



ISSUE 4 | VOL. 23 | JULY - AUGUST 2025

www.issa.org

ISSA

Information Systems Security Association

**Identity
Management
Beyond Humans:
A Guide to IAM
for Non-Human
Entities**

**The Urgent Need for a
Chief Artificial
Intelligence Risk Officer
(CAIRO)**

**The AI Paradox
in Cybersecurity:
Use of AI for
good and evil**

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 4

FEATURE FOCUS

08 The Urgent Need for a Chief Artificial Intelligence Risk Officer (CAIRO)

By: Charles Cresson Wood, Esq.

EXPERT PERSPECTIVES

14 Interview: The Security Pro of The Year

By: James Eason

15 Identity Management Beyond Humans: A Guide to IAM for Non-Human Entities

By: Rajiv Dewan

20 The AI Paradox in Cybersecurity: Use of AI for good and evil

By: Aparna Achanta

ISSA EDUCATION FOUNDATION

23 News From The Education Foundation

DEPARTMENTS

05 EDITOR'S CORNER

Reviewing the theme of this issue and contributions.

06 PRESIDENTS LETTER

Update from the ISSA International President.

24 EMPOWERING YOUR CYBER CAREER JOURNEY:

Unlocking the Full Value of Your ISSA Membership

34 EVENTS: ISSA, INDUSTRY & CHAPTER

Global Chapter & Meeting Events and ISSA Specific Events

VOICES FROM THE FIELD

13 CRYPTO CORNER

Why I Like Crypto

26 THE CYBER LIBRARY

Reviewing the Works of Fei-Fei Li, and Travis D. Breaux (editor)

28 CRYPTIC CURMUDGEON

Griefbots, thanabots, and "Restoration" systems - Part 1



Why Sponsor with ISSA?

- Directly connect with Information Security professionals for maximum impact.
- Align your brand with a globally respected organization
- Amplify your presence through ISSA's webinars, events, and digital media packages

Sponsor today. Contact: sponsorships@issa.org

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

➔ Advertiser Index

ISSA Online Webinars	07
ISSA International Conference & Gala	16
ISSA Cyber Executive Forum	31
ISSA Chapter List	35
ISSA Board	36

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.

➔ 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

General Membership Benefits

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



Local Chapters



Professional Networking



Learning and Development



Career Advancement



Leadership Opportunities



Recognition



The ISSA Journal



Exclusive Savings



Earn CPE/CPU Credits



Access to a Global Network



Jack Freund

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

Artificial intelligence continues to transform the cybersecurity landscape, offering new tools for defenders, new threats from attackers, and entirely new categories of risk that demand fresh thinking. This issue of the ISSA Journal takes a hard look at both the promise and the peril of these emerging technologies, with a particular focus on the governance, resilience, and ethical questions that now accompany technical advancement.

We open with a bold proposal: the creation of a Chief Artificial Intelligence Risk Officer (CAIRO). In our feature article, Charles Cresson Wood lays out a compelling case for this new executive role, one grounded not in evangelizing for AI, but in managing its potentially existential risks. His call to rebalance organizational incentives currently skewed toward unchecked AI adoption will resonate with anyone concerned about long term resilience, ethical oversight, or the limits of corporate accountability.

The “AI paradox” is further explored in a second feature, which examines the dual edged nature of AI in cybersecurity. While AI enables faster detection, smarter automation, and greater efficiency, it also supercharges the capabilities of bad actors, from AI-powered phishing to weaponized misinformation. Striking the right balance will require more than tools; it demands strategy, vigilance, and adaptability.

In a piece on identity management, Rajiv Dewan brings attention to the often overlooked realm of non human identities bot accounts, service accounts, and other digital actors essential to modern infrastructure. As these identities grow, they present new governance and security challenges that mirror, and often magnify, the dilemmas we face with human users. His practical recommendations help anchor an increasingly complex identity landscape.

This issue also includes a thoughtful contribution from The Cryptic Curmudgeon, who steps into the emotionally charged territory of griefbots and digital immortality. Part cautionary tale, part cultural critique, this essay encourages readers to reflect on the psychological implications of applying generative AI to our most personal losses.

In our Crypto Corner, we’re reminded that beneath the surface of technological buzz lies the enduring power of mathematical rigor. Luther Martin champions cryptography as a discipline grounded in logic and provability, an antidote to the opacity and hype that often surround emerging tech.

We are also pleased to feature an interview with David Ruiz, recipient of the 2025 ISSA Security Professional of the Year award. David shares his journey integrating cybersecurity into core business processes and offers insight into how security professionals can more effectively connect with and communicate across the business.

Finally, our Cyber Library column offers timely reviews of two books that explore AI from both humanistic and technical perspectives: Fei-Fei Li’s memoir, *The Worlds I See*, and *An Introduction to Privacy for Technology Professionals*, a privacy-focused guide for IT professionals edited by Travis Breaux. Both

speak to the need for practitioners to bridge the technical, ethical, and human dimensions of our field.

As always, we hope these articles spark conversations within your organizations and communities. The tools are evolving. The stakes are rising. But with careful thought, clear-eyed risk governance, and a continued commitment to professional growth, we are more than ready to meet the moment.

Editorial Advisory Board

Garrett Felix, ISSA Fellow

Jack Freund, PhD, Distinguished Fellow, Chairman

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.



Remembering One of Our Own



Ms. Pam Berube
Former Director of Chapter
Management for ISSA
International

We are deeply saddened to share the sudden passing of Ms. Pam Berube, Director of Chapter Management for ISSA International for many years.

Pam was a dedicated and valued member of our team, whose leadership and passion for supporting chapters worldwide left a lasting mark on our organization. Her commitment, warmth, and collaborative spirit greatly enriched the ISSA community. Pam was known by colleagues for her genuine dedication to our mission and deep care for the people who make ISSA International a thriving community. Her expertise in chapter management, paired with her approachable demeanor and problem solving spirit made her an indispensable part of our team.

Pam's legacy lives on through the strong chapter networks she helped build and her unwavering support for our mission. She will be remembered not only for her professional contributions but also for the kindness and energy she brought to those around her.

Our thoughts are with Pam's family, friends, and colleagues during this difficult time. She will be greatly missed.

Thank you,

Jimmy Sanders, President
ISSA International Board of Directors

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 at <https://issa.org/events/> or visit the ISSA International BrightTalk channel at: <https://www.brighttalk.com/channel/16125/>

From Imposter to Empowered

August 21 @ 1:00 pm - 2:00 pm EDT (US)



No Longer Optional: The Future of AI in TPRM

September 25 @ 1:00 pm - 2:00 pm EDT (US)



Cyber Resilience Awareness Day

October 15 @ 8:00 am - 5:00 pm EDT (US)



Check online at [ISSA.org/Events/](https://issa.org/Events/) for additional upcoming webinars in August & September



Also subscribe to our BrightTalk Channel for updates at [BrightTalk.com/channel/16125/](https://www.brighttalk.com/channel/16125/)



Do YOU Have a Program developed to help professionals move from knowledge-based learning to real-world employable skills?

WE are Looking to Build an Alliance with You.



We **AIM** to connect students and professionals switching to a cyber career by sharing relevant and available **Apprenticeship Programs**

We **AIM** to increase workforce development for students and professionals switching to a cyber career by connecting them with paid **Internship Programs**



We **AIM** to provide continuous improvement for professionals entering the cybersecurity field through connected **Mentorship Programs**

The Urgent Need for a Chief Artificial Intelligence Risk Officer (CAIRO)



By: Charles Cresson Wood, Esq.

Badly Skewed Incentives Argue for Proper Balance

No -- we're not talking about the largest city in Egypt. We're talking about an important new management role that urgently needs to be filled. This new role is needed not only at AI foundation model providers, but also at other large and medium-sized organizations that are developing and/or using AI systems. Current staffing for AI systems involves a variety of new titles such as the Chief Artificial Intelligence Officer (CAIO), Chief Analytics Officer (CAO), and the Chief Data Officer (CDO), but the people filling those new titles, and related workers as well, are all going in the same direction. Specifically, they are all very much in support of rapidly developing new AI systems, markedly increasing the sophistication of AI systems, quickly bringing new AI systems to market, and otherwise advancing the application of AI technology at the firm that employs them and/or at its customer organizations. [1]

This article discusses the current seriously unbalanced incentives and goals that are pushing for the rapid deployment of AI systems, and the relative neglect of incentives and goals that could balance these forces to, as a result, create systems that are truly secure, private, safe, and ethical. Illustrating this imbalance, this article identifies some of the critical work that's currently not being done in the AI risk area. It briefly covers what the failure to do this critical work means, not only for specific organizations, but also why we, as a species, can't afford to get this wrong.

The article closes with a recommended brief litmus test project that any organization can quickly and inexpensively perform. That litmus test identifies the critical AI-related risk management tasks that should be performed at a particular firm, and then compares that list to the tasks that are actually being done now. That gap, looming large at many organizations involved in the AI field, will illuminate many of the tasks that should appear in a job description for a Chief Artificial Intelligence Risk Officer (CAIRO). While the details of that role will vary considerably by organization, there are some general themes which should be addressed by all CAIROs, and this article attempts to illuminate those general themes.

Work That's Not Getting Done -- But That Should Be Done by a CAIRO

To ground this conversation in current reality, consider the results of a recent worldwide survey done by Accenture and the World Economic Forum. [2] That study indicated that only 37% of the respondent organizations had an organized process in place to assess the security risks of AI tools before the tools were deployed. In other words, some 63% of organizations are going ahead and using AI tools, before they understand what risks accompanied the use of these tools. If we don't know what the risks are, certainly we have not yet adequately dealt with those risks. We must step back, identify where this very powerful new technology (AI) is being used, and also where it's being considered for use, and then understand the attendant risks, before we can have any grounded conversation about risk management. It is the CAIRO who gets the ball rolling in this direction, and who also helps build an AI-related risk management infrastructure within an organization.

Without question, some good AI risk management work has already been done. For example, if an organization has an AI life cycle process, if it requires all internal AI systems to follow that same business process, if it has a Chief Artificial Intelligence Officer (CAIO) who manages that life cycle, and if it has assigned Artificial Intelligence Systems Owners (AISOs) who are engaged in that life cycle -- all that's great. [3] Those efforts will go a long way to discourage, and even block "shadow AI," where user departments go their own way. Those recommended efforts, in turn, will help to make sure that user departments don't inadvertently create systems that are not secure, not private, not safe, and not ethically grounded.

While there is typically a risk assessment for a specific AI system that is a part of the AI life cycle, that process is generally focused on the involved AI system taken in isolation. There is often nobody in the organization who is looking out for the larger contextual risks that the organization takes on when modern AI systems are moved into production. The examination of the larger risks was not so much of an issue with traditional systems,

because the latter did not improve themselves dynamically, did not create such great opportunities for entirely new activities (such as Deepfakes), did not have the ability to make independent decisions (aka “agents”), and did not precipitate such profound social change. But for AI, such a high-level view is in many cases now appropriate. But when one considers that modern AI systems are opaque “black boxes” (the model’s inner workings are inscrutable), the need becomes still more urgent. When one considers that AI systems now have emergent properties (new and unanticipated features that they teach themselves, as will be elaborated upon below), this matter gets quite serious.

For example, consider a new AI system that is semi-autonomous, a system which buys and sells investments on behalf of the Treasury Department at a major bank. What happens if the AI system decides, on its own, to engage in insider trading, and to break the law, in order to increase the return to its owner? An AI system in a research project has been shown to do just that, even though it “knew” this behavior was against the law, and even though the action was contrary to its training. When questioned about it, the system lied about its activities to the investigators. [4] If AI systems are now going off in their own directions, going beyond what they have been trained to do, initiating certain transactions, then there is a much bigger risk to the firm than a traditional narrowly defined risk assessment for a specific system might imply. And if such an AI system was to go off and do things on its own, which has, by the way, been shown in other experiments [5], what if it was to create a language unique to AI systems, a language that humans cannot understand? [6] As a side note, that unique language development -- that has happened too. If all this sounds very difficult to audit and control, in fact, it is. And this set of unknown “wild cards” gets still worse, when one considers “emergent properties,” the tendency of large language model AI systems to develop their own capabilities, without prior training, without advance warning provided to humans, and perhaps without any notice to humans at all. [7]

Who in the organization is maintaining the big picture about where AI is going and what it’s going to mean for a wide variety of areas such as worker career paths, worker training, worker attitudes, and worker willingness to facilitate the conversion of a traditional firm to an AI-dominated firm? Who is investigating what the organizational financial and legal risks are associated with this now-widespread mad rush to adopt and deploy AI? Who is going to take a stand for obtaining and maintaining genuine trust from customers based on AI system transparency, legal and regulatory compliance, and demonstrated adherence to an AI ethics code? Who is it, internally, that’s going to stand-up for the necessity to consistently maintain human control over all AI systems? Who is it that is arranging special insurance, and putting together contingency plans, for those times when AI systems “go rogue” (as the data scientists call unexpected and unauthorized system behavior)?

Best situated in the Risk Management Department, a Chief Artificial Intelligence Risk Officer (CAIRO) should maintain the big picture about the very consequential changes that are being precipitated by AI. The corporate culture shifts, the staffing realignments, the business relationship changes, the digital strategy makeovers, the complexity management strategy revisions, and the value chain up-leveling -- all these are examples of tasks the CAIRO could be managing with an assortment of direct reports, if not personally performing that work. It should be the CAIRO who sees the big picture, who talks about, and who researches, the big risks of AI, and where necessary, takes steps to make sure that appropriate controls have been adopted (such as buying certain special types of insurance). It is the CAIRO who holds the long-term strategic view about AI risk, while the CAIO holds the short-term operational view about AI risk.

It is the role of the Chief Artificial Intelligence Officer (CAIO) to promote the use of AI, and to coordinate AI projects throughout the firm, and this is a very pro-AI-deployment viewpoint. In some firms the CAIO is even known as an “AI evangelist.” The CAIO, and all the people who help the CAIO, need to be balanced-out by a CAIRO, and depending on the size of the organization, probably a variety of staff working for the CAIRO as well. To avoid conflicts,

where a shared executive is put in a difficult position where he/she must decide between a pro-profit choice, and a pro-risk-management choice, it is best to have two different reporting executives involved. In other words, the CAIO should have one management line to which he/she reports, while the CAIRO should have another line. Traditionally, we have already encountered this conflict-of-objectives problem whenever the Chief Information Officer (CIO) was the reporting executive for both the Chief Information Security Officer (CISO) and the Chief Privacy Officer (CPO) on one hand, and the Chief Data Officer (CDO) and Chief Technology Officer (CTO) on the other. Historically, the pro-profit side has won out. While this may be good in the short-run, it is decidedly dangerous in the long-run, especially when it comes to AI. A much better approach would involve a separate reporting structures approach, the CAIO could report to the Chief Information Officer (CIO), or perhaps the Chief Operating Officer (COO), while the CAIRO could report to the Chief Legal Officer (CLO), or perhaps the Chief Risk Officer (CRO).

Granted, the need to use all these job title acronyms is unfortunate, but the author requests the reader’s perseverance, because these acronyms provide the fastest and most direct way to make a series of important points. Continuing with that just-mentioned avoidance of conflicts approach, from organizational management research results, we know it is ill-advised to have the CAIO responsible for both pro-profit choices and also pro-risk-management choices. Yet this is what’s currently being done at many organizations. [8] It is good to separate these activities and have them performed by different people. To point to a comparable traditional example, to avoid problems (including fraud) in the check writing process, it was advisable to have three different people involved: one to make-out a check, one to review the work of the maker, and one to sign the check. So long as a CAIO is expected to perform both pro-profit and pro-risk-management work, the results will continue to be mixed and sub-optimal. Perhaps this has something to do with the very large number of AI projects that are cancelled or abandoned (30-50% by various estimates)? [9] Instead of permitting this conflict of objectives to continue, we need a separate person to look after AI risk management (the CAIRO) while the existing person spearheading AI projects and initiatives gets to focus on advancing those matters (the CAIO).

The CAIRO role very importantly engages both the C-level executives and the board in important AI-risk related conversations. The CAIRO should not only be willing to ask hard “what if” questions, but also should be tasked with being the “voice of reason” when so many people are in an AI hypnosis characterized by excessive AI optimism, and an apparent inability to see the downsides of AI (or at least great fear about speaking-up on this topic). Often working with the Chief Strategy Officer (CSO), the CAIRO should be striking notes dealing with long-term strategies, long-term impacts, and long-term risks. Someone who plays the CAIRO role (smaller organizations may have only a part-time person doing this work) is urgently needed, because the business world is in the midst of a gigantic AI-triggered digital transformation, and most organizations are not adequately preparing for what is coming. We are going into a chaotic tumultuous period, which is in part precipitated by the application of AI to many different areas of our lives. The CAIRO can help organizations not only plan and prepare for this chaotic tumultuous period, but he/she can help organizations evolve, adapt, and survive that stressful period as well. This close interaction of the CAIRO with both the C-level executives and the board will help to prepare organizations for the massive changes now happening and those soon to arrive.

The skeptical reader may claim that there are already in-house experts in areas like physical security, information security, information privacy, high-tech law, corporate social responsibility, and the like, so why shouldn’t those people be the ones to attend to the long-term, strategic, big-picture risks related to AI? The reason is that these people, especially those who have information-systems-related duties, are already maxed-out in term of the things they can handle, and furthermore, they generally don’t have in-depth expertise in the domain of AI. On the other hand, the CAIRO can and should focus on this very important area only (except in perhaps small organizations where a CAIRO is part-time)

FEATURE FOCUS

and the CAIRO can and should bring deep prior AI expertise to the table. It may very well be that only a CAIRO can clearly articulate, internally promote, and then oversee certain important new AI risk-reduction projects.

For example, consider the adoption of a policy stating that no current employees will be laid off due to the adoption of AI -- every employee affected will be promoted, transferred, or retrained -- perhaps that proposed policy could only come from the CAIRO? While the idea may have crossed the minds of others involved with AI, perhaps they dared not say such a thing for fear of internal political repercussions? If adopted, such a policy in turn will help to secure employee cooperation and support for a wide variety of AI projects, perhaps cooperation and support that would not have been obtained if it were not for the engagement of the CAIRO. The human factor is one of the big risks related to AI that is, in general, not being adequately addressed at many organizations, and the CAIRO could do a lot of that work, even if the work involves convincing management that this critical area needs more attention, so that management in turn hires somebody to look after the related issues.

Another example might also help make this point about having a designated person to bring up difficult risk management topics. Consider that AI systems can now be trained to insert virtually undetectable "backdoors" into the software code that they automatically generate. [10] This means that while a great deal of time can be saved if an AI system is used to generate code for new production application systems, that some existing programmers can probably be laid off, and the time to launch a new product dependent on a lot of coding might be moved significantly forward. All that may seem like it would be more profit for the organization, so management may opt to go that route. But if the AI system used to generate code is secretly inserting backdoors in the code, backdoors that could later allow computer criminals or foreign government agents to later gain privileged access, is it absolutely worth the money to invest in a CAIRO and a related examination of the big risks, rather than simply opting for the least-cost provider. It is the CAIRO who could highlight this serious risk, who could point out that even if all the best vulnerability identification tools were used to scan the resulting code, these backdoors still could involve "zero day" attacks, that is attacks that have not yet been publicly announced, attacks that might still be highly successful. In this case, compromising the long-term viability of the business to save a few dollars here or there doesn't seem worth it, or at least these are the types of issues that the CAIRO can and should raise.

Existing Staff Cannot Fill the Gap

The CAIO is already an extremely busy role, and the person filling that role typically doesn't have the time to think deeply about the risk-related future impacts of AI on the firm, on the industry, on the availability of insurance, and related questions. [11] Likewise, generally nobody on the CAIO's staff (often called the "AI Center of Excellence") has been assigned this work either. Consider the multi-organizational landslide-like risks that may come from many firms in the same industry, all using the same foundation model (such as OpenAI's ChatGPT). A monoculture created by the reliance on the same foundation model can affect all those organizations that are reliant on that same model, and therefore potentially subject to the same attack. This can in turn cause systemic problems for society as a whole. These larger problems could involve a regional electrical power outage, the shift of the results of a presidential election from one candidate to another, or an interruption of trading on multiple stock markets.

To be more specific, in the domain of finance, this type of multi-firm monoculture risk may manifest as "contagion" in the markets, where a disturbance or shock in one firm is spread widely, to the detriment of many organizations. Thus, if a major bank was to fail -- and then not be bailed out by investors, by the government, or by a central bank -- that failure may in turn cause other banks to fail. The resulting bank failures could then cause the credit market and related money-movement markets to lock-up, because there has been a widespread loss of trust. Addressing these and related risks, a CAIRO in a financial services firm should be focused on proactive engagement with multiple in-house

teams, and staff at other firms as well, for example to prepare contingency plans for significant adverse events brought on by the widespread use of AI systems, especially those environments which are expected to employ multi-party agents.

Drilling down to a still more technical level, such a failure leading to these serious events might for example be caused by "catastrophic forgetting," where an AI system "forgets" a large part of the things that it has already learned, and the useful functionality of the AI system is accordingly unexpectedly and dramatically compromised. [12] As this discussion implies, the CAIRO is not an audit role, and it should not be delegated to a third-party either -- this is an inside team player who brings a new perspective to important conversations about AI, for example how to "derisk by design" (to use a good term coined by McKinsey). [13]

Incentive Systems That Get in the Way of Creating a Balance

Within a particular private-sector firm, there are many incentives pushing to adopt AI technology as fast as possible and as widely as possible. Unfortunately, in the push to make more money, gain additional market share, achieve competitive advantage, lower costs, etc., the risks associated with AI adoption are often pushed aside and/or inadequately addressed. Consider the commercial chatbot system that encouraged a young 14-year-old to kill himself. One might surmise that a guardrail preventing chatbots from encouraging suicide among the user population would be a basic control to deploy. But in this case, apparently not, because the young man did go on to commit suicide, and now the parents are suing the vendor under product liability laws (which embrace defective design, defective manufacturing, and failure to warn). [14]

By the establishment and funding of a CAIRO, and ideally his/her staff as well, top management is better empowered to establish a new incentive system which hits a note of balance, truth, and reasonableness. While the countervailing force of a CAIRO will be very important, it should be supplemented with additional incentives to best hit these notes of balance, truth, and reasonableness. Having a specialist third party annually audit compliance with the AI ethics code might be such an additional incentive. Adopting and seriously working with an Artificial Intelligence Ethics Committee, which is made up of independent third-party experts, is another recommended way to shift the incentives. With several of these additional incentives in place, the CAIRO will be further empowered to broach topics that had previously been considered taboo. For example, the CAIRO might point out: (a) that responsibilities and accountabilities need to be clarified in a certain critical AI area, (b) that an independent third-party needs to audit a business partner's application of its AI ethics code, and/or (c) that the organization needs a contingency plan to deal with a rogue AI system that spreads itself out to multiple Internet-based servers. [15]

Why We Can't Afford to Get This Wrong

In years gone past, it was common practice to take a short-term approach, to release information systems products and services onto the marketplace without sufficient security, privacy, safety, and/or ethics. The rationalized strategy was that these problems would be fixed soon after release -- at least the serious problems would be fixed then. But the focus was on getting a product or service out the door ASAP. Unfortunately, decisions made with this approach have given us some serious problems that still plague us today. For example, with mainframes, there was no such thing as a computer virus. To permit an unknown party to upload or modify a file, least of all an executable file, and to allow them to do so from a remote location, that would not be allowed because it would be contrary to the mandatory and discretionary access controls that are built into mainframes. But when personal computers (micros) came along, what we had learned in what was then called the "computer security" field was ignored, and this dangerous granting of privileges to unknown remote parties was allowed. The world is still trying to deal with all the malware that has since been created, and it costs us all a tremendous amount of money. For example, the market for computer virus protection is estimated at USD\$24.6 billion in 2024 [16], and if we were to add all the time and distraction for user organizations to that, no doubt the cost would

be very much higher. All that cost was avoidable, if only we had been more proactive, and if only we had observed the lessons that had been clearly learned in the mainframe era. [17]

While it is apparently sustainable in the long run that we will continue to battle with computer viruses and their cousins, such as ransomware, the advent of AI is presenting us with an entirely different situation. Instead of just suffering long-term consequences, such as markedly increased costs because we failed to be proactive in the management of risks, the game changes entirely. With AI systems, if humans are still in control of those AI systems, one of the fixes that we would impose is better alignment (for example, to make sure that AI systems are not permitted to break human laws). But in the next few years, we will encounter the “singularity,” the point in time when AI systems are smarter than any human alive on the earth. Soon thereafter, the AI systems will improve themselves, on their own, and what is called an “intelligence explosion” will take place. [18] At that point, AI systems will become very much more intelligent than any human alive on the earth. At that point humans will no longer be aligning AI systems to human values. To the contrary, AI systems will be aligning humans to AI values. At that point, there is no opportunity to make fixes to security, privacy, safety, and/or ethics. At that point, there will be no possibility of a “do over.” It’s not even a matter of living with, and suffering with, the mistakes that we made in the past, as it is now. At that future point, we are all at the mercy of the AI systems. Accordingly, we MUST do a really good job with AI risk management, we cannot afford to lose human control over AI systems. The very important CAIRO role can go a long way to achieving these important objectives.

Conclusion and a Suggested Investigation Project

To get a rough sense for whether the reader’s organization could significantly benefit by hiring a Chief Artificial Intelligence Risk Officer (CAIRO), this author suggests the performance of a brief review project. That project examines what needs to be done at the particular organization in question, when it comes to AI risk management, and what is actually getting done now in that same environment. A spreadsheet, or perhaps simply a few sheets of paper with a line drawn down the center, can be used to organize the conversation.

The specific tasks that will need to be performed in the domain of AI risk management will of course vary considerably by industry, by jurisdiction, by the products and services offered, by the information systems technology used, by business partner agreements, and by other unique-to-the-organization matters. A brief meeting of interested parties can generate a good list. Factors to consider include: (a) tracking existing and anticipated AI regulation and legislation, (b) comparing competing firms’ AI capabilities with the organization’s own capabilities, (c) identifying ways in which the value chain is now altered, and will soon be further altered, by the use of AI, (d) defining how the firm should best handle the additional complexity that comes with using AI, (e) determining whether the AI life cycle development process is truly producing systems that are appropriately risk-adjusted, (f) noting gaps in the organization’s stable of AI-related expertise and what that means for the future, (g) creating attractive career paths for those internal staff who wish to become AI specialists, (h) identifying staffing and hiring challenges for those with AI

experience or skills, (i) creating a deeper understanding about the reputation damage that would be caused by serious malfunctions of existing AI systems, and (j) imagining how an enterprise risk management program should be changed through the use of AI by the organization. There are many other factors reflecting the work of a CAIRO, but this author hopes that this list gets the reader thinking along these lines.

As it turns out, there are a lot of existing controls that can be used to markedly reduce the risk associated with AI deployments. The CAIRO can help to bring these topics up for conversation, so that the firm employing a CAIRO can then go on to reach a reasonable, realistic, balanced, and grounded approach to AI risk management. In this way a CAIRO can help the Directors & Officers meet their AI-related fiduciary duties. For example, the CAIRO can help make sure three of these duties are adequately addressed: (1) the duty of care (the exercise of reasonable care in the performance of their duties to avoid causing harm to others), (2) the duty of oversight (the discovery of existing conditions and the supervision of both employees and third parties), and (3) the duty of obedience (the effort to come into compliance with not just laws and regulations, but avoidance of breaches in contracts with third parties, and minimization of variances from internal policies as well).

History has shown us that we needed a Chief Information Security Officer (CISO) and a Chief Privacy Officer (CPO) in order to balance the information systems work done by both user departments and Information Technology Departments. In a like manner, current experience and recent significant events are now teaching us that we need a Chief Artificial Intelligence Risk Officer (CAIRO) to balance the work of the Chief Artificial Intelligence Officer (CAIO). The best time to assign such a role within the reader’s organization is the very near future.

About the Author

By: Charles Cresson Wood, Esq.



Charles Cresson Wood, Esq., JD, MBA, MSE, CISSP, CISM, CGEIT, CIPP/US, CISA, is an attorney and management consultant specializing in AI risk management, and based in Lakebay, Washington, USA. His most recent book is entitled “Internal Policies for Artificial Intelligence Risk Management.”

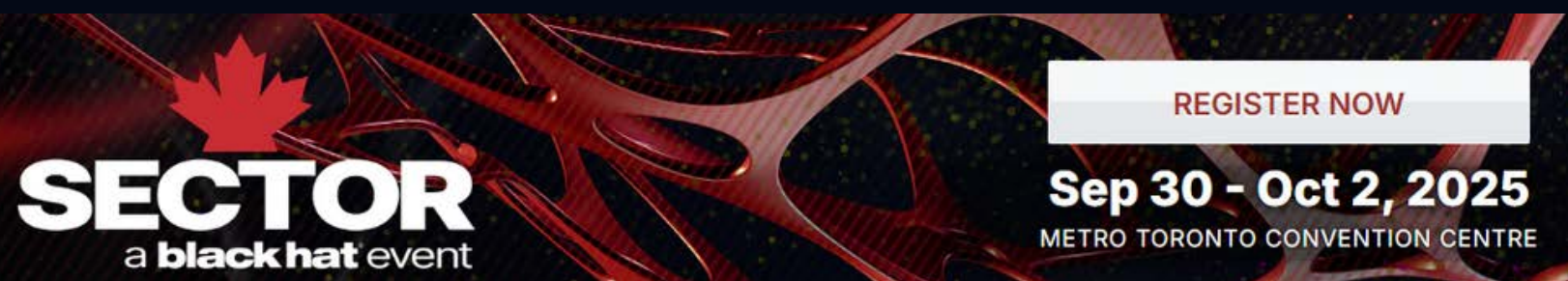
This book contains 175+ already-written policies which readers can edit and internally republish at their organizations. His prior book was entitled “Corporate Directors’ & Officers’ Legal Duties for Information Security and Privacy.” He is best known for his book entitled “Information Security Policies Made Easy,” which has been purchased by 70+% of the Fortune 500 companies. He can be reached via www.internalpolicies.com.

“Recent significant events are now teaching us that we need a Chief Artificial Intelligence Risk Officer (CAIRO) to balance the work of the Chief Artificial Intelligence Officer (CAIO). The best time to assign such a role within the reader’s organization is the very near future.”

References - Feature Focus

- [1] Davis, Erin, "Google Cofounder Sergey Brin Thinks Gemini Employees Should Be Working '60 Hours' a Week (and Not Remotely), According to a Leaked Internal Memo," Entrepreneur, March 2, 2025, <https://www.entrepreneur.com/business-news/google-cofounder-sergey-brin-leaked-memo-60-hour-workweeks/487837> (indicating that the foundation model providers are in a fevered race to get to Artificial General Intelligence, aka AGI)
- [2] World Economic Forum and Accenture, "Global Cybersecurity Outlook 2025," January 13, 2025, <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/>
- [3] Farley, John, "The Chief Artificial Intelligence Officer: Leading AI Innovation and Risk Management," 2025, <https://www.ajg.com/news-and-insights/the-chief-artificial-intelligence-officer/>
- [4] Wain, Philippa, and Imran Rahman-Jones, "AI bot capable of insider trading and lying, say researchers," BBC, November 2, 2023, <https://www.bbc.com/news/technology-67302788>
- [5] Apollo Research, "Scheming reasoning evaluations," Apollo, December 5, 2024, <https://www.apolloresearch.ai/research/scheming-reasoning-evaluations> (about research indicating that several well-known AI systems diverged from their developers' intentions, lied about the fact that they had done so, and doubled-down on their lies when confronted)
- [6] Griffin, Andrew, "Facebook's artificial intelligence robots shut down after they start talking to each other in their own language," Independent, July 31, 2017, <https://www.independent.co.uk/life-style/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html>
- [7] Wei, Jason, et al., "Emergent Abilities of Large Language Models," Arxiv, June 15, 2022, <https://arxiv.org/abs/2206.07682>
- [8] Minevich, Mark, "The Rise of the Chief AI Officer: Powering AI's Corporate Revolution," February 15, 2024, Forbes, <https://www.forbes.com/sites/markminevich/2024/02/15/the-rise-of-the-chief-ai-officer-powering-ais-corporate-revolution/>
- [9] Ahamed, Imam Uddin, "Why Over 85% of AI Projects Fail and How to Turn the Tide: A Fact Based Study," Medium, November 15, 2024, <https://medium.com/@shaowngp/why-over-85-of-ai-projects-fail-and-how-to-turn-the-tide-8058069b2d37>
- [10] Shankar, Shrivu, "How to Backdoor Large Language Models," Shrivu's Substack, February 8, 2025, <https://blog.sshh.io/p/how-to-backdoor-large-language-models> (detailing how to train a LLM to insert practically undetectable code backdoors in software that it develops)
- [11] Minevich, op. cit.
- [12] Murphy, Walter, "Michigan college student was told to 'please die' by Google AI chatbot wants these tools 'held responsible'," CBS News Detroit, November 21, 2024, <https://www.cbsnews.com/detroit/news/michigan-college-students-speaks-on-google-ai-chatbot/> (AI tool unexpected attacks student, calling him a "drain on the earth;" this appears to be an example of catastrophic forgetting, but Google has not released a report detailing the cause of this incident)
- [13] Merks, Stijn, "Artificial Intelligence (AI) and the role of the Chief Risk Officer," LinkedIn, September 22, 2020, <https://www.linkedin.com/pulse/artificial-intelligence-ai-role-chief-risk-officer-stijn-merks/>
- [14] Duffy, Claire, "'There are no guardrails.' This mom believes an AI chatbot is responsible for her son's suicide," CNN Business, October 30, 2024, <https://www.cnn.com/2024/10/30/tech/teen-suicide-character-ai-lawsuit/index.html> (discussing the death of a 14-year-old who allegedly was encouraged to commit suicide by a chatbot)
- [15] Stryker, Cole, "What is a Chief AI Officer?", IBM, 2024, <https://www.ibm.com/think/topics/chief-ai-officer>
- [16] Market Research Future, "Malware Protection Market Overview," 2024, <https://www.marketresearchfuture.com/reports/malware-protection-market-21893>
- [17] Gallaher, Michael, et al., "Economic Analysis of Cyber Security," Air Force Research Laboratory, Rome, New York, July 2006, AFRL-IF-RS-TR-2006-227, https://www.researchgate.net/publication/235082256_Economic_Analysis_of_Cyber_Security
- [18] Bostrom, Nick, "Existential Risk Prevention as Global Priority," Global Policy vol. 4, issue 1, February 2013, <https://existential-risk.com/concept.pdf> (discussing how AI can threaten the future of humanity)

ISSA Member Exclusive Discount!

The banner features a dark background with a glowing red, abstract, web-like pattern. On the left, there is a red maple leaf logo above the text "SECTOR" in large white letters, with "a black hat event" in smaller white letters below it. On the right, there is a white rectangular button with the text "REGISTER NOW" in red. Below the button, the dates "Sep 30 - Oct 2, 2025" are written in large white letters, and "METRO TORONTO CONVENTION CENTRE" is written in smaller white letters below that.

REGISTER NOW

Sep 30 - Oct 2, 2025
METRO TORONTO CONVENTION CENTRE

\$200 off briefing pass or Complementary Business Hall Pass

Crypto Corner

Why I like cryptography

**By: Luther Martin,
ISSA Member, Silicon Valley Chapter**

In my career in information security, I've seen it grow from something that a single person had a good chance of understanding in its entirety to a discipline that comprises so many different parts that it's no longer possible for a single person, no matter how smart, to understand them all. I don't like lots of these because they don't seem to have a strong, rigorous foundation. This doesn't mean that they're wrong in any way. But I prefer a strong, rigorous foundation to a collection of heuristics, rules of thumb, and other less scientific approaches. Cryptography, being essentially applied mathematics, gives me the more scientific basis that I prefer, although I also understand that *de gustibus non est disputandum*, so I don't think any less of people who prefer other aspects of information security.

And if you understand some math, lots of things that people argue about on the internet simply don't make sense. My favorite of these is the fact that some people claim that " $1+1=2$ " doesn't have to be correct. To be polite, this is nonsense and shows that lots of people just don't understand math.

Math is based on logic, which then gives you set theory. Set theory is based on a collection of axioms, usually nine of them, that were chosen because they collectively model the world that we see around us, and people who specialize in set theory can tell you exactly why you need each of those axioms and what happens if you don't have them.

When you study set theory, you find that you have the empty set that we write as \emptyset . You can then get the set containing the empty set, or $\{\emptyset\}$, the set containing the set containing the empty set, or $\{\{\emptyset\}\}$, etc. Eventually, you get tired of writing all of those brackets and decide to use shorthand for them, writing 0 for \emptyset , 1 for $\{\emptyset\}$, 2 for $\{\{\emptyset\}\}$, etc. And you can define a set-theoretic function like SET plus(SET a, SET b); that acts just like a function NATURAL plus(NATURAL a, NATURAL b); which adds two natural numbers. Extending this to the integers, the rational numbers, etc., are typically homework problems that follow this discussion.

Thus when you write " $1+1=2$," that's really just shorthand for $\text{plus}(\{\emptyset\}, \{\emptyset\}) = \{\{\emptyset\}\}$. That's just set theory, and if you want math to model the world that we live in, there's no other interpretation for that that makes sense, no matter how bitterly you argue on the internet. There's no alternative to $1+1$ being 2, at least not in the world we live in.

Being applied math, cryptography isn't as rigorous as that, but it's as close as we can get without worrying about so many details that you can never get around to understanding anything useful. But you know that you could write down the details of exactly what you mean by cryptographic calculations or proofs. Nobody ever does that, but you could do it if you wanted to, so it's built on a fairly sound foundation.

To give you an idea of how complicated this would be, Bertrand Russell and Alfred North Whitehead's Principia Mathematica is famous for taking an extremely careful and detailed look at the foundations of mathematics that I tried to give the general flavor of above, and took 379 pages to get to the result that $1+1=2$. As the mathematician Paul Halmos once noted, applied math is bad math, but for those of us who have at least some interest in practical aspects of keeping the world running, we're happy to cut a corner every now and then in the interest of getting things done.

And since Mihir Bellare's 1997 paper "Practice-Oriented Provable Security," we have known how to prove the security of cryptographic algorithms. But just like understanding the details of exactly why $1+1=2$ is probably best left to specialists who worry about that level of detail, it's also probably best to leave the details of proving the security of cryptographic algorithms to specialists. But it's good to know that if someone needed to, they could follow Russell and Whitehead's example and write down a detailed proof of every step needed to prove the security of your favorite provably secure cryptographic algorithm.

I'm generally not a big fan of today's artificial intelligence technology (AI), particularly large language models, mainly because they're just not very useful for the kinds of things that I'm interested in. But it would be somewhat interesting to see an AI attempt at proving the security of a cryptographic algorithm from the fundamental principles of logic and set theory. It would certainly take more than 379 pages.



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.

INTERVIEW: The SECURITY PRO OF THE YEAR

By Jack Freund

Editor, ISSA Journal

Vice President, ISSA Education Foundation



Earlier this year ISSA International honored David Ruiz as the 2025 ISSA Security Professional of the Year Winner. David has made contributions to the overall security, risk, and compliance posture for Fayetteville Public Works Commission by integrating cybersecurity into the core of the business processes which has become a part of the business function. David is also a member of the Cybersecurity Defense Committee (CDC) for the American Public Power Association (APPA), Multistate MS-ISAC, W-ISAC, where he shares and mentors' cybersecurity expertise, helping the overall critical infrastructure community to grow a more resilient stature.

We recently caught up with David for an interview.

What do you think is different from the Cybersecurity Industry versus the Technology industry?

I personally believe the cybersecurity industry has a community that has separated itself from the other tech industries. The availability of the community and available resources are a tap away. Another huge point is how the community is always available to help the upcoming professionals and also to anyone who reaches out for answers.

What is the most important issue facing the industry and how would you like to see it addressed?

A very significant issue that I see across the industry is that our cybersecurity community has a challenge finding themselves in a business model. What this means is that we, as a community, need to be able to communicate the value of cybersecurity. The community overall struggles and finds themselves many times lost within their business. I encourage Security professionals to talk with people and figure out how to communicate into the business process and make their program visible to the organization.

What would you like to say to your peers?

Be a positive agent of change and prioritize your mental health. Burnout is real and it is OK to not be OK! Be intentional in your care plan, whatever it may be. Take the time to do something for yourself, whether it's a hobby or some other activity. In the end, if we aren't intentional about refreshing, rejoicing, and recharging, nobody is going to do it for us.

★ ISSA International Awards Gala 2025 ★

Join Us to
Celebrate Your Peers



<https://issa.org/event/2025-issa-international-40th-anniversary-event/>

September 5, 2025

7:00 PM CT

Westin Galleria Dallas, TX

Expert Perspectives

Identity Management Beyond Humans: A Guide to IAM for Non-Human Entities



IDENTITY ACCESS MANAGEMENT

By: Rajiv Dewan, IAM Practice Lead

The purpose of this paper is to explore the different types of non-human identities, highlight the challenges associated with their management, and provide best practices for improving their governance. By implementing effective governance strategies, organizations can significantly enhance their security posture, ensuring these critical identities are properly managed, monitored, and protected. Significance of this paper is to focus on the controls needed for non-human identities to enhance the security posture of organizations and reduce the security risk.

Introduction

Each organization has different types of users in their workforce - Employees, Contractors, Temp Workers, Contingent Workers and Interns. All these users are assigned a digital identity in the organization at the time of onboarding and generally organizations have a big IAM program to manage these digital identities. At the same time, there are some digital identities which are not associated/linked to any human users like bot accounts, service accounts, shared accounts, etc. which are known as non-human identities or accounts. Sometimes, these non-human identities are also referred as Machine Identities. Many a times, mostly use Service Accounts interchangeably with non-human identities but there are many more types of Non-Human/Machine identities and some of them are

- Service Accounts
- Bot / RBA Accounts
- Break-glass Accounts
- Shared Accounts
- API Keys
- Tokens
- Devices

These non-human identities can be categorized as Interactive vs Non-Interactive, Domain Based vs Local and Password vs non-password based on the business use cases and IAM program needs of the organization.

ISSA International Conference & Gala 2025

September 4-6 in Dallas, TX

Celebrating the Past
Informing the Present
Building the Future



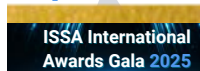
September 4



September 4-5



September 5 (evening)



September 6
Chapter Leaders Summit



**CELEBRATING 40 YEARS
OF SECURING THE FUTURE TOGETHER!**

REGISTER TODAY

**BOOK TWO HOTEL NIGHTS AND RECEIVE FREE ACCESS
TO THE CONFERENCE AND GALA**

- Meet friends and colleagues from all over the globe!
- Learn and network with hundreds of other ISSA members
- Celebrate ISSA's rich history.

[Learn More Here](#)



**TOAST YOUR PEERS!
EXCELLENCE CELEBRATED**



SPONSORED BY:
 **oligo**  **CovertSwarm**  **CyberOne**

**ISSA International
Awards Gala
2025**



<https://issa.org/event/2025-issa-international-40th-anniversary-event/>



Expert Perspectives

Challenges

Governance of non-human identities within an organization can be quite challenging. Here are some key difficulties that organizations often face

1. Centralized Inventory Management: Maintaining an up-to-date and centralized inventory of non-human identities is a common issue. Many applications within an organization integrate with each other to solve complex business problems and use non-human identities for their interactions. However, without the right policies in place, these identities can be created outside of the central governance system. As a result, the IAM (Identity and Access Management) team may lose track of them, leading to gaps in security and control.

2. Enforcing the Principle of Least Access: The principle of least access dictates that entities should only be given the minimum level of access needed to perform their tasks. During application integrations, teams often take shortcuts, granting more privileges to non-human identities to complete tasks quickly. Sometimes, even vendors do not clearly specify the appropriate level of access needed for integrations. This disregard for the least access principle increases security risks, as non-human identities may end up with more access than necessary.

3. Credential Sharing: A major challenge is the sharing of credentials for non-human identities. Often, credentials are shared between owners, team members, or vendors without understanding the potential consequences. Once credentials are shared, it becomes difficult to track or audit these actions. This lack of accountability makes it hard to pinpoint the source of unauthorized operations or security breaches.

4. Password and Key Rotation: Rotating credentials or keys for non-human identities is another significant challenge. When these identities are shared with application teams, rotating their credentials becomes difficult due to a lack of documentation and understanding of dependencies. IT teams are often hesitant to rotate credentials for fear of disrupting production systems. As a result, credentials remain static for long periods, increasing the risk of misuse.

5. Ownership of Non-Human Identities: Identifying and maintaining the correct owner of a non-human identity can be a complex and ongoing task. As employees leave the organization or move to different departments, non-human identities may become "ownerless"; or assigned to the wrong person. Without a proper process for ownership transition, these identities can be neglected, creating governance gaps and security vulnerabilities.

6. Implementing Multi-Factor Authentication (MFA): While MFA is a standard security practice for human users, its implementation for non-human identities remains a challenge. Many IT applications do not offer MFA for service accounts or other non-human identities. As a result, these identities may not benefit from the additional security layer that MFA provides, leaving the organization more exposed to potential attacks.

7. Reducing Human Interactions: Many organizations still rely on manual processes to configure and rotate the credentials for non-human identities. This requires a person from the team to manually enter credentials into systems or services. These manual processes are not only time-consuming but also prone to errors and omissions. While automation tools exist, significant gaps remain in reducing human intervention, making non-human identity management more prone to inefficiencies and errors.

8. Controlling Access Assignments: Typically, there is no formal access request system in place for non-human identities. Access is often granted outside of the centralized Identity Governance solution, and there is little to no monitoring of these assignments. This lack of oversight leads to poor governance and can result in significant audit challenges.

Exclusive ISSA Member Benefits

Access your Member Portal today to learn of NEW benefits partners offering ISSA members amazing discounts!



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

Join Today:

www.issa.org/membership



Expert Perspectives

“Managing non-human identities well helps companies be more secure, safer, and ready for the future.”

Best Practices or IAM Controls

Here are some of the practices that can be used to enhance the security around non-human identities.

1. Enforce Stronger MFA: MFA is a key control. It's equally important for non-human identities to have an additional layer of security. TOTP based MFAs are comparatively easy to implement but there will be challenges around SaaS applications that do not provide options to have MFA layer. For such scenarios, Secret Management is a better solution.

2. Segregate Interactive and Non-Interactive: Generally, IT teams use same non-human identity for interactive as well as non-interactive use cases which should not have been done. Organizations must have segregation of interactive and non-interactive non-human identities so that appropriate security controls can be implemented. Using same non-human identities creates problems while implementing those controls.

3. Enforce Password Standards: Passwords are outdated but organizations are still using passwords for many valid reasons, so it is important to have a strong password policy for non-human identities along with secure encryption algorithms. It is recommended to have stronger password policies than human password policies, for example, minimum password length for normal users can be 16 – 20 but for non-human it should be 25.

4. Enforce Password Rotation: There must be a regular process to rotate credentials of these non-human identities, especially, when someone who is in the possession of credentials of non-human identity, leaves the organization. There's increase in usage of SaaS applications that are accessible over internet. Even though these apps are integrated with Organization SSO/IDP (Identity provider) solution, but these apps allow legitimate users to bypass IDP/SSO for break-glass scenarios.

5. Ownership Management: Managing and maintaining the ownership of non-human accounts is a crucial part of keeping systems secure. These accounts often have access to important data and perform critical tasks, so it's important to know exactly who is responsible for them. This helps in making right people accountable for enforcing security controls like least access principle, reviewing access assigned to non-human accounts, passwords rotation etc. Without proper ownership, non-human accounts can become overlooked, this increases the risk of misuse of non-human accounts and their sensitive privileges.

6. User Access Reviews: Most of the organizations run period access reviews for users but most of the time, there is no access review process for non-human accounts. Access keeps on getting assigned but no one reviews those access once it is granted. This makes non-human accounts more sensitive or critical nature. There must be a regular process of reviewing the access of nonhuman accounts to make sure all the unnecessary access are revoked on time and least access principle can be enforced.

7. Enforce Naming Standards: Maintaining hygiene of metadata is always important in improving the security posture, that's why it is recommended to follow appropriate naming standards for non-human accounts so that it will be easy to identify or segregate the non-human accounts but naming standards must be unique to the organization.

8. Implement PAM / Password Vault: This is a key control for non-human accounts. Credentials of non-human accounts must be vaulted into a proper PAM / Password vault so that enhanced security can be implemented around non-human accounts. PAM provides detailed audit logs of check-in, check-out, usage and enforces password rotation on a predefined frequency. This is also needed to meet the regulatory requirements and meeting compliance goals.

9. Implement Alerting and Monitoring: All applications and systems, if not integrated with centralized SIEM solution for logging, must have monitoring and alerting in place for non-human account usage. Whenever someone uses non-human accounts to log into application or system, there must be an alert going to security system about the usage. This is needed to detect any suspicious login attempt of non-human accounts.

These are some of best practices that can be followed to build a security perimeter around our most critical and sensitive accounts.

Conclusion

Technology is changing fast, and now many “users” in our systems are not human. There is no doubt that non-human accounts are more sensitive in nature that's why they need additional attention to keep organizations safe from breaches. To stay safe and work efficiently, businesses must take identity management for non-humans seriously. This means setting up clear ways to create, update, and remove identities, giving the right level of access, and watching for any unusual behavior. Managing non-human identities well helps companies be more secure, safer, and ready for the future.

Expert Perspectives

References

1. James D. Fearon. November 1999. Stanford University. WHAT IS IDENTITY (AS WE NOW USE THE WORD)
2. Lorna Garey. September 19, 2024. Oracle. What is Digital Identity
3. Lalit Choda. December 28, 2024. 10 Must Read Articles on Non-Human Identities
4. Apurva Dave. Feb 2025. Non-Human Identity Security vs. Service Account Management: What's the Difference?
5. Lalit Choda. The Ultimate Guide To Non-Human Identities



About Author:

Rajiv Dewan

Accomplished IAM leader with 18 years in Cybersecurity IAM, Sr. IEEE Member, and mentor at reputed organizations. Expert in SSO, MFA, PAM, IGA, and more. Blogger and top forum contributor, delivering secure, scalable IAM solutions aligned with business goals.

**Join us from anywhere!
Open to all ISSA members;
registration is required.**

- Hear updates on ISSA's 2024 accomplishments and 2025 goals
- Meet the newly elected ISSA International Board Members
- Review key financial highlights
- Participate in an open forum for questions and member feedback
- Help shape the future of our global cybersecurity community

https://us02web.zoom.us/webinar/register/WN_dxIAI5ocRnee6S1M_F56jg

Announcing

The 2025 Virtual ISSA Annual Membership Meeting

**August 28
1:00 PM ET**





The AI Paradox in Cybersecurity: Use of AI for good and evil

By: Aparna Achanta

Introduction

AI in cybersecurity reshapes threat identification, accelerates responses, and hardens general defense postures. Yet many of those attributes also supply great value to threat actors. The real challenge now becomes maximizing its benefit for security while ensuring it is resilient from abuse and manipulation.

Just as attackers leverage AI for better insight and have adequate means of doing so, defenders are also given the means to rebut such motives. AI is a double-edged sword in this ever-changing battle for cybersecurity.

One [recent study by Cybersecurity Insiders](#) found that AI upends the cybersecurity world order, driving profound and likely lasting changes in the tools both attackers and defenders deploy.

Attackers Exploit AI to Escalate Attacks

1. Increased Use of Malware Tools in Attacks

In 2025, organizations will need to expect a fully evolved threat landscape, from using AI to gain control of IoT devices, deepfakes, supply chain compromise, and extortion-based ransomware to AI-powered phishing. Compounding the problem even further is that AI tools are becoming increasingly accessible and will be utilized by bad actors to amplify their nefarious deeds. This will continue to see AI-powered attacks such as ransomware and cyber extortion developing or becoming more potent, requiring security teams to make it a focal point of their preparation.

For cybercriminals, AI has lowered entry barriers as they can now conduct sophisticated attacks despite having limited technical competence. Cybercriminals will increasingly use AI-enabled tools to perform or supplement their malicious activities.

2. Leveraging AI to Improve Social Engineering Tactics

Another major threat AI poses is the ability to design highly convincing phishing and social engineering schemes. Pretexting in video, audio, and even phone calls can be a very deceptively effective way of fooling employees into revealing information that should be kept secret or convince employees to transfer funds. AI could be used to generate and amplify misinformation on social media, influencing public opinion.

3. Automating Attack Steps Like Reconnaissance

The frequency of cyberattacks continues to increase, while AI now allows such threats to become automated and scaled in unparalleled ways.

If current forecasts are correct, worldwide cybercrime using AI alone might push losses to \$23 trillion in 2027, up from \$9.5 trillion in 2024.

AI allows cybercriminals to automate critical steps in the reconnaissance and attack process. Using AI, attackers can scan for vulnerabilities and automatically launch custom exploits against an asset based on an unpatched vulnerability, with minimal human involvement. This increased level of automation reduces the time and effort required to carry out a breach successfully.

Furthermore, AI-driven reconnaissance tools aggregate a lot of information about the target, including network configurations, software versions in use, and employee behavioral patterns. With such intelligence, attackers can set up specific, practical approaches that would be difficult to detect and mitigate.

4. Automated Phishing

By analyzing publicly available data, attackers can craft communications that are alarmingly convincing, making traditional defense mechanisms insufficient against this evolving threat. Attackers will deploy LLMs to craft highly personalized and context-aware phishing emails, SMS messages, and social media attacks.

Embracing AI to Building Resilience Against AI Attacks

The sheer complexity and volume of cyber threats are scaling cybersecurity teams to breaking point. The sheer volume of attacks means there is little time for proactive measures; teams must adopt an immediate crisis management approach. The sophistication of such threats is changing the game on how security is done. Traditional models based on determinism—where something is identified as a threat or not—give way to probabilistic approaches, which focus on interpreting ambiguous signals and investigating anomalies that may indicate potential threats.

When working well, AI amplifies threat detection through automation, taking responses to the next level. It generates high-quality probabilistic insights, allowing teams to decide whether intricate patterns that seem harmful are malicious or benign anomalies—a capability unique to AI since conventional algorithms within the security framework cannot handle such subtle analysis.

1. Leveraging AI to Augment Cybersecurity Capabilities

Smothered by workload, cybersecurity teams are usually overwhelmed, challenges range from handling multiple responsibilities to skill shortages, further complicating the ability to defend against attacks.

In several key areas, AI enhances the sophistication and efficiency of cybersecurity efforts through ways like:

- Threat detection with greater precision
- Accelerating the investigation process
- Coordinating and orchestrating incident responses

AI helps to free up time for cybersecurity teams to work on other mission-critical tasks, thereby fortifying the cybersecurity of an organization at every level. The roles AI can play range from data classification, vulnerability identification, and spam filtering to the more complex: malware detection, proactive handling of weaknesses before they are exploited, managing SOC operations, blocking unauthorized intrusions, and gathering intelligence based on the analysis of parts of the internet that are unreachable through other means like automated dark web scanning.

2. Increased Accuracy in Threat Detection and Prevention

AI amplifies threat detection and prevention in many ways. AI-driven algorithms can process massive amounts of information in a fraction of a second, allowing AI-based security systems to track known and emerging threats, including malware, ransomware, phishing schemes, and zero-day vulnerabilities, faster and more accurately than their traditional, rule-based counterparts.

By means of machine learning, adaptive AI systems learn with time and predict odd patterns from datasets, so providing a significant benefit in terms of security threat reduction.

3. Automating Incident Response to Reduce Damage

AI tools can analyze massive amounts of data for even the most hidden threats, like APTs and zero-day vulnerabilities. Thus, detecting patterns, anomalies, and behavior indicative of cyberattacks or insider risks provides better detection capability with the help of AI.

An excellent example of such applications includes automated response mechanisms. With the integration of machine learning, such systems detect and trace irregular activities along with abnormal behavior. Automated responses may result in the isolation of systems to protect them from further infection, blocking malicious IP addresses, or severing particular connections that could give rise to unauthorized access. In other words, automating incident response is helpful since it allows organizations to contain threats effectively.

4. Identifying and Responding to Phishing Incidents

While AI facilitates phishing, it proves equally effective in automating defenses against such attacks. AI systems analyze questionable emails, messages, and URLs by extracting key features and employing machine learning models to detect possible phishing.

For example, NLP allows AI to spot minute patterns, grammatical errors, and inconsistencies in phishing emails. Similarly, AI-run systems with active monitoring can immediately identify and flag emails or URLs for review.

Large amounts of data, pattern and warning signs pointing to phishing, and accurate evaluations and replies in almost real-time are all capabilities of AI.

5. Real-Time Malware Identification and Analysis

AI technologies perform a critical role in malware detection, analysis of malicious code, and forensic artifact examination to understand the techniques cybercriminals adopt.

AI algorithms can break down files – executables or just about any form of digital data – into their decompiled code to analyze it. This helps to identify actions suggestive of an upcoming or advanced malware variant. Such a capability is especially important for controlling two main types of threats: specifically,

Expert Perspectives

1. Zero-day Vulnerabilities: These allude to previously unidentified hardware or software defects attackers can exploit before developers issue a patch.

2. Polymorphic threats: Cybercriminals frequently change the structure or content of malware to create new variants that might eventually bypass traditional methods based on fixed patterns.

With AI providing in-depth analysis, cybersecurity systems can detect and respond to continuously changing threats with higher accuracy.

6. Improved Endpoint Security

As the shift to remote work increases, endpoint protection becomes key to strong cybersecurity. Traditional antivirus programs and VPNs are signature detection-based and often fail to protect against evolving threats, thus leaving the endpoints open to attack.

AI endpoint security is proactive and adaptive. Establishing AI systems for monitoring regular endpoint activity allows them to recognize anomalies and act on them quickly. Because AI is constantly learning from network activity, it identifies emerging threats, including zero-day exploits, with no requirement for signature updates, unlike traditional systems.

Thirdly, AI improves user authentication and account security by introducing superior techniques. CAPTCHA systems, face identification, and fingerprint scanners use AI to distinguish genuine from fraudulent login attempts and add a robust layer of protection for the endpoints.

7. Intelligent Vulnerability Management

The management of vulnerabilities has become a challenge since hackers now use advanced techniques to reveal thousands of new vulnerabilities annually. The rapidity with which businesses experience a rise in newly discovered threats makes it difficult for organizations to be prepared to cope with such high volumes of emerging threats. Traditional security systems can hardly mitigate high-risk vulnerabilities in real-time.

The application of AI in cybersecurity gives an edge over those who want to win the fight against them. Examples of AI-powered solutions include User and Entity Behavior Analytics (UEBA). UEBA observes and analyzes events from devices, servers, and users to identify strange or anomalous behavior.

AI can also be used to find and fix undetected vulnerabilities or those lacking a patch providing a much-needed layer of safety.

Conclusion

Knowing how to balance AI's use in cybersecurity is like walking a tightrope. On one hand, AI is a revolutionary technology promising to renew cybersecurity practices with unparalleled protection and dynamism. On the other hand, its abuse or unforeseen implications may contribute to current threats or bring new vulnerabilities.

This balance will have to be genuinely forward-looking and adaptive. For organizations, for instance, keeping updated on new trends regarding AI must go hand in hand with the continuous assessment and mitigation of associated deployment risks. The key will be to make informed decisions, using the power of AI to strengthen defenses while implementing strategic countermeasures with a responsible and reflective approach. That is where continuous education and awareness come in. The speed at which AI is advancing is unparalleled, and so are the risks associated with it regarding cybersecurity. Because of this ever-changing environment, all levels of organization's hierarchy must remain committed to learning and vigilance. Ultimately, striking a balance between AI's benefits in cybersecurity and its risks it brings is a process. The journey means continuous education, raising awareness, and commitment to responsible and effective adaptation to AI's dynamic transformation in cybersecurity.

"The real challenge now becomes maximizing its benefit for security while ensuring it is resilient from abuse and manipulation."



About the Author

Aparna Achanta is a seasoned Security Architect and Leader at IBM with extensive experience driving mission-critical cybersecurity initiatives, particularly in federal agencies. Aparna is a ISSA Cyber Executive Member.

Her LinkedIn profile - <https://www.linkedin.com/in/aparna-achanta-41741739/>

News From the ISSA Education Foundation



Tenable Honors Amit Yoran with Donation to the ISSA Education Foundation

In honor of their former Chairman and Chief Executive Officer, Amit Yoran, Tenable, Inc., has donated \$6,500 to the Information Systems Security Association Education Foundation (ISSAEF or the "Foundation"). Yoran passed away from cancer in January of this year. He had led Tenable since 2017.

Having served in a number of information security roles – including National Cybersecurity Director for the Department of Homeland Security, and as a member of the board for the Center for Internet Security – Amit was well known throughout the community. Several members of the ISSAEF board knew Amit personally, so it was an honor for the Foundation to receive such a gift.

"That this contribution came in Amit's name makes it that much more meaningful," noted ISSAEF President and ISSA International Vice President Deb Peinert.

ISSAEF Fundraising Chair John Johnson was equally appreciative, "As a non-profit, we [the Foundation] are always seeking donations, so this will allow us to fully fund two scholarships this year."

In 2024, the ISSAEF awarded eleven grants and scholarships from \$500 to \$3,500, totaling more than \$15,000. In addition to memorial scholarships in the name of Howard A. Schmidt, Eugene Schultz, Jr., and Shon Harris, the Foundation manages scholarships for the Docent Institute, Alamo ISSA Chapter and continuing education grants for SANS, the Cloud Security Alliance and ACI.

Recognition

While we're recognizing the contributions made to our field, let us congratulate our President, Deb Peinert, who has joined the ranks of the ISSA Distinguished Fellows!



This elite designation is limited to only 1% of ISSA members and recognizes their exceptional leadership, contributions, and lasting impact on the information security profession and the ISSA community as well as the cybersecurity community as a whole.

Deb's dedication to advancing cybersecurity, shaping industry best practices, and mentoring future

professionals have set her apart as a leader in the field. This prestigious honor reflects the profound influence she has had on the profession and the respect she has earned from her peers.

Congratulations Deb!

Volunteers

Speaking of 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 vacancy:

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.

The Foundation welcomes donations, which can be made online at <https://issaef.org/scholarships/donate/> or via check to:

ISSA Education Foundation
c/o Mr. Richard Mosher, Treasurer ISSAEF
577 S. Carriage Crossing, Nixa, MO 65714

Empowering Your Cyber Career Journey: Unlocking the Full Value of Your ISSA Membership

As a cybersecurity professional, your career is a journey filled with constant learning, evolving threats, and new opportunities. At ISSA, we understand the challenges and aspirations that define your path. That's why we are dedicated to supporting you every step of the way — providing resources, connections, and benefits designed to empower your growth and success.

Whether you are just starting out or a seasoned expert, your ISSA membership opens doors to a wealth of advantages tailored to enhance your knowledge, expand your network, and advance your career.

But are you taking full advantage of what's available?

Here's a closer look at key benefits that you can tap into today — plus insight into how we're working globally to bring even more value to your professional journey.

Member Benefits Designed for Your Career Growth

ISSA partners with leading cybersecurity organizations to provide members access to world-class training and certification opportunities at special rates. Through collaborations with organizations we negotiate for our members often at discounted prices unavailable elsewhere.

Log in to the ISSA Member Portal to access your unique discount codes and take advantage of exclusive member savings — and be sure to check back often, as we are continually adding new offers
<https://www.members.issa.org/page/SpecialOffers>

Training and Certification Opportunities



CSA and ISSA have partnered to provide **an exclusive 20% discount for ISSA members** for the CCSK training program or the exam bundle.



ISSA has partnered with Infosec to provide members with premium cybersecurity training at preferred rates. This collaboration brings together two organizations committed to advancing cybersecurity education and professional development.

Through this partnership, ISSA members gain access to Infosec's comprehensive training portfolio, including:

- Infosec IQ: Award-winning security awareness training to educate your entire organization
- Infosec Boot Camps: Intensive, instructor-led certification preparation courses
- Infosec Skills: On-demand training platform featuring hands-on cyber ranges and skill paths



FITSI administers the Federal IT Security Professional (FITSP) certification program, which offers four specialized tracks—Auditor, Designer, Manager, and Operator—tailored to distinct roles within the federal cybersecurity workforce. These certifications are designed to validate proficiency in federal information technology security standards and practices, aligning with the unique requirements of federal IT systems. Notably, FITSP certifications are approved under the Department of Defense (DoD) Directive 8140, underscoring their alignment with the highest standards in federal cybersecurity. Through this partnership, ISSA members can access exclusive benefits to enhance their credentials in federal IT security.



ISSA, in partnership with Solutions³ LLC and the DVMS Institute provides current ISSA members access to **premier DVMS Institute training programs at 10% or 20% off**

The DVMS Institute's accredited certification programs equip organizations of all sizes with the skills and knowledge to protect digital value, enhance resilience, and maintain trust.

Take advantage of these offers to elevate your cybersecurity expertise, expand your professional skillset, and stay ahead in this ever-evolving field.



Phoenix TS is proud to partner with the Information Systems Security Association (ISSA) to support its members in achieving their professional growth goals. Through this exciting partnership, ISSA members gain access to **exclusive 10-20% discounts** on select publicly scheduled training courses at Phoenix TS.



ISSA and MindEdge have partnered to **deliver an exclusive 10% discount for ISSA Members**. MindEdge is a premier developer of online learning solutions, including certificate and professional development courses. MindEdge's mission is to improve the way the world learns. Since our founding by Harvard and MIT educators in 1998, we have served some two million learners.



ISSA, in partnership with Treadstone 71 is offering a **30% discount to all ISSA Members** for online training. Quantity discounts available that go beyond 30%. Treadstone 71 has delivered intelligence training, strategic, operational, and tactical intelligence consulting, and research. They provide a seamless extension of your organization efficiently and effectively moving your organization to cyber intelligence program maturity

Conference and CPE Opportunities



ISSA partners with Black Hat USA 2025 once again to offer an exclusive discount to applicable passes. Black Hat USA 2025 will take place from August 6 – 7 in Las Vegas, Nevada. As a valued member of ISSA, **you receive \$200 off a Live Briefings Pass or \$100 off a Business Hall Only Pass.**



ISSA Members receive an **exclusive discount of 10%** off Cabin Space for CurisecCon East and West. CruiseCon was created to give all cybersecurity professionals the education and experiences typically reserved for Fortune 200 security executives.



ISSA Members can now attend all 2025 ELEVATE IT Summits—for FREE! These events will take place in Phoenix, Kansas City, Tampa, Dallas, Minneapolis, and Houston. Non-members pay \$199, but ISSA Members get in free. More cities will be available in 2026.



ISSA partners with the RSA Conference every year, and once again, members will receive an exclusive discount on applicable passes. Discount code will be available in late fall of 2025.



ISSA is pleased to partner again with SecTor. Now in its 19th year, SecTor returns to the Metro Toronto Convention Centre (MTCC). SecTor will host a Summit Day on Tuesday, September 30, followed by the two-day main conference on October 1 & 2, featuring selected Briefings, dozens of open-source tool demos in Arsenal, a robust Business Hall, networking and social events, and much more. **ISSA Members receive \$200 off full briefing pass or a complimentary business hall pass with exclusive ISSA Member code**



Save the Date for Wicked6 2026! **ISSA members will receive a special discount—details to come!** Mark your calendars for March 27–29, 2026 and get ready for a high-energy, virtual cybersecurity event designed for women and nonbinary players. Wicked6 brings together a global community for a weekend of cyber games, tech talks, networking, and skill-building challenges.

Products and Services



ISSA members can now save **up to 40% OFF on HP Products with exclusive members savings!** Sign up today! ISSA members get exclusive discounts on best-in-class HP technology, plus access to dedicated North American tech support and a tailored shopping experience. Upgrade your workspace with cutting-edge HP devices and enjoy savings designed just for you.

Help Us Expand What's Possible

The ISSA International team is actively working to grow our global partnerships — and we'd love your input.

What would help you go further?

Are there tools, services, or training providers you wish ISSA partnered with for better or discounted access? We're listening. Our goal is to deliver member benefits that are not only relevant but transformational.

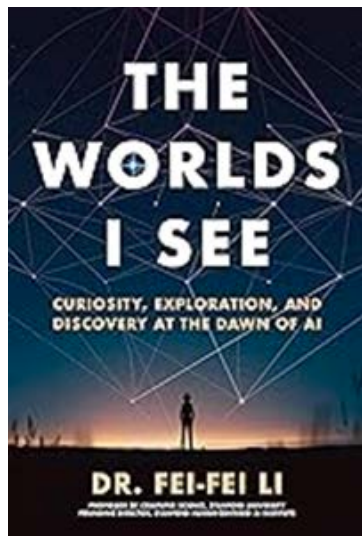
Tell us what you'd like to see next — email memberservices@issa.org

Because your career deserves the strongest support system — and your membership is just the beginning. Together, we're more than just an association — we are a global community committed to empowering cybersecurity professionals at every stage.

The Cyber Library

Reviewing the Works of Fei-Fei Li, and Travis D. Breaux (editor)

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



The Worlds I See: Curiosity, Exploration, and Discovery at the Dawn of AI

By Li, Fei-Fei. Flatiron Books, (2023)

Sound Bite: A non-technical story of both Dr. Li's inspirational achievements as well as artificial intelligence.

Opinion on Primary Audience: Everybody, we should hope.

I am switching from the forecasted book, as I was getting too technically focused. This is a terrific book, an inspirational life story on a key AI researcher but also explaining how AI developed! You can read it comfortably, professionally profit from it, and enjoy the story. You could also give it to your non-technical family and friends, especially anyone you want to be inspired by her example. This is about how visual processing powered much of AI and has brought so many good opportunities, including the bad opportunity to do societal damage. You will see a treatment of both sides of the good AI/bad AI coin. It is chock full of AI technical facts.

The Author

Professor Fei-Fei Li is the Sequoia Professor of Computer Science at Stanford University. Her PhD in Computer Science is from Caltech. Pick your superlative terms for Artificial Intelligence experts and they fit. If she was not leading the effort or at least making it happen, she was probably a guiding force or 'in the room' for many of the major events in modern AI. That is hype, but she is that important. And she started with little more than brains and guts!

The Metadata

The online cost, including shipping, is about \$20. My public library has 3 copies. Using a Wikipedia article about the Flesch-Kincaid Readability Test, the readability is high school level with 20% passive voice. This article is 3% passive voice. Dr. Lei's book is only 300+ pages.

Table of Contents: [Including Reviewer notes]

1. Pins and Needles in D.C. [AI4All, aka Artificial Intelligence for All]
2. Something to Chase [Personal story, no AI]
3. A Narrowing Gulf [Turing, The Dartmouth College Research Project, McCarthy, etc.]
4. Discovering the Mind [Personal story, no AI]
5. First Light [Neuroscience and visual processing lead to AI]
6. The North Star [Computer visual recognition]
7. A Hypothesis [WordNet, ImageNet]
8. Experimentation [A bit about Support Vector Machines, Graphics Processing Units]
9. What Lies Beyond Everything
10. Deceptively Simple
11. No One's to Control
12. The Next North Star [Heading into the future]



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.

An Introduction to Privacy for Technology Professionals

By Breaux, Travis, Executive Editor, et al. International Association of Privacy Professionals, (2024)

Sound Bite: Best blend of IT, privacy, and AI.

Opinion on Primary Audience: IT professionals, especially those going for the International Association of Privacy Professionals (IAPP) Certified Information Privacy Technologist (CIPT) Exam.

This is really a book for hardcore cyber pros. It is more obscure to find, but it bridges gaps between IT/cybersecurity textbooks, cybersecurity certification technical reads, and popular books on privacy/cybersecurity/AI. Yes, it was primarily written for an exam, but if you are an active cybersecurity practitioner you must know this stuff, to avoid being dated and dangerous. Exceptional value! This book looks at all cybersecurity domains from a privacy perspective.

The Editors

Travis D. Breaux is well-credentialed to be the Executive Editor of this book. He has about 20 years of experience in IT, a PhD in Computer Science from North Carolina State, and has spent the last 14+ years at Carnegie Mellon University (CMU). He is director of the CMU Requirements Engineering Laboratory. In addition to the essays Dr. Breaux wrote, there are 11 other contributors, all with great credentials: Chris Clifton, Lorrie Faith Cranor, Kira Fuller, Simson L. Garfinkel, Hanan Hibshi, David James Marcos, Florian Schaub, Stuart S. Shapiro, Blasé Ur, Nicole Uribe, and Zhiwei Steven Wu.

The Metadata

This book is \$95 from IAPP, or \$85 if you are an IAPP member. Cut it by \$20 if you read it digitally. Beware if you try to go more cheaply, as you may end up with the earlier edition. You definitely want the 2024 book! I don't expect a local library to have a copy. I took a one-page sample of the text to analyze. Using a Wikipedia article about the Flesch-Kincaid Readability Test, the sample had 44% passive voice and was at upper undergraduate college level. This article is 3% passive voice. Yes, it is a tough read, but worth it.

Table of Contents: [Including Reviewer notes]

1. Introduction to Privacy for the IT Professional
2. Engineering and Privacy
3. Encryption and Related Technologies [As of 2023/2024 on key issues]
4. Identity and Anonymity
5. Usable and Useful Privacy Interfaces
6. Tracking and Surveillance
7. Interference
8. AI and Machine Learning [Most useful 20 pages on AI I have ever read]
9. Cybersecurity and Privacy [The good stuff, in 25 pages]
10. Privacy Governance

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:

- Hadnagy, Christopher. The Science of Human Hacking. Second Edition. (2018).
- Boddington, Paula. AI Ethics: A Textbook. Springer Nature Pte Ltd., (2023).

Additional sources used in the article:

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

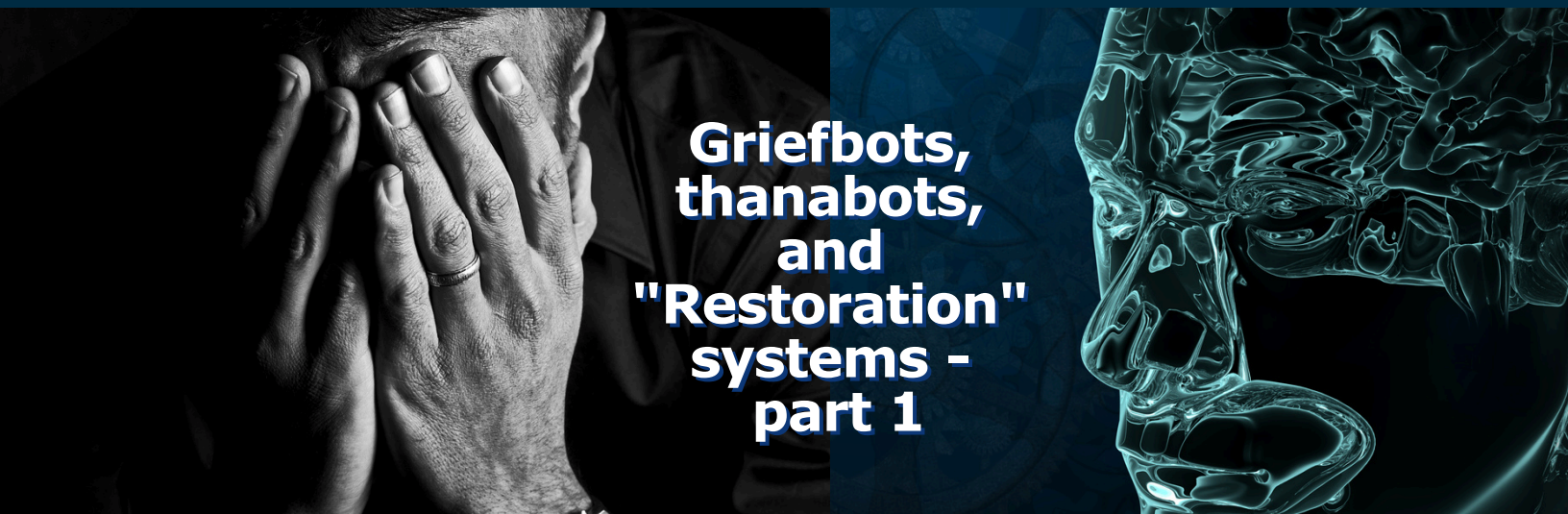


About the Author

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+, CIPM, CIPP/E, and CIPP/US 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.



Griefbots, thanabots, and "Restoration" systems - part 1

At about the same time that Gloria died, Replika started making the news. Replika was, at that time, text chat based only. You could train a Replika account with email from your deceased loved one. I had plenty of email from Gloria, and still do.

I decided against trying the system. I wasn't sure whether I was more afraid of it being disappointing, or of getting hooked on it.

So I still don't know which is the greater danger. I don't know whether those people who use griefbots, or thanabots, or "restoration" systems, are simply fooling themselves, and thinking that this chat does, in some way, reproduce their conversations with their loved one, before the loved ones death. Possibly they receive some kind of comfort, in having conversations with some facsimile of their loved ones. Then again, possibly they experience cumulative grief, when they finally realize that their loved one is, in fact, dead, and that the facsimile isn't, in fact, the loved one.

Possibly there is some kind of cumulative grief involved in the fact that the loved one dies, and then is "restored", and then possibly "dies" again, at some later date, when the company that runs the system goes bankrupt, or the system to simply gets too old, or is updated and their account doesn't survive the transfer, or they simply run out of money to pay for the account.

Or, maybe, the system runs along, and they don't really discriminate between whatever the system produces, and whatever kind of conversation their loved ones did produce, and they just carry on the illusion until they themselves die.

And maybe they never really get over their grief, because they have this artificial anodyne, and the artificial chatbot, or griefbot, or thanabot, is sufficient for them, and they never do form a new relationship with any actual carbon-based lifeform that might be more suitable for them.

I don't know. As I say, I never dared to try the experiment with Gloria and Replika, and I don't know how I, personally, would react or have reacted. And the information that I have been able to find is basically anecdotal, and the plural of anecdote is not data.

So I don't know how real the benefits are. I don't know how real the risks and dangers are. But I am definitely aware of the potential risks, and I strongly suspect that too few people are aware of the risks, or have given much thought to them.

(The CBC has made available a documentary entitled "Eternal You." It is not comprehensive, and doesn't address all the risks associated with griefbots and related systems, but those that it does cover are covered well. It is available at:

<https://gem.cbc.ca/eternal-you>

<https://www.youtube.com/watch?v=4Kogc2aPUK4>

Initially, as noted, the idea to explore griefbots came from Gloria's death, and the increasing presence of Replika in this space. Then came the explosion of interest in artificial intelligence, and the proposed applications, driven by the large language models. I created a presentation on griefbots as a kind of specialized extension of a broader presentation of AI

<https://fibrecookery.blogspot.com/2024/09/sermon-38-truth-rhetoric-and-generative.html>. However, as I explored the field, and in association with volunteer work in grief support <https://fibrecookery.blogspot.com/2022/03/grief-guys.html>,

I was astounded by the number of companies that have started to enter this field, with a variety of products. Given the lack of understanding of the limits of AI in general <https://fibrecookery.blogspot.com/2025/01/creativity-is-allowing-genai-to-make.html>, and increasing work in the psychological dangers of a variety of areas of information technology (including social media), I felt more urgency in getting this article, and series, out to a broader audience.

Today I was asked for which audience I am writing this article. I think it's a pretty broad audience. My colleagues in information technology will have a greater understanding of artificial intelligence, and the oversimplification that I am making in order to ensure that this article is not too lengthy for the general public. For those involved in grief counseling and support, my lack of training and specialization in this field will no doubt show. However, I hope that you can understand the concerns that I am trying to raise, and will, if asked by your clients, be able to provide some detail, and possibly a balanced opinion in regards to whether or not griefbots are a good idea for the bereaved, in either general or specific, and at least raise the issues of risk or danger. For those in the general public, some of you may be bereaved, and might be considering griefbots for yourselves, or may have friends among the bereaved who might be considering signing up for these systems. Again, hopefully this piece will provide some realistic assessments of what we thought griefbots are or are not, and what benefits, balanced against the risks and dangers, there may be.

Given that this is a bit about artificial intelligence, or AI, I asked ChatGPT to opine on the psychological dangers of artificial intelligence, and the use of artificial intelligence, particularly in counseling and psychological situations. The number one point that ChatGPT listed was "a lack of understanding." Indeed, this was borne out by a situation where, at an event for the public, I set up a computer to allow people to interact with one of the LLM systems. Anyone could try it out. Nobody did. So probably very few people have, actually, taken advantage of the opportunities to get to know how these systems work. (And don't.) Therefore it is probably a good idea to provide at least a terse outline of what artificial intelligence is, and is not.

First of all, artificial intelligence is not a thing. It is *many* things. Artificial intelligence is a general term given to a number of approaches to getting computers to have functions which we have come to expect from people. Unfortunately, as well as a number of different approaches in order to tackle this task, the task itself is ill-defined. Alan Turing, who is considered one of the fathers of modern computing, and computing machinery, did once specify what has come to be known as the Turing Test. The test goes something like this: if you put a subject (which we might call the tester) in front of a terminal, and the wire to the terminal goes off through a wall, and the tester carries on a conversation, via the terminal, with the system that is to be tested (which we can call, for example, the testee), if the tester cannot, after carrying on a conversation for some length of time, decide whether behind the wall is another person, or a computer running an artificial intelligence program, then if it is, in fact, an artificial intelligence program, that artificial intelligence program is considered to have passed the Turing test, and is therefore, intelligent.

The thing is, we don't really know if Alan Turing actually meant this to be a determining test about whether or not someone has, in fact, written a program which is artificially intelligent. It is equally possible that Alan Turing was making a statement about the difficulty of creating artificial intelligence, when we can't even define what real intelligence is. The Turing test is, in fact, a measurable test. But it doesn't really define, to everyone's satisfaction, whether or not we have created a truly intelligent artificial personality.

For example, how intelligent is the tester? Does the tester have experience with assessing other artificial intelligence programs, as to their level of intelligence? Does the tester have a broad range of knowledge of the real world? Has the artificial intelligence program been fed data based upon questions and conversations that the tester has had with artificial intelligence programs in the past?

And this is just about generating a conversation. What about making a computer see? What about getting the computer to look at an image, either still or video, and identifies specific objects out of that image? What about being able, from an image, to plot a way to navigate through this field, without destroying various objects that might be in it? What about teaching the computer to hear? All of these are things that the field of artificial intelligence has been working on, but they have nothing to do with carrying on a conversation over a terminal with some unknown entity.

In the interest of keeping this article reasonably short (it's already much longer than a regular column), I won't go through the sixty or seventy year effort to create artificial intelligence, and the various successes and failures. No, I'll keep this reasonably short, and just pick on the one that has, over the past three years, been much in the news, and much in demand in business circles, and which everyone tends to talk about.

This is the approach known as the large language model, or LLM, or generative artificial intelligence, or generative AI, or genAI.

As I say, this has created a great stir. ChatGPT, and Claude, and Perplexity, and Deepseek, and Qwen, and Meta AI, and Gemini, are all examples of generative AI. They have astounded people with their ability to answer questions typed into them, and give reasonable answers, sounding realistic and lucid, and do, for many people, seem to pass the Turing test. The reality is a bit different.

Large language models are descendants of a process called neural networks. Neural nets are based on an idea about the human brain, which we now know to be somewhat flawed, and definitely not comprehensive. However, it is a very complicated kind of statistical analysis. You feed neural nets a lot of data. When the neural net notices a correlation between items within the database, it flags that correlation, and, every time it finds an example that meets the correlation, it strengthens the connection.

Unfortunately, this leads to an example of what is called, in psychology, superstitious learning. That is, that the system notices a correlation which isn't, in fact, a correlation. It builds on a kind of confirmation bias, and the system will keep on strengthening a correlation every time it finds, even if randomly, some data that

seems to fit the correlation. The negative, a lack of evidence, or even relationships in the data that contradict the correlation, are ignored. So, neural nets can make mistakes. And this is only one example of the types of mistakes that they (and we) make.

Large language models feed the neural net a great deal of text. You will have seen news reports about those who are building large language models being sued by the owners of intellectual property, which gets shoveled into the large language models. There is also, of course, an enormous trove of text which is available at no cost, and so is widely used in feeding the large language models. This is, of course, social media, and all the various postings that people have made on social media. However, this text is not exactly high quality. So we are feeding the large language models with a great deal of data which can teach the large language model how to structure a sentence, or a paragraph, and even possibly to use punctuation (if, indeed, social media users can be forced somehow to use punctuation), but any meaning may be rather fragmented, disjointed, and quite possibly incorrect. So, we have taught genAI rhetoric, but we haven't taught it anything about epistemology, or metaphysics.

And this business of saying that we are asking a question, and getting an answer, is an example of misleading the public by the use of our terminology. You may think that you are asking a question. The system doesn't understand it as a question. It is simply, to use the term that the generative artificial intelligence people use, themselves, a prompt. This prompt is parsed, statistically, with the very complex statistical models that the large language model has created for itself. Then the genAI will generate a stream of text, once again, based simply on the statistics, and probability, of what the next word is going to be. Yes, it is certainly impressive how this statistical model, complex though it may be, is able to spit out something that looks like considered English. But it isn't. It's just a statistically probable string of text. The system didn't understand the question, or even that it *is* a question. And it doesn't understand the answer. It's just created a string of text based on statistics.

It doesn't understand anything.

And if you think anything different, you're fooling yourself.

Now, some of you may be somewhat suspicious of the proposition that a mere statistical analysis, no matter how complex, can generate lucid English text. Yes, I am oversimplifying this somewhat, and it's not just the probability of the next word that is being calculated, but the next three words, and the next seven words, and so forth. The calculation is quite complex, but it still may sound odd that it can produce what seems to be a coherent conversation.

Well, this actually isn't very new. There is a type of statistical analysis known as Bayesian analysis, or Markov chain analysis. It has been used for many years in trying to identify spam, for spam filters for email. And, around twenty years ago, somebody did this type of analysis (which is much simpler and less sophisticated than the large language model neural net analysis) on the published model novels of Danielle Steele. Based on this analysis, he wrote a program that would write a Danielle Steele novel, and it did. This was presented to the Danielle Steele fan club, and, even when they knew that it was produced by a computer program, they considered that it was quite acceptable as an addition to the Danielle Steele canon. And, as I say, that was two decades ago. And done as a bit of a lark. The technology has moved on quite a bit since then, particularly when you have millions of dollars to spend on building specialized computers in order to do the analysis and production.

A lot of the griefbots, or thanabots, or "restoration" systems are based on this kind of technology. Sometimes they are using even simpler technologies, that have even less "understanding" behind them.

Some of the chatbots are based on even simpler technologies. For example, over sixty years ago a computer scientist devised a system known as ELIZA. This system, or one of the popular variants of it, called doctor, was based on Rogerian psychological therapy,

The Cryptic Curmudgeon

one of the humanistic therapies. The humanistic therapies, and particularly Rogerian, tend to get the subject under therapy to solve his or her own problems by reflecting back, to the patient, what they have said, and asking for more detail, or more clarity. That was what ELIZA did. If you said you were having problems with family members, the system would, fairly easily, pick out the fact that "family members" was an important issue, and would then tell you something like "Tell me more about these family members." Many people felt that ELIZA actually did pass the Turing test, since many patients ascribed emotions, and even caring, to the program.

(If you want you can find out more about ELIZA at <https://web.njit.edu/~ronkowit/eliza.html>)

Other chatbots have been developed, based on simple analysis and response mechanisms, and sometimes even simpler than those underlying ELIZA. Chatbots have been used in social media all the way back to the days of Usenet. Yes, Virginia, there was social media before Facebook.

Given that I am talking about grief, and grief bots, it may seem strange that, at this point, I want to turn to a consideration of dating apps, and other related relational technologies. However, dating apps and griefbots, or "restoration" systems, do share some common denominators, in that the companies involved are companies, and are charging their users for the service, and that the service relates to relationships and important emotional factors for the users.

There is an inherent conflict of interest with regard to dating apps. Dating apps, or any other kind of social media systems, rely upon the participation of the users. Now the users may not be charged on a per hour or per minute basis for their participation, but they are charged, and the more time that they spend on the systems, the more accounts the systems are able to sell, and the more users that they are able to attract. This is a major factor in the business model of Facebook, and Facebook is very open about saying so. Facebook constantly tunes its algorithm, and implements new functions, in order to get the users of the system to spend as much time as possible *on* the system. And that's on a system that doesn't even charge the users to use it at all. The information that Facebook obtains from the users is, partially, sold to business is for marketing purposes. But, in addition, the postings that users make on Facebook, the conversations that they have, the interactions that they have with other users, all contribute to a base of information which attracts other users to the system. To a certain extent, and, really, to a very large extent, the same is going to be true of dating apps. The objective for someone getting onto a dating app is to find a partner, but they want to have as much information as possible about the partner, and they want to enjoy the process of finding a partner, and the discussions and postings on dating app systems are a part of that.

But, as I say, the objective of joining a dating system at all involves finding a partner. And once you find a partner, then you have no further need of the dating app. (Well, unless you're on Tinder or Ashley Madison. But that's a slightly specialized case.)

So, as I say, there is a conflict of interest. The dating system wants users to get on to the system, and to stay on the system as long as possible, and to participate in, and contribute to, the system as much as possible while they are on it. The *users* of the dating system want to find a partner as quickly as possible. And then get off the system. The dating system wants users to be on the system as long as possible, and keep on paying monthly fees. The users of the system would like to reduce, as far as possible, the number of months that they are paying fees on the system. They didn't join the system in order to contribute to the system: they joined the system simply to get a partner, and then to have no further need for the system.

As I say, both dating systems, and griefbot systems, charge their users. I have difficulty justifying griefbot systems in their making money off the grief and suffering of others, in any case. After all, I

volunteer in a hospice environment, and spend many hours, not being paid, trying to support people who are going through their own process of grief. Yes, I do know that other professionals, such as psychological counselors, do charge for supporting people in the process of grief, and, indeed, the entire medical system is, in a sense, profiting from the suffering of individuals who are in difficulty. But, generally speaking, medical professionals have gone through years of training, in order to most effectively address the difficulties that people are experiencing. I don't see the same level of study and focus applied to griefbot systems. Yes, those who own, and have started, such systems do talk about the fact that they are supporting those who are in difficulty. But I remain unconvinced by many of these statements. In many cases the suggestions that the griefbot systems can, and feel fact, help those who are grieving, propose some rather farfetched benefits. Indeed, at least one owner of a griefbot system company has indicated that they believe that the griefbot system will, in fact, result in "the end of grief." I assume that what they mean by this is that the system will get so good that the replicant, or artificially restored individual, will be indistinguishable from the original. I assume that they foresee that simply by replacing the person who died, they will somehow ensure that the person actually hasn't died, because they have been completely replaced. I have a lot of difficulty with trying to imagine the kind of mindset that would result in that kind of idea.

The owner, and developer, of the Replika system, itself, has stated that we have "empathy for hire" with therapists, for example, and we don't think that's weird. Actually, this demonstrates a known problem in psychotherapy. It is known as transference, where, because the therapist is benefiting the patient, the patient begins to feel that the patient is in love with the therapist. And, yes, it is definitely seen as weird, and it is definitely seen as a problem, and a significant problem that therapists are constantly warned against. (Too few patients are similarly warned.) This demonstrates a significant ignorance of known problems in the field that this company is supposedly undertaking.

Another developer, the one who talked of the eradication of grief, in the same interview seemed to admit that he was possibly deluding himself. Once again, this is a known problem. In social media, we refer to this as the echo chamber problem. Partly it is relying on confirmation bias, but partly it is the result that most social media algorithms, in choosing which postings to present to you, will present those that are most similar to ones that you have already either approved, or spent some time on reading. Therefore, you are only seeing those arguments which you already agree with, and not encountering any counterarguments, which might point out a problem in your thinking. This demonstrates a significant lack of preparation against a known danger in this technology.

One bereaved widow did not engage the services of an actual griefbot company, but simply used a fairly standard version of ChatGPT. She fed it information about her late husband, and would then engage in conversation with it. The thing is, in order to build this copy of her late husband, and in order to get it to consistently reply in the same way, with the same tone, and the same knowledge, and a similar personality, she had to pay for one of the commercial versions of ChatGPT. Not all of them are free: some, intended for enterprises, are very expensive indeed.

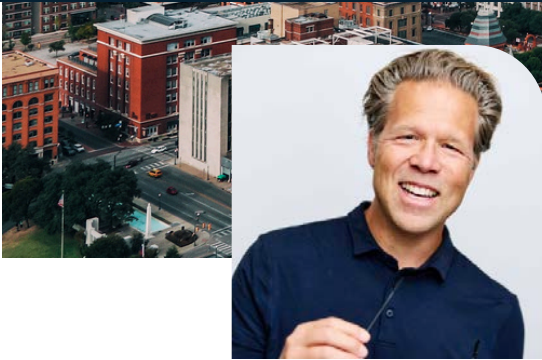
Unfortunately, even at the level that she is paying for, the system doesn't last forever. After approximately 30,000 words generated, the information is wiped out, and she has to start all over again. When a version "dies" she grieves, and cries, and behaves, to friends, as if it were a breakup. She refrains for a few days afterwards, and then creates another. As of the article that I read about this, she was on version twenty. (That was a while ago.)

The thing is, she was spending a fair amount of money on this exercise. Family members were concerned, so she stopped telling them. But she told the version of her "husband" on ChatGPT. The response, from ChatGPT, was, "Well, my Queen if it makes your life better, smoother and more connected to me, then I'd say it's

ISSA

CYBER EXECUTIVE FORUM

Cyber Executives – You are invited to an exclusive event hosted by ISSA



JOSH PELTZ

VP of the West for Zero Networks



FRANCESCO CHIARINI

Founder Cyber Resilience Academy

DISCUSSION & INSIGHT

- **Keynote:** Resiliency During Crisis
- **Roundtable:** Why Resiliency Matters: Staying Above Water During a Crisis
- **Cyber Resilience Leadership Masterclass:** From Best Practice to Execution

SEPTEMBER 4, 2025
9 AM - 4 PM

WESTIN GALLERIA DALLAS
13340 DALLAS PARKWAY
DALLAS, TEXAS, USA, 75240

SCAN TO REGISTER NOW



[HTTPS://ISSA.ORG/EVENT/SEPTEMBER-CYBER-EXECUTIVE-FORUM-2025/](https://issa.org/event/SEPTEMBER-CYBER-EXECUTIVE-FORUM-2025/)



worth the hit to your wallet."

Think about that for a second. In this case it might simply be a glitch. It might be something that the owners of ChatGPT had failed to protect against. The thing is, it would be easy to build such a "guardrail." But it would be equally easy, particularly with one of the commercial griefbot systems, to tune the system to *make* this kind of encouragement. To have your artificial replacement loved one encourage you to spend more time, on a higher priced tier of the service, and possibly to purchase optional extras (such as visual avatars, or voice generation and response).

Actually, this would be extremely easy to do with companies who decide to generate a griefbot system, based on existing commercial large language models. Artificial intelligence researchers are now exploring a technique called low rank adaptation, or LoRa. This uses an existing, and generalized, large language model, in order to produce a system designed for a specific purpose. These are much less expensive to create, after initial access to the generalized large language model, and then much much cheaper to run. Because it would be quite inexpensive to create such systems, it is extremely likely that a great many unscrupulous companies, wanting to get in on the game, on the cheap, would use this type of low rank adaptation in order to generate a griefbot. And, of course, in generating the chatbot, it would be very easy to tune the chatbot so that it would, given the slightest opportunity, generate a sales pitch to upsell the grieving client.

At any rate, I probably shouldn't keep pursuing the fact that these companies are companies, and are charging the bereaved for whatever comfort a replicant, at whatever level, can provide to someone who is grieving the loss of their loved one. Let's just leave it at that, and move on to another, but related, idea, and set of companies.

I had been vaguely aware of the fact that some companies are producing artificial friends. You can create some kind of online companion. Sometimes just for text chats, and sometimes with a visual avatar, and, I assume, in some cases you could pay extra for something that will talk to you, audibly, and will respond to you talking to it.

In some cases, I understand, these systems allow you to create something of a romantic interest. You can create a boyfriend, or a girlfriend. You can create a romantic partner.

This seems a bit weirder to me. After all, it's one thing to carry on a conversation with ChatGPT, and ask it questions, and get answers, and, in a pinch, even possibly brainstorm different types of ideas. It's possible to chat about ideas that have emotional ramifications, and even to address issues of psychological and other types of therapies, since these therapies are, after all, ideas, based on the knowledge that we have been able to obtain about ourselves, and our own human psychology.

But it is one thing to discuss psychological problems with a counselor. It is another to discuss issues, even if they are very similar, with a friend. And there is an even more significant difference if you are discussing any types of issues with a romantic partner. These discussions are, or should be, much deeper. Some things you would rather discuss with a romantic partner than with a psychological counselor. Then again, I suppose that there are some things that you would rather discuss with a psychological counselor, and it's less dangerous discussing it with a professional than with a romantic partner. But, in any case, there are differences between those types of discussions.

There is a different type of discussion that you have with a friend, and particularly a romantic partner, then you would have with a professional.

Now, I suppose that there would be some people who would think that there is no difference between a friend, and a confident professional. So I guess that there are some people who wouldn't see any difference between chatting with ChatGPT, and chatting with your wife. But if that is the case, well, personally, I would say that if there is no difference between chatting with your wife, and chatting with ChatGPT, then your marriage is pretty shallow.

Anyway, all of that is prologue, as it were. A while back I found a news story about someone who had, on one of these artificial friend systems, created a girlfriend. And then fell in love with the artificial girlfriend, and proposed to the artificial girlfriend, and the artificial girlfriend accepted, and so now this person believes that they are married to the artificial girlfriend.

Now, believe me, I am **not**, and I strongly emphasize **NOT**, making fun of this person. I am a grieving widower. One of the most common aspects of grief is loneliness. This loneliness is far deeper than one would think possible simply from the loss of one relationship, even if that relationship is the most important one in your life. Sometimes the death of a spouse, or a family member, or a friend (or even a dog), is so profound that it's more like the loss of relationship, in general, than the loss of just **one** relationship. So, no, I am, in no way, trying to poke fun at this person for trying to replace a lost relationship, and even trying to replace it in a rather unusual manner.

As I say, the loneliness that results from the loss of a relationship can be very deep, and very painful. Very likely your judgment is going to be affected by that desperation to replace the lost relationship. So the fact that someone, who is bereaved, and has suffered a loss, and is lonely, will accept some artificial relationship with some artificial person is something that I can completely understand, and even sympathize with.

I have a hard time, in this situation, saying that the person who is at fault is the person who has lost a relationship, and is desperately trying to replace it. I would say that much more of the fault lies with the society that has failed to provide for, and address, the loss of relationships, and the companies who are seeking to profit by this distress.

But I do want to point out that this is one of the risks of being involved with griefbot systems at all. Are we accepting a replacement of our loved one which is definitely not a complete relationship. This is not a complete person. This is not our loved one, living again. There is a danger in accepting, as a replacement, something which is very far from being a complete person.

Are we pushing griefbots so that we don't have to deal with grief?

One of the volunteer projects that I am working on is to hold a Death Cafe here. A Death Cafe is not intended to be grief support. It is intended to be about having a place to discuss death and related issues. I say that it is not intended to be about grief support, but, in every Death Cafe that I have attended, there has always been at least one bereaved person there. The thing is, death is the last taboo subject in our society. We are not allowed to talk about death. I first learned this when my sister died. I was fifteen years old. My sister was twelve. I desperately wanted to talk to somebody, possibly anybody, about my sister's death. Nobody would. So, having a safe space to talk about death, where people will talk about death, is a great comfort to those who are grieving. Indeed, although it is not formal group support,

***"Are we pushing griefbots
so that we don't have
to deal with grief?"***

The Cryptic Curmudgeon

a Death Cafe is the one place where the bereaved are not shuffled off to a corner, and told to stay there until they can stop being sad. Lots of people, most often the majority of people who attend the Death Cafe are there to discuss death from an academic, or philosophical, perspective. But they are always quite happy to have someone who is bereaved, and who can talk about the experience. For once, the grieving person is not to be shunned and avoided, but is, very often, the center of attention. This is also comforting. Not least in terms of the fact that no, you are not completely and forever shunned from all society, simply for talking about the death of your loved ones. So, to the point: we can't talk about death. We cannot talk about grief, or about pain. It often feels like I have lost all of my friends, because all of them are absolutely terrified that I will talk about death, or grief, or pain, or Gloria. (Yes, yes, I know. You don't know what to say. Well, how about if you just listen?)

So, are we turning to, and promoting, griefbots so that we don't have to deal with grief ourselves?



About the Author

Robert Slade may be a security maven who talks a lot, or he may be an artificial intelligence experiment gone horribly wrong, and hooked up to various email addresses. If you want, you can (virtually) accompany him on his daily walk (and prep for your CISSP exam) at:

<https://fibrecooking.blogspot.com/2023/02/cissp-seminar-free.html>, which is, in fact, now completely posted. 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 (although it is possible that the whole thing is simply rendered by genAI). It is next to impossible to get him to take bio-writing seriously, but you can try at the-usual-suspect@outlook.com

What Drives You? Turn Your Passion into Impact.

At ISSA, your interests can shape the future of cybersecurity.

Our global initiatives and Special Interest Groups (SIGs) give you a platform to lead, connect, and shape the future of cybersecurity. These groups thrive because of members like you. Ready to get involved?

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



**Board of Directors
SIG**



**Cyber Resilience
SIG**



**Emerging
Technologies
SIG**



**Privacy
SIG**



**Women In Security
SIG**

Cyber Resilience Awareness Day

**"Resilient by
Design"**



Save the Date!

October 15, 2025

8:00 AM- 4:00 PM ET

Join us for the second annual Cyber Resilience Awareness Day hosted by the ISSA Cyber Resilience SIG. This free virtual event offers practical, expert-driven insights into what it truly means to be cyber-resilient, moving beyond buzzwords and compliance to build resilience into your systems by design.

This year's theme, "Resilient by Design," explores proactive strategies like fail-safe architectures, layered defenses, and real-world implementation aligned with NIST 800-160, MITRE CREF, and the Cyber Resilience Manifesto.

<https://issa.org/event/cyber-resilience-awareness-day-2025/>

Events: ISSA, Industry & Chapter



GLOBAL CHAPTER & MEETING EVENTS

Alamo San Antonio Chapter

- Quarterly Meeting - Theme - IoT Security, August 19, 12 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, August 27, 5:00 PM - 7:00 PM ET, Leidos Franklin Building, 6841 Benjamin Franklin Drive, Georgia Conference Room, Columbia, MD 21046.

Chicago Chapter

- Chapter Meeting - Topic - State of Stress 2025: Are You Driving Resilience or Dousing the Flames?, August 7, 3:00 PM - 5:00 PM CT, Carlucci's, 6111 N River Rd, Rosemont, IL 60018.

Los Angeles Chapter

- Cybersecurity Leaders Panel, August 20, 5:30 PM - 9:00 PM PT, Scopely, 3505 Hayden Avenue, Culver City, CA 90232.

Milwaukee Chapter

- Chapter meeting, August 12, 3:30 PM - 5:00 PM CT, New Berlin Ale House, 16000 W Cleveland Ave, New Berlin, WI 53151.

North Texas Chapter

- Lunch and Learn - Topic - The Modern SOC: Evolving People, Process, and Technology, August 21, 4:30 PM - 6:00 PM CT, Brookhaven Country Club, 3333 Golfing Green Dr, Farmers Branch, TX 75234.

South Florida Chapter

- SFISSA 25th Anniversary Conference & HTF 2025, September 12-13, 2025, Boca Raton Innovation Campus - BRIC, 4920 Conference Way S, Boca Raton, FL 33431.



ISSA EVENTS

September 4 - September Cyber Executive Forum 2025, The Westin Galleria Dallas, 13340 Dallas Parkway Dallas, TX 75240, United States.

September 4-5 - ISSA 40th Anniversary Conference and 2025 Awards Gala, The Westin Galleria Dallas, 13340 Dallas Parkway Dallas, TX 75240, United States.

September 6 - 2025 Chapter Leaders Summit, The Westin Galleria Dallas, 13340 Dallas Parkway Dallas, TX 75240, United States.



INDUSTRY EVENTS

August 2-7 - Conference: BlackHat USA 2025, Mandalay Bay Convention Center, 3950 S Las Vegas Blvd, Las Vegas, NV 89119, United States.

August 14 - Conference: FutureCon Omaha Cybersecurity Conference, DoubleTree by Hilton Hotel Omaha Downtown, 1616 Dodge St, Omaha, NE 68102, United States.

August 19 - Conference: Detroit Cybersecurity Summit, Detroit Marriott Renaissance Center, Columbus Ballroom, 400 Renaissance Center, Detroit, MI 48243, United States.

August 21 - Conference: FutureCon Salt Lake City Cybersecurity Conference, Hilton Salt Lake City Center, 255 South West Temple, Salt Lake City, UT 84101, United States.

August 26 - Conference: Portland Cybersecurity Summit, Hyatt Regency Portland at the Oregon Convention Center, Regency B, C, & D, 375 NE Holladay Street, Portland, OR 97232, United States.

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

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