iSMG
INFORMATION SECURITY
MEDIA GROUP

CyberEd

Cybersecurity Education, News & Insights • March 2023

Welcome to our inaugural issue!

Learn about our NEW CyberEd Cybersecurity Training and Education Platform

p. 6

Mitigate Risks with Zero Trust

A conversation with
◀John Kindervag

p. 8

John Kindervag
Creator of Zero Trust
Senior Vice President, Cybersecurity Strategy
and Group Fellow
ON2IT

70% of cybersecurity leaders say they **don't have enough skilled cybersecurity employees.**

CLOSE THE GAP.

Staff deficits put organizations at risk of a cyberattack.

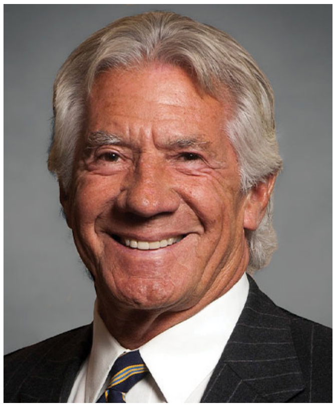
CyberEd.io is reinventing cybersecurity education and closing the skills and knowledge gap. With our comprehensive courses, custom learning paths and award-winning faculty, you can upskill your team and become a cyber warrior now.

Source: The 2022 (ISC)2 Cybersecurity Workforce Study

CyberEd.io

375.456.3350 | Cybered.io | info@cybered.io

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 our new 2023 CyberEd.io magazine, published to accompany the relaunch of CyberED.io, the cybersecurity education division of Information Security Media Group. The inaugural issue of our new quarterly magazine is designed to offer worthwhile intelligence on cybersecurity-focused educational topics. To that end, we will bring meaningful insights from our expert cybersecurity thought leaders every quarter, which we hope you will find both informative and entertaining.

You're no doubt aware of ISMG, but did you know we're set to turn 17 this year? Our pilot media site, BankInfoSecurity, debuted in May 2006. What an amazing journey it has been. From a single publication serving North American banks, we've grown into a global enterprise with more than 35 media properties worldwide. GovInfoSecurity, HealthcareInfoSecurity and DataBreachToday are among the best known, but did you know about other newsworthy developments in 2023? In addition to our CyberEd.io edtech initiative, we launched CIO.Inc, partnered with the Cyentia Institute, and acquired a majority stake in Grey Head Media and XtraMile, an Israel-headquartered, B2B lifecycle marketing company.

Since our inception, we've created educational assets for our audiences, including webinars, interviews, panel discussions, and conference sessions. CyberEd.io includes our exclusive 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 two of this issue's features:

- John Kindervag, creator of Zero Trust, Senior Vice President, Cybersecurity Strategy, ON2IT Group Fellow at ON2IT – and a huge advocate of cybersecurity education. John, with employer advice in our exclusive interview: "As far as education is concerned, without a dramatic improvement in both treatment, coverage and scale, we will continue to have a tough time adapting to the speed of technological evolution. Our practitioners need current, relevant, just-in-time education and that's why I am partnering with CyberEd.io. This training service was designed by CISOs for cybersecurity and is the best there is."
- Learn about CyberEd.io – Discover more about our comprehensive, learner-centric platform, as well as our broad curriculum and impressive faculty advisory board. I know you'll 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.

Current and Upcoming 2023 Issues

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

CyberEd

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
Mitigating Risk with Zero Trust
8

Letter from the Editor ... 3

Masthead ... 4

Upcoming Issues ... 4

ISMG Launches CyberEd.io ... 6

Mitigating Risks with Zero Trust ... 8

Cybersecurity Awareness Training ... 12

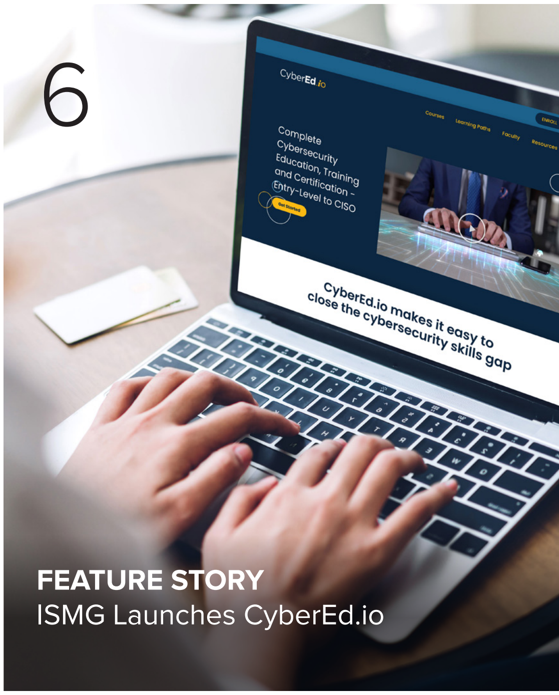
Featured Faculty ... 18

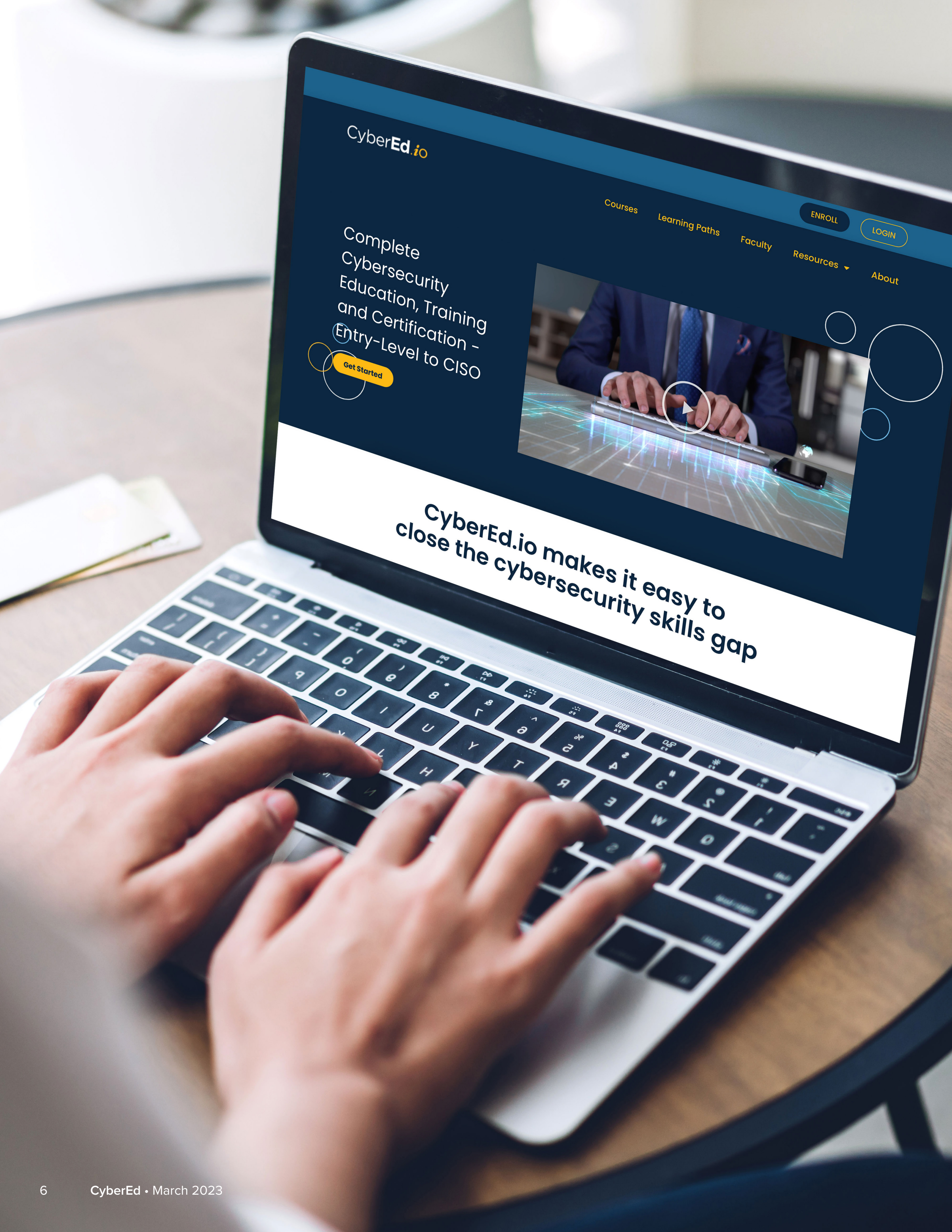
New Coursework: Value-at-Risk ... 20

Cyber Threat Blocking, DNS, & Threat Intelligence ... 24

Learning Path Spotlights ... 30

Back Cover ... 32


CyberEd.io
Complete Cybersecurity Education, Training and Certification – Entry-Level to CISO
CyberEd.io makes it easy to close the cybersecurity skills gap
6
FEATURE STORY
ISMG Launches CyberEd.io



Complete Cybersecurity Education, Training and Certification – Entry-Level to CISO

CyberEd.io makes it easy to close the cybersecurity skills gap

ISMG Launches CyberEd.io

Offering Comprehensive Cybersecurity Education to Help Close the Gap

Across a broad spectrum of vital industries, from banking to finance, to healthcare and critical infrastructure, ISMG is driven to deliver the best, most in-depth cybersecurity and risk management information and education.

Through the years we've witnessed cybersecurity's evolution, which has expanded organically and exponentially since ISMG was founded in 2006. Today, our global reliance on digital technology is driving an overwhelming need for more and better training and education.

That's why we launched CyberEd.io, our innovative eLearning platform to meet the needs and challenges presented by the realities of our ever-evolving digital world.

Comprehensive, learner-centric training

CyberEd.io offers a single, comprehensive eLearning platform dedicated to educating cyberwarriors, and upskilling professionals across every level, from the earliest stages of cybersecurity understanding, through to top-level executive boardrooms. Our curriculum-driven, learner-centric platform helps users develop critical thinking skills needed to bring immediate tactical advantages that help mitigate risks.

CyberEd.io is structured to meet the needs of cybersecurity professionals and non-professionals alike, with technical, hands-on, active defense and defense-forward training, to help address our ever-expanding skills gap.

Curriculum to unify fragmented options

Against a backdrop of patchy alternatives with no centralized source of trust, CyberEd.io brings a single, comprehensive educational platform, delivered just in time, featuring the broadest range of curated and relevant classes and training. With thousands of courses and unique learning paths, our CISO-led curriculum delivers content-rich, lecture-style coursework accompanied by Continuing Professional Education (CPE) credits to satisfy any individual user's ongoing certification aspirations.

Unparalleled insights and expertise

We've also launched the inaugural issue of our quarterly CyberEd Magazine, which will feature interviews with faculty advisors who understand how CyberEd.io contributes to the broader cybersecurity dialogue, and how to address the challenges every organization faces in protecting vital resources. This month, John Kindervag, creator of Zero Trust, provides a progress report on Zero Trust's evolution, as well as his take on need for more and better investments in education to better protect mission-critical assets and operations.

Let us know what you think. Reach out to us at cybered.io.

John Kindervag
Creator of Zero Trust
Senior Vice President, Cybersecurity Strategy
and Group Fellow
ON2IT

Mitigating Risks with Zero Trust

A Conversation with John Kindervag

Following the landmark presidential executive order E.O. 14028 and an OMB memorandum that were drafted to support Zero Trust principles, the concept of 'never trust, always verify' has grown into a global cybersecurity standard embraced by public and private sector entities.

In an interview with CyberEd.io, Kindervag discusses:

- What organizations should do to reduce deployment complexities;
- Regulatory fatigue and other factors driving the current cybercrime 'golden era';
- The need for greater CISO representation on corporate boards.

Kindervag is considered one of the world's foremost cybersecurity experts. He is best known for creating the revolutionary Zero Trust Model of cybersecurity.

Kindervag currently advises both public and private sector organizations with the design and building of Zero Trust networks and other cybersecurity topics. He holds, or has held, numerous industry certifications, including QSA, CISSP, CEH and CCNA. He has a practitioner background, having served as a security consultant, penetration tester and security architect. His expertise lies in the areas of secure network design, wireless security and voice-over-IP hacking.

Can you describe how Zero Trust has progressed in recent years?

JOHN KINDERVAG: The presidential executive order changed the rules of the game. I used to joke that Zero Trust was like Fight Club, you don't talk about it. President Biden now recommends that you should talk about it. The E.O., and later guidance that came from the Office of Management and Budget (OMB), advanced Zero Trust concepts.

Since then, the NSTAC report from the President's National Security, Telecommunications, Advisory Council Subcommittee on Zero Trust and Trusted Identity Management published findings that have only furthered the cause. Now it seems everybody's talking about Zero Trust, which is amazing as I never thought we'd be in this position.

Tell us more about the uptake you've seen.

KINDERVAG: I recently returned from a two-week European trip to Spain, the Netherlands and Germany. There I found several large organizations working on Zero Trust projects, really buying into it. Increasingly, I find organizations are starting to work on such projects. Some are farther along than others. But that's the cool thing about Zero Trust, it's not an all or nothing proposition. It's incremental. It's iterative, it's non-disruptive.

Where do you anticipate enterprises may struggle in their zero trust journeys?

KINDERVAG: The biggest challenge comes from thinking you must do it all at once. Many organizational leaders believe they must do everything, all at once. But Zero Trust inverts that concept. Instead, Zero Trust was designed so you can focus on one protect surface at a time, such as say, a credit card database. That's one project. The next project may involve protecting your human resources system. Another may focus on hospital elevators. That's an important thing to protect since elevators are controlled by computers. You can make each of those things a Zero Trust project.

Eventually you will work your way through protecting the entire enterprise. It's also important to note, there are likely many things that don't need much protection, if any. I see people spending millions of dollars to protect websites, for example. But if the only thing on your site is information that you are trying to give away your customers, you don't need to spend inordinate sums of money on something that the organization gives away for free.

In the last year, Russia's invasion of Ukraine topped the news. How has that conflict impacted cyberattacks?

KINDERVAG: Two things come to mind. I've noticed is that many organizations were forced to move people, plants, processes and materials out of Ukraine. Many organizations had to relocate facilities, including IP facilities to other parts of the world. Ukraine was renowned for good programmers and some good IP folks and some interesting companies. That's all changed.

The second thing is both the Ukrainian and the Russian governments are crowdsourcing new attack methodologies, from people who wouldn't otherwise work in that part of the ecosystem. Both sides have declared it's your patriotic duty to create new attacks for our battle against the other side. And those methodologies are starting to filter into the hands of nation-state actors, and cybercriminals. Who knows what will come of that, but it's definitely something that we must keep an eye on.

We increasingly see attacks that bypass weak multifactor authentication (MFA). What can be done to prevent organizations and users from falling prey to MFA fatigue?

KINDERVAG: Most people still to put too much faith in identity protection solutions, that were once called two factor authentication. We changed the numeral 'two' to the letter 'M' and suddenly MFA became new and sexy, though it's been done for years. MFA does not equal to Zero Trust. It's not good enough. Think about two attackers: Snowden and Manning. The organizations they attacked both had strong MFA in place, users were authenticated, but nobody looked at packets, post-authentication.

You can't make an access decision based on a single piece of information, such as the authentication information from MFA, or any single IAM solution stack. Of the four Zero Trust design principles, principle three involves controlling access on a 'need to know' basis (least privilege). And Zero Trust design principle four involves inspecting and logging all traffic. If you go beyond MFA and use design principle three, and somebody gets past your MFA or IAM solution, you have a way to stop a bad thing from happening. If you currently rely on MFA alone, that's a problem. I've seen many organizational leaders lean into ramping up MFA to resolve identity and access challenges, mostly because they were told MFA is all you need.

Shifting to the regulatory landscape, post-E.O., what developments do you expect in 2023?

KINDERVAG: Yes, I see more cybersecurity regulations coming in the weeks, months ahead. However, as you know compliance does not equal security. New regulations may incentivize better security practices, but as we previously discussed with MFA fatigue, we may be heading into compliance or regulatory fatigue.

What are the implications of the ongoing recession on cybersecurity spending?

KINDERVAG: Cybersecurity spending will go down as every organization tries to cut budgets, but the attacks won't decrease. Our attackers are not affected by regulatory issues or the economic climate. It's not like, oh well, we can't afford to attack anymore. In fact, this is 'go time.' This is a golden era for cybercrime.

Putting this into perspective, companies must invest in cybersecurity. Right now they spend too little. And for every data breach, I believe risks could have been mitigated for less than the cost of the legal fees involved. They need to know cybersecurity is a warfare domain. It's foundational to keeping your business alive and running. Without systems and networks, your business does not run. No matter what business you're in. This is especially true for large organizations that we rely on every day. That's why I constantly say, 'get your house in order.'

What will it take to get one's house in order?

KINDERVAG: Corporate boards must add cybersecurity professionals immediately. If cybersecurity is foundational, leaders must focus on doing the right thing to keep the organization running. Cybersecurity can't be considered simply a cost center. It's the thing that keeps your organization alive. It's like your heart that keeps the blood flowing to the brain, which runs the business. Perhaps this metaphor doesn't work. But the lack of understanding about cybersecurity at the highest organizational levels is unnerving. I teach for CyberEd and run webinars to explain cybersecurity and Zero Trust to boards of directors. Most boards really don't understand, nor take it seriously. But they absolutely must. So far, only one cybersecurity expert I know has a board position at a publicly traded company. That's crazy. Instead, cybersecurity experts should be snatched up for boards, right and left, due to the value they bring in terms of realistic guidance that organizations need to stay alive.

John Kindervag inside ISMG Studios.

How important in your estimation, is cybersecurity education right now?

KINDERVAG: "As far as education is concerned, CyberEd is foundational and without a dramatic improvement in terms of treatment, coverage and scale, we will continue to have a tough time adapting to the speed of technological evolution. Our practitioners need current, relevant, just-in-time education and that's why I am partnering with CyberEd.io. This training service was designed by CISOs for cybersecurity and it's the best there is."

Cybersecurity Awareness Training

Why a Managed Service Delivers the Best Outcome

We widely recognize that a significant gap exists between supply and demand for skilled and trained human resources in Cybersecurity. We also know that over 95% of breaches can be tracked back to a human error, largely inadvertent, yet catastrophic for the employer.

We contend however, that the gap and the fallibility are exaggerated by a lack of cultural consciousness and that security awareness and certification training programs have historically focused on individual employee mobility versus that of the sponsoring organization.

In other words, it doesn't do an employer much good to roll out a security awareness training program without a contextual infrastructure – e.g., what it means to the organization as a whole – and refreshing it infrequently means that any fundamental lessons learned from prior programs will be forgotten. When scheduled sporadically and on an ad-hoc basis, we send a message that building a security awareness culture is not important to the organization and as a result, the programs themselves find it difficult to achieve the traction they seek.

In addition, the context has atrophied against the current threat landscape as most of these programs are not updated to reflect the current risk models. And, most security awareness training today is focused on the individual versus the organization, and as long as that remains the case, we will fail to integrate any consciousness into the cultural fabric of the underwriting organization.

It also doesn't further the employer's cause when we randomly agree to sponsor an employee's request for certification training in one of the fields through which they may earn a badge that proves they have had that particular training – these courses are expensive (e.g., the total cost of a CISSP certification can easily get to $3,000) and require 70 hours to complete – and since a passing grade on the final exam is not revealed, (it must be 700 on 1,000), we never get to know whether the learner got 999 or 701 – which are two very different outcomes.

In the vast majority of these loosely managed cases, that employee, having received his or her certification, will soon be working for someone else at a much higher salary than the one they are earning now.

With a managed service program, that employee will be certifying in skills on his or her learning path, designed to serve the employer's best interests and be much more closely aligned to the overall organizational objective and in line with cultural goals. Thus reducing the chances that they will seek new employment elsewhere. When people are engaged, they are less likely to seek alternatives.

Most organizations delegate the administration of D&T programs to the HR and/or employee development function. Others try and push training back into the CISO's organization or onto security teams.

Which is OK, assuming the CISO, HR and D&T folks have the skills and bandwidth to execute that duty, but the reality is that they don't. Asking an HR team or security team who are already resource-constrained to administer a Cybersecurity Training and Educational program is essentially a guarantee that the program will not be effective. Not because they aren't good at what they do – they are. They just don't have the bandwidth to manage it.

While there have been great strides made in both acknowledging Cybersecurity as a set of risks and in developing defense products and service to combat those, we have not done an equally good job of developing the skills and culture internally to assure we can support future threats.

Culture Trumps Strategy.

While Cybersecurity training tends to center on technology upskilling, creating that culture of security consciousness is actually of equal importance – we know this because 95% of breaches track back to human error – and developing the mentorship programs that lead to that culture must be managed in a very deterministic process. Organizations will never achieve a goal of cultural consciousness by scheduling security awareness training twice a year.

The “science” of Cybersecurity is complex and the challenges of absorbing new layers of technology into our existing eco-system on a continual basis argue strongly in favor of continual education and upskilling – new network, container, cloud, edge computing, DevSecOps, and remote engineering skills are essential just to maintain pace with current growth initiatives let alone the pressures of the 4th industrial revolution and digital transformation.

Falling behind is not an option.

But, equally important and complex is the human cultural influence, the art, on organizational resilience in Cybersecurity. Attending classes on AWS Containers in order to certify is very different than attending classes on AWS Containers because there is a passion to learn – a passion to get better, to contribute to an improved overall organizational security posture and the pride a learner can take away from their participation.

In today’s DIY training and education model, we work from a course catalog and hope that our students are sufficiently self-motivated to absorb the new skills and apply them on our behalf. If we collect metrics around phishing, for example, it will tell us something superficial about our security culture. It’ll tell us what people are doing, not why they’re doing it.

Understanding the “why” is absolutely crucial because it will become our point of influence to change behavior and begin to create that culture of consciousness that we seek. The “why” helps in understanding underlying assumptions and determining what we can do to address gaps between what the security team needs to accomplish and what people are actually doing.

Understanding the organizational culture, mission and values will inform a change model and establish a baseline for progress toward Cybersecurity cultural objectives, against which metrics can be applied to assure that the more challenging program goals are effective and being achieved.

Seven Advantages of Managed Cybersecurity Education and Training.

Managed Cybersecurity Education and Training is the contractual agreement between an employer and a third-party provider, where the employer transfers the management and responsibilities of all Cybersecurity training to a company who specializes in delivering it on a rigorous and disciplined schedule over a set time frame.

The recent popularity of outsourced education is being driven by the COVID pandemic, recessionary economic pressures, a shortage of skilled resources and the increase in sophisticated Cyber-attacks against which organizations are unskilled to defend.

Three factors have escalated cyber risks for organizations worldwide. First, the attack surface continues to expand. In part, that’s due to the burgeoning number of IoT connections that will reach 83 billion by 2024, up from 35 billion connections in 2020. Second, cyber attackers are beginning to skirt firewalls and security software that might have been effective in the past. And third, fragmented cybersecurity solutions leave gaps that make data vulnerable.

We have now entered a near perfect storm of conditions that threaten to set back the progress Cybersecurity defense has made through both labor and technology over the last five years. Without a complete reengineering of our approach to Cybersecurity training, we will needlessly expose ourselves to vulnerability exploits throughout our environment, retain the layers of excessive trust found in our networks and cloud configurations, and continue to add layers of complexity onto our eco-systems without any visibility into our attack surfaces.

Whether on the awareness training front or on the AWS Container front, we need to address these vulnerabilities with a heightened sense of urgency as Industry research continues to tell us that the gap is widening and our sills are below par.

1. Reduced Cost – Leveraged Pricing Advantage w/Single Source

As opposed to seventy some odd catalog companies claiming to be eLearning platforms, where customer organizations are left to navigate on their own to find and schedule, monitor and track, and report on progress for their learner population, CyberEd.io provides structured learning pathways designed around a curriculum vetted and peer-reviewed by industry CISOs, that guarantee outcomes around specific competencies.

Ranging from Delta Cyber-warrior training to Pentesting and Red Teaming to Data Privacy, CISO Up-skilling and Operational Controls, the CyberEd.io coursework is designed to produce a pre-determined level of competency across the complete family of NIST-defined Cybersecurity job roles.

Our program onboarding process begins with the assigned customer’s success manager working with sponsoring users to determine the specific training outcomes desired, identifying the learning candidates, and structuring a program that will accommodate successful learning paths for each culminating with an earned certificate of accomplishment within each job role addressed.

Onboarding includes the cultural discovery phase and the roll out of our security cultural consciousness campaign details, mentoring program specifics, and a schedule of participation for the year.

Amazon / Wal-Mart Economies of Scale

In addition to the more obvious efficiency savings inherent in joining an existing, best practices program that has been designed to scale to customized versions for a variety of customers, and one that is run by Cybersecurity experts who have a thorough understanding of what training is required for competency in defense of today's threats, we are able to leverage our relationship with a dozen catalog partners to negotiate reduced program fees and we pass those retail discounts direct to our customers.

2. Assured Relevancy through Curated Coursework by CISO Advisors

Our faculty advisory team is comprised of CISO volunteers from all walks of industry, who continually vet our course curriculum and learning paths to assure we are sharing the most relevant information related to today's active threats and that we establish the proper context for high probability absorption and retention.

Unlike so many of our competitors who simply present their catalog from which students self-direct their learning without regard to a greater picture upon which the organization will depend for future cybersecurity defense, our managed services advisor insures that all coursework pursued is within the context of a pre-set learning path, designed specifically for the needs of your organization.

Think of this as a concierge service designed to select exactly the right training and education that fits your company or organization security posture.

3. Zero Risk of Delivery Failure through Contractual Focus

One of the primary causes of failures in all, on-demand security awareness training is that most programs fall out of use over time. In a managed services agreement, part of our SLA is measured on managing the delivery of the training content in a rigorous, disciplined, participative and orderly manner.

Our job is to make sure that monthly and quarterly training reviews are fresh and entertaining, that they match your cultural values so that your learners are comfortable and that they are interesting enough to keep your learners engaged.

We deliver this result through a combination of long term review and testing aligned with calendar management, CISO reviews, our mentoring program which assists in managing organizational transition, and active cultural development programs witch underscore change management.

Our objective is to become an institutionalized business partner with our client organizations and work alongside their security team to continue driving and extracting value over time.

4. Increased Efficiency through Designed Learning Paths

Our learning paths have been developed by our faculty advisory team within the context of work roles and curriculum designed to populate and modernize cybersecurity teams, competent to manage operations, compliance, defense and technology amid heightened risk from a broad variety of threat actors across an expanded threat landscape. Hybrid Cloud, Containers, Mesh, Edge, Open APIs, Open Source Supply Chain software and 5G are only now becoming realities that must be dealt with soon and the bad guys have already begun to develop their exploits of the vulnerabilities inherent within.

Part of the value we add is to anticipate the challenges in Cybersecurity education before they become realities in our everyday lives and design education and training programs that address every one of them. We make sure that we have learning opportunities for new technology announcements before they become markets so that our customers don't have to.

Each learning path is designed within context, so we eliminate redundancy, avoid missed necessities, and each path becomes a living extension of the overarching curriculum. Thus, our customers save both time and money along with their new-found ability to detect, identify, categorize and mitigate zero-day threats before they become breaches.

5. A Defined Journey to Cybersecurity Consciousness as Culture

The by-product of a managed security program is the growth of a culture of Cybersecurity consciousness that, when distributed widely through the organization, can accelerate its institutional development.

Combined with an active mentoring program that brings employees involved directly with Cybersecurity into influencer relationships with employees outside the Cybersecurity domain and planned programs of competition and acknowledgement can rapidly transform security-passive organizations into security-native movements based on best practices and workplace responsibility.

The benefits are substantial and long-lasting. Just providing people with risk information doesn't mean they will change their behavior to activities that are less risky, But, when they can understand

what's at stake with what they can see with their own eyes, encouraged by confirmation from their mentor, it is remarkable how quickly the culture can transform.

Improved Employee Retention through Mentoring and Cultural Momentum

One of our programs that add to the entertainment and discovery side of the leger is what we call the George Finney Cybersecurity Personality Rorschach. As we've said, we believe that one of the highest value components missing from traditional security awareness programs is helping people believe that they can make a difference when it comes to cybersecurity.

Our test, which is part of our onboarding process, will help learners discover which of the 20 different cybersecurity personality types they more closely match and which learning traits will carry the most value to the learners.

The first step in changing habits is to understand that there's a well-defined Habit Loop. Thanks to Mr. Finney, we have "Hacked" that Habit Loop and pass results along to our learners in the form of "recipes" for strengthening cybersecurity habits, and understanding each learner's Cybersecurity Habits Profile can help them protect themselves and their community.

Once institutionalized, we believe learners will begin to build and apply them every day and our cultural meet-ups will encourage the sharing of strengths and blind spots with other student members to help build a diverse team.

Leaners will receive our bi-weekly newsletter covering breaking news from the cybersecurity industry, written in consumable language. When there's a breach, learners will know about it and about the context in which it occurred. When there's a new scam, learners will hear about it before it affects their organization.

Our customer success manager will meet with the entire team once a month and review the progress, problems, and opportunities in mentoring assignments, analyze new threats that are relevant to the learners' environment providing recommendations that will act to prevent similar cyber-attacks and assuring that the focus of the team remains centered on Cybersecurity best practices at least 12X per year.

6. Custom Curriculum Opportunities

Depending upon licensing agreements, employers who sign up for Premium service will be able to work with our team of CISOs and Instructional Designers and Trainers to design completely customized courses, learning paths and curriculum, in addition to our base service offering.

This ability of course extends to labs and cyber ranges, where we will stand up a fully customized range integrated with the tools and technologies our customers use every day and/or SIEM, firewalls, and other SOC tools from leading manufacturers to simulate as closely as possible the actual threat environment our customers face.

We use industry specific scenario planning, supplemented by customized tabletop planning to enhance traditional tabletop exercises and a phased approach which allows customers' skills to remain up to date, as the threat landscape evolves and new threat vectors emerge.

Even certifications and badges unique to the customer's environment can be created to reflect higher competency through an industry-specific intensity of study (e.g., Banking at JPMC, Industrial Automation at Rockwell, Cryptocurrency at Coinbase, Quantum at IBM, etc.).

Better Training.

- Cybersecurity training and education designed and continuously curated for relevance by leading CISOs.
- Delivered through a Managed Services contract bounded by SLAs based on pre-determined learning paths aligned with NIST work roles and framework
- The creation of a managed Culture of Security Consciousness and mentoring programs assure growth, retention and change momentum
- Supported by internal marketing programs and content, including testing, newsletter, meetups, table top exercises, and competitive acknowledgements keep top of mind Cybersecurity awareness and nurture cross-organizational demand
- Custom curriculum, coursework, learning paths and design available to premium customers to most closely resemble their actual use cases and computing eco-structure
- A single source for all Cybersecurity education and training requirements through a trusted partner supported by an all-star cast of global CISOs with built in progress and compliance reporting
- Overall cost is lower than alternatives, due to economies of scale and leverage with 12 of the world's top content providers yielding retail savings passed along directly to customers

We have invested significantly over the past year and a half in developing the architecture of the program, the coursework, the learning paths, the delivery system and the certification staging. We are passionate about creating the most comprehensive, credible and relevant online learning product/service offering on the market.

Our objective is the provision of focused, prescriptive, in-depth, in-context Cybersecurity education when and where you need it. If you have any comments or questions please send them to sking@ismg.io. Thanks.

CyberEd.io Featured Faculty

CHUCK BROOKS

CISO, Adjunct Faculty, Graduate Cybersecurity Program at Georgetown University

Chuck is on the Adjunct Faculty in the Graduate Cybersecurity Program at Georgetown University and a widely respected Cybersecurity thought leader, influencer, and technology evangelist.

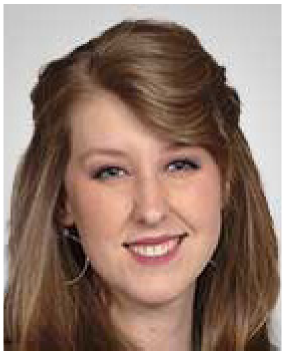
He is a featured writer/speaker/blogger on homeland security, cyber security, CBRNE, artificial intelligence (AI), Internet of Things (IoT), science & technology, public/private partnerships, Risk Management, blockchain, and security innovation.

DR. CHASE CUNNINGHAM

Doctor of Zero Trust, Chief Strategy Officer, Ericom

Known as the Doctor of Zero Trust, Chase is an early advocate and proponent of the Zero Trust strategy and is currently Ericom's Chief Strategy Officer. In this role, Chase 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.



KELLY HOOD

EVP and Cybersecurity Enigeering Expert

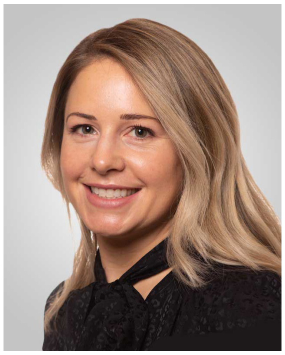
Kelly is an EVP and Cybersecurity engineering expert supporting organizations to develop and implement strategies to manage the cybersecurity and privacy risks to their business. Her focus is on cybersecurity best practices, controls, and standards, principally the NIST Cybersecurity Framework, CMMC, SP 800-53, SP 800-171, and ISO 27001. Kelly assisted the NIST Cybersecurity Framework team in the evolution of the Cybersecurity Framework and has supported the CMMI Institute in their development and expansion of the CMMI Cybermaturity Platform. Describing her as an expert in the CMMC space is an understatement.

JOHN KINDERVAG

Senior Vice President of Cybersecurity Strategy, ON2IT

John is currently the Senior Vice President of Cybersecurity Strategy at ON2IT, a Zero Trust-focused cybersecurity Managed Services Company, and the co-founder of the CyberTheory Institute.

He is the 'Father of Zero Trust', who as an analyst at Forrester, invented the term and defined the reference architecture for a network whose five basic principles defined the notion of Zero Trust.



LYNN PEACHEY

Director, Business Development, Arête Incident Response

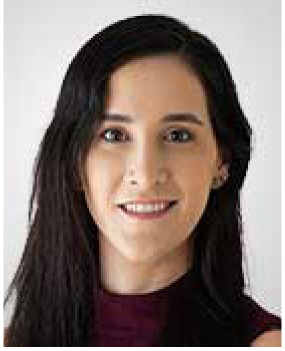
Prior to Arête, Lynn exclusively handled Cyber/Tech E&O/Media insurance claims for two of the largest US cyber carriers, AXA and AIG for six years and earned her two undergraduate degrees in Labor and Industrial Relations and Psychology from Rutgers and her JD from the Elisabeth Haub School of Law at Pace University.

ARI REDBORD

Head of Legal and Government Affairs, TRM Labs

Ari is Head of Legal and Government Affairs at TRM Labs, a blockchain analytics company that helps organizations detect, assess and investigate crypto-related fraud and financial crime.

Prior to his role at TRM, Ari was the Senior Advisor to the Deputy Secretary and the Undersecretary for Terrorism and Financial Intelligence at the United States Treasury. In addition, Ari worked closely with regulators, the Hill and the interagency on issues related to the Bank Secrecy Act, cryptocurrency, and anti-money laundering strategies.



DR. NIKKI ROBINSON

Senior Cybersecurity Engineer, IBM

Dr. Nikki Robinson is a senior IBM Cybersecurity Engineer with 15+ years' 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.

DR. CHAR SAMPLE

Chief Cybersecurity Research Scientist, Cybercore Division, Idaho National Labratory

Char is the Chief Cybersecurity Research Scientist for the Cybercore division at Idaho National Laboratory. She is a visiting academic at the University of Warwick, Coventry, UK, and a Guest Lecturer at Bournemouth University, Rensselaer Polytechnic University and Royal Holloway University.

Char has over 20 years' experience in the information security industry. Her research focuses on deception and the role of cultural values in cybersecurity events, and more recently she has focused on the relationship between human cognition and machines.

New Coursework Coming This Quarter: Value-at-Risk

The value-at-risk mathematical function is a risk model that has been widely adopted by the financial services industry, referring to the tradeoffs between value gained and the potential risks assumed when evaluating a deal. A good example in the IT space might be the migration of assets into a public cloud environment. Such a migration could result in significant loss of visibility and control of the information assets, but will definitely result in substantially lower cost. The question is what additional cost is associated with increased security over those assets and how will that investment affect the ultimate risk alignment.

Three Components

Generally, there are three components involved with the value-at-risk model: risk appetite, vulnerability, and asset value. The challenge is to objectively evaluate the value of the assets at risk, the present danger of the risk materializing combined with the exposure of the assets to that risk (vulnerability) and the overall appetite for risk among the stakeholders.

Assuming you want to do this (and you should), when evaluating your company's assets, you will need to include both tangible assets like infrastructure (network and hardware), systems or production capabilities, and intangible assets like Intellectual Property, personal and sensitive customer data, reputational impact and damage to the brand.

Soft Value Too

The value of these assets is determined by estimating the costs associated with the actual hardware, network components and software if damaged, the quantified time and effort required to recover, restore and reconstruct, the actual third party costs associated with reconstructing lost data, providing credit reporting services for at least a year for all affected customers, liability insurance loss cap costs and the requisite public relations and corporate communications campaigns which may be necessary to limit and recover reputational damage and impact to your stock price, supplier, partner and customer relationships overall.

A public breach can instantly become the equivalent of a slip of phrase from a professional athlete that causes the loss of all endorsement contracts, speaking engagements, representational contracts and associated income. Everyone is susceptible regardless of how big or small, rich or poor in assets, and seemingly inconsequential on the surface.

Reputational Damage Can Be Huge

Estimating these costs is tricky and most people wildly under-calculate. Realistic scenarios are to be found at Target and Sony where perhaps in the former case it didn't dawn on anyone that Target would be footing the bill for what may end up being a lifetime of complimentary credit background services for every customer, past present and future. And, in the latter case, it probably didn't occur to anyone that executive emails would be made public which turned out to be career devastating for several key people including the CEO, who had a phenomenal track record of performance prior to her emails being displayed on the web for all to see.

Vulnerabilities and Exposures

Vulnerability goes to the systems that you have put in place to protect and defend your assets from invasion. Part of the assessment process is subjective in that you not only have to consider whether your defenses are sufficient relative to your assets and risk-appetite, but you also have to consider the ease or difficulty with which your adversaries must contend when considering an attack. If you have established a formidable protection scheme, your adversaries may decide that it is just not worth the effort.

If alternatively, you have been unable or unwilling to spend sufficiently to create that level of protection, your adversaries may decide that your target assets are exposed in a way that makes it tantalizing enough to jump all over. Hackers are prone to finding the most exposed vulnerability and spending their resources exploiting that opportunity. If your assets rest behind that vulnerability, then you have a much higher degree of risk than you would have otherwise. Windows is a classic example of a target rich environment.

SCADA, OT and Third Party Risk

Vulnerabilities also extend to SCADA devices and depending on the intrinsic value of the overall target you may have a much greater exposure than you think. If for example your production devices form part of a larger supply chain to an ultimate high-value target, your operation may represent the most cost efficient component target in the overall target puzzle. So, an attack on your devices may have nothing to do with any single asset value of your own, but rather it simply may be a means to a higher value target

further on down the chain. As a participant in discovery, you may be in the embarrassing public position of playing a central though unintentional role in the taking of something huge.

Target Stores is the poster child for a third party component attack.

Risk appetite usually translates to budget, resources and perceived asset value or threat assessment. Because threat assessment is dependent on your ability to think through all of the variables involved in your operation and objectively analyze the complete body of possible scenarios under which you may become involved in attack, the outcome impacts both your vulnerability assessment and the way in which you value your assets. For example if you start with budget, you will automatically downgrade your asset value and your threat assessment, as the outcome you require depends on an inconsequential asset leading to a low possibility of threat.

Instead of starting with your budget constraints, try identifying all of the impacts you can think of that may result from a breach and estimate the costs of those impacts. You may find that what used to be thought of as discretionary expense moves quickly up to mandatory expense.

I can pretty much guarantee you that if your CEO thought that his or her email would be floating freely on the Web, the money you require would magically appear. Risk appetite is a moving target.

Connecting the Dots

The value-at-risk model depends on an objective analysis of the interconnectedness among these three components, and as you go through the exercise you may find that your assets are actually higher in value or have more significant consequences than you thought or that your adversaries are probably more willing to spend the resources necessary to achieve their objectives.

You may also discover that you are using dated, dead, forgotten and thus highly vulnerable systems for both infrastructure like non-supported or unpatched versions of older operating systems and databases, and applications like ERP, accounting, HR and production control. These factors present a more attractive target and influence your value-at-risk determination by increasing the volume and likelihood of attacks. If you depend on SCADA controlled devices for your operation, you may realize suddenly that they are part of a larger puzzle you hadn't considered and/or have greater vulnerability impact to your business and will also influence your overall value-at-risk determination.

Quantifying Value-at-Risk

Value-at-risk is a highly useful method for establishing actual risk in much the same way as it is essential for investors determining how much of their resource they are willing to extend in a bet on a given company, sector, currency, commodity or future state. Like anything else, if abused, value-at-risk can influence over-response in one direction or the other and should be used only as a guidepost for determining the most reasonable assessment of risk given the enormous population of unknowns and the remarkable rapidity of change in the information and cyber-security threat landscape.

The question at the end of the day is what are you doing to quantify and value the impact of a breach? If you have begun to analyze these factors and extended your thinking out to the edges of the problem space, have you begun to take cyber threats seriously yet and is the information you have discovered about your organization compelling enough to raise your own stakes in the game?

Most people in my business argue that small and medium sized businesses have fallen far behind where we should be in terms of preparedness and as a consequence, these attacks will continue to increase in volume and intensity. It is well beyond time that we do something to stem this tide and learning the elements of value-at-risk is a great place to start.

The Course

Our coursework is taught by Industry experts with a focus on solutions pertaining to risk management. The solutions include frameworks, models, tools, policies, practices, technical guidance, and training that allow organizations to assess, analyze, and manage organizational, operational, strategic, and technical risks to mission-critical assets, processes, systems, and infrastructures.

Cyber Threat Blocking, DNS, and Threat Intelligence

Pat McGarry of ThreatBlockr and Steve King, our Managing Director at CyberEd.io

Pat McGarry

Chief Technology Officer,
ThreatBlockr

In a recent interview with Pat McGarry, Chief Technology Officer at ThreatBlockr, Steve and Pat discuss the ins and outs of Cyber Threat Blocking, DNS, Threat Intelligence and the difference between threat actor behaviors and threat vector behaviors, what to look for in each and why.

Pat has been in the Cybersecurity business for 25 years, has two degrees from Virginia Tech in computer science and electrical engineering. He's been in the engineering and software technology world for that whole time and mostly served between product management and chief technology roles.

Background

KING: Why don't you, if you don't mind, give us a brief background on yourself and a little bit on ThreatBlockr as well.

MCGARRY: Sure. You hit it pretty good. I've been doing this a long time. I came fresh out of school - Virginia Tech - back in the early 1990s, and immediately started doing hardware and software engineering. Quickly morphed into the software space, initially, in telecoms and then quickly thereafter with internet-facing telecommunications, and then I piggybacked into a variety of interesting roles, almost entirely cyber focused for the better part of the last 20 years plus, both on the federal government side, in the intelligence community and whatnot, and then back and forth on the commercial side.

ThreatBlockr has a novel approach to protecting networks, data and users that most of the traditional security stacks don't have. And that's why I'm here and how I ended up here. And I've been here for three and a half years now. And absolutely love it!

How Threat Blocking Works

KING: That's great. And we're on the same page about the threat and the challenges, putting it mildly, that we have in defending against it. Can you tell us a little bit about how threat blocking works, and the actual mechanics of it?

MCGARRY: Yeah, absolutely. There's a couple of things, when you start looking at what we do versus what the industry is doing. And the hole that that we saw there. For the past 12-15 years, since the advent of that next-generation firewall, and 12 years later, we're still calling it next-generation firewall - that should be a lightbulb moment right there - how's it still next generation 12 years later? When Moore's Law says things change every two years, so it's six generations later now? Problem!

And that’s what's happened in the industry, and it's been the crux of my opinion, the problems in the industry and why people keep getting hacked, is we've been sold a bill of goods by a few vendors that say, there is a one size fits all approach. But there's not. There's not a one size fits all approach. You have to take the best of breed of a lot of things to make it a robust cybersecurity stack. And what we do differently than everybody else is we've tried to focus on the problem upside down. Everybody else thinks the problem is "I got to stop the threat vector, how I'm being attacked?" Whether it's a brute password attempt, whether it's a phishing attempt, whether it's a supply chain attempt, whether it's just somebody didn't update their software attempt.

Instead of looking at it that way, which clearly isn't working, or there'd be no headlines in the papers, we focus on the threat actor, the folks doing those things. My favorite example is how do you stop a serial killer? You catch them.

Threat Actors, Not Threat Vectors

You don't try to figure out what he's used and you don't try to figure out some other detail. You have to catch them. How do you stop a threat coming into your network or leaving your network? You stop the guy doing it. If there were no threat actors, there would be no threat vectors. So we focus on the threat actor, and that's very different than everyone else in the industry. So when we say threat blocking or threat blocking as a service, we are distinctly focused on identifying all of the known threat actors, so that regardless of how they're attacking your network, we can stop it, even if we don't know how they're doing it.

If I know that that guy Pat McGarry is a bad dude, I am not going to let him talk to my grandmother no matter what. I don't care if he's speaking English, French, Romanian, it doesn't matter. That guy is no good to me. I'm not letting him talk to anybody I know. That's what we do. That's how we're different. We focus on the actor, not how they're doing it. And that's why our eye-opening tagline of "block every threat" has so much value. Because we're blocking every threat that these known threat actors are sending your way, whether you know about it or not, whether it's known as a vulnerability, or whether it's zero day, if that guy, Pat McGarry, that nasty dude is doing this, he's stopped. And that's how we're different than everybody else.

And we do it with a set of patented technology, which kind of changes the game, because to date, most security controls out there by virtue of increasing your security, decrease your network performance, because they have to consume cycles to run. They do something called deep packet inspection to dive into the low level details of a packet and look at the data itself. We don't do that. We look just at the person sending that data in each direction and decide based on that, whether or not we should let it through or not. So we don't have to look at all that low level gory detail. We don't care if it's encrypted 1, 2, 3, 4 times, doesn't matter to us. If it's going to that guy, Pat McGarry, it ain't allowed through. And that's the big difference.

Seeing Through Disguises

KING: That makes a lot of sense. But how do you determine whether that bad actor at the other end is in fact the real Pat McGarry or facsimile thereof?

MCGARRY: You got it. This is one of the other things that we do well. And it's the core of why we created the company, well, before I got here. What these guys saw, and why I liked them when I vetted them three and a half years ago for that VC I was telling you about, what I liked was they recognize the only way you beat the bad guys, is if you use all the information available from all the good guys. What does that mean?

That means being able to take all this real time intelligence from big name vendors, like Webroot, Proofpoint, DomainTools, Bitdefender, Malware Patrol, the list goes on and on about the ISACs, like in healthcare, the H-ISAC, or energy ISAC, financial services ISAC, federal feeds when they're available from DHS or CISA, they are trying very hard to partner with commercial entities, especially here in North America, to make sure everybody stays protected.

Threat Intelligence

If you can take all that information from all those good guys, and more, plus guys in your own organization, or Sally in your IT department is collecting all this data, pulling all that data. And also, if you can pull all of this data in and leverage it in true real time, you have a chance. And that's what is critical, being able to ingest any amount of intelligence, whether it's threat intelligence, or whether it's business intelligence. For example, if I'm a Google business user, and we happen to be a threat blocker, we use Google Suite, and Google Suite publishes their known good business IPs, then I know that I can let those IPs through.

I know Google is telling me these are the real Google IPs, you're safe to use as a business, as opposed to their pool of Google Cloud Platform addresses that the whole world can use, including the bad guys.

You obviously don’t want to make those willy-nilly accessible, but all their Google Suite IPs, you want to make accessible. So the combination of all that data is how we do it. And we do it in a way that makes us very partner friendly. All those names, I rattle off, they all love us. Why? Because we don't compete against them for number one. And number two, we're eating our own dog food, saying that, hey, look, we want more and more and more intelligence, we will pull all of it in. And we pay for some of those feeds. In some cases, our customers pay for those feeds. In some cases, they are free, open-source feeds, some of the ISAC feeds.

Third Party Data

KING: What I understood you to say just now is that you find Pat McGarry not because you're looking for Pat McGarry, but because you're looking for the ones that aren't Pat McGarry. And then what's left over is a group of or a single bad guy that no one had been able to discover.

MCGARRY: That's part of it. And we do have some customers using it that way. But it's more about taking as much of this third-party data as possible, because one of them is going to know who that bad Pat McGarry is, and they're going to publish it. They're going to say this guy is really bad, you should not be talking to him, if he's in your network right now. Do something about it.

KING: And you're going to know because Pat struck before and that they have logs or they've got that strike in the past.

MCGARRY: Bingo! My favorite real world example is, and I'll plug one of the companies that we work with here, we do not pay them directly. Our customers pay for their feeds, and it's passed through costs from us called Proofpoint. They're well known in the industry, they do a tremendously good job of detonating malware in a way that's very difficult for the bad guys to detect. And I'm sure you know this, Steve, or maybe many of your audience probably does, too. But it's pretty easy in 2023 for the bad guys to figure out when you're running malware in an enclosed environment, i.e. they're looking for guys like you and me trying to find them.

So they're going to do things that don't let themselves be found. Proofpoint is world class in their ability to obfuscate the fact that they're trying to obfuscate the environment. It's an extra level. And so the bad guys think they're running on real infrastructure, and they're running their full malware kit now.

Well, as that malware kit runs that rootkit or whatever it is, and they're doing things out to the internet, and back, Proofpoint's checking all that and they can definitively say, these source and destination domains and/or IPs are coming from this very bad actor, through who cares what the threat vector is, because it could be something we know about or something we don't know or a zero day, we don't know, necessarily, but you know, that this thing is going somewhere, or trying to get information from somewhere that it shouldn't be. And that's what some of these companies are very, very good at. And they've taken to the next level.

Threat Hunting

I hate industry buzzwords, like AI and whatnot. But some of these companies do a very good job of incorporating AI into these behavioral modeling/behavioral analysis of threat actors and the vectors that they're using.

Here's an example: There's a new domain, which is registered, that traces back to a known fishy ISP in Romania. Since it's only a couple hours old, we're going to assume it's bad. And we're going to run it through our AI training models and see if it agrees. So they train the trainer, the model, to say, this thing is probably bad. Let me know if you agree, they say this is probably pretty bad, we probably shouldn't do anything with this. And they'll flag and give it a really high confidence score that's bad for a while now. If over time, it turns out to be good, they just change the score. Pretty easy!

So those kinds of models become very valuable when you're doing these kinds of cyber hunting for threat actors all over the planet. And that's something these guys have gotten very good at. Three of the ones I rattled off earlier are very good at this – Webroot, DomainTools and Proofpoint, they all do a very good job. And what I always caution folks is, the more the better. Don't think you can just go to a one-stop shop and call yourself done. Just because Webroot has more IPs that are known bad than anybody else doesn't mean its good enough by itself. You also need these other sources to build out that level of threat intelligence from all the good guys all over the planet.

KING: And you would think that, at least it occurs to me that if I were a bad guy, I would not use those same malicious domains, if you will, as a second order. Why not use legitimate domains for the first three bounces, for example. You trace that all the way back to whatever IP address it ends up at.

MCGARRY: That's right. That's exactly what these companies are very good at with their sensors deployed onto the planet to track that stuff down. That's also why we have made a conscious decision at ThreatBlockr, never to create any of our own threat intelligence. We never want to be seen competing against our data partners. We want to be the vehicle to make sure all of that data from all the good guys around the world can truly be used in real time.

So you don't kind of filter it down or believe some other vendors who say you don't need all that. Yes, you do. You need all of it. And, having said that, we have some cool technology that we can find some amazing things that no one else has figured out yet. But we have taken the approach. And we will continue this approach that it's more about leveraging all the good data that's out there. Because right now, just being brutally honest, there's nobody else that can take in that amount of data, we're the only ones.

Everybody else can ingest the data and put it in a big database, or SIEM like Splunk, or QRadar or something where they can make an action that will block the stuff. They can tell you after the fact that you were attacked. But I'd rather not be attacked in the first place. Maybe that's just me. And so that's the conscious decision that we've made is never to compete against our data providers. In fact, in a couple of cases, we worked with them to make their solutions better. From information that we knew.

DNS Dangers

KING: Just personally here, do you think that the unsecured DNS domains are getting enough attention by CISOs these days? I've seen an awful lot of unsecured DNS at the highest possible levels. Federal agencies breaking away big banks, big retailers, and it looks to me like it's an easy pathway for bad guys.

MCGARRY: It's a very easy pathway, and it's a confounding problem too because it sounds at the top level, like it should be easy to solve. There's a huge set of problems that go along with it, though. So I get why people haven't approached it what I think is the right way. On a personal note, what I feel just haven't done the attacking before is, I love the fact that everybody is now using encrypted backchannel DNS. Because every browser is using it, I can circumvent corporate policies that can't see all the DNS all the time very easily now.

And now we're in the era of hybrid workforces and work from home, when I'm at home here, I have a wife and kid, they're on the network, they're doing stuff, I got a smart TV, I got smart appliances, it's pretty highly likely that this stuff could be compromised. And very easy.

If I'm down the street in a Starbucks, if I'm in my car these days, and I'm hooked up to the internet, which most new cars are, all these things are new tech that brings to the attack surface points for the bad guys to get in. And what people forget in these environments, when you're talking about DNS and whatnot, is all this stuff can now be encrypted DNS lookups. So you're not only seeing that. It's very easy to circumvent corporate policy now, so to speak on some of these things. And what that basically means, though, is that we should all just quit and give up? No!

What it does mean, though, is understanding how the Internet works. It's funny, how a lot of folks will have us believe, erroneously, that it works because of DNS. No! The internet works based on IP addresses. DNS is a way to discover IP addresses. So when you have that "aha" moment, like, oh, yeah, I'm just looking up xyz.com., some server somewhere tells me it's at this IP address. And now I go and talk to that IP address. So if one of my threat feeds knows that IP address is bad, I'm not talking to them.

Even though my doubly encrypted backchannel DNS service, they gave me this IP address for xyz.com, said this is the right thing. My threat intelligence feed over here says 1.2.3.4 is trying to go to is absolutely positively a command and control server running out of some site somewhere that we know is bad, we're not letting you go to it. That's the difference.

So it's that "aha" moment, which is like, oh, yeah, DNS has value. But since it's multiply encrypted, since the bad guys can spin these things up and down, what it results to is the IP addresses that matter in the end. That's how computers talk to one another. It's the IP address. And that moment of understanding changes the game when you recognize them that that's how you focus on that threat actor - IP addresses, regardless of where they are, whether they're hopping around might initially go to some AWS server. But remember, like I mentioned, some of these public services now provide this threat information are very good even in identifying bad behavior in public cloud infrastructure.

AWS, Azure, GCP. The bad guys' playgrounds like Digital Ocean, some of the stuff from Rackspace, and the list goes on and on and on. But that's that "aha" moment when folks realize, you use DNS, but you use it to get an IP address, and that's what you talk to. So if you can do your intelligence based on IP addresses, it doesn't matter how the DNS has been being arrived at. It's one of those little moments that changes the game in cybersecurity when you have that realization.

Trust, But Verify

KING: It's still curious to me as to why you're solution is not widely popular.

MCGARRY: I think, honestly, the main reason I seriously believe this, I've seen it with some customers. So one of the things that we do to help people understand this massive hole they have is we tell them look, you don't have to take me from my word. I wouldn't take me from my word. I would always make people prove. Trust, but verify. That's one of the great sayings of all time. Yeah. And we saw that in the government and military side all the time.

What we say is, we want you to verify that we're not lying to you. So we tell folks is whatever firewall you currently have - Palo Alto Fortinet, Cisco, Sophos, Zscaler - whatever, it doesn't matter what you're using, or if you have multiple of them, some people use multiple of those things I just named, which is fine, too. That's a good thing, not a bad thing, in all cases. Send those logs to us. And we'll tell you at the exact date and time that that thing let something through, if we would have blocked it.

When they start to see that, the first thing is when they get this report back, it's all automated. So it's very fast. And we said we would have blocked 10,000 more things today alone. And they're like, no, that can't be right. There's no way. We have best of breed this and best of breed that and best of breed number three, there's no chance. And we're like, excuse me, these were your logs, not ours. This got through your network. And we would have blocked it and can tell you exactly why. And when we point out it's a server in Iran, it's pretty blatantly obvious why it should have been blocked, and their stack let it through. Not because their stack is bad. But because no other solution is focused on the threat actor. They're all focused on the threat vector.

That's how we get people to see the light that they got to layer this in. And then the beauty of it, one of the things that I'm the CTO, I'm not a sales guy. I'm an engineer by trade, always had been my whole life. I love it. But our stuff in comparison to other stuff out there is very cheap. People hate when I say the word cheap, like inexpensive or value or whatever, it's cheap. And it's very, very simple to when they see the value to get people to buy it and install it. That's usually not the problem. The challenge that we have sometimes is they're still in the state of denial. They don't believe it.

They think just because my existing stack is configured wrong, I can fix this myself. You can't. Because you're not focused on threat actor, you don't realize it yet. They'll go back to their vendors and say, how can we do what they do? We can't do that like that. You need the first 1,000 bad things, you can put those on our controls. What about the next 1,000? Those don't matter? Yes, they do. And that's that "aha" moment. They also realize, I see the hole here. We'll layer this in. Now, suddenly my security stack is significantly more robust at a very low cost.

Cybersecurity Awareness Training

KING: Absolutely. I wanted to get your take on cybersecurity awareness training. In your opinion, how come it hasn't worked so far?

MCGARRY: That's one of my favorite questions. To be brutally honest. I love when people ask it, because I think it's probably the single most important question in cybersecurity.

I'm a huge believer in training people. I've always believed in every walk of my life that I've dealt with government side, private injury side, that people are your most important resource, always have been, and always will be. That's why we're all here. Life's about life. And the number one thing that I see with this is, human behavior rears its ugly head.

What do I mean? It's the mentality of "it'll never happen to me." You can't train that out of people, unfortunately. It'll never happen to me, that's going to happen to the other guy, it's not going to happen to me, can't happen to me, won't happen to me, and bam! It happens to you. If we could change the way we're doing cyber awareness training, to focus on the fact that it will happen to you unless you do something as opposed to just telling people, make sure you update your passwords regularly. Make sure you update your software regularly. We're telling people to do it, they're not doing it, because they think it'll never happen to them. But it will.

And that's also where I get an issue sometimes with the federal government and how they decide to regulate everything for whatever reason. They're regulating oftentimes the wrong things. Why don't they regulate businesses updating their software regularly? Why don't they regulate rotation of passwords regularly? Make those you regulation criteria, because those are the two things that matter day to day. You do those things, and we train people to do that, and we had regulations behind it to say if you don't do this, you're going to get in trouble or fines or whatever, people start to pay attention. That's why I think we failed. We've neglected the human component to it, which is it'll never happen to me. And the regulations that we're doing are the wrong regulations.

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:

- Risk Analysis Warrior
- Cloud Warrior

RISK ANALYSIS WARRIOR LEARNING PATH

The Risk Analysis Warrior program is designed to build Enterprise Risk Management skills focused on Cybersecurity risk. Understanding the entire class of Enterprise vulnerabilities from a Risk Framework point-of-view will increase an organization's readiness and ability to out-think adversaries by anticipating attack vectors and preparing visibility, detection, intrusion suppression and capture capabilities in advance of a specific attack. Understanding Secure Code essentials will prepare security teams to identify exposures to any inadvertent insider threats before code is committed.

The combination greatly improves an organization's overall cybersecurity risk posture.

CLOUD WARRIOR LEARNING PATH

Similarly, the Cloud Warrior pathway is composed of four courses, including cloud networking, cloud applications and cloud security. Our Cloud Essentials+ is the only internationally recognized, vendor-neutral certification utilizing key business principles and fundamental cloud concepts that validate data-driven cloud recommendations. It stands alone in this field by demonstrating that all necessary staff members – not just IT specialists – understand how to increase efficiency, manage costs, and reduce security risks for organizations whenever tasked with making cloud technology decisions.

We cover and test students in AWS and Azure, Engineering and Operations. Our AWS (Amazon Web Services) Cloud Practitioner certification serves as the ideal starting point for technical and non-technical professionals to build expertise in the AWS cloud. This course provides a foundational introduction to AWS's most popular cloud services, including EC2, Lambda, S3, EBS, VPC, and RDS. You'll learn the core concepts of cloud computing and cloud security and compliance solutions, covering every objective required by the Cloud Practitioner exam. This is the most complete cloud pathway offered anywhere.

Visit CyberEd.io learning paths to learn more.

Risk Analysis Warrior

Risk Analysis Warrior

- Authorization Fundamentals
- Enterprise Security Risk Management
- Vulnerability Assessments
- Vulnerability Assessment Project
- Developing Secure Code
- NIST DoD RMF
- NIST Cybersecurity Framework
- NIST Cybersecurity Framework Project

Cloud Warrior

Cloud Defender

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

Cloud Guardian

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

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