UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington Corporation and Health-ISAC, INC., a Florida Corporation,

Plaintiff,

v.

Joshua Ogundipe,

and

John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Civil Action No.

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

DECLARATION OF ERROL WEISS IN SUPPORT OF *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER

I, Errol Weiss, declare as follows:

1. I am the Chief Security Officer of the Health Information Sharing & Analysis Center ("Health-ISAC"), which is a Plaintiff in this action. I make this declaration in support of Plaintiffs' Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

2. I have been employed by Health-ISAC since April 2019. In my role at Health-ISAC, I created and staffed Health-ISAC's Threat Operations Center in Orlando, Florida, providing global health organizations with meaningful and actionable threat intelligence relevant for information technology and information security professionals in the healthcare sector. Health-ISAC is a non-profit industry organization that represents more than 1,000 member organizations

both in the United States and globally including hospitals, medical devices manufacturers, pharmaceutical manufacturers, insurers, and health IT organizations.

3. I began my career with the National Security Agency (NSA) conducting vulnerability analyses and penetrations of highly classified U.S. Government systems and then spent ten years with consulting firms delivering information security services such as managed security services, security product implementations and secure network designs for Fortune 100 companies. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

4. I have over 30 years of experience in Information Security. Prior to joining Health-ISAC, I was the Senior Vice President at Bank of America (2016-2019), overseeing the Global Information Security and Cyber Threat Intelligence teams. I worked with internal partners to protect information, customers and staff by reducing the impact from cyber threats. From 2006 to 2016, I led Citigroup's Cyber Intelligence Center, a global organization that provides actionable intelligence to thousands of end-users across the entire enterprise. In 2012, I testified as an expert witness before the U.S. House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises at the "Cyber Threats to Capital Markets and Corporate Accounts" hearing.

5. Since 2012, I have worked with Microsoft to disrupt criminal malware and botnets responsible for significant fraud losses impacting both healthcare and financial institutions and their customers, resulting in subsequent civil actions including successful disruptions of the malware families Zeus (2012), Citadel (2013) and Shylock (2014). Most recently, I was personally involved in Health-ISAC's efforts in connection with the successful disruption of the Cracked Cobalt Strike Operation in the Eastern District of New York in 2023.

I. OVERVIEW OF RACCOONO365 AND PHISHING

6. My declaration concerns RaccoonO365-branded phishing kits that are advertised and promoted as being able to circumvent the security features of Microsoft products, steal Microsoft 365 credentials and bypass multi-factor authentication. *See* Declaration of Jason Lyons in Support of Plaintiffs' Application for An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Lyons Decl.") ¶ 27. I received information from Microsoft in connection with its investigation of the RaccoonO365 Defendants. Based on that information, I understand RaccoonO365 Defendants have developed, sold, and facilitated the deployment of phishing kits that enable other cybercriminals to create and deploy phishing attacks with ease. The RaccoonO365 business model of selling phishing kits and services to cybercriminals is known as Phishing-as-a-Service ("PhaaS"). I understand that RaccoonO365 services are marketed through a private Telegram channel with over 800 users. *Id.* ¶ 32. *See also* Declaration of Nick Monaco in Support of Plaintiffs' Application for An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Monaco Decl.") ¶ 7. Threat actors have been able to leverage RaccoonO365-branded phishing kits and PhaaS subscription services to carry out credential theft, information exfiltration, and subsequent end-user terminal attacks.

7. Phishing attacks continue to be a major cybersecurity concern for Health-ISAC members and the broader health sector, with significant financial and operational consequences. Phishing schemes are a dominant attack vector in the healthcare sector, and they are involved in a significant percentage of cyberattacks. According to the IBM X-Force Threat Intelligence Index, phishing scams are the top infection vector in cyberattacks on healthcare organizations. This aligns with findings from the US Department of Health & Human Services,

Health Sector Cybersecurity Coordination Center (HC3), which highlights phishing as a "common tactic" used against the health sector. According to the Health Industry Cybersecurity Practices (HICP) guidelines, phishing simulations conducted in healthcare organizations often reveal click rates between 10% and 30% for employees who fall for phishing emails during tests. HICP noted that healthcare employees are particularly vulnerable to phishing due to the high volume of emails they receive daily and the urgency often associated with their work. This makes them more likely to click on malicious links or attachments. The average downtime for a healthcare company successfully attacked by a cybercriminal is 19 days—during which time patient care can be severely impacted through canceled surgeries, diverted ambulances, and compromised medical records. The average cost of ransomware in the healthcare sector is staggering, reflecting both the financial and operational toll these attacks impose. Here's a breakdown of the key figures:

- **Average Ransom Payment**: Healthcare organizations paid an average ransom of **$2.57 million** in 2024, according to the HIPAA Journal.
- **Recovery Costs (Excluding Ransom Payments)**: The average cost to recover from a ransomware attack in 2025 (excluding ransom payments) was **$1.53 million,** as reported by Sophos. This figure includes downtime, personnel time, device costs, network costs, and lost opportunities. For larger healthcare organizations with 1,000–5,000 employees, recovery costs can exceed **$1.83 million**.
- **Total Costs (Including Ransom Payments)**: When factoring in both ransom payments and recovery costs, the financial burden becomes even more severe. For example, in 2024, the average total cost of a ransomware attack on a healthcare organization was estimated at **$4.4 million**, with downtime alone costing up to **$900,000** per incident.

- **High-Profile Example**: The 2024 ransomware attack on Change Healthcare serves as a stark example of the potential financial impact. This attack exposed the personal health information of 190 million people and left numerous medical facilities unable to process claims or receive payments. The estimated direct costs associated with this attack reached **$1.15 billion**.

8. The RaccoonO365-branded phishing kits make hospitals and other healthcare organizations vulnerable to ransomware attacks and the costs associated with defending against and remediating them.

9. Based on Microsoft's investigation, I understand that RaccoonO365 Defendants sell their phishing kits on a subscription basis making these phishing kits a low-cost, and potentially high-reward opportunity for cybercriminals. And because these kits are not designed for one-time use, they can be used repeatedly during the duration of the subscription. For several hundred dollars, a cybercriminal can launch thousands of phishing attacks against healthcare companies.

II. MY INVESTIGATION INTO RACCOONO365

10. I investigated the impact that the RaccoonO365 Defendants and the phishing kits they sell have on the healthcare industry. I received threat intelligence data from the Microsoft DCU investigators regarding victim information that they had collected in connection with their investigation. The victim information included identification of Health-ISAC member organizations where DCU had observed phishing activity that was traced to a RaccoonO365 phishing kit. Microsoft provided me with information that at least 17 health sector organizations, of which, nine are members of Health-ISAC, were hit by RaccoonO365 phishing kits. Using information from Microsoft about the characteristics of the RaccoonO365 phishing kit emails and

the community of Health-ISAC members I regularly work with, I was able to identify eight additional victim organizations that were targeted by the RaccoonO365 phishing email scam campaigns. In total, I am aware of 25 health sector organizations impacted by RaccoonO365 phishing emails.

11. Microsoft does not have the ability to see the downstream effects of the observed phishing activity. For example, Microsoft cannot determine if a recipient of a phishing email opened the email, clicked on a link, or downloaded an attachment. Using the information from Microsoft that identified the victim member organizations, I investigated and verified whether anyone had opened the RaccoonO365 phishing email and clicked on the weaponized links or attachments, whether the attack resulted in credential theft or intrusion into the accounts, and whether the victim organization was subject to a ransomware or malware attack. I was able to obtain further information concerning the downstream effects of a RaccoonO365 phish for nine of the health sector organizations that were identified by Microsoft and Health-ISAC, as detailed above.

12. I have verified that phishing emails directed at Health-ISAC member organizations have been opened, and the recipients interacted with the phishing email and links or documents attached to the phishing email. For example, I have confirmed that two entities identified by Microsoft received phishing emails attributable to RaccoonO365, but the organizations successfully blocked delivery of the emails to the recipients. In two other instances, I confirmed through my investigation that the RaccoonO365 phishing email was delivered and opened by the recipients, who then clicked the malicious links contained in the phishing email. The organization successfully blocked access to the RaccoonO365-controlled website. My investigation revealed that the RaccoonO365 phishing emails were delivered and opened by the recipients of five other

member organizations. The recipients clicked on the RaccoonO365-controlled links and entered their credentials into the RaccoonO365-controlled website. The Health-ISAC member organizations detected this activity and were able to successfully reset the credentials before further malicious activity could occur.

13. From my investigation, I determined that of the 9 member organizations for which I was able to verify Microsoft's data, 5 organizations were successfully phished with a total of 10 internal staff members providing their username / password credentials on RaccoonO365-controlled websites. Those organizations detected the incidents and responded appropriately by resetting each individual employee's credentials. Based on my 30 years of information security experiences, on average, I estimate that each individual that gave up their credentials, the member organization had to expend four hours of incident response time, including time from the response team, investigators, systems administrators, human resources (HR), company managers and individual employees. To date, and as a result of RaccoonO365 Defendants' cybercriminal activities, Health-ISAC member organizations have incurred at least $12,000 in damages. Health-ISAC had incurred at least $ 38,000 in connection with its investigation and remediation.

III. PHISHING ATTRIBUTED TO RACCOONO365 WILL LIKELY ESCALATE TO OTHER CYBERCRIME

14. In general, ransomware is a form of malicious software (malware) designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Because a ransomware attack on a hospital can result in delayed medical procedures, disruption of life-saving surgeries, or taking the entire system offline, the consequences of these attacks can have devastating consequences and endanger people's lives.

15. Health-ISAC has been tracking ransomware attacks since 2020 and has identified

over 25,000 incidents impacting all critical infrastructures listed in our database (as of July 2025). Of these, 1,651 attacks, or 6.6%, were in the health sector.

16. For the first half of 2025, Health-ISAC observed 4,159 ransomware cases and 281 in the health sector. At this rate, we're on track for the 2025 totals to surpass what we saw in all of 2024. Today's modern-day hospitals require a complex set of integrated IT systems to function. From July 2023 through June 2024, nearly 400 U.S.-based healthcare institutions were successfully hit by ransomware. When hospitals get attacked by ransomware, critical IT systems become unavailable and hospital services decline rapidly.

17. In my experiences as Health-ISAC's Chief Security Officer since 2019, I am aware of the consequences of ransomware attacks on healthcare companies such as hospitals. I have personally investigated ransomware attacks that have caused the following harm:

- Ambulances forced to divert from hospitals;
- Delays in providing emergency patient services, delays or cancellation of providing treatments for cancer patients, delays in receiving lab results, delays in scheduling appointments;
- Hospitals forced to cancel elective procedures;
- Electronic Health Record systems being taken offline, which prevent hospitals, doctors, and providers from accessing any portion of the patient's electronic file.
- Malware and ransomware attacks that have crippled IT systems and have led to the breach of sensitive health information; and
- Financial losses, including ransom payments to cybercriminals, legal fees, and regulatory fines.

18. Although I have observed attacks from the Raccoon 0365 Defendants on Health

ISAC members, I have not yet observed ransomware or malware attacks that can be directly linked or attributed to the RaccoonO365 kit. That does not mean that there is no risk of such attacks. Given that 5 of 9 of the member organizations I investigated, acknowledged that the phishing attacks had induced personnel to provide their username and password credentials to the RaccoonO365 phishing sites, it is my opinion that this phishing kit has succeeded and that those organizations thwarted further harm. It is inevitable that allowed to continue the RaccoonO365 Defendants will continue their attacks and ultimately launch ransomware and other malware.

19. Additionally, according to DCU's investigation, RaccoonO365 first emerged in July 2024 and has been expanding their cybercriminal operations since. Successful phishing attacks are a precursor to ransomware and malware attacks. Once the cybercriminal has successfully intruded into the system (such as when a Health-ISAC member organization's employee interacts with the link contained in the phishing email), it is not a question of if there will be subsequent attacks, it is a question of when. It is very common for cybercriminals to escalate from phishing to more crippling forms of cybercrime. Phishing attacks are a critical precursor to ransomware attacks in healthcare organizations because threat actors, like RaccoonO365 Defendants, exploit human vulnerabilities to gain initial access to systems, which attackers can then leverage to deploy ransomware payloads.

20. I understand that last year, Microsoft filed an action against a similar cybercriminal organization that also sold phishing kits, the Fake ONNX Defendants. Although Health-ISAC was not involved with this action, I am familiar with Microsoft's takedown of the Fake ONNX Defendants. *See Microsoft Corporation and LF Projects LLC v. Abanoub Nady and John Does 1-4*, Civil Action No. 1:24-cv-2013-RDA (E.D. Va. Nov. 12, 2024). According to Microsoft, Fake ONNX Defendants started with phishing and business email compromise before escalating to

malware and ransomware attacks. Lyons Decl. ¶¶ 11-12. Additionally, DCU investigators have concluded that there are many operational and technical similarities between Fake ONNX and RaccoonO365 Defendants and the phishing kits sold. *Id.* Accordingly, I believe that unless RaccoonO365 is stopped, consistent with the relief requested in Plaintiffs' Temporary Restraining Order, RaccoonO365 Defendants will succeed in their attacks.

IV. MALWARE AND RANSOMWARE ATTACKS CAUSE FURTHER IRREPARABLE HARM

21. RaccoonO365-branded phishing kits harm the brand reputation of Health-ISAC's member organizations. For example, given that RaccoonO365 kits offers the ability to customize the phishing kits to target specific victims, the emails that RaccoonO365 Defendants send to Health-ISAC members are customized to appear as legitimate communications from or concerning the Health-ISAC member organization. Because Health-ISAC member organizations are under attack, they are forced to expend tremendous resources to defend themselves. When member organizations are attacked, their brand and reputation are irreparably harmed when patients are no longer able to rely on their healthcare providers, including calling into question the trust, safety and security of patient data and the healthcare network system as a whole.

22. As a result of Defendants' attacks, Health-ISAC's member organizations have experienced harm to their brand and reputation. Given the amount of publicity that attacks on healthcare organizations receive, this reputational harm is significant. Additionally, member organizations that are victims of attack face a loss of goodwill, members of the public incorrectly attributing the source of the emails to the member organizations (rather than attributing the harms to the malicious actors who are deploying RaccoonO365-branded phishing kits).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 25th day of August, 2025, in New York, New York.

Errol S. Weiss

EXHIBIT 1

Errol S. Weiss

Summary

Accomplished information security executive recognized internationally in the healthcare and financial services sectors as a visionary and a leader in threat intelligence operations and management. Proven ability to build information security strategies aligned to business risk and corporate goals.

PROFESSIONAL EXPERIENCE

Health Information Sharing & Analysis Center (Health-ISAC) April 2019 to Present
Chief Security Officer, Orlando, FL

Part of the senior leadership team setting direction, strategy and oversight for the entire Health-ISAC organization. Responsible for the strategic vision and direction of Health-ISAC's day-to-day Cyber and Physical Security Services offered to Health-ISAC member organizations. Managing the delivery of Cyber and Physical Threat Intelligence and oversight of the Health-ISAC Threat Operations Center functions and staff in the United States and Europe. Providing direction and leadership for identity services, community exercises and other special interest services for the Health-ISAC membership.

Bank of America, Global Information Security, Senior Vice President May 2016 to April 2019

5/2016 – 10/2017: **Director, Cyber Threat Intelligence**, Developed the strategy and vision to create a world-class cyber threat intelligence function. Established a new organizational structure to support the intelligence management lifecycle (requirements, collection, analysis, dissemination and feedback) and recruited diverse top talent into key leadership positions. Created new services and intelligence products, increased outreach and internal partnerships, established 24x7 follow-the-sun analyst coverage, rolled out a new mobile app intelligence monitoring service and began implementing a responsible vulnerability disclosure program. Enhanced the collaboration and partnerships between the firm and public sector entities including US Treasury, US Secret Service, DHS and FBI.

11/2017 – 4/2019: **Business Process Cyber Assessments Executive**, Responsible for end-to-end assessments of critical applications across the Bank of America enterprise. Leading business process assessments of critical systems focusing on cyber risks from people, processes, technology and third parties. Manage teams of assessors conducting reviews on an on-going basis.

Citi September 2006 to April 2016
Cyber Intelligence Center Director, New York, NY

Identified the need and obtained senior management support to create an intelligence collection and analysis center. Successfully built and grew a world-class Cyber Intelligence Center focused on providing actionable intelligence of threats against the financial services sector and those specifically targeting Citi employees, assets, business operations and technology infrastructure worldwide. Established intelligence management processes, implementing them in an on-line platform supported by analysts in strategic global locations to support a 24x7 follow-the-sun model. Formulated interaction models with key parts of Citi including fraud risk management, incident management, information security, threat management, physical security, investigations and business operations. Accountable for organizational plans and managing a staff of 40 in seven global locations. Provided mentoring, completed performance reviews, managed budgets and influenced change to global policies and procedures. Reported directly to Citi's Chief Information Security Officer and Global Head of Information Security. Presented at several FS-ISAC Conferences and met with peer financial institutions to share concepts about the intelligence management functions and helped others build their own intelligence capabilities.

Member of Citi's Information Security Risk Operating Committee, responsible for setting enterprise information security policy, reviewing operational metrics and performance and interaction with regulators globally including the Federal Reserve Board and the Office of the Comptroller of the Currency (OCC) in the US and the Monetary Authority of Singapore in Asia.

Interacted regularly and promoted information sharing and cyber security with top level management at other financial institutions, US Congressional Leaders and their staff, US Government organizations, US Intelligence Community, senior officials and regulators from foreign governments, and third-party providers. Partnered with private banking and institutional investment staff to present regularly to high net worth individuals and commercial institutions about staying safe on-line and providing simple advice to them stay secure on-line.

SAIC **February 2004 to September 2006**
Assistant Vice President, Managing Director, Reston, VA
Division manager for 20 staff including two operations managers and a chief scientist. Responsible for daily operations and customer relationships for the Information Sharing and Analysis Center (ISAC) and Open Source Monitoring (OSM) services. Provided cyber and physical vulnerability, threat and incident information to more than 1,800 financial institutions predominantly in the United States and customized consultative threat intelligence to large international corporations.

Responsible for personnel management, profit and loss management, financial planning, new sales, service delivery and service quality. Held frequent interactions with customers, including the FS-ISAC Executive Director and the Board of Directors. Actively participated in monthly board meetings, bi-annual membership meetings and membership campaigns. Improved service quality through feature enhancements, partnerships and oversight of operations.

Led the selection and transition teams responsible for migrating ISAC operations to another service provider. Worked closely with the new management and operations teams to ensure a smooth, seamless transition and complete customer satisfaction.

Solutionary, Inc. **August 2002 to January 2004**
Vice President of Technical Services, McLean, VA
Managed the professional services organization for a security services provider based in Omaha, Nebraska. Areas of responsibility included oversight of project management, information security services delivery and sales engineering for services such as Risk Assessments, Visa CISP Certifications, Secure Network Designs, Security Product Implementations, Managed Security Services, Incident Response and Penetration Testing. Provided senior technical leadership and consulting support for information protection and assurance programs to clients in the finance, banking and insurance areas. Responsible for business development with key named accounts.

Predictive Systems, Global Integrity and SAIC (Northern Virginia) **May 1996 to July 2002**
Global Integrity was a wholly owned SAIC subsidiary. Predictive Systems acquired Global Integrity in 2000.

12/2000 – 7/2002: **Vice President Services Strategy.** CTO of managed services unit responsible for product management and services strategy including managed firewall, managed intrusion detection, information sharing, Open Source Intelligence, managed vulnerability assessments, and Incident Response / Digital Forensic services. Collaborated with engineering, operations, business development and sales organizations to establish a suite of packaged services that could be implemented and delivered with high value. Responsible for establishing and maintaining relationships with security product vendors and resellers strategic to future growth plans.

8/1998 – 12/2000: **Vice President and Division Manager**, Managed Security Services. Created the vision and implemented a new Security Operations Center to provide remote monitoring and management of firewalls and intrusion detection systems. Recruited staff and provided key leadership. Performed business development operations support for the entire operation and achieved more than $2 Million in revenue. Established several key reseller and channel marketing opportunities. Recognized by management team as a key individual contributing to the success of Global Integrity.

5/1996 – 8/1998: **Division Manager**, Information Protection Operations, Responsible for division management of a $4.6 million business and for the supervision of over 30 employees. The division had four major information security programs, including computer and network vulnerability assessments for Fortune-100 clients.

Computer Sciences Corporation (CSC) **November 1995 to May 1996**
Senior Member Advisory Staff, Hanover, MD
Directed computer and network penetration efforts for US Government and commercial customers. Task area leader for INFOSEC Technical Services. Conducted marketing activities, wrote white papers, formulated a vulnerability assessment methodology. Lead author on several commercial INFOSEC proposals that resulted in $1 million in new business.

National Security Agency (NSA) **August 1987 to November 1995,**

12/1993 - 11/1995: **Senior Network Security Analyst**. Technical team leader on network security analysis and evaluation projects for the Systems and Network Attack Center. Provided technical guidance to evaluation team analysts and to end-users. Performed network vulnerability assessments and penetration testing on classified US Government networks and assessed the ability of insiders and outsiders to penetrate network systems. Conducted research on vulnerabilities of operating systems, hardware platforms, software applications and network protocols. Authored detailed technical reports on system vulnerabilities and appropriate countermeasures and provided INFOSEC engineering support to end-users.

8/1987 - 12/1993: **Computer Engineer and System Development Manager**. Provided system level developmental support for a major intelligence production system. Studied secure computing architectures and coordinated strategic plans for the transition of operational systems to implement a secure computing infrastructure. Developed system security requirements and specifications for an advanced intelligence processing system.

AFFILIATIONS and PROFESSIONAL MEMBERSHIPS

Singapore Healthcare Cybersecurity Advisory Panel **October 2019 to October 2024**
Appointed by Singapore's Ministry of Health to represent the Health-ISAC and U.S. perspectives on the evolving threat landcape, best practices and current and future cybersecurity initiatves for Singapore's healthcare sector.

Board of Directors, Financial Services ISAC **March 2010 to April 2016**
Board of Directors, Financial Services Information Sharing & Analysis Center (FS-ISAC). Non-profit organization owned and operated by the banking and finance sector and led by a Board of Directors of senior executives and security professionals from the world's top financial institutions. Delivered strategic direction for mission and purpose, ensured effective organizational planning, provided resources for key activities, determined and monitored programs / services offered to the membership and enhanced the organization's public image. Served as Vice-Chairman, Board of Directors (2016).

Key accomplishments include:

- Following a sharp rise in fraud, created the Account Takeover Task Force in 2010 and led it for two years. The task force was made up of over 120 individuals from thirty- five financial services firms, ten industry associations and processors and representatives from seven government agencies. The task force developed best practices focused on prevention, detection and responsiveness to ensure an improved and effective defense against cyber crimes, including account takeover. The task force created surveys and collected actual fraud loss figures from hundreds of financial institutions to create a baseline that could later be used to demonstrate the effectiveness of industry efforts (like this task force) to reduce fraud.
- In 2012, championed the partnership between FS-ISAC and Microsoft to work together on disrupting criminal malware and botnets responsible for significant fraud losses impacting financial institutions and their customers. Personally led the finance sector efforts and coordination of legal,

technical and public relation strategies for three subsequent civil actions including Zeus (2012), Citadel (2013) and Shylock (2014).

FCC CSRIC Appointed Member May 2013 to May 2015
Appointed member to represent the financial services sector on the Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council (CSRIC).

Advisor to Board of Directors, Financial Services ISAC February 2006 to March 2010
Appointed as Advisor to Board of Directors, Financial Services Information Sharing & Analysis Center (FS-ISAC). Provided guidance on business processes, operational improvements and marketing support to the Board of Directors.

EDUCATION

Johns Hopkins University, MS, Technical Management with a focus in Organization Management
Bucknell University, BS Engineering, Computer Engineering with a minor in American Literature

PATENTS

Co-Inventor (patent 6,807,569, issued October 19, 2004) for "Trusted and anonymous system and method for sharing threat data to industry assets"

PUBLICATIONS

Network Forensics & Analysis Tools, **cover story** for Information Security Magazine, February 2002.

A Case Study: Penetration Testing, National Computer Security Center / National Institute of Standards and Technology Conference Proceedings, October 1996.
http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper045/nissc.pdf

EXPERT TESTIMONY

June 1, 2012, testified before the House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises at the "Cyber Threats to Capital Markets and Corporate Accounts" hearing. http://financialservices.house.gov/Calendar/EventSingle.aspx?EventID=296813
Video Archive: https://www.c-span.org/video/?306361-1/cyberthreats-us-financial-industry

2024 Speaking Engagements

- Feb 21, 2024 - Podcast - What Keeps Healthcare CISOs Up at Night? | A Conversation with Michael Bray and Errol Weiss | Cy Beat Podcast With Deb Radcliff
    - https://cy-beat-podcast.simplecast.com/episodes/what-keeps-healthcare-cisos-up-at-night-a-conversation-with-michael-bray-and-errol-weiss-cy-beat-podcast-with-deb-radcliff-COOkmylv?utm_source=itspmagazine&utm_medium=web
- March Health-ISAC APAC Summit, Melbourne, Australia (March 20-21, 2024)
    - Health-ISAC Partners with Microsoft to Disrupt Ransomware Botnet
    - Information Sharing: Where do I start and how do I get the approval to do this?
    - CISO Panel
- Healthcare Innovation Summit, Tysons Corner, VA, May 2
    - https://www.hisummits.com/capital_area_summit_2024/Agenda2
    - Cyber Corner: What All Healthcare Leaders Must Know About Cybersecurity in 2024 and Beyond
    - Fireside Chat with Health-ISAC
- Google Breakfast at RSA Conference, May 7
    - Accelerating Resilience: Industry Strategies and Information Sharing
    - https://rsvp.withgoogle.com/events/accelerating-resilience-industry-strategies-and-information-sharing
- Cyberse - May 8, RSA Early Stage Expo
    - https://www.rsaconference.com/usa/expo-and-sponsors/early-stage-expo
- Spring Americas Health-ISAC Summit, Orlando FL May 23 -- CISO Panel

- Invited Speaker - White House Roundtable Discussion on cybersecurity and the healthcare sector, May 29, Washington, DC
- May 30 - DataConnectors Healthcare & Pharma Virtual Cybersecurity Summit
  - Keynote Speaker: Sorry, The Bad News Just Gets Worse.... 2024 Outlook of Cyberthreats in Healthcare
  - https://www.engagez.net/DC-HC2024?skin=new&snc=1810216#~lct=lobby
- CHIACON 6/12/2024, Palm Spring, CA
  - https://californiahia.org/page/chiacon
  - Session Title: The Healthcare Cyberthreat Landscape & Staying Safe On-Line
- ISMG - NYC July 18
  - Panel - Strengthening Healthcare Security: Advanced Supply Chain Risk Mitigation Strategies
  - Hugo Lai, CISO, Temple University Health System
  - Errol Weiss, CSO, Health-ISAC
  - Christopher Frenz, AVP of IT Security, Mount Sinai South Nassau
  - John Banghart, Senior Director for Cybersecurity Services, Venable LLP
  - https://ismg.events/summit/healthcare-2024/#agenda-engsingle
- Probely - September 10
  - HEALTHTECH WEBINAR:
  - Unveiling Hidden APIs and Securing Vulnerabilities in the Healthcare Sector
  - https://meet.probely.com/webinar-unveiling-hidden-apis-and-securing-vulnerabilities-in-healthcare
- mWISE Conference, Denver (Google/Mandiant), Sept 19
  - Panel: Building Resilience: Healthcare Industry
  - https://mwise.mandiant.com/conf24/session/2321435/building-resilience-healthcare-industry
- Microsoft - The Microsoft Threat Intelligence Briefing: Healthcare, October 2024
  - https://www.microsoft.com/en-us/security/security-insider/emerging-threats/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks
- Health-ISAC European Summit, Athens, Greece, Oct 17, 2024, CISO Panel
- AHIMA Conference: Current and Emerging Cyber Security Threats in Healthcare, Plus Staying Safe Online, October 28, Salt Lake City, UT
  - https://www.ahima.org/news-publications/press-room-press-releases/2024-press-releases/ahima24-to-address-current-and-emerging-cybersecurity-threats-in-healthcare/
- Cyware Innovation Summit, McLean VA November 20, 2024
  - Keynote Talk: The Community of Communities
  - Breaking the Barriers to Information Sharing
- Booz Allen Executive Threat Briefing & Insights Event - Dinner Speaker, Nov 21, 2024, Washington DC
- Health-ISAC Fall Americas Summit, CISO Panel, Dec 5 (Phoenix, AZ)

SECURITY CLEARANCES

2009 – Present: Active TS-SCI through U.S. Department of Homeland Security's Private Sector Clearance Program