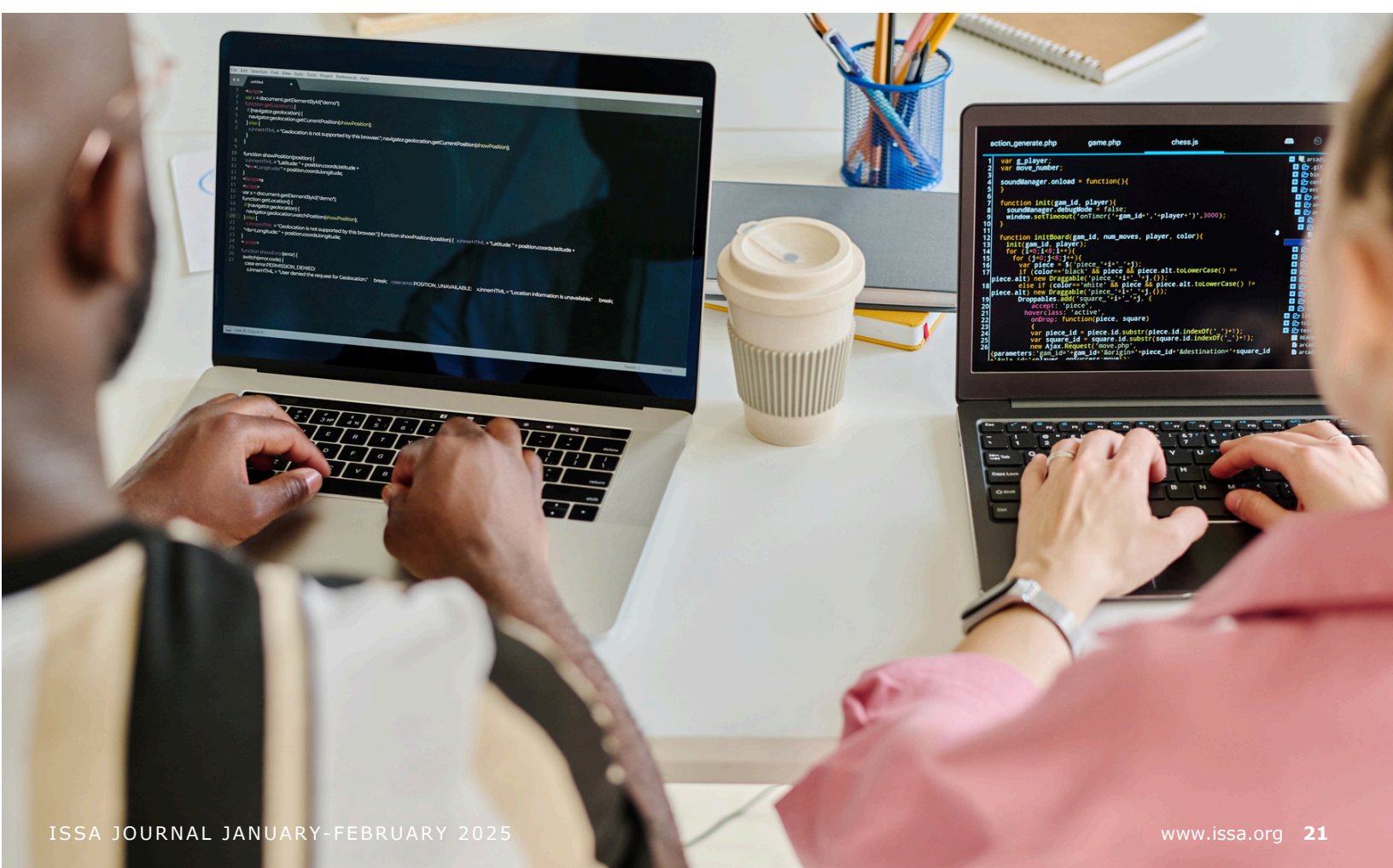
Because of these new challenges, the future generation of security professionals needs to be duly equipped to understand the unique risks brought in by AI and LLM. This paper discusses some of the key strategies on how to train future security professionals in the security of AI and LLM applications, building from foundational AI knowledge, identifying risks specific to GenAI and LLM, and navigating regulatory requirements laid out by the likes of the EU AI Act.

Laying the Foundations

First, grounding in the fundamental concepts of AI gives the security professional the ability to manage risks associated with AI. Differently stated, one enables professionals to identify typical vulnerabilities that could be expected in an AI system; therefore, the first step in training necessarily deals with core concepts that include a broad overview of how AI works, including machine learning and neural networks, and the differences between traditional models of AI and GenAI.

The important element of basic training should cover differences between **supervised, unsupervised, and reinforcement learning** - variants currently in common usage in the development of AI. Understanding which variant is in use is critical because each variant has very different security implications. For instance, models developed through supervised learning are susceptible to a kind of attack called data poisoning, whereby manipulated data biases model outputs. Equipped with this explicit understanding, the security professional will be better prepared to watch for and defend against identified vulnerabilities.

The training also has to involve basic concepts of model training, data quality, and the role of feedback loops since those directly tie into model integrity and security. Also, it is important that security people understand how GenAI produces its output and in what respect it differs from classical AI. This would help in identifying vulnerabilities in systems that, with the use of AI, automatically create texts, images, or other kinds of output.



As responsible AI practices continued to soar, ethics and governance also turned out to be fundamental knowledge today. In inculcating the feeling for ethical considerations such as mitigation of bias, privacy, and accountability, security professionals are able to make contributions in helping organizations build AI systems in keeping with standards of safety and ethics so that even much safer and more responsible applications are provided.

Understanding Generative AI and LLM Risks

Large language models and generative AI have just started getting baked into modern enterprise applications, and with those come an increasing need by security professionals to manage new kinds of security vulnerabilities that no traditional AI-structured rules possess. While such kind of risks are already being addressed by security professionals using different kinds of frameworks, the OWASP Top 10 for LLMs [2] is among those that come to the fore. These highlighted areas comprise the list of critical vulnerabilities in LLMs and give very actionable guidance for defense.

The following is an overview of each of the OWASP Top 10 risks for LLMs:

1. LLM01: **Prompt Injection** is a vulnerability whereby an attacker manipulates input prompts either for unexpected outputs or leakage of sensitive information. Prompt injection requires strict input validation and sanitization practices.
2. LLM02: **Insecure Output Handling**: Many a time, LLM could emit unsafe code or sensitive information within the generated outputs for lack of validation. Professionals in this domain should implement verification whether such generated content does not open up any vulnerabilities.
3. LLM03: **Training Data Poisoning**: While data training is the mainstay of performance in LLMs, it also has the potential to distort model behaviors or produce harmful outputs if any poisoned data is present. Protection of integrity in these training datasets therefore calls for frequent audits and monitoring of such data.
4. LLM04: **Model Denial of Service (DoS)**: Attackers could leverage different types of interactions with LLMs that are load-intensive to the system and result in system downtime or degraded performance. This risk can be diminished through rate limiting and anomaly detection.
5. LLM05: **Supply Chain Vulnerabilities**: Most of the LLMs are dependent on third-party components; hence, they might be very vulnerable to supply chain attacks. It is very important to be regularly auditing and verifying the dependencies with a view to minimizing such risks.
6. LLM06 **Sensitive Information Disclosure**: LLMs will disclose sensitive information if proprietary or private information exists in training data. Recommended strategies for mitigation include data anonymization and strict access controls.
7. LLM07 **Insecure Plugin Design**: Plugins to LLM can extend LLM functionalities, but if poorly handled or designed, it may also introduce security vulnerabilities. Ensuring plugins are secure and isolated from core functionality reduces exposure.
8. LLM08: **Excessive Agency**: LLMs might be given too much autonomy and freedom in executing decisions without having sufficient oversight from humans. The boundaries have to be strictly defined concerning the work of the model as an effective way to avoid not foreseen actions.
9. LLM09: **Over-reliance**: Where very strong confidence in the data output by LLMs is seen, flawed decisions might result. The user training regarding critical evaluation of AI-generated output is an important human control to perform in trying to avoid reliance upon data that may be wrong.
10. LLM10: **Model Theft**: Exfiltration of LLM model information and its intellectual property themselves can be a result of unauthorized access. Protection against such exfiltration and unauthorized access shall include credential protection, monitoring usage, and implementing encryption.

Apart from the understanding of such risks, security professionals should get acquainted with the mitigation strategies specific to each of these vulnerabilities. The inclusion of OWASP Top 10 into the training programs will give structure to find, understand, and address LLM vulnerabilities in order to prepare for securing AI-powered applications against future threats.

Understanding the Implications of AI Risks

This rise has consequently brought regulatory initiatives all over the world on the proper and responsible use of this new technology in AI. Many therefore try to put boundaries on the use and deployment of this artificial intelligence, or AI. Probably the broadest ranging framework for governance of AI could be the **EU AI Act [3]**, introducing a structured risk-based approach toward the management of the AI applications.

Understanding this regulatory landscape is important, given that compliance with international standards - as one might expect - is going to play a significant role in securing AI systems.

It categorizes AI systems, in relation to their use, as **minimal, limited, high, and unacceptable risks**, considering the consequences an individual and society will face due to those systems. Examples of applications of AI in the high-risk domains: AI applied to health, law enforcement, and finance, where severe damage can be the consequence of a simple error or misapplication. Transparency, Security, and Accountability High-risk AI systems should be subject to strict requirements. Because of this, it becomes important that security professionals understand categories and can assess the level of required scrutiny for different uses of AI; such will determine the required security controls to put in place.

With that in mind, the understanding of key regulatory principles that are foundational to the EU AI Act-transparency, data privacy, and fairness- are indispensable since the security professional will integrate these into foundational risk management and compliance. One would add, transparency allows users and stakeholders to have an idea about how a decision is made by an AI system. It comes into effect in areas where the AI system is affecting aspects that touch on finance or personal well-being. They manage to do this through techniques such as explainable AI, where the process of arriving at a certain decision is documented and can be accessed through the AI model. This makes the auditing of the AI systems easier and gives insight to stakeholders on how a particular outcome came about.

Another important principle that could well be considered in the EU AI Act is data privacy. Large volumes of data are fed to the AI models, and these usually contain sensitive information protected by protection laws such as the General Data Protection Regulation (GDPR). Security professionals are compelled to apply different methods of preserving privacy: anonymization of data, encryption, and differential privacy. This would go a long way in ensuring the minimization of regulatory risks and protection of user privacy if only proper management of personal information could be made certain.

Adding regulatory compliance to this security training in AI will ensure that professionals derive comprehensive insights into the management of AI risks. In tune with understanding the implications of the EU AI Act and other similar regulations, security experts can build appropriate safeguards that meet both the requirements of legality and the need for public-trusted AI systems. This will balance security with ethics and regulations in the foreground, making the process of deploying AI responsibly by organizations without lagging behind globally enacted regulations

Hands-On Training for AI and LLM Security

Usually, theoretical aspects in cybersecurity goes only so far. Without hands-on training, it would not be possible to prepare security professionals effectively against such sophisticated threats imposed by AI and large language models. In such practical and hands-on learning, the professional knows how to understand and respond to real-world threats, thereby helping them in working for securing an AI-driven system.

The most effective way of preparing professionals for security incidents related to AI is **simulation-based learning**. In this respect, laboratories can be set up where professionals will be able to have firsthand attack effects of scenario simulations including but not limited to: prompt injection, model theft, and training data poisoning. Generate a simulated scenario, for example, of a malicious actor trying to carry out a model inversion attack against an LLM to get sensitive training data. The lab goes through developing an attack and seeing its consequences, and the students develop countermeasures against this unfolding attack. Hands-on training will also provide students with an understanding of how the attack is carried out and how they can act as fast as possible in a real-world environment.

Practical Lab Environments are also helpful for learning how to secure AI systems. Environments can also be set up to emulate real-world deployments of AI and LLM systems, where professionals can have a playground on safe grounds for the detection of vulnerabilities and application of security controls. Input validation, with a view to reducing the risk of possible prompt injection attacks, or model access control, to avoid unauthorized use with possible theft of the models, are some lab-set exercises that maybe performed. Professionals learn technical skills through hands-on technical skills through hands-on labs in which they engender confidence in applying security measures that protect AI systems directly.

Moreover, integration of the **MITRE ATLAS** (Adversarial Threat Landscape for Artificial-Intelligence Systems) Framework [4] into these labs adds depth to how adversaries approach an attack on AI systems. ATLAS provides structure to the tactics and techniques utilized against AI by attackers, enabling professionals to analyze actual threat behaviors. Incorporating ATLAS into the lab exercises would, therefore, allow such learners to identify an attack and predict adversarial moves with a view to enhancing their capabilities of defense. For example, a simple exercise will be studying ATLAS for tactics such as model weakness exploitation or injecting adversarial inputs with a view to developing methods of countering such threats.

Continuing this line of thought, hands-on learning can also be supplemented through **Industry Certifications and Specialization Paths** that would systematically put a professional on track to specialize in AI security. Certifications in AI Ethics and Governance, and GenAI Security, among others, give insight into both the theoretical framework of knowledge and the practical ability with which to approach the protection of AI systems. These certifications also include some coursework and hands-on labs that give professionals more depth in their expertise, along with the ability to stay up to date with constantly evolving security best practices.

Building professional capacity for the security challenges of AI and LLM can include simulation-based learning, lab environments, and resources like the MITRE ATLAS framework as part of the security training programs. Indeed, such hands-on and technical proficiency will inculcate proactive habits to keep the systems secure within today's dynamic threat landscape.

The Way Forward

The more that AI and large language models continue to emerge and be integrated into practically all aspects of modern technology, the more the need is growing for professional security experts who may provide protection for these systems. Training the security experts of tomorrow in the security of AI and LLM applications is not only an upskilling technically but also crucial to ensure safety, privacy, and ethical responsibility on a worldwide basis in the implementation of AI.

What should the organizations do? The organizations shall adopt thorough AI security training programs that strike a balance between theoretical learning and practical competencies and regulatory compliance. The modern security practitioner should embrace lifelong learning, pursuing specialization opportunities in AI/LLM security, to remain relevant as industries continue to transform in record time. These favors are returned by the practitioners who have experience through mentoring and passing knowledge on to the next generations, hence building an environment of learning and sharing knowledge that would make the world of AI resilient in security aspects.

Securing AI is everyone's responsibility. To us, this means training, mentorship, and security practices that will make sure users use AI technologies safely, responsibly, and with ethics. As we set the course for the next wave of security professionals, we prepare for a resilient, secure, and trusted AI-driven future.

References:

1. Gartner. 2025 Top Strategic Technology Trends. <https://www.gartner.com/en/articles/top-technology-trends-2025>
2. OWASP. OWASP Top 10 for LLMs and Generative AI Apps. <https://genai.owasp.org/llm-top-10/>
3. European Parliament. EU AI Act: First Regulation on Artificial Intelligence. https://www.europarl.europa.eu/topics/en/article/20230601S_T093804/eu-ai-act-first-regulation-on-artificial-intelligence
4. MITRE. MITRE ATLAS Framework. <https://atlas.mitre.org/>



About the Author

Parth Shah, CISSP, is a Sr. Security Research TPM at Microsoft and has a Master's degree in Cybersecurity and Leadership from the University of Washington. Parth serves as ISSA Rainier Chapter President, advancing security practices and mentoring professionals.



ISSA
Information System Security Association
International

Rainier Chapter



Supplementary Segment

THE PYTHON PROGRAMMING LANGUAGE Numerical Analysis/ Machine Learning Series

By: Constantinos Doskas
ISSA-NOVA VP of Education
MASTER IN INFORMATION ASSURANCE
CERTIFIED SCRUM MASTER

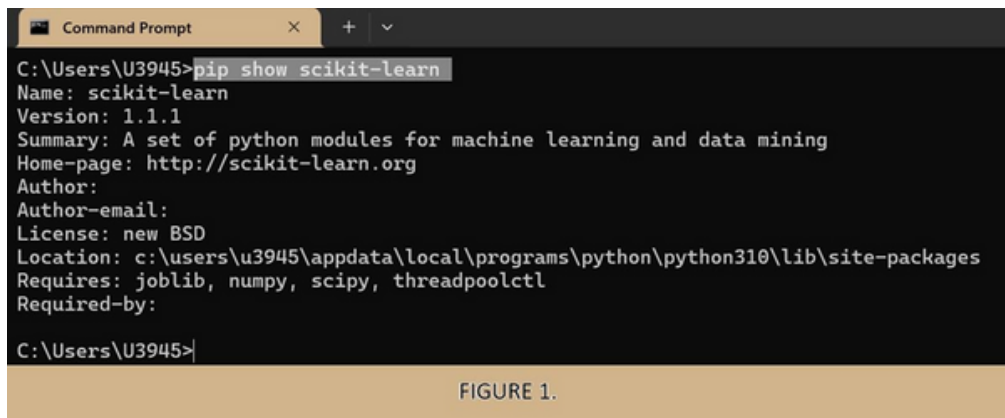
This article is part of a series of articles which deal with topics in programming using the Python programming language. In previous articles we presented Python programs which use various Machine Learning Algorithms. We also presented a program that associates ISP information with IP addresses. The program used the whois service and loaded and processed the data on SQL database tables.

In this article we will review the various ML algorithms which have been presented and proceed with an introduction to neural networks and deep learning.

ML REVIEW

As it was stated in previous articles, Machine Learning (ML) is a collection of algorithms which implements various approaches in predicting a value based on the values or relationships of given variables. The main tool which was used thus far is the Sklearn library. This library contains most of the logic of ML algorithms and makes it easy for programmers to use it. Note, however, that Sklearn is now deprecated. You will need to use Scikit-Learn instead. To find out if you have Scikit-Learn installed, open a Command Prompt window and type `pip show scikit-learn`.

You will then see the result as in Figure 1.



```
Command Prompt
C:\Users\U3945>pip show scikit-learn
Name: scikit-learn
Version: 1.1.1
Summary: A set of python modules for machine learning and data mining
Home-page: http://scikit-learn.org
Author:
Author-email:
License: new BSD
Location: c:\users\u3945\appdata\local\programs\python\python310\lib\site-packages
Requires: joblib, numpy, scipy, threadpoolctl
Required-by:

C:\Users\U3945>
```

FIGURE 1.

If you do not have this module installed, you can download it by the use of the command `pip install -U scikit-learn`.

Also note that you will still import modules from scikit-learn by using the `sklearn` keyword.

Other modules that we used were Numpy, Pandas, Scipy, and Matplotlib. Those modules are used for data manipulation and presentation. In ML it is important to pre-process the data in order to make it readable by the ML algorithms. This is a very important step in Data Science. Visualization of the data is accomplished by the use of Matplotlib. The data which was used in our articles is stored in datasets that are incorporated in the Scikit-Learn datasets module. Datasets that you may find online from various sources can be used as well.

There are two methods to teach the algorithms how to process the data; supervised and non supervised learning. Most ML algorithms that we used so far were based on supervised learning. Therefore, the data needed to be split into a training subset and a test subset. These ML algorithms are subdivided based on the type of target variable. If the target variable is discrete (categorical) then the algorithm to be used must be a classification algorithm. But if the target variable is continuous then a regression algorithm must be used. Let us review some of the algorithms that we have used in this series of articles:

Random Forest Regressor: This algorithm is very popular because it can be used for both classification and regression. It is, however, prone to over-fitting and needs more memory than other algorithms.

Support Vector Regression: Very good algorithm when the dataset is not large. It can tolerate well outliers.

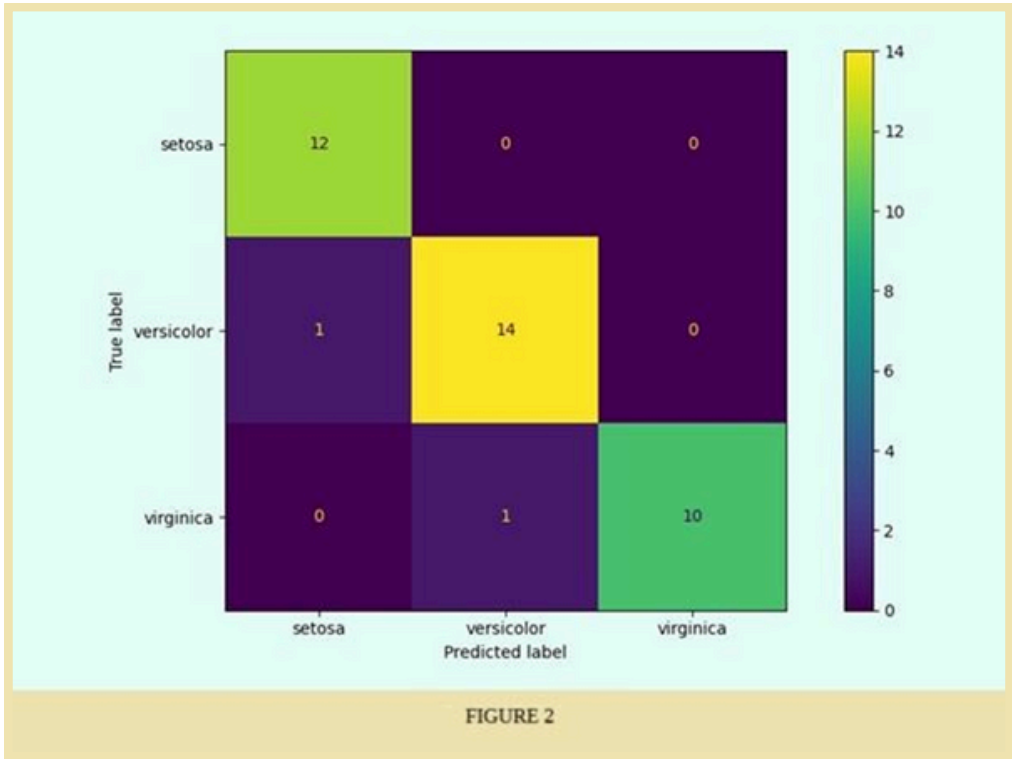
Support Vector Machine: Very effective classification algorithm which can handle easily high-dimensional data. Preferred by many for image recognition and bio informatics because of very good memory usage and robust performance.

Decision Tree Regression: It works with continuous or discrete variables but suffers from the possibility of over-fitting.
 Gradient Boosting: Works as regression or classification algorithm. This ensemble learning model may be used in web searching and fraud detection although it is computationally intensive.

Naive Baynes: It handles well multiple dimensions and regardless of its simplicity it works well in various implementations especially in spam filtering and text categorization.

K-Nearest Neighbors: Suitable for both regression and classification, KNN, is a lazy learning Algorithm. Very effective with non-linear data makes it a good choice for processing jobs related to pattern recognition and anomaly detection.

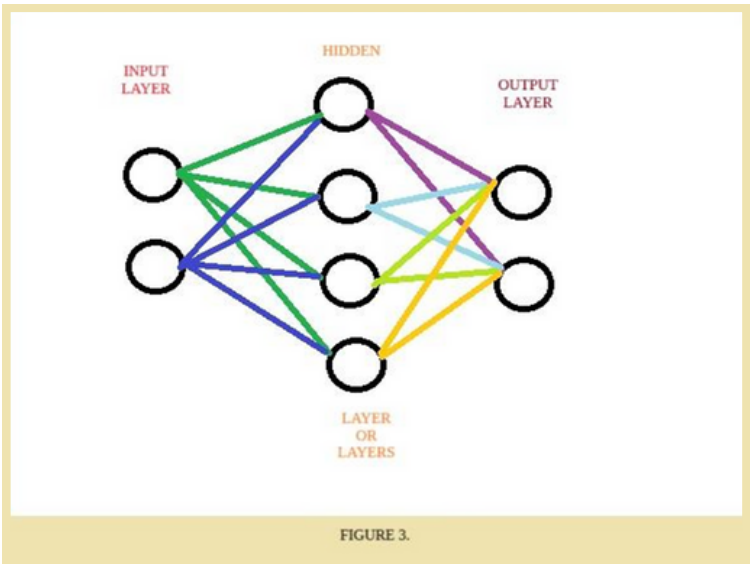
Scikit-Learn comes with a set of standard metrics. We have used some of them in previous articles. Accuracy is one of these and it is defined by the ratio of (True Positives+True Negatives)/total observations. Another metric Precision is defined by the ratio True Positives/(True Positives+False Positives). Also the Confusion Matrix metric proved to be beneficial. See the following example from the iris dataset:



Note that in the above matrix two instances were confused. One *setosa* was confused for *versicolor* and one *versicolor* was confused for *virginica*.

BEYOND BASIC ML

As technology improved more complex algorithms were developed and even more are still in research and development labs. In practice, data is most of the time very complex. Therefore, there is a need of AI systems that are able to train themselves in finding patterns in the given data. Finally, another branch of AI was developed and placed in its own category. This branch is DL or Deep Learning. DL is using a technology called ANN (Artificial Neural Network). This technology is using nodes that are interconnected and work together to learn and process from the given input or inputs. Each node, called a neuron, may pick up to process and learn a piece of the puzzle of incoming data. It, then, takes a bunch of neurons to understand and process that entire puzzle (unstructured data, most of the time). Visually, the basic concept of ANN is as follows:



Note that each neuron of the hidden layer(s) receives input from either the input layer neurons or the previous hidden layer of neurons (in case of multiple hidden layers). Finally, each neuron of the last hidden layer provides output data to each neuron of the output layer. DL requires more data than traditional ML during training. Also DL requires a faster processor when it is used in actual production applications.

The software requirement of the following articles would be *TensorFlow* and *Keras*.

If you need to install *TensorFlow* open a command prompt window and use the following command: `pip install tensorflow`

or depending your python version: `pip3 install tensorflow`

if there are any conflicts with currently installed packages you may need to uninstall them and install them back again.

For instance if you have a conflict with *numpy* and *scipy* versions then do the following:

```
pip3 uninstall numpy
pip3 install numpy
```

```
pip3 uninstall scipy
pip3 install scipy
```

TOPICS OF INTEREST

To better understand AI concepts you may want to do some additional reading on your own. Here are some topics that you may want to search for:

Curse of Dementionality
Feedforward Neural Networks (FNNs)
Convolutional Neural Networks (CNNs)
Recurrent Neural Networks (RNNs)
Natural Language Processing (NLP)
Long Short Term Memory (LSTM)
Large Language Models (LLM)
Transformers in deep learning

IN THE NEWS

Today in the news we learned that over 3000 employees of META are scheduled to lose their jobs. They will be replaced with AI. Many other smaller companies are doing or planning to do the same. Let me know what do you think about that. Is there an ethical issue of the deployment of AI? What measures should the government take in order to protect the people who are all of a sudden found without a job? What do you think that the impact of AI would be to the unskilled worker?

WHAT IS IN THE NEXT ARTICLE

In the next article we will start creating AI programs using *tensorflow* and *keras*. Keep all of the posted articles in your library because the code in each article assumes that you are already familiar with concepts previously posted. Please note that my email (cdoskas@megabizhost.com) is available for your comments. Use this email address if you have any questions related to specific topics that were presented in this article.

CONCLUSION

To conclude, this article presented a review/summary of the ML topics which were presented in previous articles. In addition, the basic concept of DL, deep learning, was presented and the DL libraries which will be used in the future were mentioned.

I encourage you to study the concepts presented in this and previous articles and find ways to improve or add to the presented code. See you again through the next article.



ISSA International

40TH ANNIVERSARY CELEBRATION!

**We're thrilled to invite you to a
special celebration
marking 40 years of ISSA
excellence!**

Join us for this **In-Person** Event
on **April 3 - 5, 2025** at **Westin
Galleria Dallas, Texas.**

Don't miss this opportunity to:

- **Celebrate Success:** Honor the incredible achievements of our members and industry peers at the Awards Ceremony during the Anniversary Gala.
- **Build Connections:** Meet friends, colleagues, and industry leaders to strengthen your professional network.
- **Expand Your Knowledge:** Participate in key meetings and sessions, including:
- **Cyber Executive Forum** (by invite only)
- Chapter Leaders Meeting

This is more than just an event, it's a celebration of our shared history and a look ahead to the future of cybersecurity leadership. Join us for this milestone occasion. Registration available soon, check your Member eNewsletter for details & room discounts!

We can't wait to see you there!

Member eNewsletters are mailed the 1st & 3rd Wednesday every month! Check your inbox for upcoming ISSA News, Events, and exclusive membership offers!

News From the Foundation



New Officers

At the December meeting of the ISSA Education Foundation, the Board of Directors elected it's officers for the 2025-2026 term. As a result of the election, we have two new officers.

President

Although Deb Peinert is our new President, she is a familiar face in the ISSA, the ISSA Education Foundation and the information/cyber security industry. Deb has over 30 years experience in information security, from systems programmer to security analyst/architect, to developing and managing information security programs for various companies.

An active member of ISSA for over 25 years, Deb previously served as President of the San Francisco Bay Chapter and is now an active member of the Denver Chapter. She is also the current Vice President of ISSA International.

One of the founding members of the ISSA Education Foundation, Deb has served in many roles within the organization, including establishing procedures, managing the website, leading fundraising, serving as liaison to the ISSA, and representing the foundation at ISSA chapter leader meetings.

Congratulations Deb!

Vice President

Previously serving as our Secretary, Dr. Jack Freund is an expert in cybersecurity and risk quantification. With over two decades of experience in the field, Jack is best known as the co-author of "Measuring and Managing Information Risk: A FAIR Approach," a guide to the Factor Analysis of Information Risk (FAIR) standard.

Jack holds a Ph.D. in Information Systems from Nova Southeastern University and advanced degrees and certificates in project management, telecommunications management, and international law. He holds multiple cybersecurity certifications.

In addition to his professional accomplishments, Jack is a passionate educator and mentor, contributing as an author and columnist for the ISSA and serving in various leadership roles within professional organizations such as the ISSA Education Foundation.

Congratulations Jack!

Fundraising

"CTRL-ALT-RISK"

And speaking of books, our new vice president has authored a new book, "CTRL-ALT-RISK: Reset Your Thinking on Cybersecurity." This anthology of short essays introduces readers to foundational concepts, such as risk appetite, quantitative analysis, and resilience building, while delving into advanced topics like cyber risk modeling, regulatory compliance, and emerging threats.

"CTRL-ALT-RISK" is available on Amazon, <https://www.amazon.com/dp/B0DRLJCP7J>

We encourage you to purchase a copy. Not just because Jack is an expert on risk, but also because he is generously donating every dollar of the proceeds from this book to the ISSA Educational Foundation so we may continue our mission of helping cybersecurity students further their education.

Thank you Jack!

The 2025 Chapter Challenge is underway!

This year's Chapter Challenge began on Giving Tuesday (December 2) and runs through July 31, 2025. ISSA chapters are encouraged to contribute to the future by helping to fund scholarships for the next generation of cyber security professionals. Chapters contributing the most (by chapter size, i.e., number of members) will be announced at the ISSA Awards Gala following the close of the contest. For more details, follow us on Facebook or LinkedIn.

Scholarships

And speaking of donations, the 2025 scholarship application period begins on February 1. If you, or someone you know, is a sophomore, junior, senior or graduate college student, or wish to pursue professional cybersecurity training, visit our website at issaef.org/scholarships for eligibility requirements and application instructions.

Professional training applications will be accepted through April 30; student applications will be accepted through June 15.

Good Luck!

Volunteers

If you have an interest in making the world a better place and want to help fill the need for talented cybersecurity professionals, please consider joining us. ISSA Education Foundation is an all-volunteer organization – we have no paid staff – and we currently have the following vacancies:

Director of Operations

Responsible for updating the Foundation's Operations manual, when necessary, including the organization chart and Board/Committee member contact lists.

Foundation Secretary

Responsible for keeping records of Board of Directors meetings and decisions. The Secretary keeps notes of all Board activities and summarizes these in a monthly report to the Board members, as appropriate. The Secretary is also responsible for ensuring that Foundation records are maintained for Board decisions.

If you have an interest and experience in these or similar roles, please contact our President, Deb Peinert at deb.peinert@issa.org.

Webmaster

Maintain and update the ISSA Education Foundation website. If you have an interest and experience in this or similar roles, please contact our Communications Director, Brent Putnam at bputnam@issaef.org.

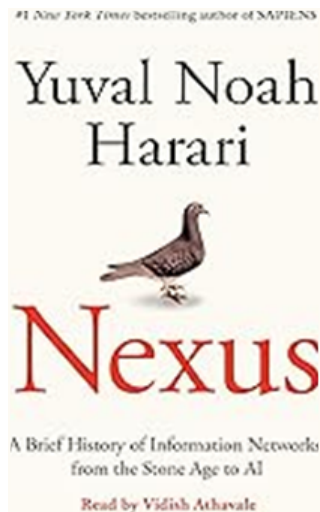
If you do not feel that you're qualified for these roles but still want to assist us, please feel free to reach out. We can always use enthusiastic individuals.

About the Foundation

Founded in 2003 by the ISSA International Board as an independent, 501(c)(3) charitable organization, the ISSA Education Foundation is qualified to receive tax bequests, devises, transfers or gifts to foster and support education and training in cyber security and related fields. Donors to the ISSAEF may be eligible for tax deductions; consult your tax advisor.

Reviewing the Works of Yuval Noah Harari, and Ethan Mollick

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



Nexus: A Brief History of Information Networks from the Stone Age to AI.

by Harari, Yuval Noah, Random House, (2024).

Sound Bite: Information gathering and networks (AI puts it all on steroids) have been part and parcel of being human, but we do not always use everything smartly.

Opinion on Primary Audience: Everyone, but especially any kind of leader.

What is a "Nexus?" Any dictionary will give you two definitions, either a network linkage or a focus point. Page 222 of the hardback copy of this book refers to a tax definition of an entity connected to a jurisdiction. I think all three definitions have artificial intelligence applicability in this book. For further information, see the book! It is at a very high conceptual level on AI implications, so you will not find technical details. There are dozens of books out there by credentialed authors talking about artificial intelligence implications. I have read many of them, and to me the best books like this one do not focus on current AI limitations but emphasize the possibilities. Sure, it starts as a history, but it is all about where we can be headed.

The Author:

Yuval Noah Harari is an Oxford PhD historian, currently a professor at the Hebrew University of Jerusalem. He is an accomplished if not famous writer, noted for his other works, among them *Sapiens: A Brief History of Humankind*, and *Homo Deus: A Brief History of Tomorrow*.

The Metadata:

A 2024 publishing date! The online ordering cost including shipping is about \$25. The hardback copy is nearly 500 pages. If your public library is like mine, you will find many copies, but multiple holds.

'Thought-provoking' is an overused term, but that is Dr. Harari's writing style. I took a one-page sample of the text to analyze. Using a Wikipedia article about the Flesch-Kincaid Readability Test, the readability is high school level. The sample had 16% passive voice. This article is under 3% passive voice.

Table of Contents: [Including Reviewer notes]

Part I: Human Networks [Reviewer note: Interesting stories on vantage points about information]

- 1 What is Information?
- 2 Stories: Unlimited Connections
- 3 Documents: The Bite of the Paper Tigers
- 4 Errors: The Fantasy of Infallibility
- 5 Decisions: A Brief History of Democracy and Totalitarianism

Part II: The Inorganic Network [Reviewer note: IT&AI is not your past scientific revolution]

- 6 The New Members: How Computers Are Different From Printing Presses
- 7 Relentless: The Network Is Always On
- 8 Fallible: The Network Is Often Wrong

Part III: Computer Politics [Reviewer note: We can make choices]

- 9 Democracies: Can We Still Hold a Conversation?
- 10 Totalitarianism: All Power to the Algorithm?
- 11 The Silicon Curtain: Global Empire or Global Split?

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.

Co-Intelligence: Living and Working with AI

By Molick, Ethan. Penguin, (2024).

Sound Bite: Do not think of AI as artificial intelligence, think of it as alien intelligence. Do not Fight AI – Use it!

Opinion on Primary Audience: Anyone in any business!

Ethan Mollick deserves the title of 'AI Whisperer.' You know how you can buy books on 'How to use your iPhone?' This book could easily fill in as 'How to use your AI assistant.' With an author of Professor Mollick's stature, that comment could be seen as demeaning. Rest assured I mean the opposite. This book is both college textbook idea quality (who says textbooks can't be fun?) and hands-on, as Dr. Mollick uses the ideas in his courses.

The Author: Ethan Mollick seems to be primarily now a business management scholar. Harvard BS (Magna Cum Laude) Science Technology and Policy, PhD from Sloan. Professor and Co-Director of the Generative AI Lab at Wharton. Call him a major and modern business management scholar!

The Metadata: A 2024 publishing date! The online ordering cost including shipping is about \$25. The hardback copy is about 250 pages. Your public library will probably have a couple of copies, but you will have to wait for the holds. It is that good! I took a one-page sample of the text to analyze. Using a Wikipedia article about the Fleisch-Kinkaid Readability Test, the readability is high school level. The sample had 23% passive voice, which is a bit high for my preference, but it reads really well. This article is under 3% passive voice, for comparison.

Table of Contents: [Including Reviewer notes]

Part I

- 1 Creating Alien Minds
- 2 Aligning the Alien
- 3 Four Rules for Co-Intelligence [Reviewer note: I will never forget this quote: "Assume this is the worst AI you will ever use."]

Part II [Reviewer note: This is the how-to part, filled with examples.]

- 4 AI as a Person
- 5 AI as a Creative [Reviewer note: That is not a typo.]
- 6 AI as a Coworker
- 7 AI as a Tutor
- 8 AI as a Coach
- 9 AI as our Future

Happy Reading!

PS: If you have a book you want me to review, or changes to the material in 'Book Reviews,' please use the email address in my bio to let me know!

Next Month:

- Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies. Oxford University Press, (2016).
- Kissinger, Henry, Craig Mundie, and Eric Schmidt. Genesis: Artificial Intelligence, Hope, and the Human Spirit. Little, Brown and Company (2024).

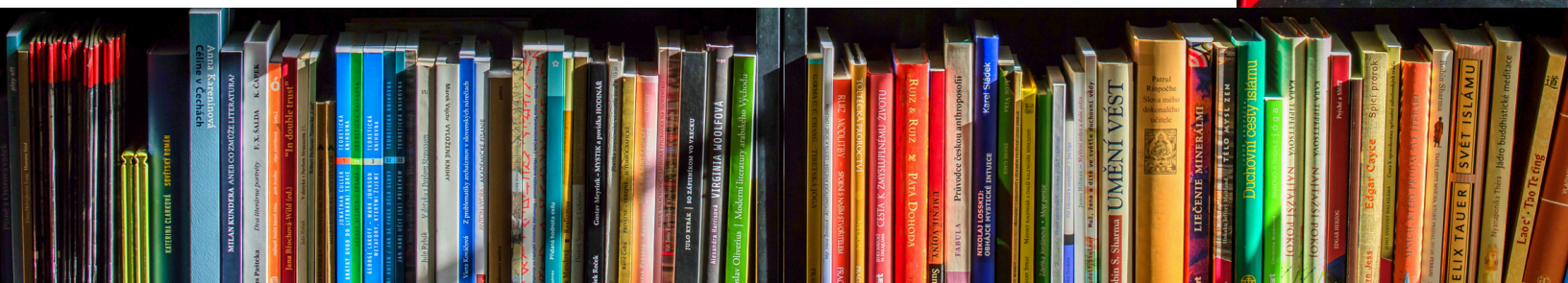
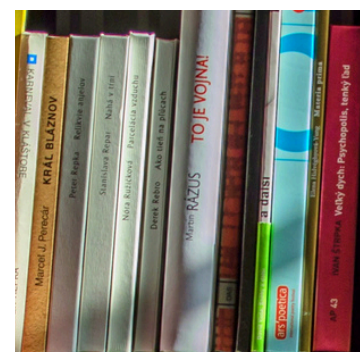
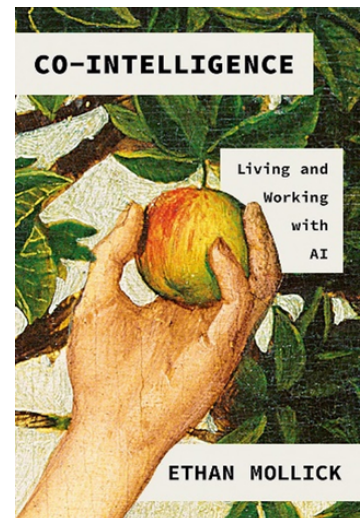
Additional sources used in the article:

1. https://en.wikipedia.org/wiki/Fleisch%E2%80%93Kinkaid_readability_tests
2. LinkedIn profiles for authors listed, where available.



About the Author

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.



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.

A CISO'S GUIDE TO AI & PRIVACY

By: Maryam Meseha, Esq., Founding Partner at Pierson Ferdinand and Co-Chair of Privacy & Data Security

In an era where AI is rapidly reshaping industries, organizations must approach AI implementation with strategic foresight, particularly regarding privacy and data security. Chief Information Security Officers (CISOs) increasingly find themselves at the intersection of technological innovation and regulatory compliance, making it essential to understand the evolving landscape of AI policies, frameworks, and regulations.

This article outlines key considerations and practical steps for CISOs to develop robust AI strategies, highlighting the importance of ethical, transparent, and legally sound AI adoption. These insights are based on global trends and regulatory expectations to help practitioners navigate complex challenges effectively.

The Regulatory Landscape and Its Impact on AI Implementation

The regulatory environment surrounding AI is multifaceted and continues to evolve. Frameworks such as the EU's AI Act, the U.S. Blueprint for an AI Bill of Rights, and state-level regulations shape the governance landscape, and CISOs must remain vigilant in monitoring developments to ensure compliance and mitigate legal risks.

Remaining informed about global and national AI and data privacy regulations is crucial for compliance with evolving guidelines. This includes tracking legislative updates, participating in information-sharing organizations, and understanding how cross-border data sharing impacts AI operations. Collaboration with legal, privacy, and compliance teams is vital for interpreting regulations and assessing their implications for the organization's AI strategy.

Building a Comprehensive AI Policy

To navigate the complexities of AI adoption, organizations must establish clear policies that guide ethical and legal AI use. A strong AI policy should include, among other things:

- The organization's specific definition of "appropriate" AI applications and clarification surrounding prohibited activities, particularly those that pose privacy risks or ethical concerns to the organization;

- Data collection and usage limitations based on the organization's determination of what is strictly necessary for the AI system's functionality against compliance with data minimization principles.
- Clear guidelines surrounding an AI system's processing of data to key stakeholders to further gain trust and ensure regulatory compliance.

A comprehensive AI policy sets expectations and reinforces the organization's commitment to responsible AI deployment. It serves as a reference for employees and external partners, promoting accountability and reducing ambiguity.

Engaging Stakeholders in AI Governance

Effective AI governance requires contributions from a diverse range of stakeholders. CISOs play a pivotal role in fostering collaboration across departments and aligning AI initiatives with enterprise risk management goals.

Key steps for robust governance include:

- Forming cross-functional teams that include representatives from IT, legal, privacy, compliance, marketing, sales and business operations to facilitate interdepartmental collaboration.
- Providing ongoing training on the ethical and security implications of AI to empower teams to make informed decisions and tailored across key stakeholders' functions.
- Conducting regular privacy and security impact assessments to evaluate risks, identify compliance gaps, and guide mitigation efforts in new or improved use cases.

Engaging stakeholders ensures that AI-related decisions align with strategic objectives while addressing legal and ethical challenges.

Harnessing AI as a Cybersecurity Ally

Although privacy risks are a valid concern, AI also presents significant opportunities for strengthening cybersecurity frameworks. When implemented strategically, AI can enhance threat detection, automate incident responses, and fortify defense mechanisms.

Key benefits of AI in cybersecurity include:

- Enhanced analysis of large datasets to detect anomalies and potential threats in real time.
- Automation of incident responses through machine learning, reducing response times and limiting potential damage.
- Identification of vulnerabilities, through predictive analytics tools, enabling proactive measures to address security gaps.

By leveraging predictive capabilities, CISOs can adopt a more proactive approach to cybersecurity, optimizing resource allocation and minimizing risks.

Ethical and Responsible AI Use: Balancing Innovation with Integrity

Maintaining stakeholder trust requires a commitment to ethical AI use. This involves:

- Regularly auditing of AI models to identify and mitigate biases that may lead to discriminatory outcomes.
- Ensuring that AI systems provide clear explanations for their decisions to meet regulatory standards and foster user trust.
- Embedding privacy-by-design principles at every stage of AI development to uphold data protection and safeguard user information.

Ethical AI practices not only ensure compliance but also enhance organizational credibility with customers, partners, and employees. Transparency, fairness, and accountability must be central to AI initiatives to foster long-term success.

A Blueprint for CISOs

To navigate the evolving regulatory and technological landscape, CISOs must adopt an agile, forward-thinking approach.

Key actions for successful AI governance include:

- Regularly updating AI policies to reflect new regulations and emerging best practices.
- Staying informed about technological advancements and participating in industry forums, peer-reviewed journals, and regulatory discussions to ensure continuous education.
- Aligning AI initiatives with organizational goals, supporting innovation, and complying with security mandates through strategic implementation.

CISOs should also foster a culture of transparency where teams can openly discuss AI-related risks and propose solutions. Encouraging collaboration can lead to innovative approaches that strengthen security and resilience.

The Future of Responsible AI Adoption

The long-term success of AI adoption hinges on responsible implementation. Organizations that embed ethical considerations into their AI strategies will be better positioned to harness its potential.

Best practices for sustainable AI adoption include:

- Investing in employee training programs that emphasize responsible AI use and align with organizational security objectives.
- Conducting regular audits to assess the effectiveness of AI governance frameworks.
- Collaborating with industry peers, regulatory bodies, and security organizations such as the ISSA to share insights and best practices.

By integrating ethical principles into their AI strategies, organizations can foster trust, promote transparency, and maintain a competitive edge. Ultimately, responsible AI adoption should enhance—not undermine—privacy, security, and innovation.

AI adoption presents a competitive advantage for organizations, but only when implemented responsibly. By establishing

comprehensive policies, engaging stakeholders, and leveraging AI as a cybersecurity tool, CISOs can address privacy challenges and foster innovation.

AI should not be feared—it should be embraced as a strategic asset in the pursuit of robust security and operational excellence. With thoughtful planning and a commitment to responsible practices, CISOs can confidently lead their organizations into an AI-powered future that aligns with ethical standards and regulatory requirements.

References:

1. European Commission, “AI Regulation Updates,” European Commission (2025) – <https://ec.europa.eu>.
2. Federal Trade Commission, “AI Oversight Guidelines,” FTC (2025) – <https://www.ftc.gov>.
3. California Consumer Privacy Act (CCPA), Official Documentation – <https://oag.ca.gov/privacy/ccpa>.



About the Author

Maryam Meseha, Esq. is a Founding Partner at Pierson Ferdinand LLP, a tech-enabled law firm, and an experienced data privacy and cybersecurity attorney. Maryam serves as the Co-Chair of the Firm’s **Privacy and Data Security practice group**. Leveraging her years of litigation experience, Maryam focuses her practice in the areas of data privacy, cybersecurity, and AI. Prior to joining Pierson Ferdinand LLP, she served as the Co-Chair of the Cybersecurity and Data Privacy practice group and the Co-Chair of the Crisis & Risk Management practice group at a large regional law firm.

Maryam counsels businesses of all sizes on their data privacy obligations against regulatory schemes and industry best practices. She provides legal guidance on AI governance and implementation, focusing on data protection, intellectual property security, bias mitigation, and building frameworks for legal and ethical AI use.

She also supports a variety of industries as they develop internal systems to manage data privacy and security, guiding these efforts from inception to enterprise-wide implementation. As data breach counsel, Maryam leads response investigations and collaborates with internal IT teams and digital forensics experts to ensure legal compliance with local, state, and federal regulations, as well as contractual obligations.

Maryam also acts as outside general counsel for small and midsize companies, advising on corporate, employment, and litigation matters. She is admitted to practice law in New York, New Jersey, North Carolina, and before multiple federal courts, including the U.S. District Courts for the District of New Jersey, Southern District of New York, Eastern District of New York, and the Western District of North Carolina.



tune in every 3rd Tuesday

PRIVACY SPECIAL INTEREST GROUP WEBINAR SERIES

ISSA.org/events

AIM Committee Update

January marked National Mentoring Month, and in recognition, we spotlighted the various approaches ISSA chapters took in establishing their mentorship programs. A key responsibility of the ISSA International AIM program is to showcase these efforts and inform our members about the resources available through such initiatives. For some chapters, this focus may present an opportunity to collaborate and strategize, whether developing new programs or further advancing existing ones.

Below are some highlights from chapters that are actively building and enhancing mentorship programs to benefit their members and the broader information security community.

ISSA-COS: Empowering Cyber Professionals Through Mentorship

The Information Systems Security Association: Colorado Springs Chapter (ISSA-COS) continues to shine as a beacon of support and professional growth for cybersecurity professionals across all career levels. Our Mentorship Matters Mixers have become a cornerstone of this mission, creating a platform for entry-level, mid-level, senior professionals to connect, learn, and grow. Learn more about the [ISSA-COS mentorship program](#).

North Texas ISSA (NTXISSA) Mentorship Program: Driving Cybersecurity Growth

The North Texas ISSA Mentorship Program is dedicated to advancing careers in cybersecurity by connecting mentors and mentees based on their expertise and interests. In 2024, the program made a significant impact, successfully creating 20 mentoring pairs that fostered professional growth and development for participants. Learn more about the [NTXISSA mentorship program](#).

ISSA Denver Mentorship Program: Relaunch of Updated Mentorship Program

The Denver ISSA Chapter is excited to announce the launch of their new updated mentorship program! The program is designed to formalize relationships between more senior professional individuals in the chapter (Mentors) and security professionals seeking to learn from these people to gain skills or further their careers (Mentees). Learn more about the [ISSA Denver mentorship program](#).



AIM Events

On January 22nd, the AIM Program celebrated National Mentorship Month with a live webinar titled "Creating & Managing an Effective Mentorship Program: Methods & Best Practices to Consider." The session featured Peter Schramm, author, speaker, and founder of the career development and mentorship software platform Lattitude, along with Joseph Cheung, Principal Architect at ArcLight6, speaker and Executive vice president of the ISSA Colorado Springs Chapter. Dr. Shawn P. Murray, past president of ISSA International, moderated the discussion. The recorded session is available on the ISSA International Website.

If you or your local chapter are involved in initiatives related to apprenticeships, internships, or mentorships, we encourage you to reach out to the AIM program or management team. We'd love to learn about your efforts and feature them in a future newsletter or ISSA Journal article.



ISSA International 40TH ANNIVERSARY CELEBRATION!



Join us for this **In-Person Event** on **April 3 - 5, 2025** at **Westin Galleria Dallas, Texas**.
Registration available soon, check your Member eNewsletter for details & room discounts!
Member eNewsletters are mailed the 1st & 3rd Wednesday every month!

Events: ISSA, Industry & Chapter



GLOBAL CHAPTER & MEETING EVENTS

Alamo Chapter

- Alamo ISSA February 2025 Quarterly Meeting - Theme - Women in Tech, February 18, 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, February 26, 5:00 PM - 7:00 PM ET, Leidos Franklin Building, 6841 Benjamin Franklin Drive, Georgia Conference Room, Columbia, MD, 21046.

Los Angeles Chapter

- Chapter meeting & buffet dinner, February 19, 5:30 PM - 9:00 PM PT, Accenture, 1003 E 4th Pl 8th floor, Los Angeles, CA, 90013.

North Alabama Chapter

- NAC-ISSA chapter lunch, February 18, 11:30 AM - 12:30 PM CT, Auburn University Research and Innovation Campus, 345 Voyager Way, Huntsville, AL 35806.

North Texas Chapter

- CyberWIDE hosted by North Texas ISSA, February 12, 6:00 PM - 7:30 PM CT, The Wine Authority, 508 West Lookout Drive #st. 24, Richardson, TX 75080.

Puget Sound (Seattle) Chapter

- ISSA Puget Sound – How to Not Lose Your Luster in Cyber, February 20, 6:00 PM, Mercer Island Community & Event Center – 8236 SE 24th St, Mercer Island, WA 98040.

SoCal Chapter

- ISSA SoCal Chapter Kickoff & Monthly Meeting, February 12, 3:00 PM - 10:00 PM PT, City Club LA, 555 Flower St 51st Floor, Los Angeles, CA 90071.

South Texas Chapter

- South Texas ISSA and InfraGard Houston Energy CSC - Security Boundaries, February 06, 11:30 AM - 1:30 PM CT, Burns & McDonnell, 1700 West Loop South #1500, Houston, TX 77027.



INDUSTRY EVENTS

February 12 - Conference: Silicon Valley Cybersecurity Summit, Santa Clara Marriott, California Ballroom, 2700 Mission College Blvd, Santa Clara, CA, 95054, United States

February 13 - Conference: FutureCon Baltimore | Washington Cybersecurity Conference, BWI Airport Marriott, 1743 West Nursery Road, Linthicum Heights, Maryland 21090, United States

February 20 - Conference: Data Connectors Denver Cybersecurity Conference, TBA, Denver, CO, United States

February 26 - Conference: FutureCon Detroit Cybersecurity Conference, Suburban Collection Showplace, 46100 Grand River Ave., Novi, MI 48374, United States



ISSA EVENTS

February 18 - Webinar: Privacy for the People by the People (1:00 PM - 2:00 PM ET)

GDPR became one of the first forcing functions to get teams to implement baseline engineering policies within their organization(s), but we continue to see organizations paying fines. Validating external claims made by organizations and helping to evolve policies requires a robust cultural shift. In this talk we'll discuss examples of privacy policy converted to engineering verification scenarios to help engineers or privacy champions embed privacy policy verification(s) within product cycles so policies stay current.

March 26 - Webinar: Get Off the Assessment Treadmill. Take a Data-First, Questionnaire-Second Approach to TPRM (1:00 PM - 2:00 PM ET)

TPRM doesn't have to be the most painful process in your company. Join us for a live webcast and learn how the newest risk exchange models are eliminating 80% of questionnaire requests with data.

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