SUMMER 2024

CyberEd MAGAZINE

COVER STORY INTERVIEW

Mitigating Risks Linked to Human Behavior

A Closer Look at Human Risk Management

PAGE 15

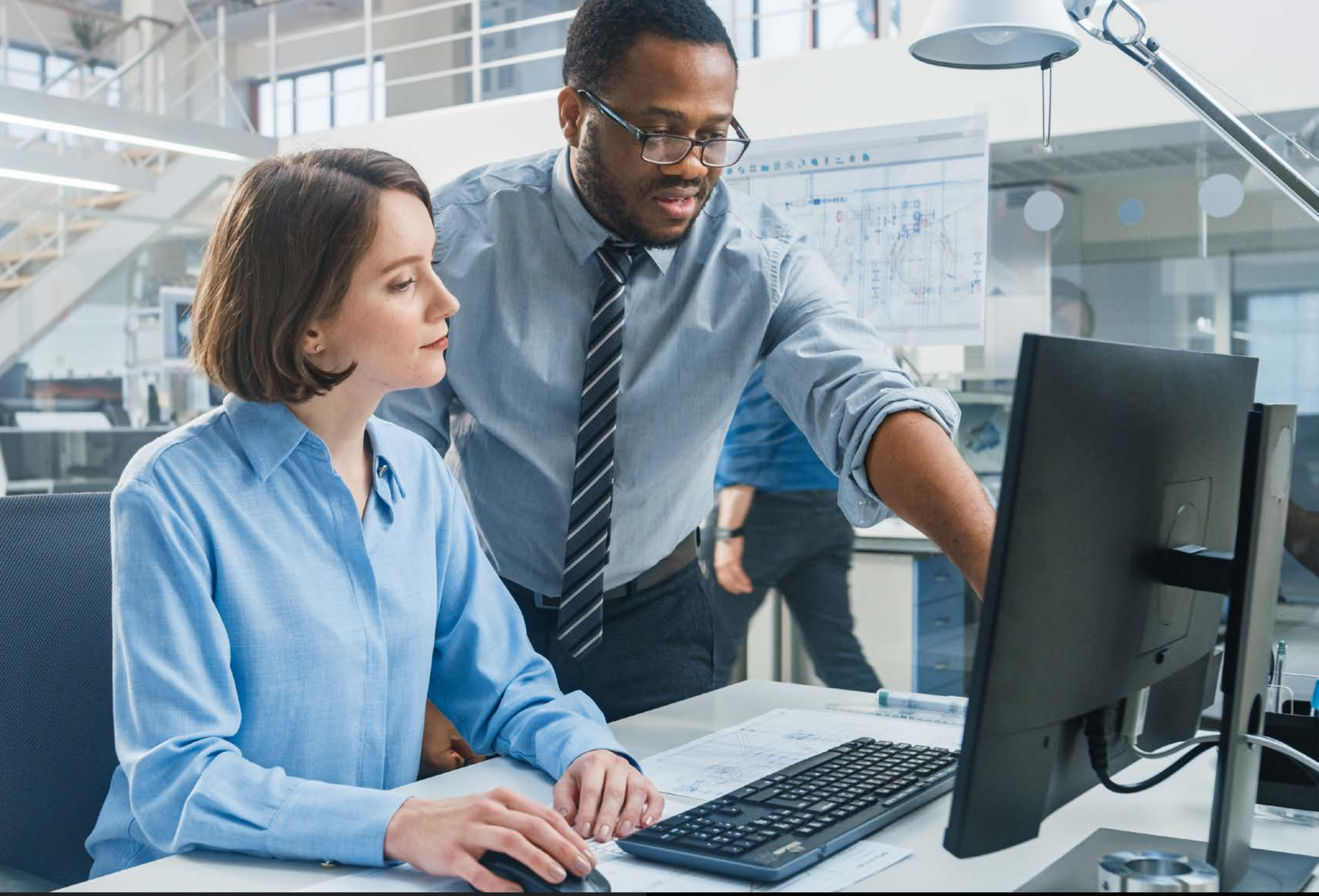
Understanding Breach Factors

PAGE 6

The Zero Trust Dictionary: Blueprint for a Secure Digital Future

PAGE 20

Dr. Brandy Harris
Director,
CyberEd.io



From the Director’s Desk

Welcome to the Summer ‘24 issue of CyberEd Magazine. As we face the challenges of the digital age, the importance of robust cybersecurity measures has never been more apparent. In this issue, we highlight a crucial aspect of cybersecurity, Human Risk Management (HRM).

Thanks to AI and other advances, the growth and sophistication of cyberthreats is exponential. Ransomware gangs are using behavioral psychology and AI to create deepfakes and incredibly realistic phishing attacks. This highlights the need to focus on human factors in cybersecurity. As the Director of CyberEd.io, I am excited to bring you insights, strategies, and stories that demonstrate the significance of HRM in fortifying our defenses.

Human Risk Management is not just about mitigating risks posed by human error. It’s about empowering individuals with the knowledge, skills, and mindset to act as the first line of defense against cyberthreats. It’s about changing behavior and creating a positive cybersecurity culture. In this issue, you will find expert interviews, research reports, and practical guides that explore how HRM can transform your approach to cybersecurity education.

Our cover story features an in-depth interview with me, where I share valuable perspectives on integrating behavioral psychology into cybersecurity training, the importance of continuous learning, and the role of personalized education in fostering a security-conscious culture. These insights also offer actionable steps that you can implement in your organization today.

CyberEd Magazine is committed to being your trusted source for the latest trends, research, and best practices in cybersecurity education. Each article is crafted to provide you with comprehensive knowledge and practical tools to understand the cybersecurity landscape. Whether you are a seasoned professional, an educator, or someone new to the field, our goal is to equip you with the resources you need to succeed.

I encourage you to actively engage with the content, share your experiences, and join the conversation on how we can collectively enhance our cybersecurity posture through effective education and HRM. Your feedback and contributions are invaluable as we strive to make CyberEd.io the premier site for effective cybersecurity education supporting your entire organization. If you have interest in presenting a Master Class session, serving on industry advisory boards that help drive our curriculum, or just generally contributing to the conversation, we would love to hear from you! Contact us!

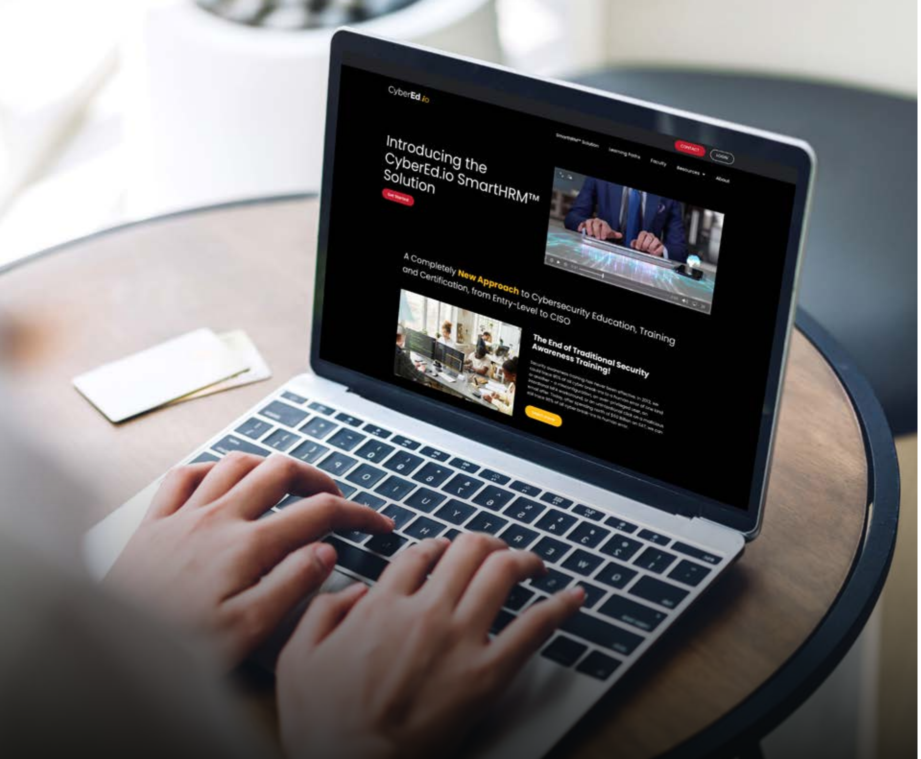
Together, we can build a safer, more secure digital future.

Best,

Brandy Harris

Dr. Brandy Harris
Director,
CyberEd.io

Dr. Brandy Harris has more than 20 years of experience in education and is dedicated to evolving the cybersecurity workforce. She promotes diversity and inclusion in cybersecurity by fostering collaboration between industry and academia, aiming to bridge the talent gap and drive positive change. She previously served as assistant dean of technology and a faculty member in the graduate cybersecurity program at Grand Canyon University.


CyberEd.io
Introducing the CyberEd.io SmartHRM™ Solution
A Completely New Approach to Cybersecurity Education, Training and Certification, from Entry-Level to CISO
The End of Traditional Security Awareness Training!

NEW COURSES

We're constantly updating the CyberEd.io platform with new course content including lectures from the world's leading cybersecurity and technology experts.

Previous Issues

See our prior CyberEd Magazine issues below:

CyberEd MAGAZINE
AI and the Art of Cyber Defense
AI Uncertainties: Enhancing or Eroding Education?

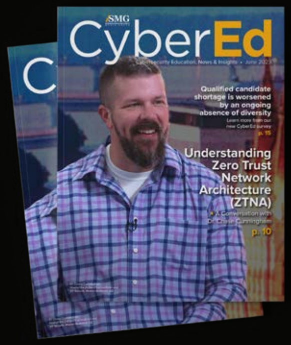
Spring 2024

CyberEd MAGAZINE
Top Ten Cybersecurity Threats in 2024
Fostering a Strong Cybersecurity Culture in 2024

Winter 23/24

CyberEd.io
Perceptions versus reality:
Overcoming the Inertia of Assessing and Securing APIs
ISMG

Fall 2023


CyberEd
Qualified candidate shortage is worsened by an ongoing absence of diversity
Understanding Zero Trust Network Architecture (ZTNA)

Summer 2023

CyberEd MAGAZINE

CyberEd Magazine Editorial
General Manager **MICHAEL D'AGOSTINO**
Director **DR. BRANDY HARRIS**
Executive Editor **BARBARA REIMERS**
Director of Global Creative Strategy **ALEXANDRA PEREZ**
Lead Graphic Designer **CAITLIN PERSICHILLI**
Social Media Coordinator **PURTIKA PANDEY**

ISMG Editorial
Senior Vice President Editorial **TOM FIELD**
Executive Editor **MARIANNE K. MCGEE**
Executive Editor **MATHEW J. SCHWARTZ**
Managing Editor **GEETHA NANDIKOTKUR**
Managing Editor **TONY MORBIN**
Managing Director **VARUN HARAN**
Director Global News Desk **BRIAN PERIERA**
Editorial Director, News **DAVID PERERA**
Editorial Director **CAL HARRISON**
Principal Correspondent **SUPARNA GOSWAMI**
Director of Production **ANNA DELANEY**

Contact
902 Carnegie Center
Princeton, NJ 08540

Toll Free: (800) 944-0401
ismg.io

iSMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Our 34 global media properties provide security professionals and senior decision makers with industry- and geo-specific news, research and educational events.

www.ismg.io

Table of Contents

COVER STORY INTERVIEW

Mitigating Risks Linked to Human Behavior

A Closer Look at Human Risk Management

PAGE 15

The Zero Trust Dictionary: Blueprint for a Secure Digital Future

PAGE 20

Understanding Breach Factors

What Every Security Leader Needs to Know

Cybersecurity risks are rising as cyberattacks increase in frequency and sophistication. This is driving CISOs and security leaders to seek out and patch-up their organization's biggest vulnerabilities.

A recent survey of roughly 300 compliance professionals found that 90 percent cited rising cybersecurity threats, with almost half saying they grew substantially in the last year, according to a Wall Street Journal report published in May.

In fact, cybersecurity topped the list of all types of risks, ranking higher than regulatory scrutiny, cited by 78% and digitization, cited by 71% of survey respondents.

Increasingly, security leaders are finding that failing to follow through on reducing key vulnerabilities often leads to significant and often costly breaches. Several recent, high-profile hacks have raised the stakes for everyone. Last September's MGM Resorts International cyberattack on its hotel and casino operations shut down operations and cost the company an estimated $100 million. In February, a ransomware attack on UnitedHealth Group's Change Healthcare unit crippled parts of the U.S. healthcare system and the company reported $872 million in unfavorable cyberattack effects in its quarterly earnings report.

The intricacies involved in managing cybersecurity stem from multiple potential breach factors, each contributing to the overall challenge.

Among the most difficult factors organizations face are:

1. The Relentless Evolution of Cyberthreats

Cyberthreats evolve rapidly with new vulnerabilities, exploits, and attack methodologies emerging continuously. Staying ahead of these threats requires constant vigilance, research, and updates to security protocols.

Proactive strategies to reduce such risks include:

- Implement continuous monitoring and threat intelligence systems.
- Regularly update and patch systems to address new vulnerabilities.
- Invest in threat hunting teams to proactively identify and mitigate threats.

2. Overcoming Human Vulnerability Factors

One of the biggest vulnerabilities in information security is human error. This can include anything from employees falling for phishing attacks to improper data handling. Training and maintaining a security-conscious culture are crucial, but challenging.

Proactive strategies to reduce human factor risks include:

- Conduct regular security awareness training for all employees.
- Simulate phishing attacks to test and improve employee response.
- Foster a culture of security where employees are encouraged to report suspicious activities.

3. Allocating Resources is an Ongoing Struggle

Allocating sufficient financial and human resources to effectively manage information security is a constant challenge. Budget constraints may limit the ability to implement the best security tools or hire the most qualified personnel.

Proactive strategies to help lower risks due to resource constraints include:

- Prioritize security spending based on risk assessments.
- Leverage managed security service providers (MSSPs) for specialized expertise.
- Justify security investments by communicating potential breach costs to stakeholders and boards of directors.

4. Seamlessly Integrating Security Practices

Integrating security practices into daily business processes without hindering operational efficiency is no easy task. Security measures often require additional steps or checks, which can be seen as obstacles by other departments.

Proactive strategies to help you better integrate security best practices include:

- Embed security into the development lifecycle (DevSecOps).
- Automate security processes to reduce friction.
- Collaborate with business units to align security measures with operational goals.

5. Keeping Pace with Evolving Regulations

Ensuring compliance with a growing list of regulations and standards (such as GDPR, HIPAA, or PCI-DSS) is not only challenging but also resource-intensive. At the same time, non-compliance can result in severe penalties.

Proactive strategies to help maintain compliance with evolving regulations include:

- Regularly review and update compliance policies and procedures.
- Conduct internal audits to ensure adherence to regulatory requirements.
- Use compliance management tools to streamline and automate processes.

6. Effectively Planning for the Worst

Developing and maintaining an effective incident response plan that can minimize damage and recover normal operations after a breach is a complex process. It requires detailed planning, regular testing, and continual improvement.

Proactive strategies to better respond and recover from breaches include:

- Develop a comprehensive incident response plan.
- Conduct regular drills and simulations to test the plan.
- Establish a post-incident review process to learn and improve from each incident.

7. Overcoming Technological Complexity

The diversity of technologies used in organizations (cloud services, IoT devices, mobile applications, etc.) adds layers of complexity to security management. Each technology can introduce new vulnerabilities and requires specific security considerations.

Proactive strategies to reduce technological complexity include:

- Perform regular security assessments of all technologies in use.
- Implement unified security management solutions to centralize control.
- Train IT staff on the latest security practices for each technology.

8. Securing Remote Workers

With many employees working remotely, securing remote access to company resources while maintaining the user experience involves ensuring the security of data across potentially insecure networks and devices.

Proactive strategies for securing remote access include:

- Use VPNs and secure access service edge (SASE) solutions to protect remote connections.
- Implement multi-factor authentication (MFA) for all remote access.
- Ensure endpoint security through regular updates and monitoring.

CyberEd Recent Events Roundup

Unveiling the Future of Cybersecurity: The Get Smarter Summit

In today's fast-paced digital world, the importance of robust cybersecurity measures cannot be overstated. Cyberthreats are becoming increasingly sophisticated, and traditional approaches to security are often inadequate. This spring, the Get Smarter Summit addressed these challenges by focusing on Human Risk Management (HRM), a revolutionary approach that emphasizes the critical role of human behavior in cybersecurity.

MOVING FROM TRADITIONAL SECURITY TO HUMAN RISK MANAGEMENT

Historically, cybersecurity has heavily relied on security awareness training to mitigate risks. However, traditional training methods frequently fall short. They often lack engagement, relevance, and timely updates, leading to a persistent vulnerability: human error. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involve human error, highlighting the urgent need for a more effective solution (ISMG Corp).

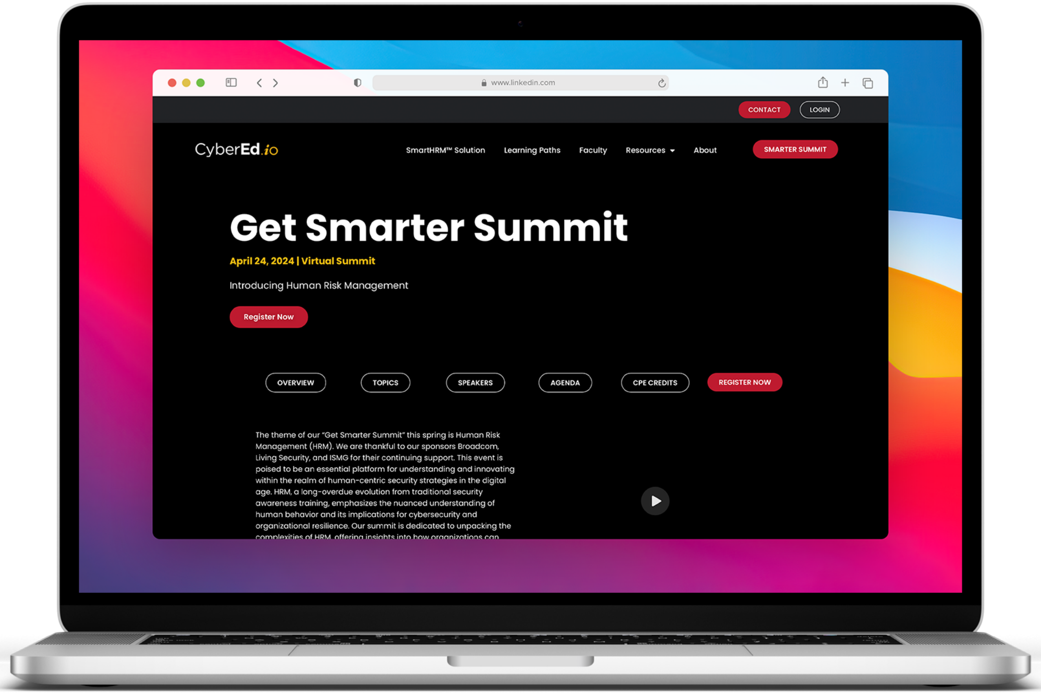
The Get Smarter Summit aims to fill this gap by shifting the focus from conventional training to comprehensive Human Risk Management. HRM not only addresses human errors but also integrates behavior analysis, targeted interventions, and a positive security culture to manage and reduce human-related risks in organizations.

EXPERT INSIGHTS AND CUTTING-EDGE DISCUSSIONS

The summit featured an impressive lineup of industry leaders and innovators who explored various aspects of HRM. Keynote speaker Dr. Brandy Harris, Director of Learning and Organizational Development at CyberEd.io, discussed the pivotal role of HRM in breach prevention. Matthew Rosenquist, CISO at Mercury Risk, shared strategies for navigating the complexities of human-related risks in today's interconnected world.

CYBERED.IO'S SMART SOLUTION FOR HRM

The 2023 RSA ID IQ Report showed that 64% of respondents and 65% of self-proclaimed identity and access management experts failed to recognize recommended methods for phishing



Get Smarter Summit

April 24, 2024 | Virtual Summit

Introducing Human Risk Management

The theme of our "Get Smarter Summit" this spring is Human Risk Management (HRM). We are thankful to our sponsors Broadcom, Living Security, and ISMG for their continuing support. This event is poised to be an essential platform for understanding and innovating within the realm of human-centric security strategies in the digital age. HRM, a long-overdue evolution from traditional security awareness training, emphasizes the nuanced understanding of human behavior and its implications for cybersecurity and organizational resilience. Our summit is dedicated to unpacking the complexities of HRM, offering insights into how organizations can

prevention. Organizations must, therefore, adopt a holistic approach to equipping personnel with the knowledge to recognize and combat threats such as phishing and credential compromise.

In a bid to address this issue, CyberEd.io launched its cutting-edge SmartHRM Solution. "We're excited to have launched our revolutionary advancement in Security Awareness Training – our new Human Risk Management (HRM) platform, SmartHRM. This breakthrough platform marks a significant leap forward, as it fully leverages a catalog of security apps and appliances that you, the customer, likely have already installed in your own environment," said Dr. Brandy Harris, Director, CyberEd.io.

This solution provides comprehensive visibility into organizational human risk posture, helping identify in real-time employees who need training in specific operational protocols such as passwords, MFA, IAM, phishing, etc. Organizations can then choose and administer the suitable training from CyberEd.io's extensive catalog of options, promptly addressing vulnerabilities and gradually reducing internal risks.

RSA Conference 2024: Unpacking AI, Cyberthreats and CISO Roles

RSA Conference 2024, held from May 6-9 in San Francisco, brought together the brightest minds and leading vendors in the field of cybersecurity. The premier gathering for security and technology leaders saw significant engagement from ISMG, the global intelligence and education organization focused on IT, OT and cybersecurity. With the theme "The Art of Possible," RSAC 2024 highlighted the convergence of emerging cybersecurity solutions, evolving threats and the shifting roles within the cybersecurity ecosystem.

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

A key highlight of the conference was an extensive focus on artificial intelligence. Discussions and presentations delved into the maturing AI market, showcasing how vendors are embedding AI capabilities into cybersecurity products. These AI-enhanced solutions are designed to fortify cyber defenses and protect large language models and their data from increasingly sophisticated cyberattacks, including those utilizing AI and deepfake technologies.

The conference underscored growing concerns about AI-driven threats, with cybercriminals leveraging AI to scale up their attacks. This has led to a surge in the development of AI-embedded cybersecurity solutions aimed at countering these advanced threats. The dialogue also extended to the protection of AI systems themselves, ensuring the integrity and security of AI applications and the data they process.

RANSOMWARE AND NATION-STATE THREATS

Ransomware remained a significant topic at RSAC 2024. The conference highlighted the latest trends in ransomware, focusing on evolving tactics of cybercriminal gangs and nation-state actors. These threat actors are increasingly targeting critical infrastructure, posing substantial risks to national security and public safety. The insights shared at the conference emphasized the need for robust defense strategies and the adoption of advanced technologies to mitigate threats.

THE CISO'S EVOLVING ROLE

With the advent of AI and the heightened awareness of emerging challenges and risks, the responsibilities of CISOs are evolving. The RSA conference explored the dynamic nature of the CISO role, particularly in the context of managing security and privacy issues related to the large-scale use of generative AI tools. Debates arose about whether the CIO, CRO or the CISO should oversee these critical areas, reflecting the ongoing debate on leadership and governance in cybersecurity.

Live shot from RSAC's ISMG studio

ISMG'S STRATEGIC PRESENCE AND COVERAGE

As one of the largest media partners for RSAC, ISMG provided its most significant editorial and research presence to date. The ISMG Studio division set up two state-of-the-art video studios at the San Francisco Marriott Marquis and the RSAC Broadcast Alley in Moscone West.

ISMG's award-winning editorial team extensively covered critical takeaways from the conference and conducted interviews with thought leaders, decision-makers, CEOs, CISOs, CIOs, researchers, and policymakers across the cybersecurity domain.

Content produced from these interactions will be crucial to defining the next era of cybersecurity and IT integration and collaboration. ISMG Studio served as the epicenter of networking and thought leadership, fostering future partnerships and content opportunities.

The RSA Conference 2024 highlighted rapid advancements in AI, the persistent threats from ransomware and nation-state actors, and the evolving role of CISOs. ISMG's strategic presence at the conference underscored its commitment to providing valuable insights and fostering cybersecurity innovation and collaboration.

As discussions and analysis continue to unfold, the industry can look forward to a deeper understanding of the challenges and opportunities that lie ahead for all of us in the ever-evolving field of cybersecurity.

Dr. Brandy Harris
Director, CyberEd.io

Mitigating Risks Linked to Human Behavior

A Closer Look at Human Risk Management

Cybersecurity threats are ever-evolving, making it imperative for organizations to adopt proactive measures in managing risks, particularly those linked to human behavior. Dr. Brandy Harris, a seasoned educator with over two decades of experience, sheds light on the critical importance of Human Risk Management (HRM) in cybersecurity. Dr. Harris, a prominent advocate for diversity and inclusion in the cybersecurity workforce, emphasizes the need for a holistic approach to HRM, underlining that approximately 90% of data breaches are due to human error, a staggering statistic that underscores the urgency of effective cybersecurity education.

As a leading platform dedicated to advancing cybersecurity education, CyberEd.io plays a crucial role in this mission by fostering collaboration between industry and academia. This partnership aims to bridge the talent gap and drive positive change in the cybersecurity landscape. Through innovative training and continuous learning opportunities, CyberEd.io equips professionals with the knowledge and skills needed to navigate the complex cybersecurity environment.

Dr. Harris has more than 20 years of experience in education and is dedicated to evolving the cybersecurity workforce. She previously served as assistant dean of technology and a faculty member in the graduate cybersecurity program at Grand Canyon University. In a recent interview conducted by CyberEd.io, Dr. Brandy Harris explores HRM, emphasizing a holistic approach that involves identifying, evaluating, and mitigating risks linked to human behavior.

What is Human Risk Management and how do you address the human element in cybersecurity risk management?

Human Risk Management (HRM) is a comprehensive approach focused on identifying, assessing, and mitigating risks associated with human behavior and activities within an organization. The number fluctuates, depending on which study you read, but around 90% of data breaches are directly linked to human error. This area of risk management recognizes that humans are often the most unpredictable and variable elements in any operational environment. We know that cybersecurity education is critical. We also know that traditional security awareness training is not effective. We have reframed how we approach the problem, starting with effective training.

How do you balance the need for stringent security measures with maintaining employee trust and morale?

Transparent communication is critical, and you have to involve employees in the process. It is crucial to explain the reasons behind security protocols and how they protect both the organization and the employees. Explain to them WHY this behavior is being monitored and HOW the information will be used. I cannot stress enough that this should not be a punitive system, but a way to provide targeted training. By providing regular training and support, and addressing concerns promptly, organizations can foster a positive cybersecurity culture without undermining employee confidence.

> “Human risk management recognizes that humans are often the most unpredictable and variable elements in any operational environment.”
>
> **Dr. Brandy Harris**
> Director, CyberEd.io

What do you think are the best practices for training employees on cybersecurity awareness?

I've seen many security awareness trainings that do not take into account how adults learn or what motivates them. The psychology behind security awareness training plays a crucial role in its effectiveness. The bad actors out there know this and incorporate these principles into their attack campaigns. Cybersecurity education teams need to do the same. Understanding and incorporating the human aspects of cognition, behavior, and motivation is key to designing training that not only provides information but also influences behavior. Successful HRM plans will include training built with knowledge of adult learning theory and tailor fit to individual needs. These plans are the foundation of a positive cybersecurity culture.

What role does leadership play in fostering a cybersecurity-aware culture, and how can leaders be more involved?

Leadership must set the tone and lead by example. I cannot state that plainly enough. The rules still apply, leaders still have to be vigilant and happily receive additional training when they make errors as well. We all mess up sometimes! That is okay! Leaders can be more involved by making HRM initiatives mandatory, actively participating in them, prioritizing security in decision-making, and ensuring that resources are allocated for continuous training and improvement. Their visible commitment to cybersecurity awareness and human risk management can inspire and motivate employees to take it seriously.

Are there any elements that you think often gets overlooked when trying to establish a positive cybersecurity culture?

Yes! We get more of what we focus on. When working with young people who have experienced trauma and have resulting behavioral issues, for example, one of the best ways to reshape those responses is to call out all the positives you can observe. That is an extreme case, but the same is true for all of us. For example, instead of merely focusing on the number of phishing links clicked in a campaign, focus on the percentage of improvement each department made. A solid HRM plan should help establish a positive culture, not be seen as a punitive program.

What emerging cybersecurity threats should we be aware of in the coming years?

Fundamental types of cyberthreats - phishing, ransomware, and social engineering - are likely to persist in the coming years. However, the sophistication and complexity of these attacks are expected to increase

significantly. For example, attackers are employing artificial intelligence to craft more believable phishing messages and to automate large-scale campaigns. The use of deepfake technology to create convincing audio or video impersonations of trusted individuals is also on the rise and getting more difficult to distinguish from legitimate media. We need to evolve to have any hope of keeping up.

If we want to implement a human risk management plan, what are the critical first steps?

It is important to start with an interdisciplinary team. Obviously, you need someone from the security team and leadership, but you will also likely need to involve your compliance manager and human resources. That team will need to set the parameters for and complete a comprehensive risk assessment to identify potential human-related risks within the organization. Next, establish clear policies and procedures addressing identified risks, including data protection, acceptable use, and incident reporting. Then, implement training programs based in adult learning theory to educate employees on security best practices and their roles in mitigating risks. If you have further questions, as always, CyberEd.io is here to help.

How do you stay updated with the latest trends and developments in HRM and cybersecurity?

Staying updated with the latest trends and developments in HRM and cybersecurity requires a commitment to continuous learning. The field is ever evolving and there is ALWAYS something more to learn. Subscribe to industry publications, participate in professional networks, attend conferences and webinars, and engage with thought leaders on social media. Visit us right here at CyberEd.io! Whichever method you choose, be certain you are keeping abreast of new insights and best practices. Always, stay safe, stay secure, and stay vigilant.

LOOKING AHEAD

The future of Human Risk Management (HRM) in cybersecurity lies in continuous innovation and adaptive strategies. As cyberthreats become more sophisticated, leveraging advanced technologies and fostering a culture of continuous learning and proactive risk management will be paramount. Leadership's commitment to cybersecurity, transparent communication, and tailored training programs will be essential in mitigating risks and enhancing organizational resilience.

For those seeking to stay ahead in the ever-evolving field of cybersecurity, CyberEd.io offers a wealth of resources and expertise. Whether you are looking to implement a robust HRM plan or stay updated with the latest trends and developments, CyberEd.io is your go-to platform for comprehensive cybersecurity education.

Visit CyberEd.io today to learn more about how you can enhance your organization's cybersecurity posture and stay vigilant in the face of emerging threats.

> **"As cyberthreats become more sophisticated, leveraging advanced technologies and fostering a culture of continuous learning and proactive risk management will be paramount."**
>
> **Dr. Brandy Harris**
> Director, CyberEd.io

The Zero Trust Dictionary: Blueprint for a Secure Digital Future

Zero Trust is more than just a cybersecurity buzzword. It's a transformative approach that offers robust protection in an increasingly hostile digital world.

By focusing on core business outcomes, adopting an inside-out design, enforcing least privilege, and thoroughly inspecting and logging traffic, organizations can significantly enhance their security posture. To delve deeper into the intricacies of Zero Trust, CyberEd.io has published The Zero Trust Dictionary authored by John Kindervag, the architect of Zero Trust.

This comprehensive guide is an invaluable resource for anyone looking to implement or better understand the Zero Trust cybersecurity framework.

ZERO TRUST: A STRATEGIC IMPERATIVE

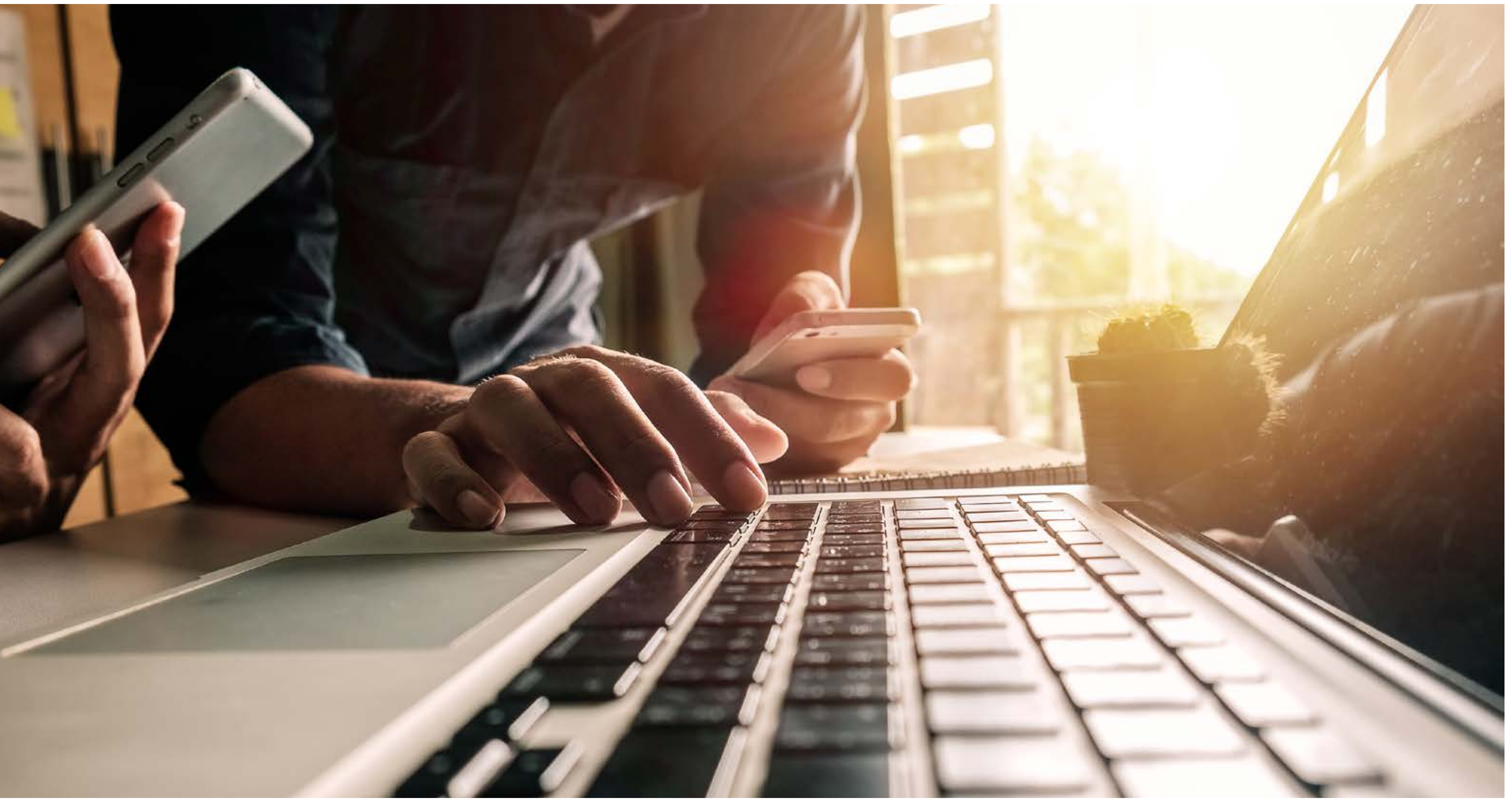
In today's rapidly evolving digital landscape, traditional security measures are no longer sufficient to protect against the sophisticated threats that organizations face. Zero Trust emphasizes the principle of 'never trust, always verify.'

Zero Trust is a strategic initiative designed to safeguard critical data and systems by eliminating inherent trust within an organization's network. This article, aims to explain the core principles of Zero Trust and encourage you to explore CyberEd.io to learn more.

ZERO TRUST DESIGN PRINCIPLES

Zero Trust is underpinned by four fundamental design principles.

1. **Define Business Outcomes:** The starting point for any Zero Trust strategy is understanding the business's objectives. By aligning cybersecurity measures with the organization's strategic goals, Zero Trust transforms cybersecurity from a potential hindrance to a crucial business enabler.
2. **Design From The Inside Out:** The focus should be on protecting the Data, Applications, Assets, and Services (DAAS) that are critical to the organization. This approach ensures that security measures are robust where they are most needed.
3. **Determine Who Or What Needs Access:** Access should be granted strictly on a need-to-know basis. The principle of Least Privilege ensures that users have only the access necessary to perform their roles, minimizing the risk of unauthorized data exposure.
4. **Inspect and Log All Traffic:** Comprehensive monitoring of network traffic, including inspection up to Layer 7, is essential for identifying and mitigating threats. Logging all activities ensures that any anomalies can be quickly detected and addressed.



DATA, APPLICATIONS, ASSETS, AND SERVICES (DAAS)

The DAAS framework categorizes the sensitive resources that must be protected within a Zero Trust environment. The key elements include:

- **Data.** This includes sensitive information such as Payment Card Information (PCI), Protected Health Information (PHI), Personally Identifiable Information (PII), and Intellectual Property (IP).
- **Applications.** These are critical applications that handle sensitive data or control essential assets.
- **Assets.** This encompasses Information Technology (IT), Operational Technology (OT), and Industrial Internet of Things (IIoT) devices, including point-of-sale terminals, Supervisory Control and Data Acquisition (SCADA) controls, manufacturing systems, and networked medical devices.
- **Services.** These are critical services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory, and Network Time Protocol (NTP), which are essential for business operations and must be protected to ensure the organization's resilience.

PROTECT SURFACE

Unlike the broad and often unmanageable attack surface, the Protect Surface in a Zero Trust environment is significantly smaller and more manageable. Each Protect Surface contains a single DAAS element, making it easier to secure and monitor. This approach allows organizations to reduce their exposure to potential attacks.

SEGMENTATION GATEWAY

A Segmentation Gateway (SG) is crucial in enforcing Zero Trust policies. Operating at Layer 7, SGs segment networks based on users, applications, and data, ensuring that security policies are applied precisely where needed. These gateways can be physical (PSG) or virtual (VSG), depending on whether they are used in on-premise networks or cloud environments. Next-Generation Firewalls often serve as Segmentation Gateways in Zero Trust architectures.

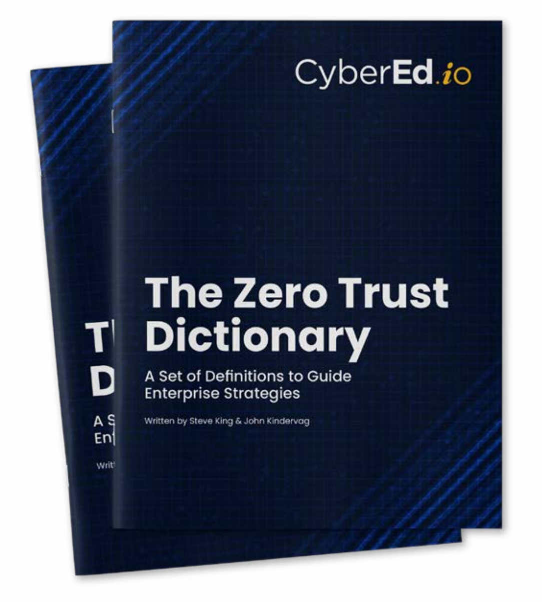
RISING IMPORTANCE, RAPID GROWTH

The rapid growth of Zero Trust adoption across various industries is exhibited in a MarketsandMarkets report that predicts the global Zero Trust security market size to reach $51.6 billion by 2026, with a compound annual growth rate (CAGR) of 17.4%. This underscores how Zero Trust has grown into a critical component of modern cybersecurity strategies.

Organizations that have implemented Zero Trust have reported significant reductions in data breaches and improved compliance with regulatory standards. By focusing on core business outcomes, adopting an inside-out design, enforcing least privilege, and thoroughly inspecting and logging traffic, organizations can significantly enhance their security posture.

To delve deeper into Zero Trust, download the full report on CyberEd.io and join the movement to realize a more secure digital future. This comprehensive guide is an invaluable resource for anyone looking to implement or understand this critical cybersecurity framework.

Download your free copy to read the full report.


CyberEd.io
The Zero Trust Dictionary
A Set of Definitions to Guide Enterprise Strategies
Written by Steve King & John Kindervag

Driving Behavioral Change through Human Risk Management

By Dr. Brandy Harris

Despite advances in technology, human error remains a significant vulnerability in cybersecurity. Phishing attacks, weak passwords, and unintentional data breaches are often the result of inadequate training and awareness.

Traditional security awareness training methods, which frequently rely on one-size-fits-all approaches, fail to address the diverse needs and motivations of adult learners. This is why it’s crucial to develop a comprehensive Human Risk Management (HRM) plan that incorporates training designed to integrate adult learning theory and behavioral psychology.

UNDERSTANDING ADULT LEARNING THEORY

Adult learning theory, or andragogy, puts forward that adults learn differently from children. Malcolm Knowles, a prominent figure in the field, identified several key key principles that included themes around:

1. **Self-Direction:** Adults prefer to take responsibility for their learning, often seeking knowledge relevant to their personal and professional lives.
2. **Experience:** Adults bring a wealth of experiences to the learning process, which can be a rich resource for themselves and others.
3. **Readiness to Learn:** Adults are more inclined to learn when they see the immediate relevance of the knowledge to their job or personal life.
4. **Problem-Centered Learning:** Adults are motivated by problem-solving rather than content-centered learning.

Applying these principles to cybersecurity training means creating programs that are self-directed, experiential, relevant, and problem-centered. For example, instead of generic training modules, organizations can develop scenarios that mirror real-life challenges employees might face to help make the learning experience more engaging and impactful.

THE ROLE OF BEHAVIORAL PSYCHOLOGY

Behavioral psychology offers insights into how individuals form habits and how these habits can be changed. Two key concepts from this field are:

1. **Reinforcement:** Positive and negative reinforcement can shape behavior. Positive reinforcement, such as rewards for completing cybersecurity training, can motivate employees to adopt safer practices.
2. **Behavioral Triggers:** Identifying and modifying triggers that lead to risky behavior can prevent security lapses. For example, implementing mandatory two-factor authentication (2FA) prompts whenever employees access sensitive information can act as a trigger to enhance security awareness and reinforce secure access practices.

Combining these concepts with adult learning principles, HRM strategies can be designed to not only educate but also reinforce and sustain secure behaviors.

IMPLEMENTING HRM STRATEGIES FOR BEHAVIORAL CHANGE

To effectively drive behavioral change, HRM strategies should incorporate elements of both adult learning theory and behavioral psychology. Here are five practical steps you can take:

1. **Personalized Learning Paths:** Develop customized training programs that cater to the varying experience levels and learning styles of employees. This could involve assessments to identify knowledge gaps and tailor content accordingly.
2. **Interactive and Experiential Learning:** Use simulations, role-playing, and hands-on activities that allow employees to experience real-world scenarios in a controlled environment. This experiential learning helps reinforce theoretical knowledge.
3. **Continuous Reinforcement:** Implement a system of regular feedback and reinforcement. Recognize and reward employees who demonstrate adherence to security protocols, and provide constructive feedback to those who do not.
4. **Behavioral Nudges:** Incorporate subtle prompts and reminders that encourage secure behavior. This can include automated alerts about phishing attempts or reminders to update passwords.
5. **Leadership and Culture:** Cultivate a security-conscious culture in which leaders model desired behaviors. Leadership buy-in is crucial for setting the tone and ensuring that cybersecurity is prioritized across all organizational levels.

A SUCCESSFUL USE CASE

Consider the financial institution that faced frequent phishing attacks. By integrating HRM with adult learning theory and behavioral psychology, the organization developed a comprehensive training program. They started with a survey to assess employees' existing knowledge and attitudes about cybersecurity. Based on their findings, they created personalized learning paths that included interactive modules and real-world simulations.

To reinforce learning, the financial institution implemented a reward system for employees who successfully identified phishing attempts. Behavioral nudges, such as regular email reminders and pop-up alerts were also employed. Leadership played a pivotal role by participating in training sessions and consistently communicating the importance of cybersecurity.

As a result, phishing incident reports decreased by 40%, and employee engagement in cybersecurity training increased by 60%. This use case exemplifies the effectiveness of a human-centric approach to cybersecurity training.

The convergence of adult learning theory, behavioral psychology, and HRM offers a powerful strategy for driving behavioral change in cybersecurity. By creating personalized, experiential, and reinforced learning experiences, organizations can foster a culture of security awareness and resilience. As cyberthreats continue to evolve, so too must our approaches to managing human risk and ensuring individuals are not the weakest link but the first line of defense.

CyberEd Featured Faculty

Dr. Chase Cunningham

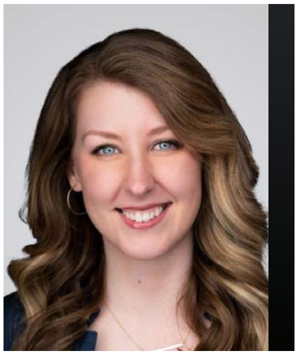
VP, Security Market Research, G2

Dr. Chase Cunningham, known as the Doctor of Zero Trust, Dr. Cunningham is an early advocate and proponent of the Zero Trust strategy and is currently the VP of Security Market Research for G2. In this role, Dr. Cunningham shapes the company's strategic vision, roadmap and key partnerships. Dr. Cunningham previously served as vice president and principal analyst at Forrester Research, providing strategic guidance on Zero Trust, artificial intelligence, machine learning and security architecture design for security leaders around the globe.

Andy Jenkinson

Group Chief Executive Officer, Cybersec Innovation Partners

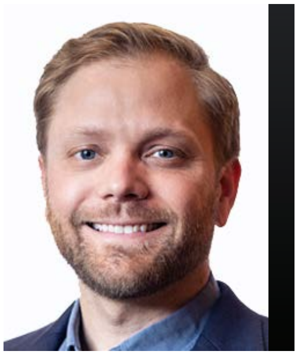
Andy Jenkinson is a senior and seasoned innovative Executive with over 30 years' experience as a hands-on lateral thinking CEO, coach, and leader. A 'big deal' business accelerator, and inspirational, lateral thinker, Andy has crafted, created, and been responsible for delivering 100's £millions of projects within the Cyber, Technical, Risk and Compliance markets for some of the world's largest, leading organizations. Andy has a demonstrable track record of large-scale technical delivery and management within many sectors including the Professional, Managed, and Financial Services.



Kelly Hood

EVP and Cybersecurity Engineer, Optic Cyber Solutions

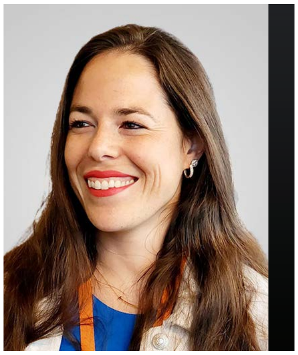
Kelly Hood is an EVP and cybersecurity engineering expert supporting organizations across sectors to develop and implement strategies to manage cybersecurity and privacy risks. She works with organizations to meet cybersecurity best practices, controls and standards, including the NIST Cybersecurity Framework, CMMC, SP 800-53, SP 800-171 and ISO 27001. She assisted the NIST Cybersecurity Framework team in the evolution and outreach of the Cybersecurity Framework.



Jimmy Mesta

Chief Technology Officer, KSOC

Jimmy Mesta is the founder and Chief Technology Officer at KSOC, the organization that triages risk across Kubernetes clusters in real time. He is responsible for the technological vision for the KSOC platform. Mesta, veteran security engineering leader focused on building cloud-native security solutions, Jimmy has held various leadership positions with enterprises navigating the growth of cloud services and containerization. At the Web App Firewall Innovator Signal Sciences (acquired by Fastly, Inc.), he led offensive and defensive teams across the Security and Engineering organizations while helping build modern, developer-friendly security solutions.



Tal Kollender

CEO, GYTPOL

Tal Kollender is the CEO and co-founder of GYTPOL, a privately held security compliance company that focuses on policy validation and detection of configuration weaknesses. Kollender, A self-taught teenage hacker, she had her sights set on flying fighter jets in the IDF, but though she qualified, she was whisked off to Cybersecurity duty in the Cyber Security-Systems Division, where she served as an ICT cyber specialist. Her professional career took her to Dell EMC where she was cyber expert and System Security Architect before creating Gytpol with her co-founders. In 2023, Tal received the Entrepreneur of the Year award from the United Cybersecurity Alliance.

Nikki Robinson

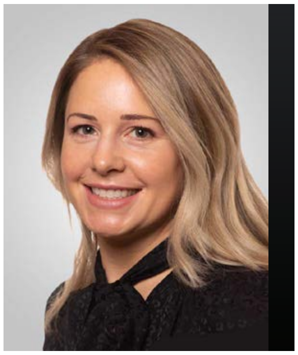
STSM - Cyber Resiliency and Recovery, IBM

Dr. Nikki Robinson is a senior IBM Cybersecurity Engineer with 15+ years of experience in the IT and cybersecurity fields. Skilled in statistical data analysis, team leadership, penetration testing, and risk management, Nikki earned her doctorate in Cybersecurity from Capitol Technology University. Dr. Robinson is certified as a CISSP and CEH and is a member of the Board of Directors for InfraGard Maryland Chapter and provides support for InfraGard at the national level on the Journal Review Committee. Nikki teaches graduate-level courses in Quantitative Methods, Incident Response, and Healthcare Mobile Device Security at Touro College and Capitol Technology University.

Char Sample

Cybersecurity researcher, ICF

Dr. Char Sample is a cybersecurity researcher at ICF with decades of experience. Dr. Sample currently supports NSF research initiatives in Computer and Network Science research. Dr. Sample's current research focuses on deception, and the role of cultural values in cybersecurity events and decision-making. One other area of research that she finds interesting is the relationship between human cognition and machines. Currently, Dr. Sample is continuing research on modeling cyber behaviors by culture, data resilience, cyber-physical systems and industrial control systems and trustworthy artificial intelligence (TAI).



Lynn Peachey

Director of Business Development, Arete Incident Response

Lynn Peachey is an expert in the cyber insurance space. Currently, she serves as the director of business development, connecting clients and partners with cybersecurity solutions at Arete Incident Response, an insurance company and security insurance space. Previously earning her two bachelor's degrees from Rutgers University in New Jersey in psychology and industrial relations, then her JD from Pace University's Elizabeth Haub School of Law, Peachey is licensed in multiple states, including New York, California, Texas and Florida, as well as admitted to the New York and New Jersey Bar.

Red and Sam Curry

CYBERSECURITY INSIGHTS PODCAST

Curry Brothers on Cyber Warfare – Part 4

Red Curry is a seasoned CMO, creative director and master storyteller with over 20 years of experience leading creative and strategic teams for RSA/EMC, METTLER TOLEDO and SSH Communications Security. He has more than a decade of experience safeguarding sensitive data and combating cyberthreats.

Sam Curry, VP and CISO at Zscaler is a 30-year cybersecurity veteran who started at Signal 9 Solutions, inventor of the personal firewall. He then executed the first commercial implementation of Blowfish, and devised early (symmetric key) VPN technology ultimately sold to McAfee. Sam holds 17 patents and teaches at Harvard University, Wentworth Institute of Technology and Nichols College and is a fellow at the National Security Institute.

In this episode of Cybersecurity Insights, Red and Sam discussed:

- What types of of individuals pursue careers in cybersecurity?
- How marketing impacts the success of cybersecurity solutions;
- Why our allergy to FUD weakens our response to rising threats;
- What makes technical alliances crucial to addressing cyberthreats;
- And much, much more.

Learn more by listening to the podcast here.

Jim Doggett

CYBERSECURITY INSIGHTS PODCAST

The New CISO Agenda

Jim Doggett is the chief information security officer at Semperis and a veteran in the information security and risk space. He previously served as a partner at Ernst & Young, where he helped build the company's cybersecurity practice over his 27-year tenure. Most recently, Jim worked as CISO and head of U.S. operations at Panaseer. He has held positions as chief technology risk officer at AIG and CSO and CTRO at Kaiser Permanente. He also served as the managing director at JPMorgan Chase, where he was the global leader of information risk and resiliency, treasury and security services.

In this episode of Cybersecurity Insights, Jim discussed:

- The paramount importance of cyber resiliency;
- The crucial role of CISOs and technology;
- Prioritizing risks;
- And much more.

Learn more by listening to the podcast here.

Tom Corn

CYBERSECURITY INSIGHTS PODCAST

How to Move Beyond the AI Hype

Tom Corn is the chief product officer at Ontinue. He oversees product management, product marketing, engineering, and security operations center, and also manages the advisory and technical account managers. Prior to Ontinue, Tom was the chief product officer at Open Systems.

Tom joined Open Systems after serving as senior vice president in VMware's Security Business Unit, where he pioneered the Cloud Workload Protection technology. He led the product team that developed the core technology behind Carbon Black Workload. With more than 20 years of experience in cybersecurity, Tom has led security product teams at market-leading companies, including VMware and RSA.

In this episode of Cybersecurity Insights, Tom discussed:

- Leveraging the power of AI;
- Balancing automation and human involvement in AI;
- Integrating machine learning into organizational operations;
- And much more.

Learn more by listening to the podcast here.

Héctor Arias

CYBERSECURITY INSIGHTS PODCAST

Cyberattacks and Generative AI

Héctor Arias is the global lead for retail banking at Red Hat. He has more than 20 years of experience within the banking sector, leading business strategy, open banking, digital transformation, and new digital businesses initiatives for Banco Bilbao Vizcaya Argentaria (BBVA) in several countries spanning the EU, U.S., and LATAM.

He works with banks globally, strategizing and planning the next-generation platform that supports technology-driven business models.

In this episode of Cybersecurity Insights, Hector discussed:

- Cyberattacks and cyber defenses;
- The rising role of generative AI;
- Key drivers behind the astronomical rise in cyberattacks;
- And much more.

Learn more by listening to the podcast here.

Learning Path Spotlights

CyberEd.io offers a new category of online cybersecurity education, providing fundamental technical skills needed to train Cyber-Warriors in the art of detection, defense, and protection. We also strive to instill understanding about why reasoning matters, why adaptability matters, why thinking like hackers matters. We help students build a culture of cybersecurity and an appetite for continuous learning.

When we partner with an organization, we partner for life. Our mission is to help defeat adversaries on all fronts. Our podcasts dive into technologies and processes that are working against adversaries. Students have access to white papers and eBooks written by industry experts, and case studies that bring cybersecurity training to life. Our daily blog also keeps us all focused on key objectives and outcomes. And our Master Class series is taught by widely recognized cybersecurity thought leaders.

There are also hundreds of summit sessions available to help students understand cybersecurity requirements in Singapore, Italy, India, Hong Kong, and elsewhere around the world.

Our industry needs experts and analysts to examine and execute cybersecurity solution frameworks, DevSecOps experts to reinforce continuous integration and continuous delivery (CI/CD) pipeline security, and more/better trained security engineers, researchers, and leaders than our enemies rely on.

We build strong teams, drive better results, generate greater unity and engineer a cybersecurity culture in each of the organizations with which we partner. In this issue, we highlight two Cyber-Warrior Learning Paths:

CyberEd Cloud Warrior

The CyberEd Cloud Warrior Pathway offers an in-depth exploration of cloud computing, covering cloud networking, applications, and security. Starting with the basics, you'll then choose a specialization aligned with your company's cloud strategy: AWS or Azure, Engineering or Operations. The CyberEd Cloud Warrior Pathway combines foundational knowledge with advanced certifications:

1. **Foundational Knowledge:** Begin with a thorough understanding of cloud computing fundamentals, including cloud networking, applications, and security.
2. **CompTIA Cloud Essentials:** Gain a solid grounding with the CompTIA Cloud Essentials certification, covering cloud concepts and models, business aspects, and cloud security.
3. **AWS Certified Cloud Practitioner:** Specialize in AWS with the AWS Certified Cloud Practitioner certification, focusing on AWS cloud infrastructure, services, and architectural best practices.
4. **Microsoft Azure Administrator:** Dive into Microsoft Azure with the Azure Administrator certification, mastering Azure services, infrastructure, and security.
5. **Google Cloud Engineer:** Explore Google Cloud with the Google Cloud Engineer certification, learning to design, develop, and manage robust cloud solutions.

CyberEd Pentest Warrior

This comprehensive program takes you from the basics of penetration testing to advanced techniques for specific environments. You'll also learn to communicate your findings and provide actionable remediation steps to your customers or leadership. The CyberEd Pentest Warrior Pathway blends theoretical knowledge and practical experience. It includes:

1. **Foundational Knowledge:** Start with a solid understanding of penetration testing concepts and the cybersecurity landscape.
2. **CompTIA Pentest+ Certification:** Prepare for the CompTIA Pentest+ certification, covering planning, vulnerability identification, attacks, reporting, and tools analysis.
3. **EC-Council Certified Ethical Hacker (CEH):** Dive deeper into advanced hacking tools and techniques with the CEH certification, ensuring you can think and act like a malicious hacker, ethically.
4. **Hands-on Hacking Lab:** Apply your knowledge in a real-world environment, engaging in simulated attacks and refining your skills in practical scenarios

+1-609-356-1499 • info@cybered.io • www.cybered.io

CyberEd
MAGAZINE