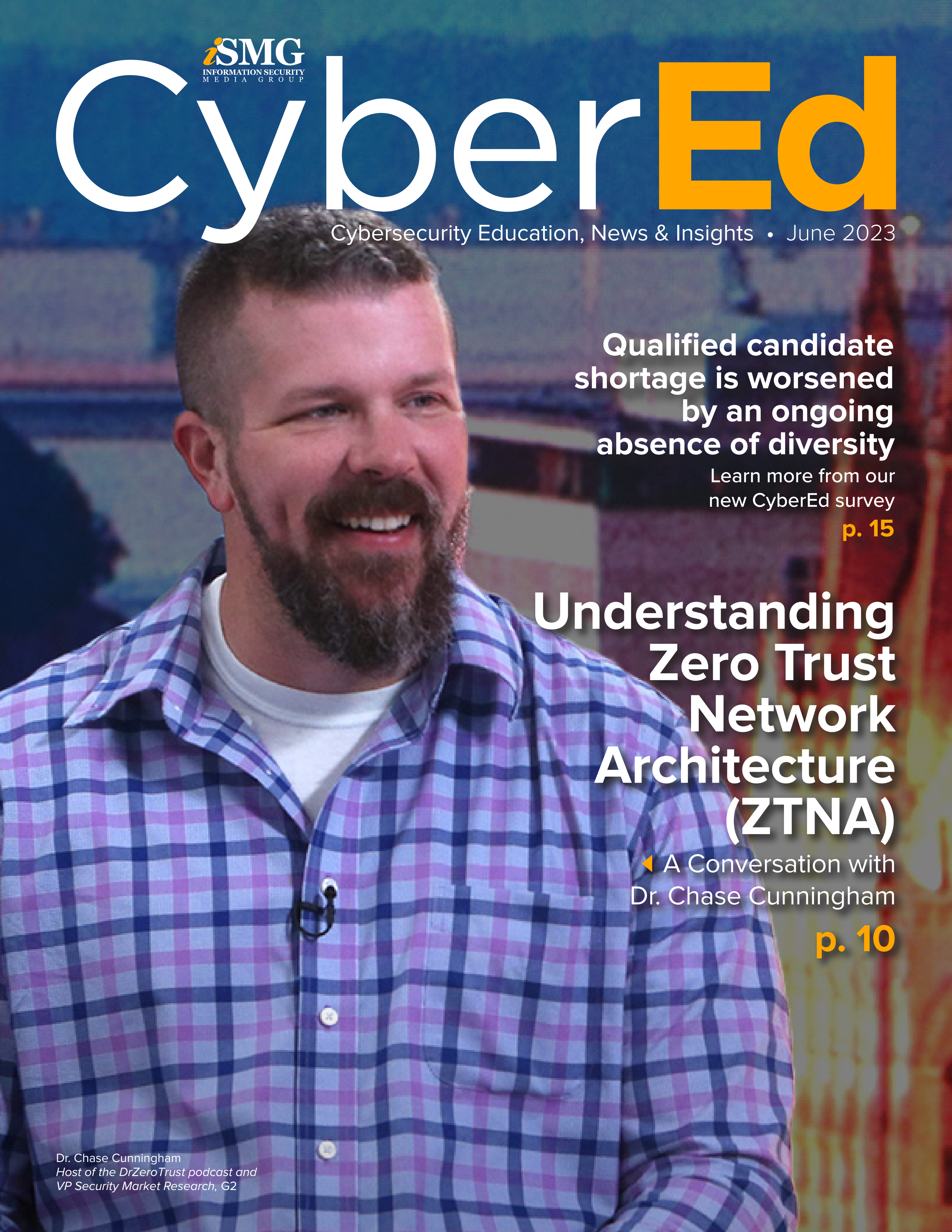
iSMG
INFORMATION SECURITY
MEDIA GROUP

CyberEd

Cybersecurity Education, News & Insights • June 2023



Qualified candidate shortage is worsened by an ongoing absence of diversity

Learn more from our new CyberEd survey

p. 15

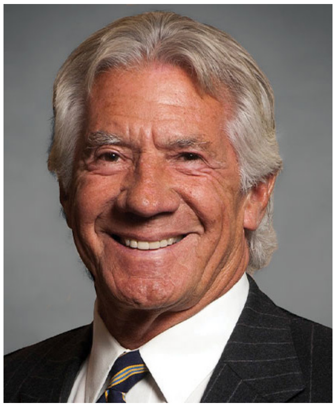
Understanding Zero Trust Network Architecture (ZTNA)

A Conversation with Dr. Chase Cunningham

p. 10

Dr. Chase Cunningham
Host of the DrZeroTrust podcast and VP Security Market Research, G2

Letter from the Managing Director



Steve King
Managing Director, CyberEd.io

An experienced cybersecurity professional, Steve has served in senior leadership roles in technology development for the past 19 years. He has founded three Cybersecurity startups with successful exits, and has served as the CISO for Wells Fargo Bank's Global Retail technology division. He also served as CIO for Memorex and was the co-founder of the Cambridge Systems Group.

Welcome to CyberEd 2.0, the 2023 Version!

Welcome to CyberEd Magazine's Mid-year Issue.

CyberEd.io magazine is published quarterly to promote our relaunch of CyberED.io, the cybersecurity education division of Information Security Media Group. This mid-year issue of our quarterly magazine is designed to offer worthwhile intelligence on cybersecurity-focused educational topics. To that end, we have provided meaningful insights from our expert cybersecurity thought leaders, which we hope you will find both informative and entertaining.

Since our inception in May 2006, we've created educational assets for our audiences, including webinars, interviews, panel discussions, and conference sessions. CyberEd.io includes an exclusive and extensive library of thousands of educational sessions, and is now complemented by 3,000 additional courses from industry leaders such as ACI, CSA, AttackIQ Academy, Range Force, Wizer, LivingSecurity, ISACA and (ISC)2.

CyberEd's coursework has been vetted and curated by our advisory faculty, which includes many of the most highly regarded CISOs in the industry. Our goal is to provide the highest quality education and training courses anywhere, with easily accessible content that is relevant across every industry segment and modern threat vector. We want to help our subscribers to continually improve their cybersecurity competency in the easiest and most effective way possible.

Check out a few of this issue's features:

- Our Cybersecurity Events Roundup shines a spotlight on AI and machine learning, indicating a need for stronger defenses, such as opting for biometric authentication as one factor of MFA, because it's much harder to crack than a 4 digit password. Overall, it's clearly best to err on the side of frequent, cybersecurity education and training.
- We interview a member of our CyberEd faculty team, Chase Cunningham, host of the DrZeroTrust podcast and VP of Security Market Research at G2, about his advocacy of the Zero Trust Network Architecture (ZTNA). He explains how the adoption of ZTNA can help organizations to reduce excessive trust in organizational networks and lower the risk of breach incidents from the levels we all see today.
- Learn more about hiring challenges and the skills gap from our new CyberEd Survey Report. With nearly 400 surveys completed in less than 30 days, its clear many leaders, across industries need this type of information to help them bridge the skills gap.

Here's hoping you find worthwhile information in this magazine, and I hope you'll take time to let us know what you'd like to see in the future.

It's your education, and it's our goal to help you achieve your mission.

Best,

Steve King
Managing Director, CyberEd.io
Information Security Media Group

NEW COURSES

CyberEd.io
Complete Cybersecurity Education, Training and Certification – Entry-Level to CISO
CyberEd.io makes it easy to close the cybersecurity skills gap

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

2023 Issues, Topics and Interviews

MARCH	Cover Story: Interview with John Kindervag Learning Path Spotlights: Cloud Security, Risk Analysis
JUNE	Cover Story: Interview with Chase Cunningham Learning Path Spotlights: Security Warrior, Penetration Testing
SEPTEMBER	Cover Story: Interview with Richard Bird Learning Path Spotlights: Digital Forensics and ICS
DECEMBER	Cover Story: Interview with Steve King Learning Path Spotlights: Security Engineering and SOC

Cyber**Ed**

CyberEd Magazine Editorial
Chief Executive Officer **SANJAY KALRA**
General Manager **MICHAEL D'AGOSTINO**
Managing Director **STEVE KING**
Marketing Director **JULIE JORDAN**
Executive Director **BRAD OLIVE**
Product Manager **JAY BOESMAN**
Product Manager **KYLE SCHMECHEL**
Executive Editor **BARBARA REIMERS**
Lead Graphic Designer **CAITLIN PERSICHILLI**
Social Media Coordinator **CAITLYN CALANDRA**

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

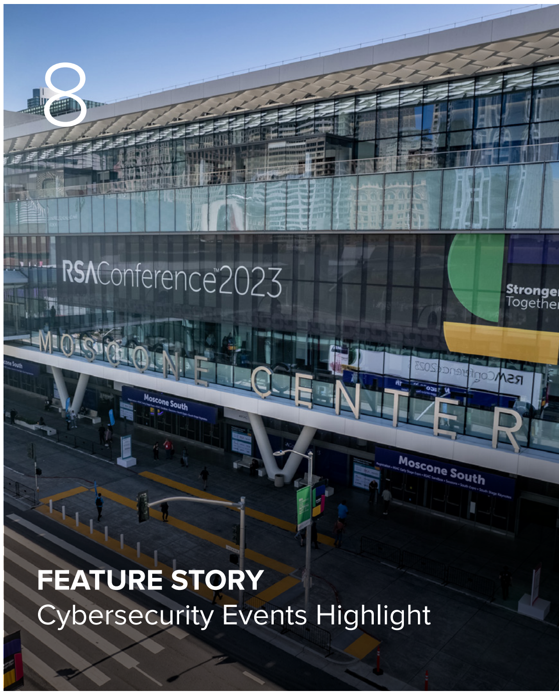
iSMG
INFORMATION SECURITY MEDIA GROUP

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

INTERVIEW
Understanding Zero Trust
Network Architecture
10



8

FEATURE STORY
Cybersecurity Events Highlight

A Roundup of Recent Cybersecurity Events

Takeaways from recent cybersecurity conferences that shine a light on the need for AI integration

After reading analyst reports from **RSAC** this year, cautious optimism is a key takeaway, combined with excitement for 2024 possibilities. Our team noted a large, enthusiastic and generally congenial crowd, and every CISO we spoke with was glad that we were back among the living, albeit a little grouchy about price increases from certain vendors.

From this and other recent cybersecurity events, we learned there is also a lack of new products that have inhaled the mystic charms of ChatGPT and are ‘engagement ready’ for use on the front lines.

For our team, the challenge with generative AI today is that OpenAI has emerged as a bright, shiny object able to vacuum up vast amounts of data and spit out custom-tailored content, with no particular outcome in mind. The cybersecurity implications of this emerging technology are huge, and many in our community are predicting that the technology will soon have the ability to overwhelm everything, including our current cybersecurity defenses.

With the **BlackHat Asia** conference in May and **BlackHat USA** coming in August, everyone is likely to see tons of self-generated malware running around networks avoiding detection by earnest anti-malware code, also developed by ChatGPT.

After all, GPT-4 is smart enough to pass the bar exam, so how could a few lines of malicious code be a problem? And thanks to the stripped-down interface anyone can use, concerns that the OpenAI tools could turn any would-be petty thief into a technically savvy malicious coder in moments were, and still are, well-founded.

RSAConference2023
adversary that's very, very smart. Well good in hiding their
#RSA

Photo Credit RSAC 2023

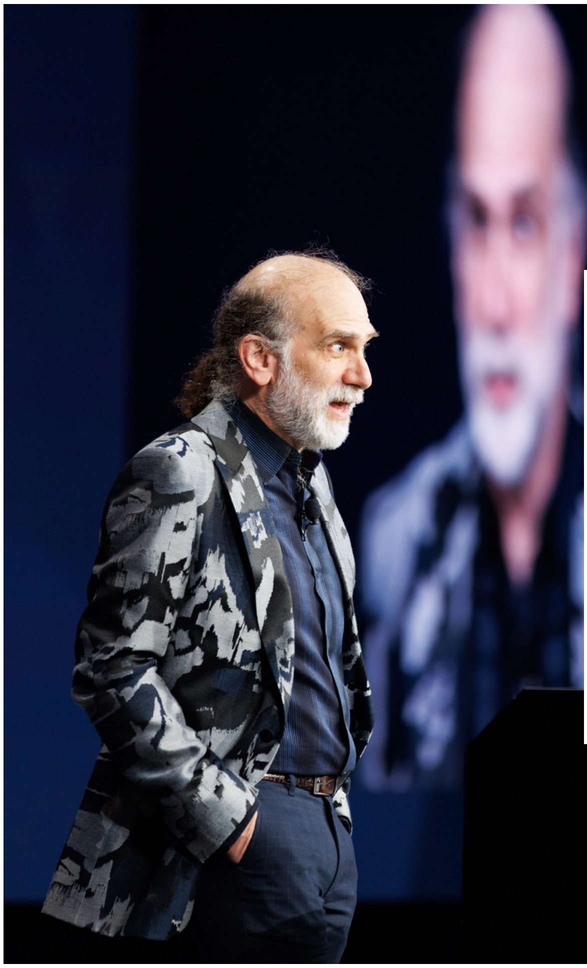


Photo Credit RSAC 2023

OpenAI co-founder Greg Brockman told a crowd gathered at **SXSW** in March that he is concerned about the technology's potential to do two specific things really well: spread disinformation and launch cyberattacks. "Now that they're getting better at writing computer code, [OpenAI] could be used for offensive cyberattacks," Brockman said.

As you would expect, current safeguards that keep users away from content deemed too violent or illegal, are ignored as users easily find jailbreak workarounds. And, legislative attempts stall at the very definition of what it is we are trying to regulate. The list of unintended consequences is spectacularly long.

But in the meantime, we are left to rely on various ‘alleged’ solutions from market leaders who still must create their own traction, and demonstrate that they can lead us to a well-protected ‘promised land.’

So far, based on the early promises of Zero Trust and subsequent attempts at enterprise-level rollouts, we have scant evidence it is working.

This is not a Zero Trust problem.

Advocates, including our team at CyberEd, are vocal and active as ever, yet the enterprise opposition seems to present a huge barrier to pushing through pilot AI initiatives. This points to a failure to communicate and a missed opportunity by consulting firms whose bread and butter should be reliant on ZT projects. We need to get smarter.

Visit us to learn more.

Photo Credit RSAC 2023

Dr. Chase Cunningham
Host of the DrZeroTrust podcast and VP Security Market Research, G2

Understanding Zero Trust Network Architecture (ZTNA)

A Conversation with Dr. Chase Cunningham

Dr. Chase Cunningham, host of the DrZeroTrust podcast and VP of Security Market Research for G2, focused on the origins and history of remote network access, VPNs and the evolution -- through design and architectural improvements -- to the Zero Trust approach to remote network access, or ZTNA. While working as an analyst for Forrester Research, Chase created the Zero Trust eXtended framework, developed the Zero Trust portfolio of accounts and provided strategic guidance on Zero Trust, artificial intelligence, machine learning and security architecture design for security leaders worldwide. He has also worked in various capacities supporting NSA, U.S. Navy, FBI Cyber, and other government mission groups. He is a deeply experienced Cybersecurity analyst and we are lucky to have him as a Senior Fellow on our CyberTheory Institute board.

In an interview with CyberEd.io, Dr. Cunningham emphasized his adamant pro-Zero Trust stance, underscoring how the adoption of a Zero Trust Network Architecture can help organizations to reduce excessive trust in our networks and lower the risk of breach incidents from the levels we all see today.

CYBERED: Why is Zero Trust so crucial, especially compared to VPNs, as a modern cybersecurity protection mechanism?

DR. CHASE CUNNINGHAM: I have nothing against virtual private networks (VPNs) in general, when after you set aside their implementation quirks, security porosity and latency, they seem fine. In fact, back in 1996, it was applauded as a revolutionary approach to establishing a virtual point-to-point connection through dedicated circuits or tunneling protocols over existing networks. ZTNA however, is so much better, it is hard to warrant much debate. But, here goes, nonetheless.

As we read in the news and in Zero Trust market analysis, there’s growing support. The DoD is aligning billions of dollars to Zero Trust initiatives. Zero Trust is now global in nature, and the strategic benefits continue to grow. However, there seem to be some misconceptions about the value proposition of Zero Trust. We often see posts and analyses talking almost exclusively about the specific technical benefits of a Zero Trust strategic approach. This makes sense because technology helps us achieve the end state we are working to reach, but technology is the "how." It is not the "why" for Zero Trust.

The "why" for a Zero Trust approach is ultimately about business outcomes, not solely technical outcomes. Traditionally, organizations focused on protecting network access with technologies such as on-premise firewalls and virtual private networks (VPN). Remote users gain access to business networks and resources by logging into a VPN, creating a secure virtual tunnel into the networks. However, problems arise when VPN login credentials fall into the wrong hands or a security risk originates within the organization. As enterprises now need to support secure remote access at scale, the risks associated with VPN use only surge.

CYBERED: Would you explain a bit about the evolution of ZTNA?

DR. CUNNINGHAM: In the wake of the digital revolution and remote work policies in response to the pandemic, the number of employees and systems outside the conventional IT perimeter has grown exponentially. Cybercriminals are exploiting this opportunity by blending in with the growing volume of data traffic and launching more sophisticated attacks.

The Zero Trust security model is designed from the ground up to prevent and mitigate the damage of such data breaches by necessitating even authorized users, devices and systems to prove they are authorized before gaining any access. Through micro-segmentation, it empowers IT teams to arrange resources in discrete zones, containing potential attacks and preventing them from spreading laterally throughout the network. Sensitive data and information are secured through the use of granular, role-based access policies.

The expansion of the data footprint is also a factor that necessitates Zero Trust. The castle-and-moat model was designed for a time when an organization's resources resided locally on-premise. But today, most enterprises' resources lie scattered across multiple cloud platforms and data centers, diffusing the traditional perimeter. We no longer have data lakes. We now have data oceans. The legacy approach to cybersecurity has become ineffective in these hybrid cloud environments.

Dr. Chase Cunningham inside ISMG Studios.

CYBERED: Given the skyrocketing costs associated with data breaches, how can Zero Trust Network Access help reverse this trend?

DR. CUNNINGHAM: The Ponemon Institute's Cost of a Data Breach Report states that lost business was the greatest expense associated with a data breach. This accounts for nearly 40% of the cost of a data breach attributed directly to customer attrition. In addition, the added cost of acquiring new customers due to diminished reputation contribute significantly to increased customer turnover. A breached business suffers across the board and history tells us 95% of all breaches can be avoided. Replacing VPN systems with a Zero Trust Network Access solution is a great first step to eliminate that threat.

CYBERED: Nowadays, many organizations under-utilize ‘best security practices’ and ‘under-invest’ in proven technological solutions. What can be done to overcome these challenges?

DR. CUNNINGHAM: Security is no different from any other market. If we ignore the realities of space and think that we are somehow different even if we are doing the same thing that others who failed did, then aren't we delusional? This is pretty simple, choose to take a different approach or expect the same outcome. Are there technologies that can help us get to the desired end state faster? Absolutely. Just as with any other market space some technologies can help us reach an end state if we use them intelligently and in line with our overarching strategic goals. Much like accounting software has revolutionized small business operations, or Salesforce has changed the game globally by streamlining the sales process, a few key technologies are critical to a successful Zero Trust strategy.

CYBERED: Can you share more about ways Zero Trust can help organizations improve their cybersecurity posture?

DR. CUNNINGHAM: The Zero Trust strategy requires an organization to continuously verify an entity's identity and treat all access requests as if they originate from a compromised, unprotected network. To do this a few things must technically happen. The technologies employed must be able to do the following four things, at a minimum:

1. Continuously validate access and requests to resources: there must be an ability to process authorization dynamically rather than access being solely based on a singular input from a policy engine. Those requests must be reliant on a time horizon. In other words, there is no unfettered access, and there is no access without a dynamic set of criteria being met before any asset is made available.
2. Provide least-privileged access: access is restricted based on identity and a variety of telemetry that powers contextual decision-making for the policy engine. The technology does not take any single input and then allows access. Multiple steps are necessary for access to be granted and intelligent telemetry is leveraged across requests in real time.
3. Separate network-level vs application-level access: VPNs use network level access and take a blanket approach to that network. Once authenticated, fraudulent or not, that access is provided to "all" resources that might be available to that user. Additionally the privilege level of many VPN's is excessively powerful and introduces risk for an infrastructure. ZTNA, on the other hand, adopts the opposite approach, providing no access unless an asset – an application, data, or service – is expressly permitted for that user. Anything not specific to the policy is invalid and outside of the bounds of acceptable use.
4. Perform device assessment: Employees in today's workforce regularly utilize personal laptops and other devices to work, it's a BYOD world. Therefore, ZTNA's device verification checking capability is crucial for a cybersecurity strategy to be optimal. A business should be able to verify that a device has the correct protections in place and that the device's patch level is up to date before access is granted. This helps manage BYOD and often can help secure a user’s home or personal device.

On average it takes 197 days for a company to **discover a breach.** Those that contain one in less than 30 days save over $1 million.

CLOSE THE GAP.

You need strong cybersecurity skills to discover and contain breaches.

CyberEd.io is reinventing cybersecurity education and closing the skills and knowledge gap. With our comprehensive courses, custom learning paths and award-winning faculty, you can upskill your team to help them become the cyber warriors you need today.

Source: Cost of a Data Breach Report

CyberEd.io

375.456.3350 | Cybered.io | info@cybered.io

Unlocking the Secrets of Cybersecurity Training:

Highlights from CyberEd's New Survey Report

Gain insights to navigate ever-evolving cybersecurity demands from our recent CyberEd Survey Report. With nearly 400 surveys completed in less than 30 days, its clear organizations need this type of information to help them bridge the skills gap. Here are a few key highlights from our recent online survey:

1. **Qualified Candidates:** Finding skilled cybersecurity professionals is a Herculean task. A whopping 55% of respondents revealed that the availability of qualified candidates falls short of meeting their needs for critical cybersecurity roles. The struggle is real!
2. **Hiring Hurdles:** Out of all respondents, a mere 20 individuals found hiring for any type of cybersecurity job "extremely easy." That's a tiny fraction in a sea of challenges. It's time to face hiring difficulties head-on!
3. **Tackling the Talent Shortage:** The global shortage of cybersecurity jobs is estimated at a staggering 3.5 million. Overcoming this shortfall demands innovative strategies across organizational levels and job roles. Are you ready to think outside the box?
4. **Roadblocks to Success:** In the relentless battle against cyber threats, two major roadblocks emerge: organizational visibility and budgetary constraints. Discover how these hurdles impede effective threat detection and response, and learn how to break through them!
5. **The Knowledge Gap:** Cybersecurity awareness training is lagging. Astonishingly, only 36% of organizations provide cybersecurity awareness training to all employees. Meanwhile, industry estimates reveal that more than 90% of breaches originate from phishing attacks. Find out how to bridge this critical knowledge gap!

With the hiring challenges, talent shortage, and rising threats due to a lack of cybersecurity awareness, relying solely on hiring processes alone is no longer sufficient. It's time to equip your workforce with the educational resources they need to better defend against cyberattacks.

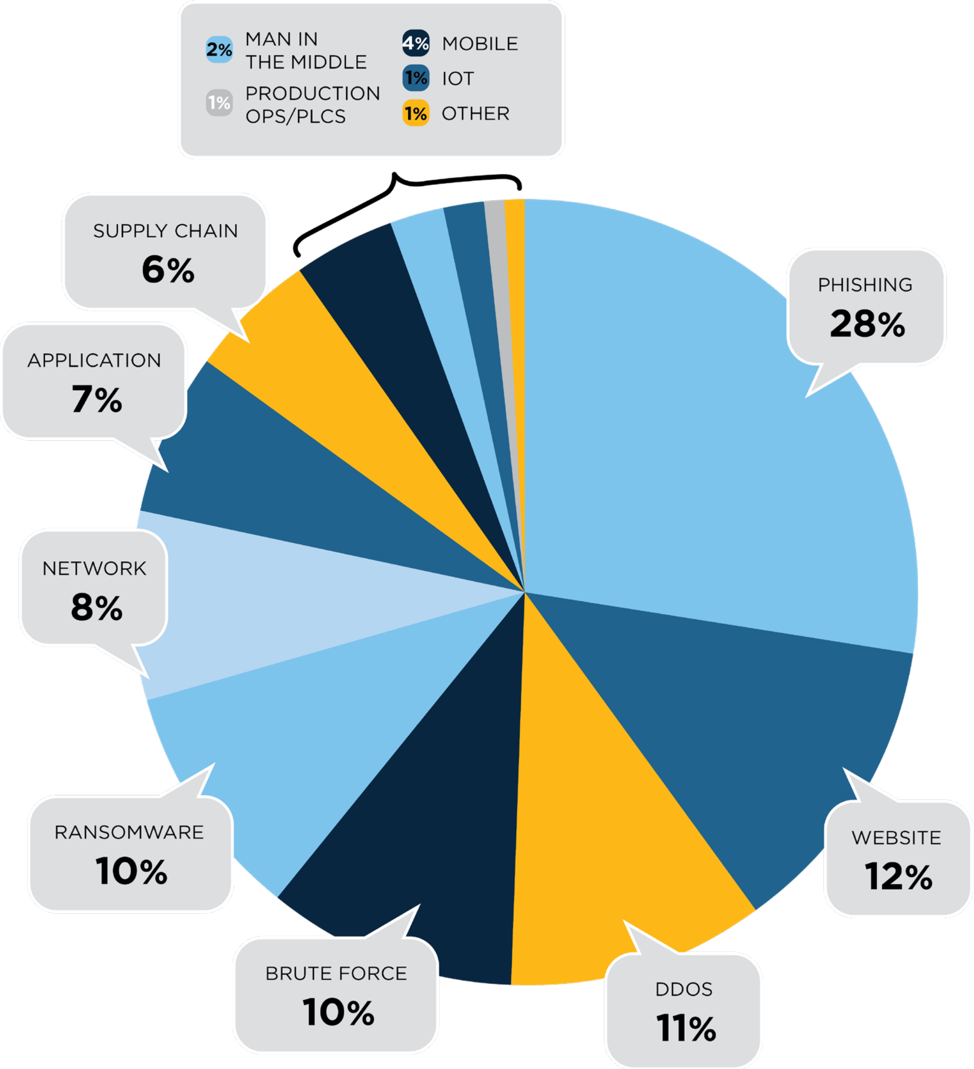
Download our full survey report here to learn more.

Greater Cybersecurity Awareness Needed

It's no secret that cyberattacks are becoming more frequent, which signals an urgent need for more cybersecurity education/training for individuals and organizational members alike.

Survey respondents said the most common cyberattack techniques by far include Phishing (cited by 28%), followed by Website Attacks (cited by 12 %), DDOS (cited by 11%), Ransomware (cited by 10%) and Brute Force attacks (cited by 10%).

Click here to read our full report.

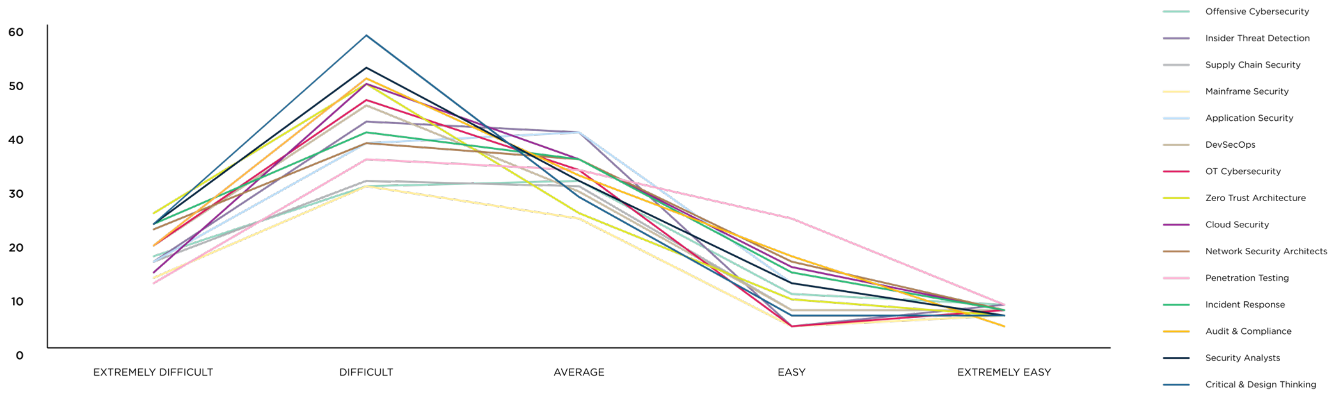


Survey Underscores Hiring Challenges

Finding qualified candidates for cybersecurity roles remains an ever daunting challenge. More than half (55%) of respondents said the availability of qualified candidates was inadequate or poor, when it comes to meeting their needs for key cybersecurity personnel.

Hiring difficulties vary, but only 20 of 393 respondents found hiring “extremely easy” for any types of cybersecurity jobs.

Click here to read our full report.



HIRING DIFFICULTY BY JOB ROLE

JOB FUNCTION	DIFFICULT	AVG/EASY
Offensive Cybersecurity	**37%**	33%
Insider Threat Detection	**41%**	40%
Supply Chain Security	**32%**	32%
Mainframe Security	**30%**	24%
Application Security	**43%**	43%

JOB FUNCTION	DIFFICULT	AVG/EASY
DevSecOps	**47%**	34%
OT Cybersecurity	**45%**	32%
Zero Trust Architecture	**56%**	29%
Cloud Security	**50%**	41%
Network Security Architects	**47%**	42%

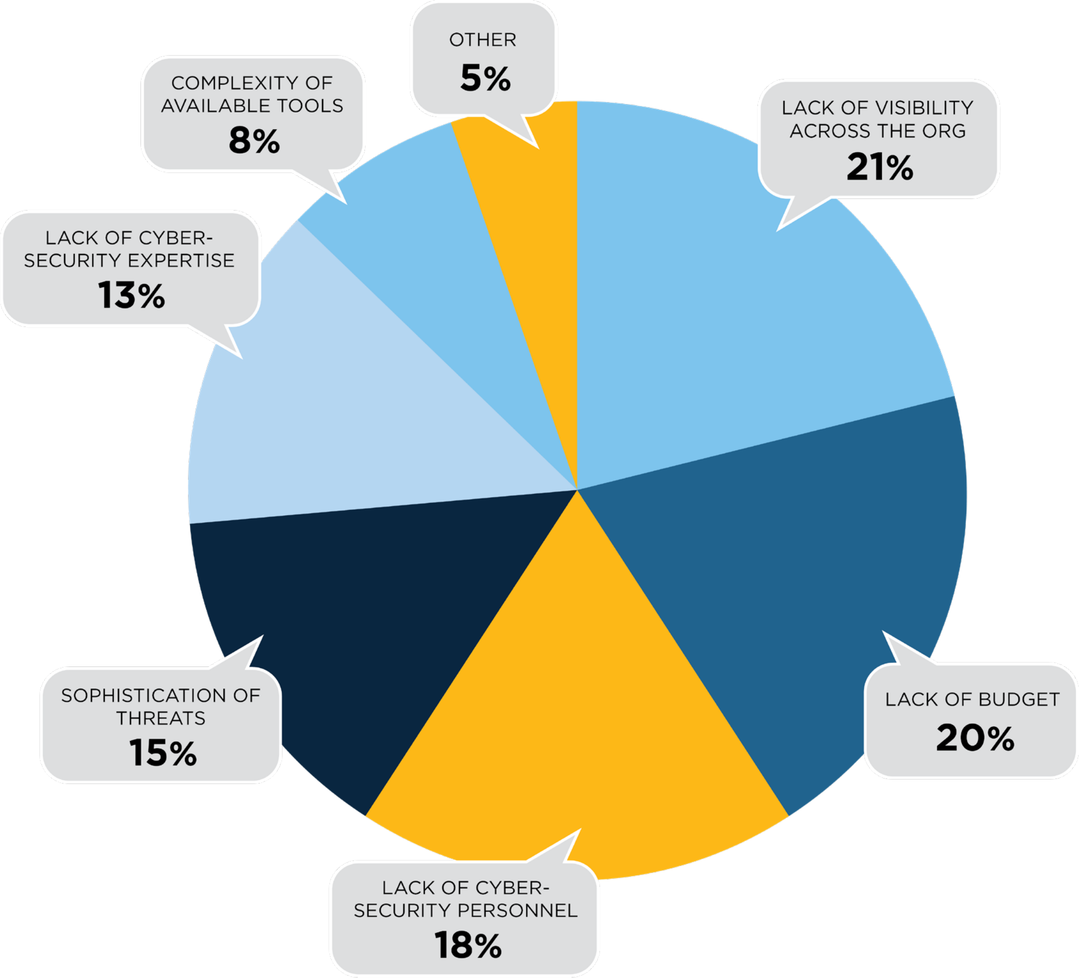
JOB FUNCTION	DIFFICULT	AVG/EASY
Penetration Testing	33%	**52%**
Incident Response	**45%**	44%
Audit & Compliance	**48%**	42%
Security Analysts	**56%**	37%
Critical & Design Thinking	**58%**	31%

Detection and Response Roadblocks

To help overcome a lack of budget for cybersecurity training, as noted by 20% of respondents, it's important to articulate the rising need for cybersecurity knowledge among today's boards of directors and business leadership. This, combined with increasing regulatory requirements levied on organizations around Governance, Risk, Compliance (GRC) make training a necessity. And both topics demand greater cybersecurity acumen and agility, in operations and in the C-Suite to better manage and strengthen cybersecurity protections.

Consider exploring ways to increase CISO and CXO engagement opportunities. Collaboration and understanding can help overcome these challenges. This sentiment was echoed in respondent comments as well. "I'd like to see a stronger association promoted between the cybersecurity and GRC domains," said one North American Industrial Security Architect/Engineer.

Click here to read our full report.



CyberEd Featured Faculty

EVE MALER

CTO, ForgeRock

As ForgeRock's CTO, Eve is a globally recognized strategist, innovator and communicator on digital identity, security, privacy and consent. She helped co-create landmark technologies such as XML and leading standards such as SAML and User-Managed Access (UMA). In prior roles she served as a Forrester analyst and risk analyst with John Kindervag. She's also a strong advocate of Zero Trust identity.

DR. CHASE CUNNINGHAM

Host of the DrZeroTrust podcast and VP Security Market Research, G2

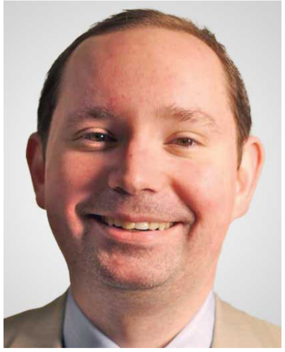
Host of the DrZeroTrust podcast, Chase is an early advocate and proponent of the Zero Trust strategy and is currently VP of Security Market Research at G2. In this role, Chase shapes the company's strategic vision, roadmap and key partnerships.

He 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.

GREG TOUHILL

Director, CERT Division, Carnegie Mellon University Software Engineering Institute

As director of the world-renowned CERT division of Carnegie Mellon University Software Engineering Institute, Greg leads researchers, software engineers, security analysts and digital intelligence specialists in researching security vulnerabilities in software products. He has contributed to long-term changes in networked systems design. He was appointed by former President Barack Obama as the first CISO of the U.S. government.



GEORGE FINNEY

Chief Security Officer and Director of Digital Interests, Southern Methodist University

As chief security officer for Southern Methodist University, George is an early Zero Trust advocate and an expert on policy, awareness, compliance, operational management and the complex legal issues surrounding modern information security. He's also a best-selling author of cybersecurity books, including the award-winning, Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future.

GRANT SCHNEIDER

Senior Director of Cybersecurity Services, Venable LLP

Grant is a recognized leader in the cybersecurity sector with extensive experience driving organizational change, developing policy and governance structures, and driving technology modernization initiatives. Having served as the U.S. federal chief information security officer (CISO) for the White House, and on the White House National Security Council (NSC) staff as a special assistant to the President and senior director for cybersecurity policy, and as the Defense Intelligence Agency chief information officer (CIO), Grant is uniquely positioned to assist global technology clients with navigating strategic, operational, and risk management needs.

SAM CURRY

VP, CISO, Zscaler

Sam is a 30-year veteran of the cybersecurity industry. Early in his career, he helped invent the first personal firewall, and also devised early stealthy VPN technology. Among many roles, Sam has served as Chief Security Architect at McAfee, head of MIT's RSA labs, CTO at EMC and SVP and CISO at Microstrategy. He holds 17 active cybersecurity patents, sits on boards of directors and teaches at Harvard, Wentworth Technology Institute and Nichols College. He's also a NIST Fellow.

JEREMY GRANT

Managing Director, Technology Business Strategy, Venable LLP

Jeremy is a member of Venable's Cybersecurity Risk Management Group, advising clients on policy implications across, IT, cybersecurity, identity and payments sectors. An early Zero Trust proponent, he is a recognized expert on identity authentication and proofing. He has also held multiple roles at NIST, leading the program office for the National Strategy for Trusted Identities in Cyberspace, and serving as senior executive advisor for identity management.

TOM KELLERMAN

SVP of Cyber Strategy, Contrast Security

As SVP of Cyber Strategy for Contrast Security, Tom is responsible for developing and overseeing the company's government and financial sector strategy, advising agencies, standards bodies, financial institutions, insurers and regulators. In prior roles, he led cybersecurity strategy for VMWare and served as chief cybersecurity officer for Carbon Black.

The Five Laws of Cybersecurity

Safeguarding Our Digital World

NICK ESPINOSA

Chief Security Fanatic, Security Fanatics

Espinosa is Chief Security Fanatic for Security Fanatics, an Illinois-based cybersecurity consulting and IT services firm. Espinosa is a leading cybersecurity industry speaker, columnist, author and a former CISO.

In our vast and diverse world, where thousands of languages and cultures coexist, there are certain universal languages that bridge the gaps of understanding. Mathematics is one such language that transcends cultural barriers. However, in today's digital age, the largest culture by far is that of internet users. With billions of people online daily, we share a common language through networking protocols, social media platforms, and the ubiquitous emoji's.

But amidst this connectivity, one language that often eludes comprehension is the language of cybersecurity. Here are the five laws of cybersecurity we must negotiate every day, regardless of language:

Law 1
If there is a vulnerability, it will be exploited

Throughout history, individuals with malicious intent have sought to exploit vulnerabilities in various systems. From the early days of robbing banks to the sophisticated hacks targeting computer networks, hackers constantly search for loopholes. This law reminds us that vulnerabilities will always be targeted, emphasizing the need for robust cybersecurity measures, and continuous thinking about the next exploit. Finding ways around everything for both good and bad purposes is so ubiquitous today, we even have a term for it: life hacking.

Law 2
Everything is vulnerable in some way

Corporations holding sensitive data on millions of individuals have been compromised, revealing the fallibility of even the most fortified systems. The discovery of vulnerabilities in computer processors further highlights the inescapable reality that everything has some level of vulnerability. For decades we've assumed our computer processors are safe and harmless, just doing the job that they were meant to do. In the beginning of 2018, it was discovered that these technological workhorses are carrying a serious mass of vulnerability that would allow a malicious hacker to wreak havoc on all of us. From minor to major, law number 2 is really inescapable. Accept it and move on.

Law 3

Humans trust even when they shouldn't

Trust is an essential aspect of our lives, enabling social cohesion and cooperation. However, because of trust, people fall for phishing scams. They believe the $20 anti-virus program they bought for their computer will turn it into Fort Knox -- it will not. They also believe that the form they're filling out online is legitimate, when sometimes it isn't. While it may seem weird to say that we have to combat trust, but we must if we're going to survive the nonstop hacking that takes place. Phishing scams, false promises of impenetrable security software, and deceptive online forms prey on the unsuspecting trust of individuals. We have arrived at peak pathological technology and Zero Trust is the only way out.

Law 4

With innovation comes opportunity for exploitation

New, unique, innovative products are constantly being made to help us live in our homes or drive our cars or even improve our health. The Internet of Things (IoT), for example, has made our lives more convenient, but it also presents significant risks. WannaCry, Petya and NotPetya, which infected hundreds of thousands of PCs and IoT devices globally, should serve as stark reminders of the exploitation possibilities that accompany innovation. On both sides.

Law 5

When in doubt, refer to Law 1

Every cybersecurity issue traces back to some form of vulnerability. By acknowledging this fundamental truth, we can better understand the importance of proactive defense. Thinking like a hacker and anticipating potential vulnerabilities empowers us to counteract threats effectively. It is time to go on offense.

Our ability to properly defend ourselves comes from understanding that human nature itself makes these laws immutable. And when we start thinking like a hacker is when we can actually stop them. So here's to our new, common language that hopefully helps us and the world stay safe online. By understanding and accepting the five laws, we can build a stronger defense against cybercriminals and protect ourselves, our information, and our digital identities from adversarial attack. We can embrace this common language of cybersecurity and work collectively to create a safer digital world for all, or we can return to the status quo and expect that the next attack will be a crippling of a core critical infrastructure.

It's up to us.

Cybersecurity Insights Podcast

Exploring the Increase in Attacks on OT and IoT

Antoinette Hodes is Security Evangelist, Office of the CTO and a Global Solutions Architect – IoT at Check Point Software Technologies. Antoinette is an experienced Global Solutions Architect, and Security Evangelist with a demonstrated history (25+ years) in the Cybersecurity industry. Accustomed to engaging with the C-Suite, she is a public speaker, customer advocate, enthusiastic trainer and devoted mentor.

Antoinette has skills mastery in Cybersecurity, Threat Prevention, Zero Trust, Zero Tolerance, Zero Touch, Operational Technology, OT, SCADA, ICS, DCS, PLC, RTU, HMI, manufacturing, utilities, IACS, CNI, critical infrastructures, IIoT, IoT, XIoT, Embedded IoT, monolithic and distributed, scalable IoT networks, sensors, Smart Asset, Smart Home, Smart Office, Smart Building, Smart City, Smart Factory, Smart Industry, Industry 4.0, SMB, SME, ROBO, Branch and Large Scale Management.

Antoinette Hodes joined us to talk about increasing attacks on OT and IoT in the past couple of years and the role of education in putting forward an effective defense against cyberattacks. In this episode of Cybersecurity Insights, Antoinette discusses:

- What is a “Check Point Evangelist?” And, how does one earn that designation?
- Check Point’s 2023 Cyber Security Report about consolidating the entire cybersecurity posture as a step toward improved defense and resilience, and how to do it.
- How big a role can education play in putting forward an effective defense against cyberattacks and where should the emphasis be in terms of topics and study?

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

Navigating the Complexities of Cyber Insurance

Libby Benet is the Global Chief Underwriting Officer at AXA XL, a division of AXA, the largest Insurer in the world. She is a licensed attorney and an insurance industry expert who specializes in emerging issues like Cybersecurity. With over 25 years in the Cyber-insurance space, no one is better qualified than Libby to lend a hand in understanding the present and future of insurance issues in the Cybersecurity space. She earned her undergrad in Political Science from Towson U and her JD from the University of Baltimore, School of Law.

Libby Benet joined us to dive deeper into the world of Cybersecurity insurance. In this episode of Cybersecurity Insights, Libby discusses:

- The changes in the world of Cybersecurity insurance in the last 12 months.
- How does the typical policy respond if the insured has a breach which results in a third party being attacked or sustaining a loss.
- How the industry is going to be commercially viable into 2024 and beyond, and the changes that will occur on behalf of the insured.

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

How to Prepare the Cybersecurity Warriors of Tomorrow

Lonnie Price is Vice President, Cyber and Information Warfare at Peraton. He leads Peraton's corporate strategy driving the development of advanced cyber solutions across Peraton's diverse portfolio of full-spectrum cybersecurity capabilities, including offensive and defensive cyber operations and information operations. Lonnie has extensive expertise in cybersecurity, technical countermeasures, counterintelligence, counterterrorism, threat analysis, cyber investigations/forensics, and emerging technologies, such as the Internet of Things (IoT). Prior to joining Peraton, Lonnie served in senior roles at the U.S. State Department, including 17 years overseas in more than 100 countries managing security risks at U.S. embassies.

Lonnie Price joined us to talk about the impact of war in Ukraine, education and so much more. In this episode of Cybersecurity Insights, Lonnie discusses:

- The impact of the war in Ukraine on the cybersecurity landscape.
- Our biggest Achilles heel.
- The impact of education on our ability or inability to defend ourselves.

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

Integrating Generative AI into Threat Detection Processes

Chen Burshan is CEO of Skyhawk Security. Chen has led product and strategy teams for companies in the security space for more than ten years, and as VP Strategy, GM and Site Manager at Dome9 (acquired by Check Point), he helped develop the company into a leader of the CSPM (Cloud Security Posture Management) space. He was brought in to lead Skyhawk Security (spinoff of Radware and backed by Tiger Global Management) to build the next generation of cloud security. His journey as a product leader and manager in technology companies began more than 20 years ago, with roles at IBM and Cisco.

Amir Shachar is Skyhawk's Director of AI and Security Research, with extensive expertise in mathematics, computer science, statistics and data science. He is the author of the Mathematical Theory of Semi-discrete Calculus, has co-invented numerous patents in various domains and has earned multiple honors and awards for teaching, publications and innovation.

Chen and Amir joined us to dive deeper into how they integrated generative AI into their threat detection process to significantly increase the speed of detecting breaches based on anomalous activity, lowering operational costs. In this episode of Cybersecurity Insights, Chen and Amir discuss:

- How Skyhawk's Threat Detector feature uses the ChatGPT API.
- How generative AI is addressing the shortage of skilled cloud security personnel.
- What the AI arms race means for the future of cloud security, and the broader cybersecurity landscape.

Learn more by listening to the podcast here.

Dr. Rebecca Wynn
Chief Cybersecurity Strategist and CISO,
Click Solutions

Regulations Every Cybersecurity Industry Professional Needs to Know

CyberEd's New Compliance Requirements Coursework

CyberEd has launched a series of eight complimentary videos that offer a helpful introduction to the regulations all types of industry professionals need to better protect the privacy of their customers and comply with current oversight requirements.

These videos provide a detailed and fundamental understanding of the most important regulations that impact cybersecurity and identify the ways that these rules affect most everyone in their day-to-day roles.

Our video series is presented by Dr. Rebecca Wynn, Chief Cybersecurity Strategist and CISO at Click Solutions Group, a global consulting firm focused on Cybersecurity Strategy, Enterprise Risk Management, Innovation Trust, Compliance, Privacy, and Transformation. Dr. Wynn is a global award-winning cybersecurity and privacy executive, and an esteemed member of CyberEd's faculty.

CyberEd's complimentary video courses aren't intended to provide 'certification-level' competency in each of the eight regulatory domains. However, once viewed, executives should be able to provide internal guidance to aid their organizations compliance efforts.

An awareness of the issues monitored and measured enables a clear understanding of the controls and processes that must be in place, as well as the general compliance requirements for each domain.

If you are a non-cybersecurity executive, analyst or department head and require current information into the scope and extent of each regulation's requirements, these videos will provide the detailed context and clarification you need.

We welcome everyone to join us. We believe together, we can do better to rise above the cyberattacks that threaten us on a daily basis.

To learn more about these videos, please visit us here.

The 8 Regulations Explained

Cybersecurity regulations covered in our CyberEd videos include:

1. Global Data Protection Requirements (GDPR)
2. Health Insurance Portability and Accountability Act (HIPAA)
3. California Consumer Privacy Act (CCPA)
4. California Privacy Rights Act (CPRA)
5. International standard on requirements for information security management (ISO 27001)
6. Payment Card Industry Data Security Standard (PCI/DSS)
7. Systems and Organization Controls 2 (SOC 2)
8. Children's Online Privacy Protection Act (COPPA)

Pentest Warrior

Defender

- Pentest Planning & Scoping
- Information Gathering & Vulnerabilities
- Attacks & Exploits
- Reporting & Communicating
- Tools and Code Analytics
- Ethical Hacking
- Penetration Testing Cyber Range

Guardian

- Web Application Pentesting
- Cloud Pentesting
- Python for Pentesters
- Mobile Application Pentesting
- Offensive Bash Scripting

Security Warrior

Sentinel

- Core Computing Concepts
- Networking Fundamentals
- Operating System Foundations
- Hardware & Operating System Security

Defender

- Linux Essentials
- Command Line Cyber Range
- Information Security Fundamentals
- Common Malware Behaviors
- Malware & Certificates
- Malware Removal & Countermeasures

Guardian

- Cryptography Fundamentals
- Network Analysis for Incident Response
- Computer Forensics
- Firewalls & Intrusion Detection
- IDS/IPS on Linux
- Advanced Intrusion Detection

Learning Path Spotlights

CyberEd.io builds cyber-warriors who can meet a broad spectrum of cybersecurity demands, think like a hacker, understand modern adversarial attack vectors, and leverage offensive security skills from hacking to penetration testing to full red team arsenals so that they can better defend critical assets, protect against broad threats, and take the battle to the enemy as well.

Our CyberEd.io Cyber-Warrior program offers custom-curated course paths designed to help guide learners through the process of mastering the primary topics required for their roles, and to prepare them for various certifications. Cyber-Warrior paths cover 290 courses organized around 33 structured and prescriptive learning paths, designed to produce training resources along the lines of a Delta-Force class Army Ranger who are capable of defending forward. The coursework was based on input received from a team of more than 40 CISOs who consulted on the design.

With diverse learning paths based on practical scenario testing and gamified security awareness, we cultivate a cyber-savvy workforce. CyberEd.io also provides learners with the competitive advantage of helping to prepare them for more than 140 cybersecurity certifications from industry-leading certification bodies along with our proprietary and accredited certificates.

Over time, CyberEd.io security certificates will confirm both the authority and competency of Warriors based on our rigorous training and the 150+ hours it takes to complete and graduate.

In this issue, we highlight two Cyber-Warrior learning paths:

- Security Warrior
- Penetration Testing Warrior

SECURITY WARRIOR LEARNING PATH

The Security Warrior program is our deepest and most comprehensive learning path, built to help students gain the foundational security skills that are needed to create competent cyber warriors who are prepped and ready to take on the fight against cybercriminals of all types. To that end, we offer three levels or tiers for students to follow on their journeys, starting at the beginner level, or CyberEd Sentinel. Next is the intermediate level, called CyberEd Defender, and our highest level or Advanced Recon level is referred to as CyberEd Guardian.

PENETRATION TESTING LEARNING PATH

Our Pen-testing Warrior path is a great way to start your career in cybersecurity. Students learn the basics and join a ‘red team’ to perform simulated attacks on their own environment, then communicate results and furnish remediation steps to customers and leaders within their organizations.

Visit CyberEd.io learning paths to learn more.

CLOSE THE GAP.

Talk to a CyberEd Expert today

CyberEd.io

Visit cybered.io

@cyberedio

CyberEd.io

CyberEd.io

CyberEd.io

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