ISSUE 3 | VOL. 22 | MARCH-APRIL 2024

www.issa.org

ISSA

CELEBRATING OUR WONDERFUL WOMEN ON THE BOARD FOR WOMEN IN CYBERSECURITY MONTH

FEATURE FOCUS:

AI Driven Threat Protection

BOARD SPOTLIGHT:

4 Questions for ISSA COO Betty Burke

Advancing Cyber Security, Empowering Professionals

ISSA

40 YEARS STRONG

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 cybersecurity professionals, ISSA is committed to fostering individual growth, mitigating technology risks, and safeguarding vital information and infrastructure.

Follow Us On:

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 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 03 - ISSUE 22

FEATURE FOCUS

SUPPLIMENTARY SEGMENTS

DEPARTMENTS

SPOTLIGHTS

VOICES

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.

Presidents Letter

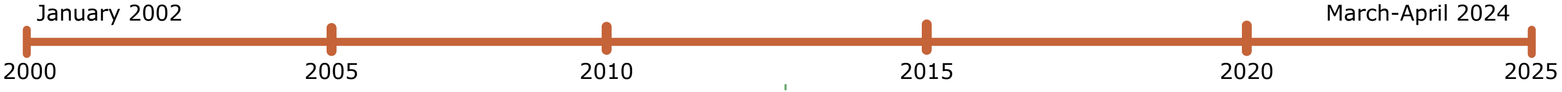
Showcasing Yesterday & Today

Howard Schmidt

Former ISSA President

Dr. Shawn P. Murray

International President



Welcome to the first issue of the all new, redesigned ISSA Password (monthly) Magazine. You may have noticed that The ISSA Password has grown steadily in the last few years. several factors contributed to this, not the least of which is the growing importance of InfoSec in just about every sector and every industry, with the resulting growth in ISSA membership.

With a monthly publication, we can provide our membership with more timely information about our shared profession, as well as ISSA and its chapters. Let us know what you think.

We also are working with Vanguard Integrity Systems to plan our annual ISSA conference along with Vanguard's 16th Annual Security Expo 2002, June 23-28, 2002 in Anaheim, CA. We partnered with Vanguard this past year and were pleased with the results, as were those that attended. The annual conference is a wonderful opportunity for networking and continuing education. The 2001 conference in Reno, NV was well attended, and featured 14 tracks with more than 113 speakers for the 224 sessions. If you are worried that the conference is only about RACF, please check the web site for updated information. As you might imagine working together with our partner Vanguard, we have added tracks and content that is relevant to a broad spectrum of ISSA members. This one promises to be even better. IT's also a good time to meet your ISSA officers, board members, chapter presidents and other leaders. This year's conference will be located near the new California Adventure theme park and Downtown Disney, so bring the family. You will hear more about this event soon.

With all that is happening in the world, ISSA's increasingly high profile is even more important. Through our leaders and members who serve on national and international committees, we are insuring that the voice of the InfoSec professional is heard.

ISSA's growth is apparent in that there currently are 39 chapters with 50+ members, six with 100+, one with 150+ and another two with 200+ (one of which has 300+). There are 48 ISSA chapters in all. Congratulations to all of them and their leadership.

Sincerely,
Howard A. Schmidt,
ISSA President

Hello ISSA Members, welcome to March!

It was a very busy February for your Board of Directors, our new management team, and the association overall. There is a significant amount of planning happening for new and existing programs, events, and chapter services. The Board met last month in person, which coincided with our first Cyber Executive Forum (CEF) of the year. What a refresh for the CEF program! We had outstanding presenters and numerous amounts of sponsors to provide an exceptional experience in Clearwater, Florida. Look for our next event to be held in San Francisco just before RSA.

There is a lot of productivity with committees, working groups and special interest groups at the moment. I would encourage you to get involved! There is an initiative to grow chapters in Central/South America and in Europe. I will be headed to Warsaw, Poland to represent our association at the SEMAFOR conference with a presentation on AI, Deepfakes, and Disinformation. I will be meeting with chapter leaders in Europe as well prior to the conference.

As we continue to celebrate our 40th anniversary, I would like to highlight the tidbits of historical information security events, advancements in our profession and past ISSA contributions that our marketing team has been compiling and sharing with our members. The evolution of our industry and the challenges we have today are significantly different! One threat that hasn't changed is the human threat! Look for additional gems from our marketing team as we continue to celebrate you, our profession, and our association!

Each year, ISSA partners with the Enterprise Strategy Group (ESG) to conduct a research survey with members of our profession and within our industry. The result of this survey produces a valuable research report referred to at the ESG Report on the *"Technology Perspectives from Cybersecurity Professionals".* It is that time of year when we are conducting the updated survey. Please look for an email or social media message with specific details on how to access and complete the project. It does take about 30 minutes to complete, so please honor the commitment to finish the entire survey. Your contribution demonstrates a commitment to have your voice heard and allows ISSA to be a valuable resource for the world once the report is released. It is a product referenced by news, agencies, academic institutes, and researchers everywhere!

As we look towards spring, I wish you all continued success in your efforts! Don't forget to take time for your personal lives and your families, as these bring much needed balance.

Regards.

Dr. Shawn P. Murray, President
ISSA International Board of Directors

Advertiser Index

NOW INDEXED WITH EBSCO

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
nick.cefalo@issa.org
Nick Cefalo

Chapter Relations
joe.moroney@issa.org
amy.velez@issa.org
Joe Moroney & Amy Velez

Member Relations
Mamen.Garcia@issa.org
nick.radar@issa.org
Mamen Garcia & Nick Radar

Executive Director
Jennifer.Hunt@issa.org
Jennifer Hunt

Sponsorships
Lisa.OConnell@issa.org
Lisa O'Connell

Journal Advertising
phil.dagostino@issa.org
Phil D'Agostino

Editors Corner

Jack Freund

Editor, ISSA Journal
NC Charlotte Metro Chapter

Dear Members,

I am thrilled to share an important update regarding our ISSA Journal. After careful consideration and valuable feedback from our community, we are transitioning to a bi-monthly publication schedule, shifting from our traditional monthly release.

This change is more than just an adjustment in frequency; it represents a significant enhancement in the depth and breadth of our content. With this new cadence, we are committed to delivering articles that dive deeper into the complexities and nuances of cyber security. Our goal is to provide you with thoroughly researched, insightful pieces that not only keep you updated on the latest industry trends and developments but also offer comprehensive analysis and best practices.

We understand that the world of cyber security is ever-evolving and rich with intricate details. By moving to a bi-monthly format, we give our contributors more time to explore subjects in greater depth, ensuring that you receive content that is not only timely but also timeless in its value and relevance.

This change is a testament to our commitment to quality over quantity. We believe that providing you with richer, more comprehensive content will create a more engaging and valuable experience. As always, we welcome your feedback and look forward to growing together in our understanding and application of cyber security principles.

Thank you for your continued support, and I am confident that this new chapter for the ISSA Journal will enrich your professional journey in information security.

Warm regards,

Jack Freund, Ph.D.
Editor, ISSA Journal

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 by 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.

BE A C.I.O.,
NOT A C.UH.OH

Privacy Section

Navigating the Complexity Security Remediation: Insights from a CSA Survey

By: Hillary Baron, Senior Technical Director for Research, Cloud Security Alliance

In the intricate and rapidly evolving domain of cybersecurity, the discipline of security remediation stands as a cornerstone for protecting organizational assets. This process, pivotal for identifying, assessing, and rectifying vulnerabilities, is essential for mitigating potential risks. The complexity and effectiveness of remediation strategies are influenced by a myriad of factors, including the cohesion of security teams and the sophistication of the tools and processes employed. CSA conducted a survey to understand current trends and practices in security remediation. Here are some of the most interesting trends.

Navigating the Visibility Maze: A primary obstacle that emerges from the survey is the struggle for comprehensive visibility within cloud environments. The challenge of achieving full transparency in these complex ecosystems, exacerbated by the adoption of containers and serverless technologies, presents a significant barrier to effective security management. This lack of visibility not only creates potential security vulnerabilities but also complicates the oversight of cloud operations, highlighting an urgent need for integrated solutions that provide a holistic view of the security landscape.

Alert Overload and Its Repercussions: The phenomenon of alert fatigue, driven by an onslaught of duplicate alerts and false positives, is a critical issue faced by organizations. This overload strains security teams, complicates the prioritization of threats, and can lead to delayed responses to genuine security incidents. The survey's findings point towards the necessity of adopting more nuanced approaches that prioritize the integration and intelligent orchestration of security tools, alongside leveraging automation and AI to sift through the deluge of alerts more effectively.

The Double-Edged Sword of Tool Proliferation: While the accumulation of various detection tools is intended to bolster security postures, it ironically contributes to a more convoluted security environment. This proliferation, without a strategic framework for seamless tool integration, results in siloed operations and diluted threat prioritization efforts. Despite the array of tools at their disposal, a significant portion of organizations feel unprepared to tackle cybersecurity threats, underscoring a disconnect between tool acquisition and actual security readiness.

The Burden of Manual Processes: The survey sheds light on the substantial manual overhead involved in vulnerability management, with security teams dedicating a significant portion of their time to manual tasks. This inefficiency not only hampers the timely resolution of vulnerabilities but also contributes to a backlog, thereby elevating the risk profile of organizations. The initial phases of the remediation process, in particular, are highlighted as time-consuming bottlenecks, necessitating a reevaluation of workflow efficiencies and the role of automation in streamlining operations.

Protracted Vulnerability Response Times: An alarming insight from the survey is the slow pace at which critical vulnerabilities are addressed, with some organizations taking days or even weeks to respond. This sluggishness in remediation efforts not only extends the window of exposure but also illustrates potential shortcomings in prioritization and response frameworks. The recurrence of vulnerabilities further exacerbates this challenge, indicating a reliance on short-term fixes rather than addressing the root causes of security issues.

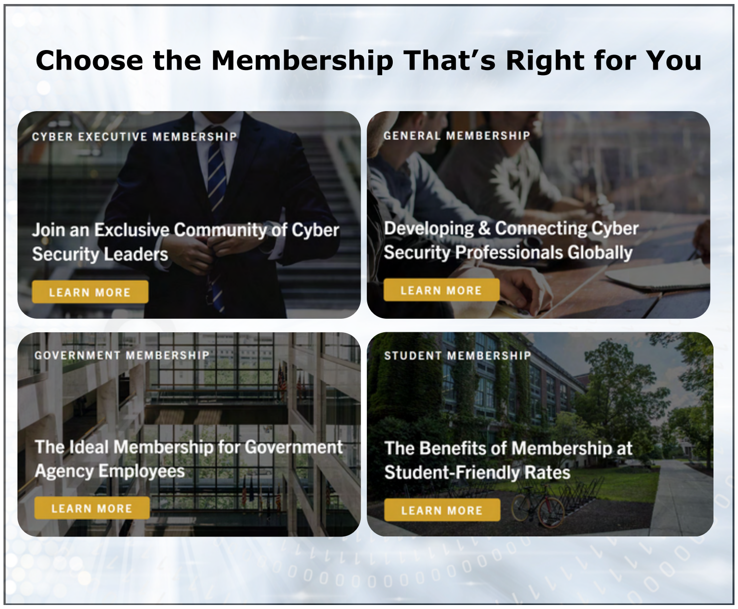
The Crucial Security-Development Divide: Perhaps one of the most telling findings is the substantial gap in collaboration between security and development teams. This divide, detrimental to the establishment of robust cybersecurity practices, emphasizes the need for a more cohesive and integrated approach that aligns development agility with security imperatives.

Concluding Insights and Forward Path

The survey's revelations underscore the multifaceted challenges confronting cybersecurity remediation efforts today. It is clear that a holistic strategy, transcending the mere accumulation of security tools, is imperative for enhancing organizational security postures. The emphasis must shift towards achieving unified visibility, improving collaboration across teams, and leveraging automation to alleviate manual burdens and streamline vulnerability management.

As we move forward, the insights from this survey underscore the necessity for organizations to adopt a more strategic, integrated, and proactive approach to cybersecurity. This entails not only the deployment of advanced tools and technologies but also a cultural shift towards greater collaboration and communication between security and development teams. Addressing the root causes of vulnerabilities, rather than relying on temporary fixes, and enhancing the efficiency of remediation processes through automation and AI, are crucial steps towards building more resilient and responsive cybersecurity frameworks.

In conclusion, navigating the complex landscape of cybersecurity requires more than just technological solutions; it demands a comprehensive approach that encompasses strategic alignment, process optimization, and a culture of continuous improvement and collaboration. As threats continue to evolve, so too must the strategies employed to combat them, ensuring that organizations can protect their assets effectively in this dynamic and challenging environment.



Temporary Elevated Access in the Cloud

By: Maria Rasner, Service Delivery Manager for IAM, Truist Financial Corporation

Temporary Elevated Access (TEA) should be a capability that enterprises can deploy to dramatically lower the risk of an event, incident, or breach and the length an attacker has access to systems. Elevated access (another word for Privileged Access) is defined by National Institute of Science and Technology (NIST) as "A user that is authorized (and therefore, trusted) to perform security-related functions that ordinary users are not authorized to perform" [1].

Essentially it is a user or account that can perform 'elevated' functions or activities than a typical end-user of the system. Temporary Elevated Access takes privileged access control to a much more secure level by, as it sounds, being temporary and not perpetual. TEA is sometimes referred to as Just-In-Time access. Think of it like the key card you get at a hotel for your stay. That card only works while you've successfully identified yourself to the hotel, gotten the temporary access card, and until you check-out. Upon check-out of the hotel, your access key card is deactivated, and you can no longer access your (previous) hotel room.

The risks addressed by TEA are primarily further removing risk of an attacker or malicious insider from doing harm within the network or system. Nearly all successful attacks are done using privileged or elevated accounts. Normal user accounts, by definition, can do little. Some notable examples of where elevated access was used to cause damage are numerous, so we'll mention a few top ones. Adidas was breached by an unauthorized party, leveraging an elevated account, to steal customer data [2]. T-Mobile has been hit several times by unauthorized parties using privileged accounts to steal customer data [3]. One of the worst, in terms of duration of unauthorized access is the Starwood hack, where they were in their system for over four years before they were detected [4]. This last one is a great example of how the word "temporary" in TEA would've paid off in huge benefits. Four years is not anywhere near temporary and would've stopped the bad actors' access four years earlier. The logical outcome of this is that the benefits of TEA are a much lower risk of a bad actor from being in your system for any longer than the length of access given to them.

The place to start on this TEA journey is in your Identity and Access Management (IAM) policy and process. A documented policy is essential for governance and ensuring compliance and adoption. Within your IAM policy, there must be a section on Privileged or Elevated Access. This section should address that all of these types of accounts must be temporary in nature, and not continuous or standing. As with all policies, there will need to be exceptions and the policy must address when exceptions can be made and define (or point to) a process where this is reviewed, approved, and the exceptions recorded in an appropriate system of record. Even these exceptions should be temporary, in that the list of accounts in this exception list are reviewed at least annually, reviewed to determine if the exception is still needed.

The process of how TEA is implemented and is required for compliance and adoption. At a high-level, the steps are as follows:

1. User logs into the portal via multi-factor authentication (MFA).
2. User then goes to the web UI.
3. User requests elevated access.
4. Request gets approved.
5. Request gets activated.
6. User starts the session.
7. Session actively is logged.
8. Elevated access ends based on the agreed access duration.
9. Access request details and session activity are captured for auditing purposes.

Each of the big three cloud service providers (CSPs) will follow this same basic flow, but with some uniqueness based upon product names and implementation. We will go through each of these, at a high-level, but recommend you look to their own websites for more detailed explanations and guidance before full deployment.

Microsoft Entra Privileged Identity Management (PIM) [5] allows an organization to assign eligible users to an elevated role, activate their permissions, allow for approval or denial of this access level, and then extend or renew the assignment depending upon length requirements. Amazon Web Services (AWS) Temporary Elevated Access Management (TEAM) via Identity Center [6] allows for a workflow for approvals, ability to view requests and session activity, use managed identities and group memberships, and a numerous choice for authorizations. Google Cloud is done via the IAM page [7] can be done with Google groups, using IAM Conditions to grant elevated permissions, Just-in-Time privileged access open-source application, or Service Account impersonation.

Sustainability, the concept of keeping this process going and (hopefully) automated is required for not only adoption, but to lower the risk these elevated accounts present to the organization. For sustainability monitoring access and auditing through cloud solutions can be provided by the CSP. Detect accounts that are not compliant and use a risk-based approach. Not all companies have the ability or resource to automate remediation so perform manual remediation if needed, but automation is your goal for sustainability. If you can only perform manual remediation, documentation that details these steps, ensuring engineers or analysts are trained, an audit trail, and oversight to ensure compliance with the manual process are required.

Temporary Elevated Access is a tool for granting roles to specific accounts in a granular, temporary manner. This allows human accounts to request for the access then leverage an approval process before they can perform with only the permissions required to get the job done. More importantly, adhering to least privilege principles acts as a foundation for more robust access controls by limiting privileges to have just duration to reduce the risk of unauthorized usage and minimize security breaches.

About the Author:

Maria Rasner works at Truist Financial Corporation as a Service Delivery Manager for IAM organization. She is CISM certified and is currently studying for her CCSK certification. Maria is also a mentor and an active member in her local ISSA chapter. She truly enjoys attending cybersecurity conferences to learn and share knowledge. She loves to travel with family internationally and is obsessed with British detective shows.

References:

[1] National Institute of Science and Technology, https://csrc.nist.gov/glossary/term/privileged_user

[2] Fortune Magazine, https://fortune.com/2018/06/28/adidas-warns-of-potential-data-breach/

[3] GeekWire, https://www.geekwire.com/2018/t-mobile-discloses-breach-exposed-customer-personal-information/

[4] National Public Radio, https://www.npr.org/2018/11/30/672167870/marriott-says-up-to-500-million-customers-data-stolen-in-breach

[5] https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

[6] https://aws.amazon.com/blogs/security/temporary-elevated-access-management-with-iam-identity-center/

[7] https://cloud.google.com/iam/docs/temporary-elevated-access

Privacy Section

Considering Privacy and Data Theft in Technical and Security Solutions:

How My Whistleblower Experience Identified Legal and Policy Gaps

By Danielle Spencer, MIS, MBA, PMP, FAC-COR III, FAC-P/PM I

While you're being vetted for a new job, have you or your references been asked questions such as: "Do you have any illegitimate children?", "What is the financial status of your family? Are any of them bribable?" and "What about your sex-life; is there anyone out there that knows anything embarrassing about you, of a sexual nature?" I'll assume your answer is no. For several years I have asked many different people that question, I haven't found anyone who has told me yes. Unlike you, my response would be a yes.

I am Danielle Spencer. I have a bachelor's degree in Medical and Research Technology, two master's degrees, one in Information Systems and another in Business Administration. I have a master's certificate in Information Assurance (Cybersecurity), and am PMP, FAC-COR and FAC-P/PM certified. In 2017, I became a whistleblower against the most powerful debt collection organization in the world, the Internal Revenue Service (IRS). My book, Digital Assassins: Surviving Cyberterrorism and a Digital Assassination Attempt documents many of the cyber events I experienced after becoming a whistleblower, to include cyber events that I would classify as privacy violations and data theft. It is my belief that anyone using the job vetting process as an opportunity to commit data theft to unearth bribable family members or illegitimate children has committed a privacy violation.

Most Information Technology (IT) and Cyber professionals spend most of their time creating, maintaining and securing technical solutions. What happens when people in trusted positions violate a person's privacy to do things that they shouldn't or to obtain information they have no business reason to access, using the solutions we have created and secured? Moreover, how does Democracy survive when these types of technology and cybersecurity threats are allowed and there are no laws or rules in place to hold people accountable. Technology is advancing rapidly; the law and policy aren't.

The goal of this article is not to explore or discuss new technical or security concepts. The goal is to bring awareness to that part of human nature that can cause well-meaning people to breach the law or violate an organization's privacy policy. As technical and security professionals, we should be mindful of these human flaws so that we advocate for laws and policy solutions that mitigate human behavior that may compromise security.

My whistleblower experience has taught me many things, including the fact that the technologies that so many technology professionals expend time and effort creating and securing, can be misused, and abused by people in trusted positions. However, the most important lesson I've learned is how technical solutions can be used to invade people's privacy.

Prior to this experience, I took my privacy for granted. I didn't fully understand how precious privacy is, and how dangerous privacy violations can be. I also didn't appreciate the fact that people in trusted positions can commit this act, without the public's knowledge and in my opinion, with no consequences.

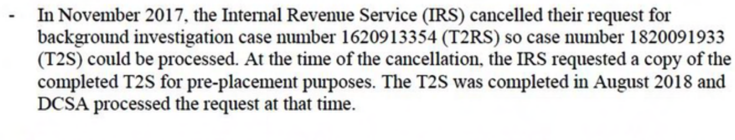
I believe this is because most people don't know, think or understand that data theft is a privacy violation.

When most people think about privacy violations, they most often think about identity theft; something executed by strangers. However, our privacy can be violated by people we know or by institutions that we trust. My experience has shown me that when our privacy is violated by known entities, the goal of the violation is to commit the offense of data theft in hopes of sharing false and/or fraudulent information or to interfere into the tax administration process.

Data Theft:

What is data theft? ProofPoint defines it as ".....the unauthorized acquisition of digital data from an entity, often driven by motives of financial profit or to disrupt business activities. It encompasses the illicit access, transfer, or storage of sensitive details ranging from personal credentials and financial records to proprietary technologies, algorithms, and processes." [1] In layman's terms it is the act of disclosing, communicating, releasing or obtaining personal information without consent. Knowledge of and being able to identify data theft is important because the person committing the data theft act could be guilty of abusing their position of trust. Therefore, whenever data theft occurs, it should be addressed immediately, regardless of whom commits it, even if it is a government entity.

In 2018, I believe I was the victim of data theft by a government entity, specifically the IRS. Without my knowledge or consent, the IRS contacted another government agency to obtain my security adjudication file, see figure 1.



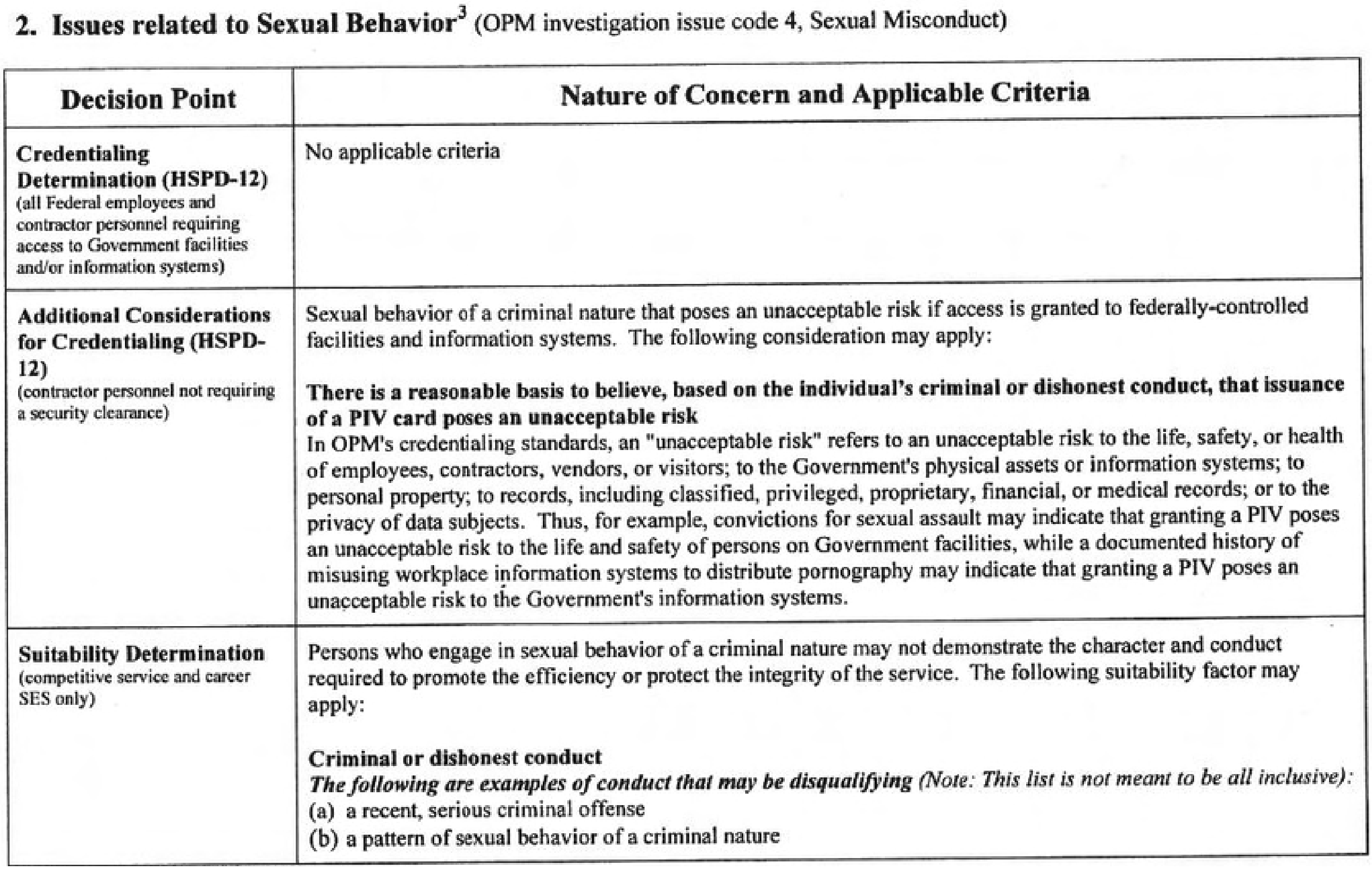
- In November 2017, the Internal Revenue Service (IRS) cancelled their request for background investigation case number 1620913354 (T2RS) so case number 1820091933 (T2S) could be processed. At the time of the cancellation, the IRS requested a copy of the completed T2S for pre-placement purposes. The T2S was completed in August 2018 and DCSA processed the request at that time.

Figure 1: Source: Portion of DCSA Response Letter, ticket number: DCSA-B 22-06285, dated: July 19, 2022

My employment with the IRS ended in October 2017. Despite this fact, the IRS contacted and received my security file, which not only contained my personally identifiable information (PII), but also the PII of people associated with me, to include family members, neighbors, coworkers, and supervisors. No one could explain to me why the IRS requested and received this information, especially since I had not been contacted by the IRS for employment opportunities.

Another example of data theft occurred in 2020. While undergoing a security adjudication background investigation at the Public Trust level, inappropriate questions were asked about me and my family. To fully understand the gravity of this event, one must understand the purpose of this type of investigation. The purpose of a background investigation is to verify an individual's fitness and suitability for federal government employment; to determine if they are reliable, trustworthy, of good conduct and character, and loyal to the United States (U.S.). The duties of an employment position determine the information to be collected via a standard form (SF) e.g., SF85, SF85P or SF86. The SF-85P is the form used for individuals who are being considered for Public Trust Positions and/or Moderate or High-Risk Public Trust Positions when there are no national security considerations; this was the form I completed and submitted.

As previously stated, my references and I were asked questions that I believe violated my privacy. All of the questions I listed earlier were out of scope for my Public Trust background investigation. The topic of Sexual Misconduct is **NOT** an area of inquiry on the SF85P. Moreover, based on the 2008 OPM information, Suitability Determination which says "Persons who engage in sexual behavior of a criminal nature may not demonstrate the character and conduct required to promote the efficiency or protect the integrity of the service.", meaning a criminal record, of a sexual nature, must exist prior to asking questions related to sexual behavior, figure 2.



2. Issues related to Sexual Behavior[3] (OPM investigation issue code 4, Sexual Misconduct)

Decision Point	Nature of Concern and Applicable Criteria
Credentialing Determination (HSPD-12) (all Federal employees and contractor personnel requiring access to Government facilities and/or information systems)	No applicable criteria
Additional Considerations for Credentialing (HSPD-12) (contractor personnel not requiring a security clearance)	Sexual behavior of a criminal nature that poses an unacceptable risk if access is granted to federally-controlled facilities and information systems. The following consideration may apply: **There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk** In OPM's credentialing standards, an "unacceptable risk" refers to an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects. Thus, for example, convictions for sexual assault may indicate that granting a PIV poses an unacceptable risk to the life and safety of persons on Government facilities, while a documented history of misusing workplace information systems to distribute pornography may indicate that granting a PIV poses an unacceptable risk to the Government's information systems.
Suitability Determination (competitive service and career SES only)	Persons who engage in sexual behavior of a criminal nature may not demonstrate the character and conduct required to promote the efficiency or protect the integrity of the service. The following suitability factor may apply: **Criminal or dishonest conduct** ***The following are examples of conduct that may be disqualifying*** *(Note: This list is not meant to be all inclusive):* (a) a recent, serious criminal offense (b) a pattern of sexual behavior of a criminal nature

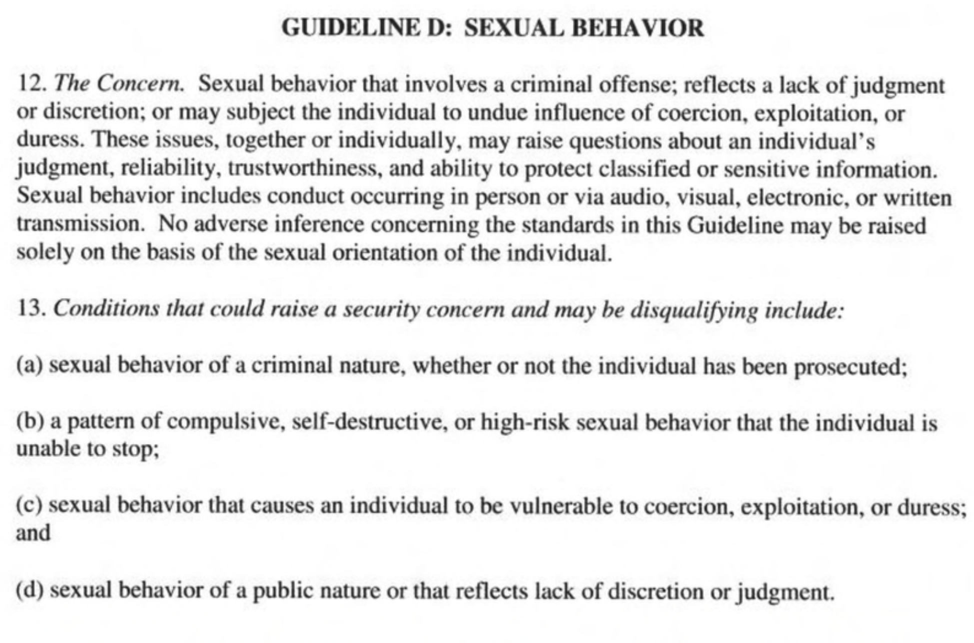
Figure 2: Source: 2008 OPM information, Suitability Determination

I do not have a criminal record. Moreover, nothing in my past remotely indicates that I had or am engaged in criminal sexual behavior. Despite this fact, the investigator decided to ask me questions pertaining to my sexual behavior.

In direct contrast to a Public Trust investigation, according to the Office of Personal Management (OPM) and the National Security Adjudicative Guidelines, Sexual Behavior **IS** a consideration in instances for individuals who being considered for national security positions and/or requiring access to classified information, see figure 3, page 12 of the *Security Executive Agent Directive 4; National Security Adjudicative Guidelines* [2].

I was directed to this document when I followed up with the DCSA concerning the privacy violation, see figure 4.

Fortunately, I had experience in position descriptions and background investigation level determinations; therefore, I knew the questions were out of scope and a



GUIDELINE D: SEXUAL BEHAVIOR

12. *The Concern.* Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

13. *Conditions that could raise a security concern and may be disqualifying include:*

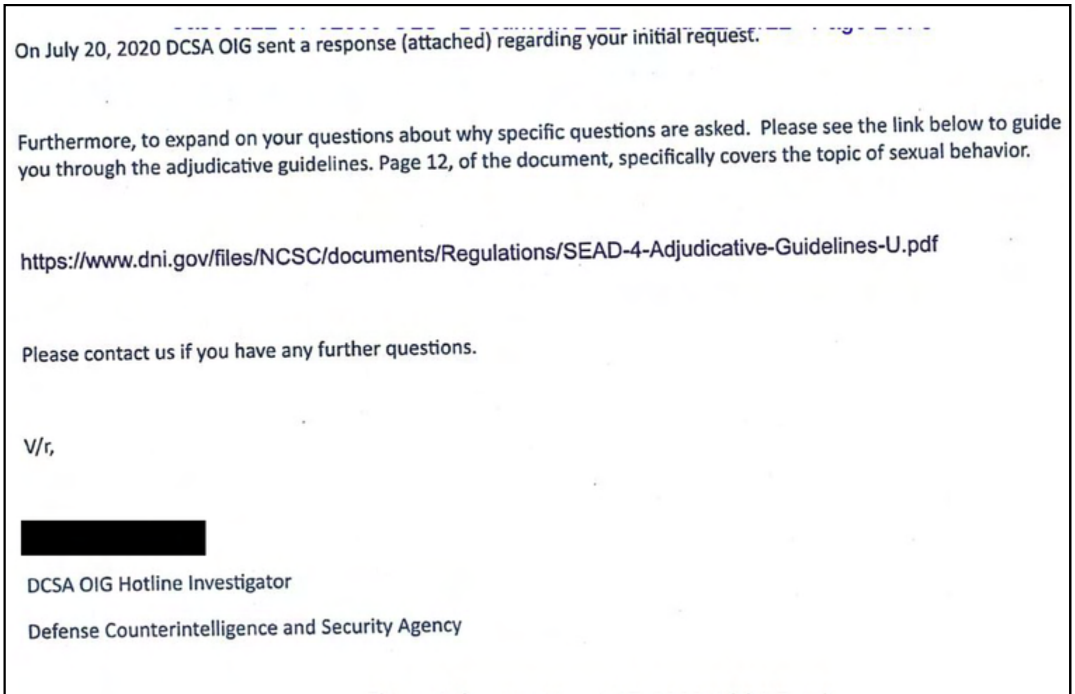
(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

Figure 3: Source: Security Executive Agent Directive 4; National Security Adjudicative Guidelines



On July 20, 2020 DCSA OIG sent a response (attached) regarding your initial request.

Furthermore, to expand on your questions about why specific questions are asked. Please see the link below to guide you through the adjudicative guidelines. Page 12, of the document, specifically covers the topic of sexual behavior.

https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf

Please contact us if you have any further questions.

V/r,

[redacted]

DCSA OIG Hotline Investigator

Defense Counterintelligence and Security Agency

Figure 4: Source: March 17, 2022 DCSA Email

form of data theft. However, how many people do not. How many people have been asked about illegitimate children or the finances of their family members and provided this information to someone who then entered it into a system.

Once data theft occurs, the acts of sharing false and/or fraudulent information or interfering in the tax administration process can be accomplished.

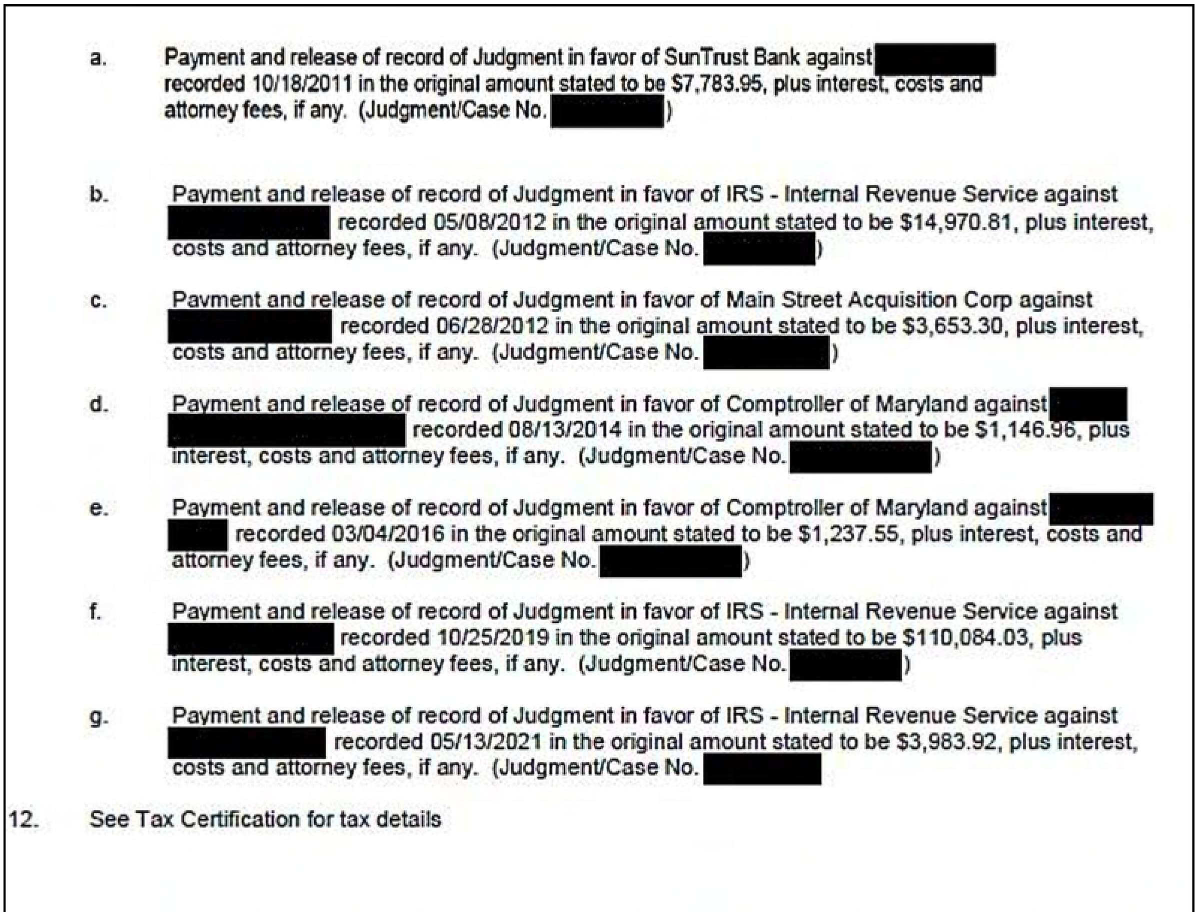
Sharing False and Fraudulent Information:

During my whistleblower journey, I had many experiences where false and fraudulent information was shared about me. However, the most extreme event occurred when, in my opinion, the privacy of individuals unknown to me was violated to intentionally create a false title search. In 2022, a title insurance company created a title search report, using the judgements and liens from people unknown to me, see figure 5.

Neither my home nor I had judgments or liens. To verify this fact, I conducted a land records search which verified that there were no liens or judgments filed under my name, see figure 6.

PII information from at least six people was used to create a title search report. From my knowledge, none of these people were contacted to obtain their consent for their judgement and lien information to be shared with people and organizations they did not know, for business purposes of which they were not involved. Despite this oversight, this company electronically produced and disseminated this fraudulent report, telling a bank my home and I had over $140,000.00 worth of debt.

To fight the false report, I had to share this PII information, which included these people's full names, partial social security numbers, addresses, account numbers, and details about the debt, such as when it became delinquent and how much was owed with other organizations. These organizations included the state Attorney General's office, the insurance regulatory organization, executives at the bank, and employees in state circuit court. Given the events that occurred, I feel confident in saying that these individuals probably did not want this information that include their PII, shared with people they didn't know, especially since they were not trying to obtain a loan.



a. Payment and release of record of Judgment in favor of SunTrust Bank against [redacted] recorded 10/18/2011 in the original amount stated to be $7,783.95, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

b. Payment and release of record of Judgment in favor of IRS - Internal Revenue Service against [redacted] recorded 05/08/2012 in the original amount stated to be $14,970.81, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

c. Payment and release of record of Judgment in favor of Main Street Acquisition Corp against [redacted] recorded 06/28/2012 in the original amount stated to be $3,653.30, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

d. Payment and release of record of Judgment in favor of Comptroller of Maryland against [redacted] [redacted] recorded 08/13/2014 in the original amount stated to be $1,146.96, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

e. Payment and release of record of Judgment in favor of Comptroller of Maryland against [redacted] [redacted] recorded 03/04/2016 in the original amount stated to be $1,237.55, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

f. Payment and release of record of Judgment in favor of IRS - Internal Revenue Service against [redacted] recorded 10/25/2019 in the original amount stated to be $110,084.03, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted])

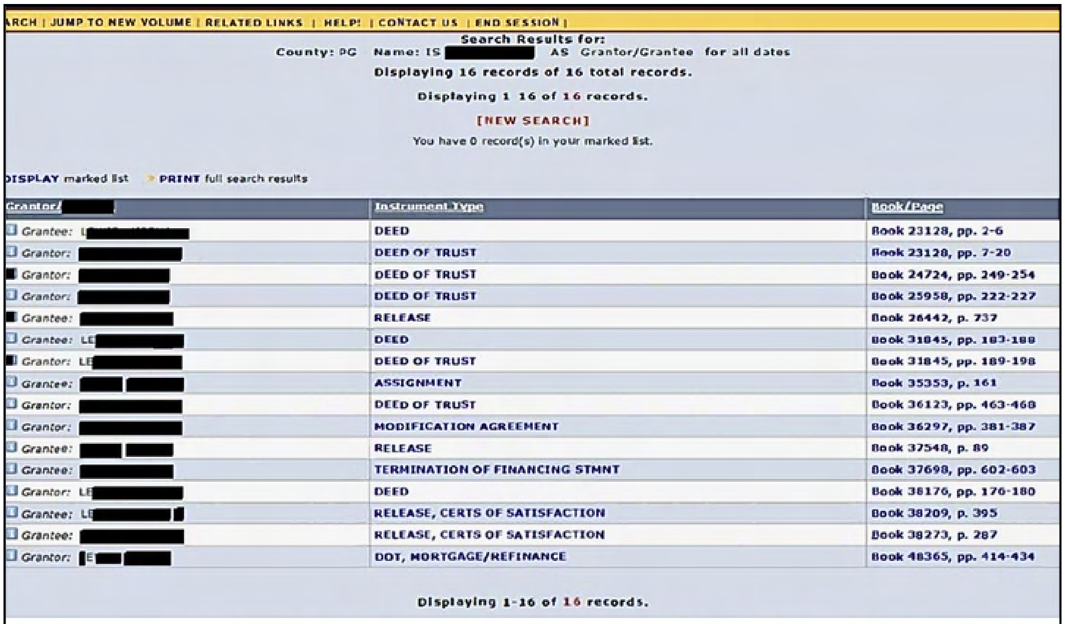
g. Payment and release of record of Judgment in favor of IRS - Internal Revenue Service against [redacted] recorded 05/13/2021 in the original amount stated to be $3,983.92, plus interest, costs and attorney fees, if any. (Judgment/Case No. [redacted]

12. See Tax Certification for tax details

Figure 5: Source: Portion of Title Search Report, Commitment Date May 24, 2022

Tax Administration Interference:

Another event that can occur after a data theft incident, is interference in the tax administration process. Tax administration is the process by which tax laws and regulations are enforced, e.g. determining if taxes are owed or if a tax refund will be given. Interfering in this process can take many forms. The most common of these are submitting false information via a tax form to report additional income or additional deductions. An individual with system access, can also use information obtained by data theft to remove tax documents. It is important to note that data theft must occur first. Without a data theft incident, tax administration interference is almost impossible, given that knowledge of one's PII is needed to pass verification and validation checks to access and submit tax information.



RCH | JUMP TO NEW VOLUME | RELATED LINKS | HELP! | CONTACT US | END SESSION |

Search Results for:
County: PG Name: IS [redacted] AS Grantor/Grantee for all dates
Displaying 16 records of 16 total records.
Displaying 1 16 of 16 records.

You have 0 record(s) in your marked list.

DISPLAY marked list
PRINT full search results

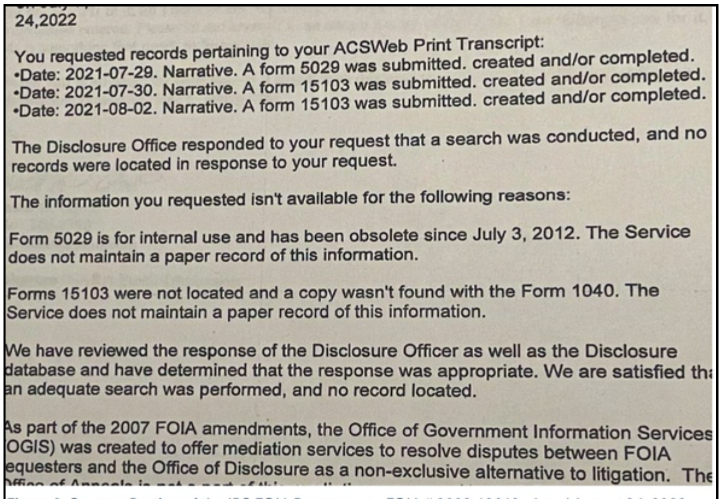
Grantor/[redacted]	Instrument Type	Book/Page
□ Grantee: L[redacted]	DEED	Book 23128, pp. 2-6
□ Grantor: [redacted]	DEED OF TRUST	Book 23128, pp. 7-20
■ Grantor: [redacted]	DEED OF TRUST	Book 24724, pp. 249-254
□ Grantor: [redacted]	DEED OF TRUST	Book 25958, pp. 222-227
■ Grantee: [redacted]	RELEASE	Book 26442, p. 737
□ Grantee: LE[redacted]	DEED	Book 31845, pp. 183-188
■ Grantor: LE[redacted]	DEED OF TRUST	Book 31845, pp. 189-198
□ Grantee: [redacted] [redacted]	ASSIGNMENT	Book 35353, p. 161
□ Grantor: [redacted]	DEED OF TRUST	Book 36123, pp. 463-468
□ Grantor: [redacted]	MODIFICATION AGREEMENT	Book 36297, pp. 381-387
□ Grantee: [redacted] [redacted]	RELEASE	Book 37548, p. 89
□ Grantee: [redacted]	TERMINATION OF FINANCING STMNT	Book 37698, pp. 602-603
□ Grantor: LE[redacted]	DEED	Book 38176, pp. 176-180
□ Grantee: LE[redacted]	RELEASE, CERTS OF SATISFACTION	Book 38209, p. 395
□ Grantee: [redacted]	RELEASE, CERTS OF SATISFACTION	Book 38273, p. 287
□ Grantor: [redacted]E[redacted] [redacted]	DOT, MORTGAGE/REFINANCE	Book 48365, pp. 414-434

Displaying 1-16 of 16 records.

Figure 6:Source: Land Records Search Results Report conducted on 9/11/2023

In my opinion, tax administration interference has the potential to be one of the most serious and severe consequences to data theft victims. These consequences can include an unnecessary tax audit or a fictitious tax bill. A tax audit can be triggered on a data theft victim by the submission of tax data that contradicts information previously submitted. A data theft victim can also be liable for a fictious and/or fraudulent tax bill if someone submits false tax information, stating that there was previously unreported income. In one specific incident, someone, with access and knowledge of my PII, faxed forms to my IRS tax account, see figure 4.

Since I was not the person who submitted these forms, I contacted the IRS, via the Freedom of Information Act (FOIA) process. The purpose of this request was to obtain copies of these documents, so that I could know and understand what had occurred. However, when the IRS responded to my request, I was told that none of the forms were available, see figure 5. In addition, one of the forms, Form 5029, was an internal use form which had been obsolete since 2012.



24,2022

You requested records pertaining to your ACSWeb Print Transcript:
•Date: 2021-07-29. Narrative. A form 5029 was submitted. created and/or completed.
•Date: 2021-07-30. Narrative. A form 15103 was submitted. created and/or completed.
•Date: 2021-08-02. Narrative. A form 15103 was submitted. created and/or completed.

The Disclosure Office responded to your request that a search was conducted, and no records were located in response to your request.

The information you requested isn't available for the following reasons:

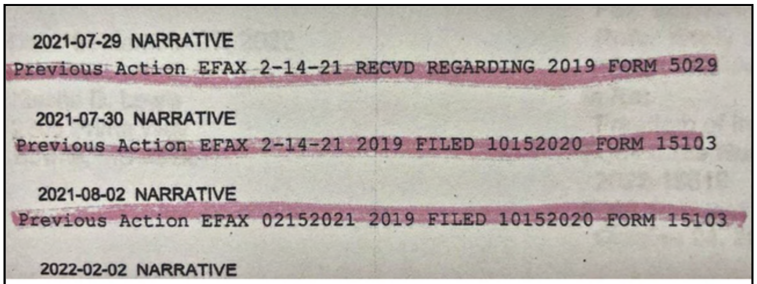
Form 5029 is for internal use and has been obsolete since July 3, 2012. The Service does not maintain a paper record of this information.

Forms 15103 were not located and a copy wasn't found with the Form 1040. The Service does not maintain a paper record of this information.

We have reviewed the response of the Disclosure Officer as well as the Disclosure database and have determined that the response was appropriate. We are satisfied th an adequate search was performed, and no record located.

As part of the 2007 FOIA amendments, the Office of Government Information Services OGIS) was created to offer mediation services to resolve disputes between FOIA equesters and the Office of Disclosure as a non-exclusive alternative to litigation. The

Figure 8: Source: Portion of the IRS FOIA Response to FOIA # 2022-18619, dated August 24, 2022



2021-07-29 NARRATIVE
Previous Action EFAX 2-14-21 RECVD REGARDING 2019 FORM 5029

2021-07-30 NARRATIVE
Previous Action EFAX 2-14-21 2019 FILED 10152020 FORM 15103

2021-08-02 NARRATIVE
Previous Action EFAX 02152021 2019 FILED 10152020 FORM 15103

2022-02-02 NARRATIVE

Figure 7:Source: Screenshot of the IRS ACSWeb Report dated: June 22, 2022

Despite asking, no one could explain to me why the forms were submitted, who submitted these forms, what impact, if any, the submitted forms had on my tax account, or why these records were missing once I requested copies.

Conclusion and Recommendations:

Technological advances are happening at a rapid pace. This phenomenon will give rise to more privacy violation and data theft opportunities. However, current laws and privacy policies do not protect citizens. Given the seriousness of the consequences, and the lack of legal protections, technology professionals need to be aware of these tactics. When creating, implementing, and securing solutions, thought should be given to how data theft can be prevented, both technically and administratively, using laws and policies. Identifying and incorporating data theft mitigating strategies will go a long way in both avoiding data theft and protecting citizens data.

About the Author

Danielle Spencer, is a senior leader with almost 25 years of experience focused on business, finance, and acquisition management. She is a chance agent, transforming and improving business operations and processes. She has two Masters degrees in business Administration and Information Systems, and a Bachelor of Science degree in Medical and research Technology, is certified in Information Assurance (cybersecurity) and Project Management. Ms. Spencer is also the author of the book, *Digital Assassins: Surviving Cyberterrorism and a Digital Assassination Attempt* (March, 2023), which was inspired by actual events and reflects the abuse of power and weaponization of private data by those who swore to protect it.

FEATURE FOCUS

AI DRIVEN THREAT DETECTION

By: Enoch Anbu Arasu Ponnuswamy

Digital technology has increased rapidly and this has led to an outbreak of data and connectivity, transforming the way how individuals and organizations operate. This transformation has resulted in massive benefits but they have brought in vulnerabilities which can be benefitted by malicious actors. Today's cyber threats need innovative approaches to cyber security.

Artificial Intelligence (AI) is primarily used for threat detection in Cyber security. It helps to detect, analyze and respond to cyber threats in a faster way. It is used to detect and prevent cyber threats, such as malware, phishing attacks, and intrusion attempts.

AI provides a simplified process of data analysis, data screening as well as detecting any risks.

EVOLUTION OF THREAT DETECTION

Traditional Methods of Threat Detection

Traditionally, threat detection was done with a focus either on the threat that was detected or in the tools like System Information and Event Management (SIEM) rules, Intrusion Detection System (IDS) rules, Machine Learning Models, User Entity Analytics.

Increasing Incident Surface

Organizations are following various technologies like SaaS applications, IoT devices, Cloud Computing, Remote/Hybrid working etc. due to increase in digital transformation. This helps them to increase their productivity and in turn increase customer experience. This results in an increase in the Incident surface for attackers.

Financial Implications

Organizations that operate with limited resources often find it challenging to allocate funds for efficient cyber security measures. For the ever-evolving threat landscape, it is financially difficult to implement 24x7 threat monitoring and response. This stands as a major challenge in today's competitive business landscape.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Definitions and Types of Artificial Intelligence Technologies

Machine Learning involves developing algorithms and statistical models enabling computer systems to learn and program themselves from experiences without being explicitly programmed. It involves creating computer systems that can learn and improve on their own by analyzing data and identifying patterns, instead of being programmed to perform a specific task.

Deep Learning is a type of Machine Learning that uses neural networks to imitate the learning process of the human brain. A neural network uses machine learning and AI to teach machines how to process data in a way that is inspired by the human brain. A neural network consists of functional layers. Enclosed in these layers, certain behaviors, tasks, or processes trigger a specific response from the machine. If there are more layers within the neural network, the more expressive and sophisticated the response.

Generative AI refers to deep learning models that consume raw data and generate new outputs that are like but slightly different from the original content, including text, audio, computer code, and images.

How AI Cybersecurity Is Different

An emerging need for creative problem-solving and complex challenges in the workplace indicate that Cyber security protection with Artificial Intelligence will never replace security professionals. A distinct feature of AI is that it can assist human security professionals by analyzing vast amount of data, recognize patterns and create insights on large volume of data. Traditional security processes might take weeks to complete the same.

Traditionally used signature-based detection tools and systems are effective for known threats. They are inadequate for novel or unknown threats. They also result in a lot of false positives and security professional's wasted efforts.

Manual Analysis of security events and event logs are required for traditional cyber security in search of indicators of a potential security breach. This requires more than one security analysts and also consumes extensive amount of time.

AI based cyber security overcomes these limitations and much more. It will have enormous impact on cyber security process and people.

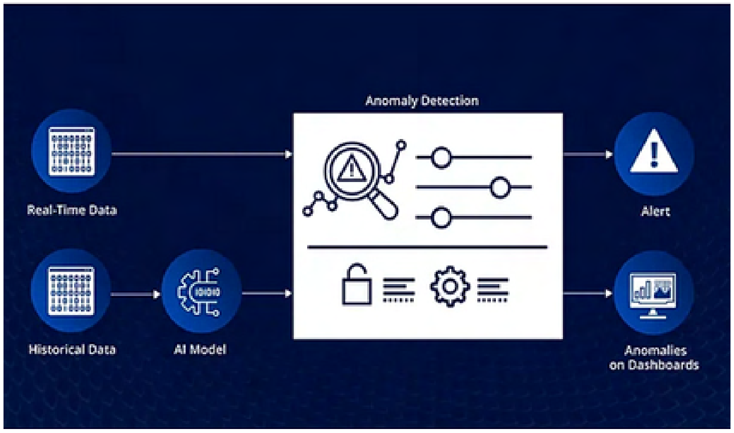
ARTIFICIAL INTELLIGENCE DRIVEN THREAT DETECTION MECHANISMS

Anomaly Detection Using Artificial Intelligence

Anomaly detection refers to identification of items or events that do not follow an expected pattern in a dataset and these are usually non detectable by a human expert.
It aims to find data patterns that deviate from a specified data distribution. It catches an unusual and abnormal behavior of data.

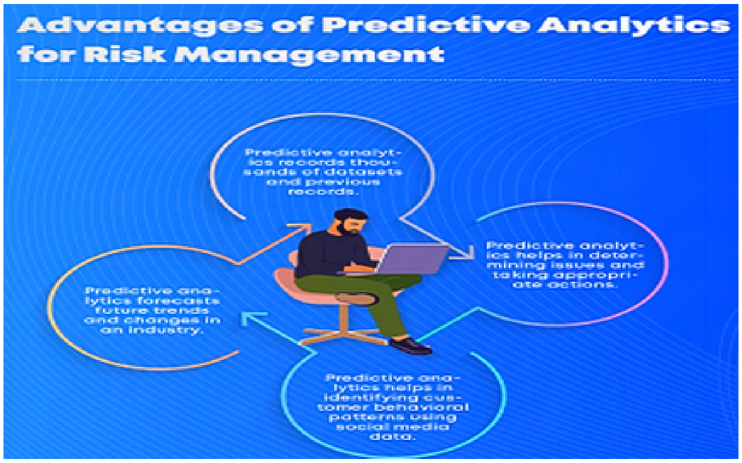
Manual observation and identification of an abnormality is not completely accurate with high data volume. A compelling need for an advanced mechanism in which the identification of the abnormalities from logs can be done in a short amount of time brings out the introduction of artificial intelligence and machine learning capabilities in the picture. Use of AI real time anomaly detection makes it possible in a blink of an eye.

AI based anomaly detection can automatically analyze data and identify abnormalities in the patterns. It enhances accuracy and prevents false triggers. It doesn't require manual intervention to understand anomalies, and this occurs even before the system is affected.



Predictive Analysis for Identifying Potential Threats

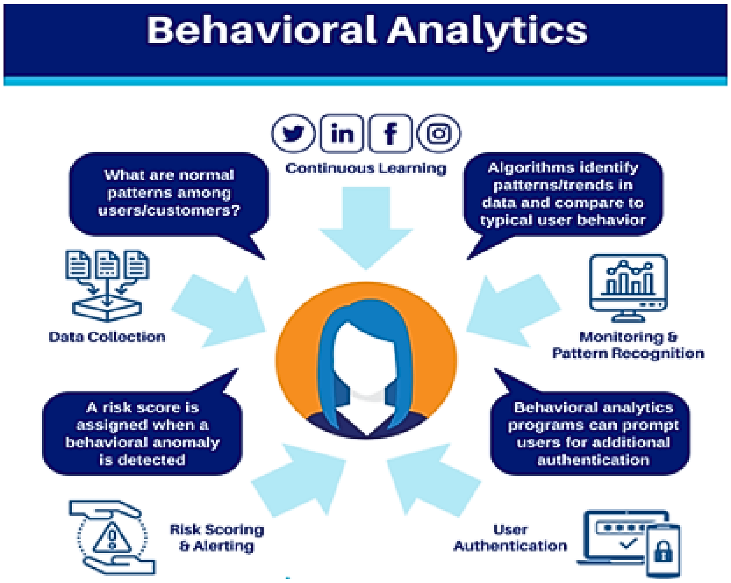
By using Predictive Analytics in Cyber security, organizations can proactively detect and respond to cyber threats before they cause significant damage. Predictive analytics uses Machine Learning algorithms, AI models to identify cyber threats before they occur. It uses trends, anomalies and past data to foresee and eliminate risks. This continuous monitoring and analysis of data provides early warning signs of possible attacks.


Advantages of Predictive Analytics for Risk Management
Predictive analytics records thousands of datasets and previous records.
Predictive analytics helps in determining issues and taking appropriate actions.
Predictive analytics forecasts future trends and changes in an industry.
Predictive analytics helps in identifying customer behavioral patterns using social media data.

Organizations must keep in mind that if the data source is limited, AI and ML will not capture all the potential risks. Applying predictive analytics from end to end of the organization improves customer experience by reducing outages.

Behavioral Analysis to Detect Unusual Patterns

Behavioral analysis uses a combination of machine learning, artificial intelligence, big data, and analytics to identify suspicious behavior to identify patterns, trends, anomalies to take appropriate actions. It provides data to identify trends and easily spot outliers, so that potential threats can be easily spotted. Traditionally, organizations identified malicious behaviors using signatures that are related to certain types of known attacks. Cyber attackers are more sophisticated and they develop new methods, procedures that enable them to enter vulnerable environments and they are also not detected by conventional approaches. Behavioral Analytics can also identify root causes, provides insights for future identification of similar attacks.


Behavioral Analytics
Continuous Learning
What are normal patterns among users/customers?
Algorithms identify patterns/trends in data and compare to typical user behavior
Data Collection
Monitoring & Pattern Recognition
A risk score is assigned when a behavioral anomaly is detected
Behavioral analytics programs can prompt users for additional authentication
Risk Scoring & Alerting
User Authentication

ADVANTAGES OF ARTIFICIAL INTELLIGENCE DRIVEN THREAT DETECTION

AI has huge benefits in cyber security and has the below advantages:

- **Improved Speed -** AI Cyber security uses machine learning, data analytics and hugely improves speed and accuracy in threat detection.
- **Improved Accuracy -** AI powered cyber security uses machine learning algorithms to identify threats with more accuracy compared to conventional threat detection methods
- **Real-time Threat Detection** - By analyzing vast amounts of data, they can detect anomalies and potential threats long before they can cause significant damage.
- **Automation** - Automation in AI based cyber security is critical for identifying threats in early stages and thereby preventing potential attacks.
- **Adaptability** - AI models adapt to new attacks which make them effective in devising attack strategies. This adaptability reduces the dependence of rule-based systems that becomes outdated.
- **Scalability** - AI based cyber security solutions are scalable which suit them for organizations of all sizes. They handle large volume of data without compromising in the size of human resources.

REAL WORLD APPLICATIONS - LOS ANGELES BASED HOSPITAL

Healthcare facilities have a compelling need to provide a safe and secure environment for patients, staff and visitors. They require protective measures that have all kinds of safety protocols to deal with possible security breaches that threat patients and healthcare workers.

Many hospitals incorporate AI based Cyber security measures with the aim of enhancing patient and personnel safety and optimizing their overall operating efficiency.

Challenge

- Implementing 24/7 monitoring of the entire hospital premises and threat detection amidst security guard shortages.
- Implementing thorough pandemic protective measures.
- Providing solution to workplace violence against healthcare workers (according to National Nurses United, in 2021, 81% of responders admitted experiencing violence either in the form of verbal threats or physical assaults).
- Preventing intrusions through non-entrance doors, other vulnerable areas.
- To increase active shooter preparedness.
- Proactive detection of fire hazards early enough which ensures a timely and more effective response during emergency evacuation.
- Safety of medical equipment, supplies and medication.

Solution

The solution provider created a comprehensive Healthcare Security Suite which aimed at providing a safe and effective risk management which in turn helped the patients and staff to have a safe and comfortable environment that is free from risks and threats.

The solution provider created an AI based software which implemented pandemic protection methods, non-contact thermal screening, and social distancing monitoring, real time people counting with face mask usage detection. It also widely identified firearms and also tracked the gunmen across the connected cameras even though the weapons were hidden.

Benefits

- Streams from multiple cameras helped the security personnel to detect fights, assaults and other threats by analyzing them in real time which prevented workforce violence.
- Slip and fall accidents are identified immediately which alerted the personnel to provide help and support.
- Alerts are sent very quickly when a patient tries to leave their bed, which minimizes the high-risk falls for fragile patients.
- Helps in detecting displeased personnel or fired staff and other individuals that happen to cause an issue all the time.
- Identifies hazardous smoke and fire and send alerts for mitigation.
- Thermal Screening helped in speeding up the process of checking individuals and eased out the concern of the staff and personnel regarding the infection.
- AI based cyber security measures expanded the coverage of the healthcare facility in terms of safety and security. It also reduced the amount of manpower.

CHALLENGES AND CONSIDERATIONS

1. Quality of Data

AI requires high quality data for work effectively. Cyber security data is often found disrupted, incomplete, or outdated, which affects the reliability and accuracy. Cyber criminals can compromise or manipulate AI to generate fake or deceptive data. In order to avoid this, data must be collected, stored and processed in a secure environment and data updating must also be done.

2. Legal and Ethical Issues

Ethical and Legal issues pose a major challenge in the usage of AI in cyber security. Decisions are automated in AI which affects the security, privacy of organizations and individuals. AI systems may not always make fair and transparent decisions and may raise doubts about the accountability of its operators. In order to mitigate this challenge, it is always advisable to follow ethical principles and best practices for AI in cyber security. Compliance of relevant laws and regulations should always be taken care of.

3. Balancing AI And Human Expertise

Lack of trust and adoption is a challenge in using AI in cyber security. Lack of awareness, confidence, fear of losing control, jobs are some of the issues which many stakeholders encounter which which make them reluctant in using AI based cyber security. There is a need for clear and transparent communication in terms of effectiveness, benefits of usage of AI in cyber security to help the stakeholders to involve themselves and reap the benefits.

FUTURE OF ARTIFICIAL INTELLIGENCE IN THREAT DETECTION

The role of AI in cyber security is set to become even more pivotal as we move forward into digital age. The increase in volume of data demands the use of intelligent, automated systems capable of quick and accurate threat detection and response. AI might become core part of cyber security strategies. Advancement in AI systems will enhance predictive analysis, which makes it possible to anticipate a wider range of cyber-attacks and proactive response. In coming years, the role of AI in cyber security has an opportunity for substantial growth. With increasing cyber-attacks, there is a need for advanced tools and technologies. AI provides powerful set of tools that addresses the present challenges and provides a roadmap for future cyber security strategies.

There will be a need for stronger AI driven defense mechanisms to counterattack AI based cyber-attacks in future. Taking the privacy concerns into account, there will be more demand in terms of ethical AI and a need for clear policies for data collection and processing.

CONCLUSION

Artificial Intelligence and Cyber security have become inseparable components and are characterized by both promises and challenges in the never ending battle against cyber threats. AI has a proven ability to analyze huge volume of data, detect anomalies, and provide real-time threat intelligence. This has helped the organizations to safeguard their digital assets. It is equally important to note AI's limitations and ethical concerns. Hence it is crucial to address them during deployment. The decision about whether to adopt AI based solutions for cyber security lies with the organizations themselves.

In conclusion, with the massive evolution of digital world, the union of AI and cyber security plays a pivotal role in safeguarding individuals, organizations and the whole society. The future of AI in cyber security is filled with both enhanced capabilities and new challenges. It provides a promise of unparalleled protection capabilities, but also demands a proactive and informed approach to manage potential risks and pitfalls.

References

1 (Source: https://www.researchgate.net/publication/372343707 AI_Artificial_Intelligence_Cybersecurity)

2 (Image Source: https://towardsdatascience.com/is-the-future-of-cyber-security-in-the-hands-of-artificial-intelligence-ai-1-2b4bd8384329)

3 (Source: https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity)

4 (Source: C. H. Park, "Anomaly Pattern Detection on Data Streams," 2018 IEEE International Conference on Big Data and Smart Computing (BigComp)

5 (https://www.algomox.com/resources/blog/ai-anomaly-detection/)

6 (Image Source: https://medium.com/predict/ai-anomaly-detection-safeguarding-systems-and-data-1327aebe6e1e)

7 (Source: https://www.researchgate.net/publication/375715292_Title_The_Role_of_Artificial_Intelligence_in_Predictive_Cybersecurity_Analytics)

8 Image Source : https://www.bluent.net/blog/predictive-analytics-for-risk-management/)

9 (Source: A. Y. Iskhakov, M. V. Mamchenko and S. P. Khripunov, "Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems," 2023 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2023

10 Image Source: https://www.authenticid.com/glossary/behavioral-analytics/)

11 (Source: https://www.researchgate.net/publication/377726525_Scalability_and_Resource_Efficiency_of_Next-Gen_AI-_Based_Firewalls_A_Case_Study_on_Cloud_Environments

12 https://www.researchgate.net/publication/375671883_AI_and_Cybersecurity_An_Ever-Evolving_Landscape)

13 (Source:https://www.linkedin.com/advice/3/what-biggest-obstacles-using-ai-cybersecurity-tt68f#:~:text=Data%20quality%20is%20a%20paramount,a%20more%20secure%20digital%20landscape.)

14 (Source: https://www.linkedin.com/pulse/future-ai-cyber-security-comprehensive-guide-crowemackay-hkige/)

15 (Source: https://www.researchgate.net/publication/375671883_AI_and_Cybersecurity_An_Ever-Evolving_Landscape)

KnowBe4
Human error. Conquered.

Security Awareness Training and Simulated Phishing Platform

Helps you manage the ongoing problem of **social engineering**

KnowBe4 Security Awareness Training

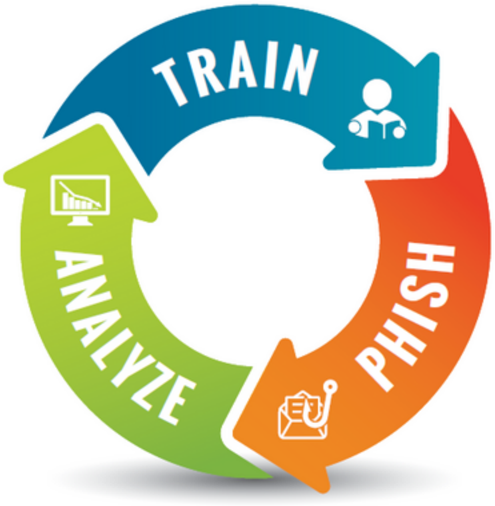
Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

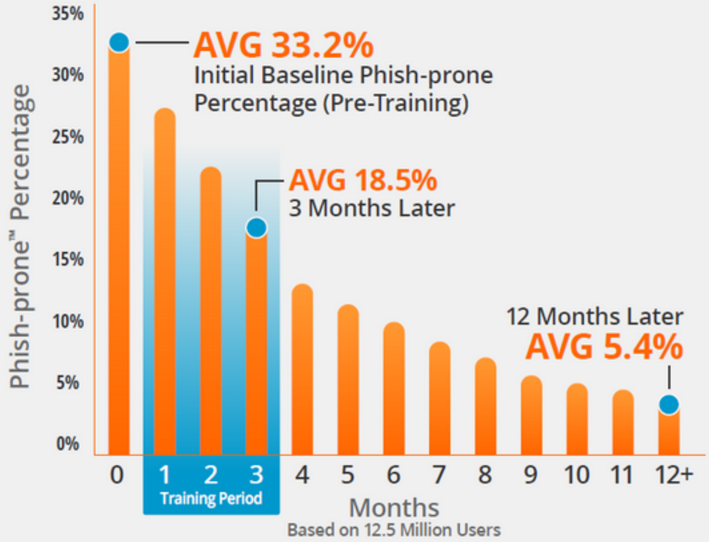
Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!





The System Really Works

With KnowBe4's massive database, we analyzed over 12.5 million users over the course of at least 12 months, and our 2023 research continues to uncover alarming results. The overall industry initial Phish-prone Percentage benchmark increased to 33.2%, up nearly one full point from 2022.

Fortunately, the data showed that this 33.2% can be brought down to 18.5% within 90 days after deploying new-school security awareness training. The one-year results show that by following these best practices, the final Phish-prone Percentage can be minimized to 5.4% on average.

See how your company's Phish-prone Percentage compares to your peers! The **Industry Benchmarking feature** is included with your subscription.

Source: 2023 KnowBe4 Phishing by Industry Benchmarking Report
Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Supplementary Segment

Women in Security Executive Speaker Series: How to Build and Present a Budget that Gets Board Approval

By: Pamela Fusco, ISSA CFO/Treasurer
Transcribed By: Debbie Christofferson, ISSA Director

How does an Executive Board approve a budget with so many competing priorities for the same pool of money? How do you prove security is worth the investment when your function is considered overhead, not a profit center? Find out what it takes to build a budget that will get approved by your Board of Executive Staff.

What is that your Board and Executive team want, and in what format, including the process for getting inserted into the approval cycle, and to match the Board's focus? We will identify what you need, how to collect it, and how to prepare for your best chance of approval, and present it to your Executives.

We will review what to include in presentation, what to leave out, and how you deliver a budget presentation for successful results.

We will take you to the starting line, the finish line, and on your next steps, for knowing what your executives want, how to start framing a budget, creating a first pass, and submitting it.

Getting Started

Getting started means you start logging your activity one and stay on top of it. Document, document, and document.

Create an executive steering committee for cybersecurity, or a legal team in audit and control. Include key stakeholders and their concerns, build a strong agenda, report progress and seek feedback.

Start to execute your plan, and begin to bring in the teams to support it.

Report on progress, continuously. Keep your reporting up, whether or not the executives ask for it. Carry your plan everywhere. Bring your plan—always—that shows "this is where we are, and this is where the money is."

Communicate consistently and keep sharing the status.

Pamela exemplifies what we are about and is also an experienced executive leader, who has been in cybersecurity for 33 years.

How do you acquire detailed information and get buy-in for your budget?

She has never hit her target budget, and probably never will, it's either over or under budget.

You may want to hire a third party to help you help establish a budget for a specific program you are trying to implement, or where you lacked resources in people or budget. A three-year program is a good place to start, but it might be early for a business with its first CISO (Chief Information Security Officer).

Advance Planning to Support Your Ask

When you ask for the money, for example, $15 Million, and this is the executive ask:
"Are you sure you're going to be able to achieve the program?"
"Are you sure you're going to be able to spend this money?"

You may not be able to spend it all if you are new and don't know the ropes and processes for your employer. How does your company work to implement spending for projects, people, or tools, to support your program? You are also dependent on other business units and their capacity. Even if you have the capability, they may not be able to hire fast enough, within the business groups you are relying on.

Do you have the support to implement your plan and the funding? Is there a consistent third-party where vetted candidates can be sourced?

Understanding the Business

You must understand the business and regulatory environment for your organization.

Using the 80/20 pareto rule—for what we focus on in cyber: 80% will meet the needs of most of the business. The other 20% of the business will have different requirements to meet regulatory and business requirements. Examples: HIPAA, clinical trials, drug approval, mergers & acquisitions (M&A), drug recipes, drugs to market. In chip or high-tech manufacturing, it might be export regulatory requirements, top secret design modules, order fulfillment or counterfeiting factories.

Every business is different, across sectors, size and current state. Understand the business and how security fits in. You cannot universally "plug and play" because of differing business needs: Plug and Play are precluded regulatory requirements, and won't work, because of different in business models. For instance, modifications to a system or application in the pharma industry must be approved by the FDA. After all, when you use manufacturing to create a drug recipe, to test trugs or to run clinical trials, the drug make-up can be altered based on the technology.

You might understand cyber and regulation. But wherever you go, you must first understand the business you are supporting.

Contingency Planning

Surprise "unearthed" events will always pop up, for example the recent pandemic, the remote workforce shift, supply chain disruptions such as worker strikes or malware shutdowns, and other disaster events. You need situational awareness, and to actively collaborate on the event, that will give you battle wounds from Day One.

Plan ahead for how you will address offsite resources to support different scenarios, such as a major security breach, if your line of business is susceptible.

Validate Your Proposed Budget

Within your draft budget, validate your existing propose and strategy. Be sure it supports a robust cyber program that supports your business risks. Address the entirety of your security program not just one aspect, such as Security Operations.

Identify your core business and the business stakeholder groups that support it. Interview those key stakeholders, especially business stakeholders, and pay attention particularly to those in M&A, sales, and your software supply chain if you're a software provider. You must be in the know!

Quality-check the process, and actively engage the business stakeholders to ensure adequate inclusion. Hold the discussions that best fit your business. This will also likely change your budget.

Look at what you are planning to implement, and its impact to the rest of the infrastructure and organization. Address other groups you have not collaborated with you on a deployment.

Benchmark Your Competition

What is your competition spending on security? Seek data in the market from repositories, alliances and organizations to see what they are spending, and on what part of their budget. Do the extra research.

Identify Your Scope

Within your role, are you all-inclusive for security, are you Operations, or what is the scope? Lay it out in a snippet to your board. Show the prior year's investment, what it was used to support, and the impact.

Create Your Cyber Security Investment Slides (Content)

Invest in Automation.

Boards will look for an ask for this. If you use open source, e.g., scripts you write that the organization depends on, these are not scalable and often lack support.

Seek a high level of automation, to gain efficiency, reduce errors, and increase productivity and accuracy. It reduces human error, and creates repeatable success. Auditors also desire automation. high level of automation. Examples include credentials and employee access so they can perform their job.

Reevaluate Your Security Program as You Go:

While creating your budget, you actually reevaluate your security program at the same time.

Legal Applications:

Ensure that legacy apps are covered in your budget, and in an update slide for your executives. Include costs, and the security risk scenario. For example: "Here's how we can transition away from these, what it will cost, ...", with other supporting details.

Risk Vs. Expectations

Always restate to the Board, what the risk is, vs. expectations. If something happens, we are limited in what we can do.

Security Operations

"This is my budget currently, how the money was spent, …" and move on. It's mostly standard.

Doing business as a third party with other businesses

First, identify what that business is. If you want to conduct business, and if you are supplying paper to your client (or whatever the product or service is), that's fine.

However, a provider, even a small company, must be examined with a certain rigor to do business with another company. A full-blown security assessment is needed to support the regulatory requirements for the business.

Build out an independent element, to manage vendors, and perform these assessments. These may fall into a group for light processing, or for a more substantial review, depending on services being provided.

Who does the third-party provider work with? If you attest to a result, be aware of what you are attesting to, and that you can support it, if later challenges arise.

Identifying Options

Pam sets up options, Option A ("everything", Option B (less but some risk, maybe a balance), sometimes an Option C (what we need to keep the lights on, but our risk is through the roof). You must present options, you cannot say "no". Smaller options can also be presented, they need not be big.

Alliances

Seek alliances to work with in the cyber space, which have tool kits for small business. This allows you to leverage what they have, or share managed services with other organizations. A little research in this space goes a long way.

All Inclusive Cyber Security Budget

Apply baseline examples, but be aware that budgets will vary for everybody. Align your program to an industry standard, even though it will differ by your own business sector and state of security.

- Keep it high level, your communication and plan are focused for a Board level.
- Your deep-down dirty details are kept behind the scenes, but be aware, so you can answer questions.
- Take the high road, give the benefit of the doubt, and stay professional.

Outcome of Previous Investment Overall Cybersecurity Posture

You showed what you spent, now you present your current state.

Current situation

Red, Yellow, and Green are applied, to depict where you are, and current state. Present a three-year model, or even just a one-year model. Show the expectation over a given time frame, and how it will progress moving forward.

Unearthed event

These are situations where you don't know what you don't know. But you can work to get ahead of it.

- Know your suppliers, your third-party vendors, and potential backup providers
- Build relationships with your business stakeholders and procurement
- Identify stakeholder communication and escalation parties in advance of a potential business disruption that originates in security

You are vulnerable to: Security incidents, breaches, the pandemic or other disruptive unknown events.

- Pay attention to holidays when staffing is low, for what is going on in year-end sales or closing, critical production deadlines, audits, etc.
- Participate with consortiums
- Work with third parties that support investigations
- Understand what is coming down pipeline
- Work on everything you can, to move your program ahead of it

State your case

If we do not work with third parties, we will only know our own internal world, we will not have trusted relationships, nor will we understand what is happening.

Get ahead of your competition!

This lets them know that you are in it to win it—for the organization and your security program. It helps you get in front of potential problems. It also helps you retain staff, because they know there is a visible supported plan. They know the plan!

Building Baseline Skills

Understand your organization's budget, its cycle, and where your function fits within. Realize the current and strategic priorities and how your cybersecurity mission supports them.

If you lack financial or budgeting strength, seek to immediately educate yourself, either with an inside colleague or staff member, or from outside. If a member within your team is an expert, utilize their strengths. Your Organization's Chief Financial Officer or comparable role may provide a good resource as a starting point.

Wrapping up Your 2024 Security Program

If you need more, identify how much more you need to budget for, in addition to what you previously asked. It might also be business as usual on costs. However, costs often increase—licensing costs, insurance, staffing, etc.

Strive for simplicity! Be honest. And do your homework. Based on that, you might say:

"I've met with X team, Y team, and collected intelligence from external resources on what they are doing."

"Here is our peak, what we see, how we are protecting critical assets that support the business."

Show statistics, and show trending metrics with supporting feedback.

You want the executive staff to trust you, and to demonstrate that your team has done everything possible, when you ask for budget.

Wrap-Up

- Illustrate! Use it as the key that every executive returns to. Be consistent.
- Present a Matrix, it's key and an illustration. Use it over and over, to resonate with your executives.
- Always reflect on historical data if you have it, such as past audits, past spending, etc. Encourage independent third-party assessments good, bad, and recommendations.

Trust is money well spent.

Share what you have with those independent third parties, under Non-Disclosure Agreements (NDAs): Give them audit results, include them in weekly staff meetings, bring them into to audit meetings, and bridge them for interaction with forensic teams and others they need to work with.

When you build out your security program and budget, it must have flexibility. If things change, or go bump in the night, you have to bend, but still be able to move forward without upending the entire plan.

When there is an incident or an issue, launch your strategic plan, so not all your resources are applied to the immediate incident. This keeps you from falling backward, for instance for a new line of business, where some security program did not get fully implemented. While you are responding to a big event, you still have to execute business.

Establish realistic expectations and show your progress.

Invest in good project managers who understand and know your business, the stakeholders and how they all function.

Identify trends to include in the budget over the next two to three years.

Apply case studies.

Factor in sustainability and accountability.

Always be honest and forthcoming.

About the Author

Pamela Fusco has over 29 years of experience in the infosec industry. An active member of the ISSA since 1998, she was instrumental in orchestrating and implementing the CISO Executive Forum, ISSA monthly webinar series and Educational Advisory Council (EAC). Fusco currently serves on the ISSA BOD as a Director and CFO, resided on the US Presidential White House Staff, held positions as CISO of Merck, Digex, Apollo Group, and EVP, Citi. An industry-recognized pioneer, Fusco was a Founder of SAFE Bio Pharma Inc., and Founding Member of the Cloud Security Alliance and Founder/President, NY Metro CSA Chapter. Fusco began her career in the US Navy as a cryptologist, focused on supporting security proceedings for government and national intelligence SPECOPS (special operations).

Resources:

ISSA Women in Security Special Interest Group Executive Series: "How to Build and Present a Budget that Gets Board Approval", Listen to the webinar from Thu, Jul 25, 2023, at www.issa.org/event/wis-getting-your-budget-approved-by-your-board-executive-staff/

More Than Shifting Left: Why Relying Solely on Third-Party Vendors to Get it Right Isn't a Security Solution

vorlon

By Amir Khayat, Vorlon CEO and Co-Founder

At the recent ISSA CEF event in Clearwater, we heard some clear themes as we connected with CISOs and other attendees. The first was that CISOs are coaching each other to become communications experts within the larger organization so they can make their case for resources across other departments and the C-suite. Many CISOs see the risks posed by an expanding network of app-to-app API connections, but need to convince others in the organization of the growing risk.

Another insight from the ISSA event highlighted a growing sense among CISOs about the challenges of being heroes in their roles. The SEC and others with regulatory power are placing a lot of pressure on companies to report everything faster, and to be more transparent about what happened in a breach. The fact that CISOs do not normally receive Directors & Officers Insurance means that they are at great risk of being held personally liable for decisions that are often out of their hands. The Uber data breach and the resulting conviction has everyone realizing that being a CISO is no honeymoon.

It was clear from speaking to so many CISOs that the third-party attack surface is a top priority, and gaining visibility seems to be a big first step with many struggling to figure out how to get that visibility.

Over-Permissive Access

What is the best way to secure the valuables in your house? Most folks will rightly start by securing the locks on their front door, back door, and garage to deter intruders. Newer technologies include smart features that allow us to activate features on-the-go, or from afar, for added flexibility and peace of mind.

But what about the other technology you use at home? Should your wifi-enabled toaster oven have access to your tax documents stored on your laptop? Should your smart fridge have access to the contact list on each family member's smartphone? Should your smart thermostat be able to control the smart lock on your door?

As asinine as these statements sound, they are analogous to the state of enterprise cybersecurity today. Each department is purchasing new applications and tools to facilitate aspects of their job, and those new tools are being granted over-permissive access to systems they needn't ever touch.

Reasonable Measures & Duty of Care

The average enterprise in 2024 publishes anywhere from a few dozen to upwards of 200 APIs. And immense resources are deployed to secure those APIs you publish. Large internal product security teams with expensive toolsets are brought on to secure and maintain them. And rightly so – API Security is incredibly important, and your organization should do everything possible to protect your customers and their data. Even with those precautions in place, you can never guarantee 100% protection—it isn't reasonable.

The same can be said of the vendors whose services and applications you consume. Think of all the time, energy, effort, and money spent to secure the APIs your company publishes. Despite those efforts, there's no guarantee of absolute protection. Multiply that by the number of APIs your enterprise is consuming. Your third-party attack surface is exponentially larger and with little to no control over how others handle their own APIs.

The reality is that app-to-app communication—or non-human communication—is the majority of web traffic today (nearly 83% according to Akamai). The average enterprise consumes more than 25,500+ APIs. And the problem only gets bigger with every new application connection that is made. You might not worry about securing your house from your toaster oven, but if you had to give your smart lock combination to 3 new smart devices every hour every day, you are bound to have questions about how they are making use of such connections.

Proactive Third-Party API Security

Some may dismiss any effort to secure another company's product as unnecessary, noting the presence of legal agreements with each third-party vendor covering them in the event of a breach. But while your legal agreement may help you recoup financial losses in case of a vendor breach, it will not save you any of the operational efforts required to return your company to normal, nor prevent the brand reputation hits that come with being connected to a breach. Ultimately, relying on the legal agreement is effectively doing next to nothing to proactively protect your data in motion, and Duty of Care will ultimately fall on your organization in a legal proceeding.

The security solution is not to tighten the legal agreement, but to take a proactive approach to monitoring third-party API communications and managing them all in one place. It's time to rethink the definition of API Security. Enterprises need to go beyond "shift left" with their own APIs. You as the CISO will need to lead the charge on communicating the importance of having visibility into the APIs the organization consumes. It's time to enable your security team to proactively manage third-party APIs, monitor the data in motion, identify legitimate vs illegitimate traffic, and quickly remediate issues as they arise—not months after a leak is made public.

We are so thankful for the warm welcome we received from the ISSA community and CEF attendees, and encourage CISOs and other security leaders to reach out to continue these conversations.

To learn more about Vorlon and proactive third-party API security, visit us at vorlonsecurity.com and request a demo.

- SPONSORED CONTENT -

Supplementary Segment

The Python Programming Language Numerical Analysis/Machine Learning Series: Dimensionality Issue - Processing ARFF Files

By: Constantinos Doskas, ISSA Member, North Virginia (NOVA) Chapter

This article is part of a series of articles which deals with topics in programming using the Python programming language. In previous articles we presented Python programs which use various Machine Learning Algorithms. We also started development of a program that associates ISP information with IP addresses.

In this article we will continue with a discussion of the Machine Learning dimensionality issue and its solutions.

DIMENSIONALITY ISSUE - PROCESSING ARFF FILES

To learn how to process multi-feature data we need to first acquire the data. We can find many public datasets on the internet for that purpose. Many of those come in a format called *arff*. Processing of datasets having this format was not presented yet in these series of articles. Therefore, I thought that it will be beneficial to you if I download and process one in this article. Also note that having the data on a local disk allows you to work offline.

The data must be normalized before it is processed by any ML algorithm. Most of that datasets that we have processed up to now were ML processing ready. Preparing the data is a science on its own. I selected a dataset which is preprocessed and ready for us to use. It is a very popular dataset and its name is MINST_784.

You can download this dataset from https://openml.org.

mnist_784

ID: 554 verified ARFF Public 2014-09-29 v.1

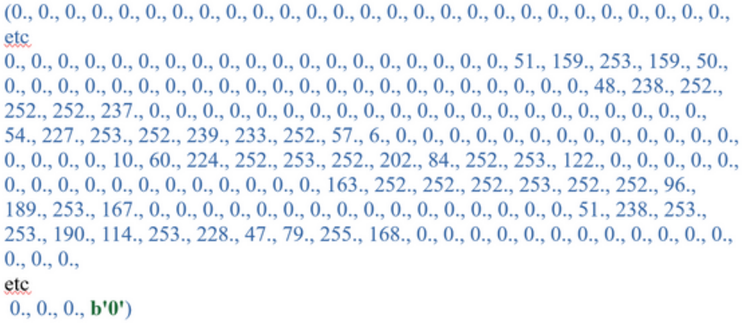
In my system I moved the dataset to the same directory where the python script is saved.

Script organization: The top area of the script contains all the needed imports from the appropriate modules. The next script area contains the functions which will do the processing. The last script area contains the *main()* function.

Dataset data examination: Find out how the data is organized. From the website we get the information that the dataset contains 70000 pixelated digits (0-9). There are 784 pixels per digit. Each pixel may have a value in the range of 0.(white) – 255.(black). The data that comprises each digit is in binary form and at the end of it there is the **value** of the digit in binary form also.

Example: Data of a zero digit.

Processing the data:



```
(0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
etc
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 51., 159., 253., 159., 50.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 48., 238., 252.,
252., 252., 237., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
54., 227., 253., 252., 239., 233., 252., 57., 6., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 10., 60., 224., 252., 253., 252., 202., 84., 252., 253., 122., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 163., 252., 252., 252., 253., 252., 252., 96.,
189., 253., 167., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 51., 238., 253.,
253., 190., 114., 253., 228., 47., 79., 255., 168., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0.,
etc
 0., 0., 0., b'0')
```

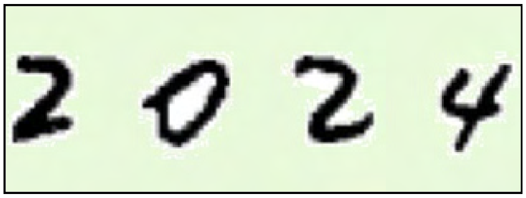
Processing the data:

The arff file is opened by a method which is contained in the module scipy (scipy.io.arff.loadarff()). The loadarff() method returns the data in two groups. The first group contains the data and the next contains the metadata. Once the data is loaded we must separate the binary data of the image of the digit from the data that gives us the **value** of the digit (ie **b'0'**). When this is done we have the X and y datasets which are needed to be used in Machine Learning. We are told that the data must be separated in 60000 digits for the training set and 10000 digits for the test set.

During the testing I found that the dataset contains the following counts per digit:

```
counts of
0 980, 1 1135, 2 1032, 3 1010, 4 982, 5 892, 6 958, 7 1028, 8
974, 9 1009
```

I also constructed a sequence of indexes which gave us the number 2024. This sequence is: Index list of 2024 [2101, 2106, 2108, 5104] The image which is produced by this sequence is:



Examining the digits in the picture above, we noticed that there is a big difference in the writing style between two 2s. The first 2 can be confused for 1 or 7.

CODE (Download from GitHub)
https://github.com/PYPROGII/MARJRL41423789BBN/blob/main/ipca_4article030424.zip

OUTPUT

We will not display here all the output because of limited space. Plenty of data in the output is just for examining the data before we develop the program. A couple of plots of sample images of the digits are also for this purpose.

Output on PYTHON SHELL:

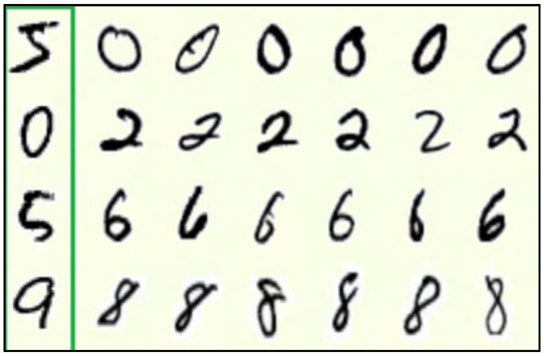
```
data, shape (70000,)
Selecting the second of the 70000 digits
data[1]
digit shape      ()
digit length     785
digit type       <class 'numpy.void'>
```

Discussion:

The data in the arff dataset contains **70000** images in binary pixel form. We select a digit data[1], to examine and we find out that the binary data of it is not in an array form. Therefore it has shape of **()** and type of class **'numpy.void'.** Also note that the length of data of each digit is **785.** We know that **784** is the actual length of the data that describes the digit. Therefore, **1** is the length of the data that contains the binary value of the digit. As we said in the beginning of the article, we need to separate these two. Note that we are converting the raw data to a *list* in order to process it; **d_list=*list*(element).** Then we can separate them; **d_list[:784]** gives us the **digit's data** and **d_list[784:]** gives us its **value**.

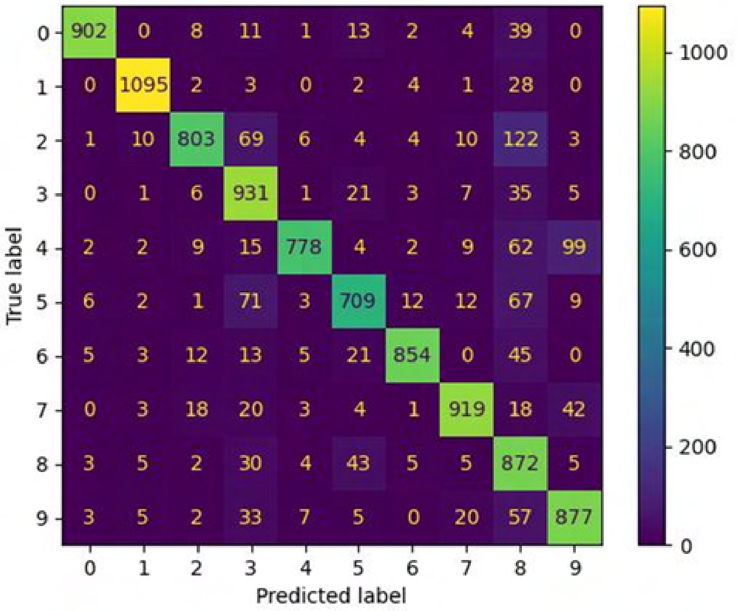
```
Prediction accuracy of test data: 0.874

Classification Report
             precision   recall   f1-score   support

       b'0'       0.98     0.92     0.95       980
       b'1'       0.97     0.96     0.97      1135
       b'2'       0.93     0.78     0.85      1032
       b'3'       0.78     0.92     0.84      1010
       b'4'       0.96     0.79     0.87       982
       b'5'       0.86     0.79     0.83       892
       b'6'       0.96     0.89     0.93       958
       b'7'       0.93     0.89     0.91      1028
       b'8'       0.65     0.90     0.75       974
       b'9'       0.84     0.87     0.86      1009

    accuracy                        0.87     10000
   macro avg      0.89     0.87     0.87      10000
weighted avg      0.89     0.87     0.88     10000
```

Output plots:



Discussion:

The first plot is the product of the vertical plot, which was produced by the function *plot_digits(),* and the combined horizontal plots that were produced by the function *horizontal_plots().* These 5 plots were manually stitched together. This final plot is provided for you to have a visual representation of handwritten digit style that exist in the arff file.

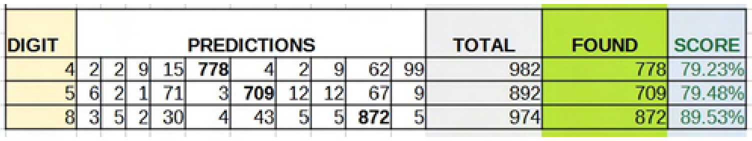


	0	1	2	3	4	5	6	7	8	9
0	902	0	8	11	1	13	2	4	39	0
1	0	1095	2	3	0	2	4	1	28	0
2	1	10	803	69	6	4	4	10	122	3
3	0	1	6	931	1	21	3	7	35	5
4	2	2	9	15	778	4	2	9	62	99
5	6	2	1	71	3	709	12	12	67	9
6	5	3	12	13	5	21	854	0	45	0
7	0	3	18	20	3	4	1	919	18	42
8	3	5	2	30	4	43	5	5	872	5
9	3	5	2	33	7	5	0	20	57	877

The second plot is the confusion matrix metric. In previous articles we had discussed extensively this metric and also the accuracy and classification reports. In the confusion matrix, the most accurate prediction is of the number **one**. With coordinates of (1,1) the result of 1095 is highlighted yellow. The color bar on the side of the plot goes from dark blue to light yellow and indicates the degree of accuracy of specific predictions.

The next picture is an example of how the confusion matrix calculates coloring.

IP INFO PROJECT



DIGIT	PREDICTIONS										TOTAL	FOUND	SCORE
4	2	2	9	15	**778**	4	2	9	62	99	982	778	79.23%
5	6	2	1	71	3	**709**	12	12	67	9	892	709	79.48%
8	3	5	2	30	4	43	5	5	**872**	5	974	872	89.53%

This project will be expanded in the next article. It is part of a series of how to collect, clean up, and process data.

WHAT IS IN THE NEXT ARTICLE

In the next article we will continue on ML algorithms and also update the IP info program which was started in the previous article. Keep all of these articles in your library because the code in each article assumes that you are already familiar with concepts previously posted. Please note that my email (cdoskas@megabizhost.com) is available for your comments. Use this email address if you have any questions related to specific topics of this article.

CONCLUSION

To conclude, this article presented code that is used to process a multi-feature dataset. The data was not flattened and as a result we had low accuracy. Some of the Python metrics were used to give us a picture of how the algorithm performed.

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

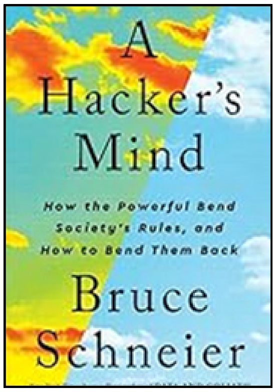
The Cyber Library

Reviewing the Works of Bruce Schneier and Michael G. McLaughlin & William Holstein

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

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.

I was a fanatical reader of science fiction in my youth and may have stopped too soon. Books like Douglas Adam's *The Hitchhiker's Guide to the Galaxy* (1997), seem to be formative influences for the movers and shakers in IT like Bruce Schneier, and they use them as communication shorthand. Expect a review in the future of that book, along with George Orwell's *1984,* another common reference. But on to this month's column:


A Hacker's Mind
How the Powerful Bend Society's Rules, and How to Bend Them Back
Bruce Schneier

Book #1:

Schneier, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Ben Them Back*. W.W. Norton & Company (2023).

Sound Bite: Fully understanding hacking as a concept will help us, particularly as AI becomes more pervasive.

Opinion on Primary Audience: World, but extremely valuable background for future CISOs.

If you are or aspire to be a CISO, read this book early in your journey. I often see writings that tell us technical people do not understand business. After this book, you will be stronger and smarter in your dealings with business leaders, and I can almost guarantee it!

I read twice all the books I review. I was especially glad of that technique when I read Bruce Schneier's new book. After the first read, I might have said "Well, bless his heart, the old master is fading. This is just a collection of his wandering thoughts on various topics; nothing new." How horribly wrong I would have been! First, Schneier hacks your reading habits. Most of you do not have an hour or more to read without any distractions. So he wrote a series of interesting story essays of only a few pages, and you can finish at least one chapter in a few minutes. Second, the value for cyber practitioners is in understanding the overall cognitive action of hacking. He says, "That's what a hack is: an actively allowed by the system that subverts the goal or intent of the system."

The Author

Bruce Schneier continues his excellence. Like other famous names in cybersecurity, hearing "Bruce Schneier" will stimulate the neurons of cybersecurity professionals. His credentials are mainly in his many books, and certainly, if you have an interest in cryptography, you have read at least some of his work. I have only read two of his books: *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,* and *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Currently an adjunct lecturer at Harvard, his academic credentials include a BS in physics and a master's degree in computer science.

The Metadata

A ***<u>2023</u>*** publishing date! The online ordering cost, including shipping, is under $15, about the same with an e-reader. The hardcover book is about 250 pages, plus notes pages. My local public library system has multiple copies, but an extensive 'hold' list.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the readability is high school level. There was about 15% passive voice in my sample. This article is about 2% passive voice.

Table of Contents (Just a few chapters listed with comments annotated in bold font (inside parenthesis) by me. Note: My comments are few, as the other chapter titles are self-explanatory)

Part 1 Hacking 101
1 What is Hacking **(Important to think broadly)**
4 The Hacking Life Cycle **(Eternal Blue)**

Part 2 Basics Hacks and Defenses **(Great stories you will enjoy - Good Hacks - Bad Hacks)**
11 Defending Against Hacks **('Hotfix' type of patching)**
14 The Economics of Defense **(Threat Modeling)**

Part 3 Hacking Financial Systems **(Current and Aspiring CISOs take note!)**
19 Hacking Computerized Financial Exchanges **(High Frequency Trading)**
25 Hacking and Wealth **(Private Equity)**

Part 4 Hacking Legal Systems
28 Hacking Bureaucracy **(Goodhart's Law)**

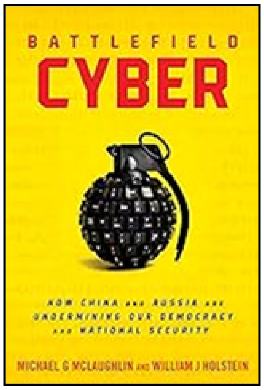
Part 5 Hacking Political Systems
37 Delegating and Delaying Legislation **(Japanese 'Ox Walking')**

Part 6 Hacking Cognitive Systems

Part 7 Hacking AI Systems
52 The **(AI)** Explainability Problem **(Possibly the most important chapter)**
56 When AIs Become Hackers **(AI in 'Capture the Flag')**
60 Governance Systems for Hacking **(His subtitles are: Speed, Inclusivity, transparency, Agility)**

Book #2:

McLaughlin, Michael G. and William Holstein. *Battlefield Cyber: How China and Russia Are Undermining Our Democracy and National Security.* Rowman & Littlefield (2023.)


BATTLEFIELD
CYBER
HOW CHINA AND RUSSIA ARE UNDERMINING OUR DEMOCRACY AND NATIONAL SECURITY
MICHAEL G MCLAUGHLIN AND WILLIAM J HOLSTEIN

Sound Bite: Through cyber, ruthless national governments with external power ambitions are well on the way to victories, and the rest of the world had better suit up and join forces in defense.

Opinion on Primary Audience: Democracies and their thought-leaders.

If I were to suggest an alternative title for this book, it would be Sun Tsu Goes Cyber. You have read The Art of War, right? For Battlefield Cyber, I saw a recommendation months ago on LinkedIn by Robert Metzger, a particularly important person in cyber and a senior attorney. I do not know Mr. Metzger personally, but I have followed his LinkedIn posts and heard him speak. I notice really smart people stop talking and listen to him, and even defer to his opinions.

Cyber threats are included in many recent books on hostile-to-democracies foreign governmental threats. One book you may see lauded is Seth G. Jones' *Three Dangerous Men: Russia. China, Iran, and The Rise of Irregular Warfare.* W.W. Norton & Company (2021). That is a fine book, but it only touches on the cyber threat. *Battlefield Cyber* is much more focused.

On the first read-through, I thought the book's solutions to the cyber threats from national governments were extremist. For example, the authors want a Cyber National Guard. Read the book twice, and you will see the reasonableness of the authors' recommendations.

The Author
Michael McLaughlin is a cyber attorney, with a strong background in US cyber counterintelligence. William Holstein is primarily a writer/journalist/editor, with an extremely strong background on China. Author of several books, he lived in Hong Kong and Beijing, where he was UPI bureau chief. This is a very experienced and knowledgeable team.

The Metadata
A ***2023*** publishing date! The online ordering cost, including shipping, is under $20. You cannot cut that cost much if you use an e-reader. The hardcover version is about 250 pages including notes. My public library has no copies.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style measurement is graduate school level, and my honest criticism is that level is unnecessarily harder for all potential readers. There was around 33% passive voice in my sample. This article is about 2% passive voice, for comparison.

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

Part I: We Are at War
1. Cyber Warfare: The Enemy Inside the Gates **(Stuxnet, NotPetya, and Gerasimov Doctrine histories, also U.S. Cyber Command and Hunt Forward Operations)**
2. Water and Oil: Weaponized Ransomware, Digital Proxies, and the Threat to Critical Infrastructure
3. Chinese Cyber Espionage: The Greatest Transfer of Wealth in History
4. The New Oil: Data and China's Digital Silk Road Strategy **(APTs)**
5. Stoking the Flames: How Malign Influence Exacerbates America's Political Divides and Ethnics Tensions **(More APTs)**
6. Software Meltdown: The Problem with Trust **(Apache Log4j and Solar Winds/Orion details) (Trivia Question: Who was Linus Torvalds?)**
7. Someone Else's Server: The Vulnerabilities of Cloud Computing
8. Stealing the War: Cyber Threats to America's Defense Supply Chain **(People's Liberation Army Unit 61398 successes)**

Part II: The Response: What Must Be Done
9. Retreat from Globalization: Easing Corporate America's Addiction to China **(Really important words - thought-provoking on 'reshoring' possibilities)**
10. Social Disorder: Reining in Social Media and Big Tech **(The 1996 Communications Decency Act Section 230)**
11. Re-Architecting Security: What the Private Sector Must Do **(About canary files - very cool!)**
12 Government Action: What the Public Secor Must Do
13 Collective Defense: How the Public and Private Sectors Must Work Together

Happy Reading!

PS - If you have a book you want me to read & review, please use the email address in my bio to let me know!

For next month's reviews,

Miller, Chris. Chip War: The Fight for the World's Critical Technology. Simon & Schuster (2022).

Sharp, Matthew K., and Kyriakos (Rock) Lambros. The CISO Evolution: Business Knowledge for Cybersecurity Executives. Wiley (2022).

Additional sources used in the article:

1. https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests
2. https://en.wikipedia.org/wk/Bruce_Schneier
3. LinkedIn profiles for authors listed, where available.
4. https://riverjournalonline.com/news/local-authors-local-books-william-holstein-the new-art-of-war/17569/. October 24, 2019.
5. https://en.wikipedia.org/wiki/The_Art_of_War

About the Author

William J. (Jay) Carson, ISSA Senior Member, ISSA 2020 Volunteer of the Year, and a past ISSA-Colorado Springs Executive Vice President. He is the part-time 'Cyber Librarian' of Semper Sec, LLC. Holding Security+ and CIPP/E certifications, he is a former high school

Cyber Executive Forum

The Cyber Executive Forum is a peer-to-peer opportunity for members to share concerns, successes, and feedback in a peer-only environment.

ISSA Cyber Executive Membership Program

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

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

Membership Benefits

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

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

ISSA JOURNAL

Find us on these socials

Information Systems Security Association (ISSA)

Information Systems Security Association International (ISSA Intl)

ISSA International (@ISSAINTL)

ISSA International (@issaintl)

Information Systems Security Association (ISSA)

NEWS FROM THE FOUNDATION

The Foundation is happy to announce that a new scholarship has just been added to our 2024 offerings. This year, The Docent Institute, a charitable non-profit educational institution based in Iowa, is sponsoring a $2,000 scholarship. To apply, please visit the ISSAEF website: www.issaef.org/apply

The mission of Docent is Technology outreach, inclusion, and STEM education for the betterment of society. Docent provides college scholarships, mentoring, apprenticeships/internships, career services and performs other public outreach related to cybersecurity education, advancing technology, and the ethical use of technology.

Donations to The Foundation's Scholarship fund were received last month from **J.P. Morgan Charitable Giving Fund,** a donor-advised fund **(DAF,)** courtesy of The Dona M. Rockstad Foundation and **American On-Line Giving Foundation** (by way of **Benevity**, one of the world's largest workplace on-line giving platforms).

Our sincerest **THANK YOU** for your generosity!

BECOME A VOLUNTEER!

The Foundation is seeking individuals to fill the following volunteer positions:

- **Director of Communications** to write short articles for the ISSA Journal and create social media posts to promote Foundation events and scholarship offerings.
- **Financial Auditor** to audit Foundation books. A CPA license is not required
- **Director of Communications.** Write news articles for the ISSA Journal and create posts for social media, i.e. LinkedIn, Facebook, etc.
- **Scholarship Committee Members.** Evaluate Scholarship applications and recommend awardees.

CPE's given for these positions. If interested in learning more, please email: Volunteer@issaef.org

What Our Members Say

ISSA members get a lot of real-world value from their memberships - from professional networking and peer support to educational and career development opportunities.

"My involvement in ISSA has opened up job opportunities and friendships that would have otherwise not existed. More specifically, I've been able to develop and sustain professional relationships that I can rely on going forward. In addition, serving as a chapter officer has helped strengthen my leadership skills, which in turn has made me more successful at my job."

William E. smith Jr. - Information Security Analyst, John Hopkins University Applied Physics Laboratory

There is still time for your Chapter to participate in this year's **Chapter Challenge Contest!** Hold a fundraising event to benefit the Foundation's scholarship fund. Contest ends on June 30th! More information can be found in the CCC Guide on the ISSAEF website. You can donate for your chapter by visiting: www.issaef.org/donate/CCC

Free Money!$!

Encourage any student you know to apply for a Foundation or Chapter scholarship or 1 of 3 Grants for Continuing Education!

- **E. Eugene Schultz Memorial** (Graduate) Scholarship $3,500
- **Howard Schmidt Memorial** (Undergraduate) Scholarship $3,500
- **Shon Harris (Women In Security)** Scholarship $2,000
- **General Scholarship -** $2,000

Alamo Chapter Scholarships

- **George "Chip" Meadows Memorial** Scholarship - 3 yr. San Antonio College or University $1,500
- **Alamo Women's Scholarship** - two awarded @ $1,000 per
- **Alamo Minority Scholarship** - 2-year San Antonio College $500

GRANTS OFFERED BY: **SANS, CSA & ACI Training**
Visit our website: ISSAEF.ORG/APPLY for details

Cyber Executive Forum

May Cyber Executive Forum 2024

Join us in San Francisco, CA, on May 4 and May 5 for the latest Cyber Executive Forum.

For more information, visit:

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

Chapter Spotlight

ISSA SOUTH FLORIDA'S BLUEPRINT FOR BUILDING A RESILIENT INFORMATION SECURITY COMMUITY

By: Yosi Attias, ISSA Member, FL South Florida Chapter

Nestled in the vibrant heart of South Florida, the ISSA South Florida Chapter stands as a unifying beacon in the realm of information security. Serving a dynamic community that stretches from Port St. Lucie to Miami and the Keys, our chapter boasts a diverse membership that includes lifetime members, general members, and students, each benefitting from tailored offerings. We are committed to fostering in-person connections along the coast and host meetings across Miami-Dade, Broward, and Palm Beach counties at esteemed institutions such as FIU, Nova University, Lynn University, and Palm Beach State college. Our pursuit of venues across counties highlights our dedication to enhancing member engagement.

At the heart of our chapter, our board, volunteers, and members are the driving force behind our vibrant community. We acknowledge various contributors across several categories. Among our board, we have long standing members who have helped the chapter earn its place as a community cornerstone. In addition, this year, we welcome four new board members and a new president, Yosi Attias, who steps into the role after serving as the director of membership in 2023.

In our spotlight, we have board member Michael Brown, a committed Fellow since 2004. Michael's progression through numerous leadership roles, combined with his impressive suite of 13 certifications, the latest being the GSNA from SANS, reflects his dedication to personal growth and the chapter's progress. Equally, from our general member segment, Luciano Nicolas Krigun, an expert from Microsoft's Corporate Red Team, recently enthralled us with his presentation on "DLL Sideloading & DLL Proxying" at our February meeting. His insights have earned him a spot at the CanSec West cybersecurity conference to present a cutting-edge Command-and-Control (C2) course.

Our monthly meetings, held every third Thursday, are not merely gatherings but forums for innovation, fostering a dynamic infosec community and enabling learning and networking. These sessions go beyond standard meetings, featuring stimulating talks, interactive exercises, and innovative formats like fireside chats and open discussions. The networking segment post-meeting is a vital aspect of our chapter, promoting relationships, collaboration, and support among members.

Our annual Hack the Flag event is a highlight, attracting hundreds of participants with a full-day agenda that engages the local community. Featuring a "capture the flag" competition and a chili cook-off, it fosters a communal atmosphere for members with varying interests in CTFs. Additionally, we offer a lock pick village and other activities, enhancing the event's appeal. The advanced CTF contest, curated by Rod Soto of Hack Miami, introduces challenges involving drones, robots, AI, web apps, and IoT. To include all skill levels, we've introduced a beginner-friendly version.

Beyond in-person events, we actively collaborate with other professional organizations, believing that partnership is vital to our community's lifeblood. Our alliances with notable local organizations like ISACA, ISC2, and OWASP South Florida are not just partnerships; they're affirmations of our shared goal to uplift the local infosec community, allowing us to host impactful joint events and initiatives.

South Florida Chapter
ISSA
Information Systems Security Association
When it comes to cybersecurity, being out of the loop is a dangerous place.
TLC

In a new venture, we're thrilled to announce a collaboration with recruitment and academic institutions, designed to offer mentorship opportunities, career services, internships, and recruitment prospects. This initiative aims to support career advancement and contribute to the broader information security landscape, underscoring our commitment to professional development and community support.

Additionally, we have the invaluable support of vendors, corporate partners, and local conferences and tradeshows, whose contributions are both integral and complementary to our mission. Their involvement not only enhances our chapter's initiatives but also fosters a collaborative environment that propels us towards our goals. We are enthusiastic about nurturing these partnerships and look forward to continued collaboration and mutual success.

In conclusion, our chapter is more than a collection of information security professionals; it's a thriving hub committed to providing valuable opportunities for learning, networking, and growth. Through our varied events, collaborative projects, and new initiatives, we invite our members to dive in, share their expertise, and dedicate their time. Whether you're joining our monthly meetings, participating in Hack the Flag, or engaging in career advancement activities, there's a space for you to learn, evolve, and make an impact. We encourage you to connect with our chapter and, if you're in the area, to join us; while our activities are region-specific, we welcome all interested parties to participate.

Board Member Spotlight

4 QUESTIONS FOR OUR COO BETTY BURKE

Interview By: Adam Boisselle, ISSA Member

With a career marked by positions of increasing responsibility and technical prowess, Betty Burke (currently serving on the ISSA International Board of Directors as the COO) has been at the forefront of information security planning, program development, and delivery. Her reputation precedes her as a decisive decision-maker and innovative problem solver, consistently achieving exceptional results while fostering effective team collaboration.

We had the privilege of sitting down with Betty, a powerhouse in the realm of Information Technology and Information Security. Boasting a rich history as the past President of the MN-ISSA chapter, Betty brings over two decades of expertise to the table. It was an honor to have her in the Woburn office, where we had the opportunity to chat about her career and what she hopes to see for ISSA in 2024.

Q: HOW LONG HAVE YOU BEEN WITH ISSA?

I have (unofficially) been a member since the early 2000s/late 90s; however, I became more involved starting in 2012. Since then, I've worked as the Marketing Director and President for the MN Chapter, now I am a Sr. Advisor for the chapter. In 2018, I was elected to the International Board and recently appointed to the COO role. I did three terms as the MN Chapter president; during that time, we increased membership from 130 to 270 by the end of my six years. It grew organically, because the programming was really good, the members were really engaged – there was a lot of interest!

Q: WHAT ARE SOME BENEFITS TO BEING A PART OF ISSA?

Benefits for anybody in cyber security, information technology, etc. is to just have your tribe, your people; you can network, grow your career, talk with likeminded individuals in the field. I recommend people get involved; don't just become a member, really get involved with your chapter and take on leadership roles with your local chapter or an International Committee. That adds so much value to your membership and personal growth. The number of people you meet by being involved goes up exponentially. Also, ISSA chapters provide a wide variety of educational programs, such as CISSP, CISA and other trainings. Other educational opportunities are the journal, several webinars every month and discounts to large conferences such as RSA. These are all learning opportunities; and if you have a current certification, attending any of these educational opportunities can earn you CPEs as well. Both the journal and the webinar are an opportunity to highlight your expertise by writing articles or by doing a presentation on a webinar. You get more value the more you get involved and partake in all these opportunities.

Q: AS COO, WHAT GOALS DO YOU HAVE FOR 2024?

I hope to be an advocate for the chapters and members. I want to ensure that continued partnership with the management team remains aligned with our overall goal to make ISSA as successful as we can. I'm looking forward to improving our programs, identifying every single value that a chapter or member gets out of ISSA, and really getting the word out there to drive membership and support our chapters. Every chapter has a story, and it would be great if we could get some more spotlights on the chapters.

Q: FROM YOUR PERSPECTIVE, WHAT IS THE PRIMARY MISSION OF ISSA, AND HOW DOES IT CONTRIBUTE TO THE CYBERSECURITY COMMUNITY?

The primary mission of ISSA is to be the community of choice for information security professionals. We provide networking opportunities, educational opportunities, and we talk about all areas of information security – cloud security, AI, anything that is new or buzzing, we talk about. We also discuss things that have been brought up in the past, but with fresh perspective. The fact that we don't have a test or certification is valuable because we support you in whatever journey you're going on. That's where you can get different perspectives from different people in different roles. Another area that we're working hard on, is the next generation of information security workers. We have the Apprenticeships, Internships, and Mentorships Program where we're really looking at how we can pull in those people who are changing careers into cyber security or reaching out to the upcoming workforce (kids in high school or college) and discussing how they can get internships or experience; that's the audience that we need to bring into information security, because there's such a shortage of information security professionals. So really tapping into that is another focus.

Translating Cyber Risk Into Broader Business Terms for Strategic Alignment and High-Level Resilience

As the cost of global cyber events rises and governments worldwide enact new cyber regulations, CISOs and cybersecurity leaders have been given an opportunity to take on greater leadership roles within the organization.

Indeed, with stakeholders beginning to understand the pivotal role cyber initiatives play in business resilience and growth, there is a pressing need for CISOs to translate the more complex aspects of cyber risk into a language that enables effective cross-collaboration.

Cyber risk quantification (CRQ) has consequently emerged as a powerful solution, transforming an organization's unique cyber risk landscape into event likelihoods and respective financial losses, equipping cybersecurity heads with the power to enhance strategic alignment with the C-suite and boardroom.

Communicating Cyber Risk to Key Executive Stakeholders

If CISOs and high-level executives speak in different professional languages, cybersecurity will never be appropriately factored into the broader business strategy, making the organization even more vulnerable to financial loss.

CRQ serves as a bridge between these parties, facilitating meaningful discussions in which non-technical stakeholders can tangibly comprehend the importance of cybersecurity measures.

Accustomed to evaluating business decisions in monetary terms, these executives will be able to visualize how much the organization stands to gain by investing in specific cyber initiatives. With its translation power, CRQ ensures cyber risk is discussed and accounted for in decision-making processes.

Prioritizing Initiatives, Justifying Investments, and Demonstrating ROI

CRQ quantifies the expected savings of a security control upgrade or structural change, equipping CISOs to prioritize investments accordingly. For example, they may decide to pursue an upgrade that reduces the organization's risk by $80 thousand rather than one that only reduces the risk by $30 thousand - information gleaned directly from the CRQ assessment.

On top of decreases in financial risk, the quantified data illuminates the ROI of security initiatives. While a certain upgrade may result in a significant risk reduction, if the cost of implementation outweighs this resulting figure, it may signal to the CISO that an alternative, more cost-effective mitigation strategy is necessary.

Ultimately, CRQ offers a means for CISOs to discuss finances and demonstrate that the cybersecurity program contributes to the economic success of the organization.

Enhancing Risk Governance and Compliance Practices

CRQ offers a simple approach for executives to discern the best policies for effectively managing cyber risk. With financial insights, key stakeholders can establish a data-driven risk appetite that realistically reflects the organization's risk landscape.

With metrics such as Average Annual Loss (AAL), CROs and budget-makers can make calculated governance decisions that facilitate broader objectives, such as investing more resources into the cybersecurity department to reduce the forecasted damage or increasing the capital reserve to ensure resiliency in the case of a cyber event.

Moreover, CRQ aids organizations in adhering to cybersecurity regulations. As governing bodies continue to require corporations to disclose processes for identifying and managing material risks and events, quantifying cyber risk becomes key, allowing CISOs and high-level stakeholders to establish benchmarks that signify materiality and streamline reporting.

Optimizing Cybersecurity Insurance Terms and Conditions

When the ROI of a potential security upgrade is revealed to be uneconomical, pursuing risk transfer is one of the most strategic alternative mitigation choices. However, due to limited historical data and global intelligence, initial cyber insurance terms are not always tailored to the organization's unique risk landscape.

Using CRQ, business leaders can compare the AAL to the overall insurance policy and quickly determine whether the proposed deductible truly offers a financial safety net. If the CRQ assessment illuminates that it is unlikely an organization's average loss will exceed the deductible, pursuing a lower deductible or limit amount may be the next logical step.

Because CRQ can also break down forecasted financial damage according to standard insurance loss scenarios, such as data theft, executives can strategically optimize the allocated insurance budget distribution.

Working together, CISOs, board members, and C-suite executives can leverage CRQ to achieve the terms and conditions optimal for cyber resilience.

Safeguarding the Organization

Securing an organization increasingly requires a holistic, collaborative approach that includes all high-level executives. By translating cyber risk into event likelihoods and financial losses, CRQ ensures that everyone can communicate effectively and develop data-driven action plans that incorporate cybersecurity and ensure high-end resiliency.

KOVRR
Cyber Decisions. Financially Quantified.

To learn more about CRQ and ensuring high-end organizational resilience, visit www.kovrr.com

- SPONSORED CONTENT -

Crypto Curmudgeon

CISSP Course on Social Media and Crypto

By: Robert Slade

Well, I've given you some idea of the CISSP review seminar that I'm doing in bits and pieces on social media. As noted, it's a bit of an experiment. I don't yet know how the experiment will come out. At the moment I'm just starting into telecommunications, which is going to take a whole. and then I've got operations, and law and investigation. So it'll be a while before this is finished.

A couple of observations, though. One relates to cryptography. I always enjoy cryptography, but somehow, doing this, cryptography gave me much more of a boost then is usually the case. I wondered why that was.

I rather suspect it is because... Well, I guess I have to go back a bit. One of the things that I don't like about information security, is that you're always thinking about the bad guys. You're always thinking about the enemy, and although we try to dress it up with terms like enemy, and adversary, and other means to make it look like this is about honorable warfare, the reality is that we are primarily dealing with fraudsters, liars, cheats, and rather disorganized organized crime. We fight not against principalities and powers, but against wretched little vermin, who are trying to make it fast buck, or are just trying to boost their own feelings about their wretched little lives, because their lives are so small, and are trying to do damage to anyone they can do damage to, in order to prove, to themselves if no one else, that they exist. It's not great having to constantly try to think like these people, and what they might be doing.

But cryptography is much cleaner than that. Oh yes, you have to think about the ways that different people might want to attack you, but you don't have to think as much about how they might attack, as whether, given what you have done in terms of protection, an attack is possible, and, if possible, how easy it is. Cryptography is a much more technical subject. You don't have to think about the enemy's motivation. Well, all right, you don't have to wonder whether this is some crypto freak with a copy of Helen Gaines' "Cryptanalysis," or a nation-state attack. But regardless of what who is doing it, the same question arises: is it possible to break the system, and, if it is possible, how hard would it be to do it? Cost and ability may come into it, but motivation doesn't. You don't have to think about the bad guys. It's a relief to be able to think about a relatively clean field, in the middle of a pretty much radically unclean field of information security.

And there's another question that arises from this experiment. I could be selling this. I'm not very good at selling, or marketing, and frankly, financing bores me stiff. But I could be selling this. CISSP review seminars are quite valuable. Not only do they get you a certificate which recruiters tend to pay attention to, and which might, indeed, automatically gets you a raise in pay even in your current job, but the jobs that you can get with the CISSP are generally higher paying, if you want to move on from wherever you are.

Yes, a CISSP review seminar is of some value, just all by itself. But I also love the fact that the CISSP covers all the fields of security. The material that you need to include in a CISSP review seminar can easily be used to structure a full-scale university course in information security, or even a full four-year Baccalaureate program. It's just a matter of how much detail you want to include, and how deeply you want to go into the more esoteric areas of the material.

So, why am I giving it away for free?

I suppose that, at my time of life, you start to think about giving back to the community. Frankly, I've never really thought in that regard. I mean, what's the community ever done for me? I did my own research, I produced my own material, and I got into the field because I already made some fairly significant contributions to it. So it's not as if I owe anything to the field of information security.

But I do, I suppose, owe something to society. And it's society that I'm thinking about in producing this material. Yes, I hope that I am helping educate the next generation of security workers, administrators, and professionals. I hope that what I am doing is of use to them, and of assistance to those who want to join their number. What I am really trying to do is to keep society safe. The world is a dangerous place. we seem to be intent on making it more dangerous. We have created the Internet, which is a wonderful thing, but which puts every person who uses it right next door to every hacker on the planet. (And pretty much every fraudster too.) We are building cars that drive themselves. And we're not too sure how those self-driving programs actually work. As far as I can tell, even with the occasional crashes that make the news, those self-driving cars are already driving better than we do, and it would probably be a good idea to mandate that nobody gets a license anymore, and that we all use self-driving software. It may be a saving of lives to do it. But we just don't know. The same can be set of artificial intelligence. Recently there have been some very entertaining developments, but they come at a cost in terms of our ability to determine the accuracy, truth, and integrity of any kind of data that we use the artificial intelligence to process.

We need, more than ever, people who can study information science, and who can ensure that it's safe for us. I hope that I am contributing to those who will work on this in the future.

About the Author

Robert Slade talks a lot. If you want, you can (virtually) accompany him on his daily walk (and prep for your CISSP exam) at https://fibrecookery.blogspot.com/2023/02/cissp-seminar-free.html
It is next to impossible to get him to take bio-writing seriously, but you can try at the-usual-suspect@outlook.com

Election Spotlight

2024 ISSA International Board of Director's Elections

ISSA Members, as your Executive Director, I want to alert you to an important event on the horizon: the upcoming elections for our International Board of Directors. This is a pivotal moment for our association, and your involvement is crucial.

The election period is fast approaching, and soon you will have the opportunity to help shape the future of ISSA by voting for your International Board of Directors. The individuals elected will play a key role in steering our association's direction, enhancing the cybersecurity profession, and supporting the growth and development of our members.

The contributions of the Board offer impact the course of ISSA, elevate the standards of our profession, and contribute to the evolution of global cybersecurity practices. The Board work alongside fellow members who are passionate about advancing our mission and upholding the values of integrity and excellence that define us.

Stay tuned for further announcements regarding the election timeline and details. When the time comes, please make your voice heard by voting in the election process. Together, we can continue to propel the excellence, leadership, and integrity we have come to trust in ISSA, the premier information security community.

Positions up for Election are as follows:

Secretary/Chief Operating Officer (COO) - 3-year term

The Director of Operations oversees and coordinates the activities of the various organization entities, especially the committees. This director is also responsible for monitoring the activity of headquarters' staff for compliance to direction by the Board of Directors.

Directors - 3 open seats; 3-year terms

Eligibility

For the role of Director, all candidates must be an experienced chapter leader, ISSA Fellow, or have comparable experience (per the ISSA By-Laws). all candidates for the role of Officer (President, Vice President, Secretary or Treasurer) must have previously served a full term as an Officer or Director on the ISSA International Board of Directors.

All candidates and campaign activities must follow the election policies.

Information on the responsibilities of the International Board of Directors can also be found in Article VI of the ISSA By-Laws.

Call for Nominations: 2024 ISSA International Board of Director's Elections

Serving on the International Board of Directors provides a unique opportunity to:

- Steer the course of ISSA
- Elevate the professionalism & impact of security practitioners
- Shape the future of the cybersecurity profession
- Cultivate your personal leadership abilities

Crypto Corner

The World Has Changed

By: Luther Martin, ISSA Member, Silicon Valley Chapter

As Galadriel said in the prologue to *The Fellowship of the Ring (2001)*, "The world has changed... for none now live who remember it." (This was actually said by Treebeard in the book version of *The Return of the King,* but I'd guess that future generations will generally attribute it to Galadriel). In the 36 or so years that I've been working on it, the information security industry has definitely changed. And as the people that I learned the business from gradually retire or die, it's definitely the case that few remember what the early days were like. Soon it will be true that none remember them.

In ancient Athens, Plutarch tells us ("The Life of Theseus," 23.1), there was a ship docked in the harbor that Theseus sailed on his legendary journey to fight the minotaur. Decaying parts of the ship were regularly replaced. Eventually nothing was left of the original ship, leaving philosophers to debate whether or not the ship in the harbor was really the one that Theseus sailed in. I've seen a similar thing happen to the information security industry, giving philosophers (perhaps one day including Vroomfondel and Majikthise) a great opportunity to debate whether or not we really have the same industry that we once had. I don't have a strong opinion on the provenance of the Ship of Theseus, but it definitely seems to me that the security industry today is entirely different from the one that I first knew so many years ago.

But enough about the past. What about the future? I suspect that there's an easy way to get an idea of what it will bring, at least in the area of IT and IT security.

Moore's Law tells us that the computing power of microprocessors tends to grow in a relatively predictable way over time, resulting in a somewhat predictable increase in processing power that a dollar will buy. Similar laws, for things like network bandwidth, storage, etc., also exist. It's probably reasonable to assume that the IT environment that we currently have (or perhaps endure) is some sort of optimal balance between the resources that these laws govern. (I like to think that CIOs enjoy doing complicated calculations using Lagrange multipliers for that when nobody's looking. I also know that they don't). But the growth rates for the cost of these resources differ. The data can be a bit fuzzy, so it's hard to get accurate values for these rates, but they seem to be fairly different.

So when we extrapolate to what we can expect to see in, say to the year 2050, we should expect to see a very different balance of IT resources being used then than we do now. It might be too early to start planning how to secure those future networks, but thinking about this might give you an idea of what technologies to start looking at to make sure that your skills will be relevant if you plan to be working at that time. If you're one of those people, getting good estimates for the different growth rates could be very useful.

And just like technology changes, the people designing, using, and supporting the technology are changing, and that will probably also affect what the IT environment of 2050 looks like. Back when I first got into information security, most of the work in the field seemed to be in cryptography, although a form of cryptography that almost seems charmingly naive by today's standards. And most people working in the field seemed to have academic backgrounds in either Mathematics or Electrical Engineering. Degrees in Computer Science essentially didn't exist back then. Degrees in Information Security or Cybersecurity definitely didn't exist.

And the users of the 2050 IT will largely be people who grew up with smartphones, social media, and whatever will come after those. Many of those people haven't even been born yet! But it's a good bet that their abilities and aptitudes will be much different from those from *two* generations before them. Like me. I don't know how they will be different. I don't think anyone else does, either.

But when I think of what the information security world will be like in 2050, I'm often reminded of what Tennyson said in Ulysses: "Though much is taken, much abides; and though / We are not now that strength which in old days / Moved earth and heaven, that which we are, we are, / One equal temper of heroic hearts, / Made weak by time and fate, but strong in will / To strive, to seek, to find, and not to yield."

Maybe it will be fine.

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.

Members in Remembrance

Mark Alan Freed

Chapter: USA: PA Delaware Valley

Member Since: 2012

Cyber Executive Member

June 25, 1964 - February 05, 2024

Mark Alan Freed, 59, of Franklin Township, Chester County, PA, passed away at home on Monday morning, February 5, 2024, after a three-year battle with colorectal cancer. He and his wife, Kimberly (Robbins) Freed, would have celebrated their 35th wedding anniversary on May 6th of this year.

Born July 25, 1964, in Sellersville, PA, he was the youngest of three sons born to John William "Bill" Freed, and Arlene (Keller) Freed. He was a 1982 graduate of Souderton High School.

Mark honorably served with the United States Marine Corps with 22 years of active service beginning in 1982, retiring in 2004 as a Master Gunnery Sergeant. He earned an MBA in Business from Averett University and a bachelor's degree in Computer Science from Park University; along with many professional certifications, he also earned certifications from the FBI Academy, for the CISO Academy for Information Security Leaders, and The Wharton School at the University of Pennsylvania, for the Wharton/ASIS Program for Security Executives.

Mark was a Vice President and Chief Information Security Officer at Corteva Agriscience. His responsibilities included Information Security, Cybersecurity, Operational Technology, and Infrastructure Services. He had over 35 years of information technology experience with the last 25 years focused on building and executing successful information and cybersecurity programs. Mark served on the Board of Directors for the Information Technology Information Sharing and Analysis Center (IT-ISAC). For the last 17 years, he also served as an Adjunct Associate Professor in support of the University of Maryland Global Campus (UMGC) online Cybersecurity Degree programs.

Mark was active with Cornerstone P.C.A. of Landenberg, PA. His hobbies included sailing, golf, and travel. He was an avid fan of all Philadelphia sports, but was especially loyal to the Philadelphia Eagles and Alabama college football. He cherished time with his family and his devoted pup, Skye.

In addition to his wife and parents, he is survived by two daughters, Jasmine Freed Smith and her husband, Matt, of Boalsburg, PA and Olivia Freed and her fiancé, Andrew Jordan, of Tuscaloosa, AL; and a son, Joshua freed of Oxford, U.K. He is also survived by two brothers, Keith Freed and his wife, Karen, and Timothy Freed and his wife, Jenny; as well as nieces and nephews.

Write-up copied over from:

https://www.tributearchive.com/obituaries/30673375/mark-alan-freed

Fred Piper

Chapter: ISSA International: Europe: UK

Lifetime Member, ISSA Hall of Fame, International Award Recipient

Professor Fred Piper sadly passed away on Monday 11th of March. Fred died of a rare neurological condition, called PSP, which impacted him for a number of years.

PSPA, which is the only charity in the UK supporting those with PSP, is making an urgent call for more research to be done into this brutal disease through their Research Appeal.

Fred made a vast and unparalleled contribution to the development of the information security profession and community.
He was the founding director of the Information Security Group [ISG] at Royal Holloway, which was the first university group established to focus on information security in the UK. In 1998 the ISG was deservedly awarded a Queen's Anniversary Prize in recognition of its work in the field of information security and Professor Piper was the inspiration and driver of that success.

He was there in 2006 as one of the founding fathers of the IISP (Institute of Information Security Professionals) as it was then, incorporating and the establishing the standards and processes needed to become a fully-fledged and respected organization. He was awarded the first Fellowship as a member of CIISec in 2016 and the first honorary Fellow in 2021. The Fred Piper Award was established by CIISec to recognize the Best Student Project in his honor.

He was a trustee at Bletchley Park for over a decade, and considered his role in helping to save Bletchley Park one of his proudest achievements.

Above all, he was a loving husband, father and grandfather who will be greatly missed.

In honor and celebration of Fred's incredible achievements throughout his life, please join us in supporting the PSPA Research Appeal. This seeks to improve diagnosis, ensure continuous standards of care, and launch trails into delaying degeneration, and improving life expectancy. Fred had shown symptoms of this condition for a number of years before a diagnosis was made, and had been incorrectly diagnosed initially.

Write-up copied over from:

https://fredpiper.muchloved.com/

Event Notes

ISSA EVENTS

April 16 - Privacy SIG: "Trust me – I'm an AI": Why explainable AI is important Webinar (1pm)

Moderated by Zachary Miller; Information Security Engineer for Kratos Defense Security Solutions, and speaker Frank Gearhart; Cybersecurity Architect for Kratos Defense, look at current AI technology, legal and ethical issues, why human-machine trust is necessary, and why it's not easy. Register for this insightful webinar at: https://www.issa.org/event/privacy-sig-trust-me-im-an-ai-why-explainable-ai-is-important/.

May 2 - Women in Tech: Delusion or Progress and What you can do about it Webinar (1pm)

Speaker Helene Shih joins this webinar to share some personal experiences in applying project management principles to a technical career planning and what you can do to track your own progress over time. Register for this fantastic webinar at: https://www.issa.org/event/wis-women-in-tech-delusion-or-progress-and-what-you-can-do-about-it/.

May 4-5 - May Cyber Executive Forum 2024

ISSA's Cyber Executive Forum is a quarterly gathering of some of the brightest minds in the cyber security world. Join us and other cyber security leaders at the Marines' Memorial Club & Hotel in San Francisco, CA, on May 4 and May 5 for the latest Cyber Executive Forum. Make sure to register for the event at: https://www.issa.org/event/may-cyber-executive-forum-2024/.

GLOBAL CHAPTER & MEETING EVENTS

Chicago Chapter

The May Chapter meeting will be 5/2/24 from 3:00 p.m. - 5:00 p.m. at Carlucci's in Rosemont, IL where the speakers will be Johnny Xmas (Martinellie), Co-Organizer of BurbSec and Lesley "Hacks for Pancakes" Carhart, Technical Director of Industrial Incident Response at Dragos.

Secure X - Training & Networking aboard the Odyssey will be 6/13/2024 and sponsorships are available.

Los Angeles Chapter

They are looking for volunteers and planners for their annual Security Summit and Women in Security Forum 9/26/24.

Middle Tennessee Chapter

Ashley Barton is the 2024 INFOSEC Sponsorship Director and is offering early bird discount to the Nashville INFOSEC 2024 Conference September 11 at Music City Convention Center. There will be the Annual Capture the Flag Event on that day.

Minnesota Chapter

The 19th annual Secure360 2024 Conference will take place on May 15-16 at Mystic Lake Center in Prior Lake, MN and is produced by the Upper Midwest Security Alliance (UMSA).

New England Chapter

There will be an in-person meeting on 5/20/24 from 10:00 a.m. - 3:00 p.m. at the Connors Center at Boston College in Dover, MA with the topic of "Developing and Connecting Cybersecurity Leaders Globally."

INDUSTRY EVENTS

April 16-19 - Black Hat Asia 2024

Held at Marina Bay Sands in Singapore, Black Hat Asia will be a Live, In-Person Event April 16-19, followed one week later by a Virtual Experience including recordings of all Briefings and Sponsored Sessions, available April 25. Register here: https://www.blackhat.com/asia-24/.

May 6-9 - RSA Conference 2024 San Francisco

In an ever-changing cybersecurity world, innovation and creativity are key. Join RSAC 2024 and discover The Art of Possible as we collectively create works that will change our perspective on what we can accomplish. Let's celebrate limitless opportunities, challenge the status quo, and explore new horizons together. Register here: https://www.rsaconference.com/events/2024-usa.

August 3-8 - Black Hat USA 2024

Now in its 27th year, Black Hat USA returns to the Mandalay Bay Convention Center in Las Vegas with a 6-day program. The event will open with four days of specialized cybersecurity Trainings (August 3-8), with courses for all skill levels. The two-day main conference (August 7-8) will feature more than 100 selected Briefings, dozens of open-source tool demos in Arsenal, a robust Business Hall, networking and social events, and much more. Register here: https://www.blackhat.com/us-24/.

November - Black Hat Middle East & Africa 2024

Black Hat Middle East and Africa is a leading cybersecurity conference and exhibition that takes place in Riyadh, KSA, welcoming over 40,000 infosec professionals, 300+ exhibitors and 300+ world renowned speakers from over 120 countries. Register here: https://blackhatmea.com/.

December 9-12 - Black Hay Europe 2024

Held at ExCeL London, United Kingdom. More details to come when available.

ISSA Strategic Goals

Goal A - Leadership

ISSA will lead the global security community collaboration to protect society from security threats.

Goal B - Program

ISSA will provide the profession with highly qualified practitioners and high-quality education and training.

Goal C - Influence

ISSA will serve as a respected and trusted source and advisor on information security-related technology, education, standards, and public policy.

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

United States

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

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