TOP CYBER NEWS MAGAZINE

SPECIAL EDITION 2022

A Pioneer Of Change

Exclusive Interview with

Adriana SANFORD

J.D., dual LL.M.

Considering A Job In Cyber

Editorial

Michelle NGUYEN

Board Member at Cyberjutsu

HOW COURAGEOUS AND SUCCESSFUL WOMEN - CYBERSECURITY PROFESSIONALS INTERNATIONALLY - BREAK DOWN BARRIERS BY COLLABORATING, SHARING THEIR KNOWLEDGE, NETWORKING, MENTORING EACH OTHER, AND ACTING TOGETHER

"Today's shaken world needs us women to join our hands in creating an inclusive and thriving future for all. The idea behind the global Cybersecurity Woman of the Year Awards is to uplift those magnificent and extraordinary female professionals by shining light on their accomplishment in which's triumph all women can glow and rejoice.

It's a way for women to genuinely show their support for one another, with comradery, love, and kindness. Even more importantly, these awards bring together women from across the world to create an excitement and inspiration for young women to join the male dominated cybersecurity field."

~ CARMEN MARSH, PRESIDENT AND CHIEF EXECUTIVE OFFICER AT UNITED CYBERSECURITY ALLIANCE

Fore Word

I would love to see more women gaining access to the challenges of digital transformation through upskilling, re-skilling, and re-framing a role of a woman in new transforming world. Along with the ever-increasing creation of practical knowledge and scientific breakthroughs.

Women have so much to contribute to the cybersecurity field by creating, initiating fresh and different perspectives to a dynamic landscape that requires agile and adaptable thinking. If women have improved access to skills development in this area, I believe it will have a positive impact for many generations to come. The skills acquired in digital transformation are transferrable to other sectors as well. The skills are practical and can lead to scientific breakthroughs. Because of this I believe there can be a generational impact.

The generational impact is important because we live in an age of commoditized information. As a society, we are relatively new to this reality and while cyber threats are the root of information security challenges, information security challenges are increasingly becoming the root of global threats. There needs to be increased involvement of more international stakeholders with the goal of improving digital transformation skills for everyone.

These skills are powerful and for that reason I will continue to promote cyber knowledge-sharing and greater access to cybersecurity education. For more women to enjoy the digital world full of surprises and rewards! If the knowledge is power than the value of knowledge shared is the power magnified. To promote the cyber knowledge sharing and access to cybersecurity education; to create an effect that ripples outwards in women's inspiration and empowerment, Top Cyber News MAGAZINE presents: Special Edition, featuring the Cybersecurity Women of the Year 2022 Award finalists!

Ludmila M-B, Doctoral Student at Capitol Technology University

Adriana SANFORD, J.D., dual LL.M., Chile and the USA

Adriana SANFORD, J.D., dual LL.M. is a Chilean American international television commentator, corporate lawyer, author, professor, and global threats expert, who provides fundamental insights about the impact of data protection reform on individuals and their privacy. A noted speaker for the American Program Bureau, Sanford has provided the keynote addresses at some of the world's top technology, cyber, security, legal, and compliance industry conferences. In her keynote presentation in 2019 at the annual SuperConference sponsored by the Association of Corporate Counsel, she addressed hundreds of General Counsel and senior lawyers from Fortune 1000 companies regarding the multi-jurisdictional challenges in the practice of law.

Sanford is a Senior Fellow at Claremont Graduate University and serves remotely as Of Counsel with Puga Ortis Abogados, which is a leading law firm in Santiago, Chile. She frequently assists companies with building a 'Culture of Privacy' within their organization and has trained executives throughout the U.S., as well as remotely in Peru, Colombia, Panama, Guatemala, Mexico, Brazil, and the Dominican Republic. Sanford is deeply attuned to the needs of businesses and promotes the concept of a worldwide dialogue. She is the keynote speaker at the 2022 CSWY Awards Gala and the inaugural winner of the CSWY Cybersecurity Law/Privacy Professional of the Year Award.

Sanford is the keynote speaker at the 2022 Cybersecurity Women of the Year Awards Gala.

Stacy PAETZ, the USA

Stacy Paetz is an award winning Television Host, Sideline Reporter and Executive Producer in the sports and entertainment industry. Paetz began her career making history. At only 19-years-old, she made her first on-air appearance on ESPN. She became the first female and youngest individual in the NBA to host every pre-game, halftime and post-game show, as well as report from the sidelines for seven seasons on Fox Sports. She also covered the NBA playoffs for TNT and NBAtv. Stacy became the first female announcer in the 90-year history of the World Famous Harlem Globetrotters, announcing on both U.S. and International tours. She joined CBS Sports in 2018, as the featured reporter of the Inaugural U.S. Major League Rugby season, including hosting the Trophy and MVP ceremonies. She recently covered eight countries competing for gold in Softball at The 2022 World Games. Paetz is currently the Studio Host for MLR All Access on Fox and Host of the National Women’s Soccer League on Amazon.

Adriana Sanford, J.D., dual LL.M. A Powerful Voice and A Pioneer Of Change

This interview is courtesy of **Stacy Paetz,** an award winning Television Host, Sideline Reporter and Executive Producer in the sports and entertainment industry. and **Adriana Sanford, J.D., dual LL.M.**, an international media personality, author, professor, transactional lawyer, and global threats expert

[Stacy PAETZ] *I had the opportunity to interview Adriana Sanford, J.D., dual LL.M., who has been selected as the keynote speaker for the prestigious Cybersecurity Woman of the Year (CSWY) awards celebration. Sanford has thrived in multiple male-dominated arenas and is a "wonderful example of someone who highly values integrity, truth and accountability." She has repeatedly broken through barriers that scale the heights of international influence and her professional journey is a showcase of courage, resilience and perseverance that continues to inspire and empower thousands of women across the world. She is also the inaugural winner of the Cybersecurity Law Professional of the Year, and the organizers of CSWY Awards GALA are thrilled to welcome her 'back on stage.'*

A Multidimensional Leader

Adriana Sanford is an international media personality, author, professor, transactional lawyer, and global threats expert, who provides fundamental insights about the impact of data protection reform on individuals and their privacy. She is deeply attuned to the needs of business and promotes the concept of a worldwide dialogue. A noted speaker for the American Program Bureau, Sanford has provided the keynote addresses at some of the world's top technology, cyber, security, legal, and compliance industry conferences. In her keynote presentation in 2019 at the annual SuperConference sponsored by the Association of Corporate of Counsel, Sanford addressed hundreds of General Counsel and senior lawyers from Fortune 1000 companies regarding the multi-jurisdictional challenges in the practice of law.

Sanford is a pioneer, guardian, and educator. She counsels, advises, and trains executives, students, and members of the global community on security, legal, and compliance risks. Her current topics include the role of the C-suite in the privacy framework and the dark side of the digital revolution.

The Pioneer

Using her stellar academic credentials from Georgetown Law and Notre Dame Law, Sanford spearheaded the development of a cost-effective program for a multinational consumer products corporation to address the counterfeiting of products in Latin America. To implement the program, Sanford met with several senior government officials to establish new channels for communication and cooperation with those countries. This senior in-house legal position was preceded by a three-year tenure as the assistant general counsel of a trade finance bank that provided short-term lending in Latin America. A senior FDIC lawyer described her as "**truly a major asset and help to government and industry leaders alike**" with "**a sound legal mind regarding international anti-money laundering and anti-terrorism matters**."

The Guardian

Sanford is a strong international human rights defender that has engaged in a wide range of public awareness, advocacy, and research activities related to international security. Her experience addressing international organized crime and linking it to corporate fraud, bribery clubs, and other forms of business malfeasance spans a 20-year period. Among the issues Sanford has tackled are a multi-year embezzlement scheme that could have resulted in widespread unemployment; resolving a criminal arrest warrant used by a foreign partner; and an illegal scheme involving Russian loans that resulted in the arrest and 30-year imprisonment of the CEO. The former regional counsel of a Fortune 10 company has demonstrated what her colleagues describe as 'noble acts of bravery,' which resulted in a sizeable settlement and a deep working relationship with national and foreign regulatory authorities. Her desire to impact global humanitarian issues was also evident in her role on the Board of Directors of Amnesty International USA and on the Advisory Board of the World Economic Forum's Partnering Against Corruption Initiative.

The Educator

Sanford has distinguished herself as the lead author of two books on global threats that were adopted by the Institute for Supply Management (ISM) for their centennial celebration. She was also featured in "***Women in Security: Changing the Face of Technology and innovation,***" which is part of the ***Women in Engineering and Science*** book series. In academia, Sanford has taught face-to-face, hybrid, and remote synchronous and asynchronous courses in law, management, ethics, privacy, and cybersecurity to thousands of graduate and undergraduate students throughout the United States and abroad. She is currently a Senior Fellow of a private, all-graduate research university, Claremont Graduate University, which is a member of The Claremont Colleges in Claremont, California.

Sanford assists companies with building a '**Culture of Privacy**' within their organization. "Executives, corporate counsel, and corporate boards must become familiar with global privacy laws, as the subject matter continues to develop and mature and the repercussions for non-compliance include hefty fines and possibly even criminal penalties in some jurisdictions," she explains. Sanford has trained executives throughout the United States, as well as remotely in Peru, Colombia, Panama, Guatemala, Chile, Mexico, Brazil, and the Dominican Republic. She is also a keynote speaker for the 2022 ISSA-Los Angeles Security Summit XII.

A Legacy

Growing up in both North American and South America, Sanford explained that she was particularly invested in the way decisions made in the Americas have global consequences. "**For most individuals. privacy is associated with security, whether it be personal or home security, community security or national security,"** she said.

Sanford (*née Koeck, pronounced Keck*) has deep familial roots in the Americas; she is a direct descendant of one of the first settlers of St. Louis, Missouri, and a 14th generation Chilean. Her great-great-grandmother, philanthropist Philippine Espenschied von Overstolz, was featured in the 1893 compendium of biographical sketches of American women, '***A Women of the Century***', and her great-great-grandfather was the 24th mayor of St, Louis, Henry Clemens von Overstolz.

Sanford is a woman with a powerful voice on matters of national and international security concern and a pioneer of change when there is corporate malfeasance, business disruptions, or physical danger to our global community. She is often described as an '**audience grabber**' and as having "**the unique ability to speak to students, captains of industry, and academicians all in the same audience**."

Advice To Women Who Are Considering A Job In Cyber!

Editorial by Michelle NGUYEN, the USA

There have been some improvements in the industry when it comes to addressing the talent gap. Women bring a different set of skills, particularly soft skills, to bridge the gap in a male-dominated field.

Being involved with the Women Society of Cyberjutsu and Cyberjutsu Girls Academy has been extremely rewarding. I found the non-profit through a mutual friend and have been volunteering for the last few years now. They organize meetups and mixers, host job boards, and connect women in the cybersecurity industry.

One of my favorite parts of the program is the Cyberjutsu Girls Academy where the STEM program meets once a month for girls, mostly but not limited to middle-school age girls, for an interactive learning workshop where they do everything from building web pages, programming robotics, creating mobile apps and more.

The best part is seeing the excitement from the girls and their reaction to the reality of cybersecurity. They're always amazed that women like me with long silver hair, who wear makeup and like fashion, work in cybersecurity. I love being able to reinforce the message to these young girls that they really can be anything and do anything they put their minds to.

My advice to women who are considering a job in cyber!

First and foremost, just go for it. As I mentioned, women can be intimidated by a false sense of being underqualified or lacking certain education and certification requirements, but a lot of times, those things can be learned on the job. What is most needed are the soft skills that many women can bring to the job: excellent communication skills, ambition, drive, and other natural-born talents.

I'd also encourage women to network with everyone! Given that there are new threats and technology solutions coming out every day, it's imperative for practitioners to always be learning and networking with industry peers. The really cool thing about cybersecurity and technology is that it is a vast area and there is something out there for everyone.

Michelle NGUYEN, a graduate of Virginia Tech, has spent 15 years implementing software and providing technology services to Fortune 100 companies. She is currently a Regional Director at Axis Security, a Security Service Edge vendor that secures seamless access to business resources. Her specialty is working with early-stage cybersecurity startups to bring disruptive solutions to the market and partnering with customers to adopt new technology to enable and secure their business.

TOP CYBER NEWS MAGAZINE

Media Partner

Cybersecurity Woman of the Year 2022

Join the Celebration of CSWY Award Winners

Welcome Reception August 08 & GALA - August 09, 2022

Follow the #CSWY2022!

Angelique
Q NAPOLEON

The Digital Sentinel – The CISO

The CISO is a Digital Sentinel with resources poised to prevent cyber-attacks and remediation activities. The CISO is the most valued position within an organization. Threats are no longer external and the insider threat is a real concern.

The CISO selects their weapons have assessed the threats and has tools that account for advances in technology, affordability, and potential shift in business operations. Adversarial tactics are targeting popular applications users who click links inviting the adversary deep into the layers of the domain. For the CISO it's a game of tactics, cyber threat intelligence plays a role in how resources are allocated towards vulnerabilities and the IR teams reactions to the unknown vulnerabilities.

The CISO fosters cyber hygiene and collaborative relationships within the organization to develop policy and cyber culture. The "people factor" is key and the challenge of balancing the needs, wants and risks within an organization. It's important for CISOs to have a strong relationship with the C-Suite and not just at budget request time, they provide situational awareness for risks that could impact the business operations and advise on realistic and affordable mitigations.

Digital wars are silently fought like a patient game of chess, each piece has a role on the board and movements on that board are controlled by the role. The CISO role acts as a Digital Sentinel protecting and pivoting across the board as they attempt to defend the cyber domain against attacks and insider threats. Each side collects one another's pieces through unauthorized exfiltration of data or breach of the domain, the game is endless, and it doesn't rely on a game clock, or the number of pieces collected by an opponent. Multiple games are at play and the Digital Sentinel is quietly watching and protecting their domain.

Angelique "Q" NAPOLEON, United States

Cyber Solutions Engineer and Senior Advisor | vCISO | Board Member | Consultant

Angelique is a Cyber Solutions Engineer and Senior Advisor for #GDIT in Washington, D.C. For 25 years. She has supported the Department of Defense and Intelligence Community in both Intelligence, Cybersecurity Engineering and C-Suite capacities. Angelique develops holistic solutions which build on the foundation for Cyber Resiliency and provides Penetration Testing, Cyber Threat Intelligence and System Security Engineering solutions. She is an Air Force Veteran and supports mentorship programs and initiatives for transitioning Military members and their families looking to enter the Cybersecurity field.

Dr. Ana FERREIRA

Access Control and the Power of Risk

One of the main points of failure in both cyber and physical systems is Identity Management and, in particular, Access Control. While it is a fact that everybody is unique, we, the cybersecurity developers, cannot expect everybody to interact the same way, with the same technology.

To implement access control decisions, a myriad of access control models and respective extensions are published every day. While these try to overcome the common identification/authentication mechanisms based mainly on three criteria (what we are, know, have), from which we expect a binary response Grant/Deny; access control, as any other interaction that happens between humans, or between humans and technology, has to be a risk-based decision. Every time we drive, walk, cook, cross the street, etc., we are (even if many times unconsciously) assessing the risk we are taking to perform these activities. This seems very straightforward however, performing risk assessment can be a very complex process and harder to translate to the daily practice of every organisation.

Some factors that can come into play are: requested data (public, personal, sensitive); technology (device, functionalities, security mechanisms); context (physical location, hardware and software in use, cultural issues, domain as in work, home, personal); or the user (goal/need of interaction, previous experiences and relation with the technology, demographics, IT/cybersecurity literacy).

We need more flexible and risk-based access control. Assessing risk of a specific interaction while integrating all the above factors (and probably others), is not trivial. Nevertheless, to guarantee high performance and more seamless and less disruptive experiences, we need to make all access control systems encompassing and intelligent, to quickly and accurately measure the risk, and execute the most secure possible access control decisions at any moment. Access control needs to better reflect our relation with technology, for an increased protection.

Dr. Ana FERREIRA, Portugal

Dr. Ana Ferreira (CISSP, HCISPP) is an information security specialist, teacher and researcher at the University of Porto, Portugal, since 2002. She is the author of more than 110 scientific publications, with 800 citations and obtained 1 high-degree Distinction, 1 Portuguese Government Praise and 15 prizes (6 of which, Best Paper Awards).

Ana frequently participates as a cybersecurity expert evaluator for the European Commission and is one of the Top100 most influential women in cybersecurity in Europe. Ana is also a Mentor for the European Women4Cyber Foundation, Co-Founder of the Women4Cyber Portugal, and Co-Founder of the Portugal (ISC)2 Chapter.

Dr. Elisa COSTANTE

Forescout Technologies, Inc.

Forescout Technologies, Inc. actively defends the Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing.

Fortune 1000 companies trust Forescout as it provides the most widely deployed, enterprise-class platform at scale across IT, IoT, and OT managed and unmanaged devices. Forescout arms customers with more device intelligence than any other company in the world, allowing organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Don't just see it. Secure it.

What defines us?

EVERYONE MATTERS

We're inclusive and diverse. All Ideas and perspectives are valued.

ONE TEAM

We're one team at Forescout. We win together. We respect each other. And we never say "That's not my job."

CYBER OBSESSED

Our technology rocks. We're obsessed with staying ahead of the bad guys.

CUSTOMER MINDED

We listen, we learn and we make it right. If a customer is unhappy, we failed. End of story.

GRITTY

We're smart, determined and we find a way. We create our own playbook, not follow others.

Dr. Elisa COSTANTE, Netherlands

Dr. Elisa Costante is the VP of Research at Forescout. In her role, she leads the activities of Vedere Labs, a team of cyber security researchers focused on vulnerability research, threat analysis and threat mitigation.

She has 10+ years of experience in the security challenges posed by the IT/OT/IoT convergence. In her prior role she was CTO at SecurityMatters, where she led product innovation activities in the field of network intrusion detection.

Elisa holds a PhD in Cyber Security from the Eindhoven University of Technology where she specialized in machine learning techniques for data leakage detection.

Dr. Fauzia IDREES ABRO

The Evolving Threatscape of Technology

Technology and digital transformation have diminished the boundaries among nations. In a world that is deeply interconnected by digital technology, cybersecurity and global security have become the same thing. While today's hyperconnected digital world has helped in generating immense wealth, it has also introduced even more threats due to its valuable nature, leaving the financial status of individuals and organisations vulnerable if not secured effectively. Its benefits are clear, but so are the threats. In 2021, we have seen that malicious cyber activity threatens national and economic security and the daily lives of individuals, communities, and organizations around the world. We saw critical infrastructure breaches and how one company's cybersecurity can have a cascading effect on many others in this closely connected world, from direct customers to end consumers, to US' Eastern Seaboard.

Remote working, distance learning and technologies like AI, robotics, quantum computing, internet of things (IoTs), and blockchain represent the future of our digital world. The potential cyber risks and vulnerabilities of these technologies defines the future of cybersecurity. Quantum computing, automation, machine learning, and IoT will introduce the biggest transformation in cybersecurity in the future. Artificial intelligence will change all aspects of cybersecurity. The advantage of computers in terms of speed, and amount of data processing over humans cannot be overlooked. Quantum computing can challenge the current encryption on which most infrastructures and economies rely. Similarly, automation and AI can facilitate untraceable cyber-attacks.

The biggest threat to the cybersecurity sector is from technology itself if it is not used responsibly. Cybersecurity professionals must step forward to advocate for using these technologies for the benefit of society as the well-being of every person, organization and country is increasingly depending on the application and security of digital technologies.

Dr. Fauzia IDREES ABRO, England

Dr. Fauzia Idrees Abro is a Professor of Information Security at Royal Holloway University of London. She is an Electronics Engineer with a PhD in Information Security Engineering, an MSc in Information Security, and an MBA. She is the first female PhD of Pakistan's Armed Forces. Fauzia has over 24 years of work experience in the Military, industry, and academia. She is the founder/CEO of Cynosure Technologies— the first female led Cybersecurity venture of her country. She is also the founding president of Women in STEM - a professional network of women in STEM. She is on the advisory board of multiple international organizations including CISO Forum, Global Foundation for Cyber studies and Research and N2Women.

Dr. Alina MATYUKHINA

From Theory To Practice

Making our world a safer place has always been a driving force in my life as a cybersecurity professional. Back to the days when my journey in cybersecurity started… In 2015 at EPFL (the Swiss Federal Institute of Technology Lausanne), I discovered that my research in math, and number theory, can be applied to solve security problems with encryption algorithms. Working in a domain that has a good impact on our society was always my goal. Back in the day, closed doors offered enough security against outside threats. But with growing digitalization, and the adoption of the Internet of Things (IoT), this physical protection is not enough anymore. Cybersecurity is more crucial than ever!

At Siemens, I am working with the core cybersecurity team on the cybersecurity vision and strategy of our products. Together with the product management team, I ensure that our products, solutions, or services have adequate built-in cybersecurity. I am responsible for designing and implementing processes, plans, and tools that safeguard our products.

Every new generation of developed product is secure-by-design: we implement cybersecurity in the initial design of the products. Together with security experts, I perform threat and risk assessments throughout the lifecycle of products to identify and mitigate potential risks. Those assessments start early in the product development process and repeat for every significant update. Before releasing a new product, we ask independent third-party organizations to test our products for potential vulnerabilities. I am supporting cybersecurity certification activities from pre-assessment to the audit by the independent certification body. Recently, our organization and products were certified on IEC62443 – one of the most well-known industrial security standards. Today I know that people are at the heart of a successful and effective cybersecurity strategy. At Siemens, we're investing continuously in training and awareness. I believe it will help safeguard organizations against cyberattacks.

Dr. Alina MATYUKHINA, Switzerland

Dr. Alina Matyukhina is the Head of Cybersecurity at Siemens Smart Infrastructure Global HQ. She is leading cybersecurity activities for building automation products and systems. Brilliant mathematician, Alina excelled in her role as the cybersecurity researcher at the Canadian Institute for Cybersecurity and Swiss Federal Institute of Technology Lausanne. The Ph.D. in Computer Science, Software Security, is the result of years of this excellence.

Alina is serving as a Chair of the "Smart Cities & Infrastructure" group at Swiss Cyber Institute and an expert at digitalswitzerland. Dr. Matyukhina's work has been featured in Forbes, World Economic Forum, Pentest Magazine, International Security Journal, and World Security Report as well as academic prestigious journals of IEEE and ACM.

Dr. Djalila RAHALI

The Human Factor in Cybersecurity as seen by a Cyberpsychologist

The importance of cyberpsychology in the analysis of cybercrimes for a better understanding of modus operandi especially among cyber offenders is no longer to be proven as long as a Phd is already operational for anyone interested without a basis in psychology thanks to Capitol Technology University and the department whose chairwoman is Dr. Prof. Mary Aiken, a psychologist expert in forensic cyberpsychology. So, who better to study the human factor in cybersecurity than a human specialist: The Psychologist. Better: The cyberpsychologist.

Acting according to her credo "The best antivirus is not sold, it is built" Dr. Djalila Rahali, an Algerian psychologist, the first cyberpsychologist in Africa and the Arab World, believes that the covid19 pandemic has laid bare the technical failures of the world and above all human ones. Confinement has had a great impact on the explosion of cyberaddiction which, according to Dr. Rahali research is also a factor that has led young people to try everything, out of boredom of having to stay “jailed” at home.

Thus, and since " we always need a good cyber defense to be in cyber safety " (Rahali, 2016), psychologists have been interested in human manipulation via social engineering by analyzing the cyber behaviors that enter into the process of neuropiracy to raise public awareness of safety and to better explain to cybersecurity agents the basic elements of the cybercriminals’ personality and what kind of intelligence they use to get ahead and succeed in their cyberattacks.

Cyber risks are somewhat human, but we can teach machines how to counter them through AI and its algorithms based on scientific research. By transposing their analyzes into cyberspace, psychologists have a significant area to explore: Cyberneuropiracy. Their role: Helping people close their loopholes for better security and safety.

Dr. Dr. Djalila RAHALI, Algeria

Dr. Djalila Rahali is the first psychologist in Africa and the Arab World to specialize in cyberpsychology (1999), founder and CEO of NafsiyaTECH, she is a researcher in “Human Factor” in cybersecurity as she has been a profiler for 17 years in “SONELGAZ company”.

Member of Women in Cybersecurity Middle East, she has been ranked TOP10 of personalities developing ICT in Algeria, TOP50 and TOP30 Women in Cybersecurity in Africa and in the Middle East. She has been a Keynote in the most important International Seminars of Cybersecurity and co-Founded the « Cyberparental Guardians» USA. She was featured at the cover of “Focus On Women Magazine” (USA) in 2019 for her article about Neuropiracy.

Soledad
ANTELADA TOLEDANO

Soledad ANTELADA TOLEDANO, United States

Soledad Antelada Toledano is the Security Technical Program Manager at Google. She previously worked for Berkeley Lab, one of the most prestigious scientific centers in the world and one of the first nodes of ARPANET, the forerunner of the Internet. Soledad was the first woman in the history of the Cybersecurity department at Berkeley Lab.

After specializing in 'penetration testing' for several years, Soledad also develops research and advancement tasks for intrusion detection systems, monitoring of high capacity networks and vision and research exercises on how cybersecurity will evolve in the next 10 years adopting techniques of Artificial Intelligence for intrusion detection and handling of BigData generated by monitoring tools.

Soledad has combined her work at the Berkeley lab in recent years with the responsibility of being the head of security for the ACM / IEEE Supercomputing Conference, the annual supercomputing conference in the United States, protecting and building the network architecture of SCinet, the fastest network in the world.

Soledad is the founder of GirlsCanHack, an organization dedicated to engaging women in the cybersecurity field, encouraging women to pursue a career in cybersecurity Soledad was named one of the 20 Most Influential Latinos in Technology in America in 2016. She has recently joined Google as a Technical Program Manager for Security.

Jennifer
COX

Cloud Security First

Visibility is key to Cyber Security. You cannot protect what you don't know exists. When it comes to Cloud security and agile environments it is increasingly difficult to be 100% sure as to the full extent of your attack surface. This is why cloud security and asset discovery is so important. Running constant discovery to identify what's on the network at all times, combined with a shift left logic means that you can identify the problem before it becomes an issue. Having great remediation rates is wonderful but if a percentage of your assets are not known to you then your risk is unquantified, potentially significant, and you're completely in the dark. You can only truly understand your risk exposure by identifying all possible assets first.

Great cloud security makes for great cyber hygiene. With development teams essentially defining cloud native infrastructure and security teams chasing with mitigations there is typically a communication gap. You want to encourage your development team to create, to be innovative and to stay competitive but you also need to make smart decisions when it comes to application security. Getting to the risks before deploying to a live environment means you can also educate your development teams on best practices and align to standardised compliance or, even better, create your own higher standards for compliance. Every Cyber Security team has the capability to become the definition of high standard if they are given full visibility across their potential attack surface.

Cloud security is still relatively 'new'. With existing teams lacking many of the skills and graduates that have the skills but are still trying to break into the industry we are at a point of change. We can do better as cloud practitioners and cloud security is where we should start.

Jennifer COX, Ireland

Jennifer Cox is a Security Engineering Manager at Tenable, a global leader in Vulnerability Management. She has achieved several promotions and awards while in Tenable, including PCR Top 25 Women in Tech in 2019 and 2020 & Outstanding Contribution to Women in Tech Ireland in 2021.

She is Head of Communications for Cyber Women Ireland, an Ambassador for Wentors global mentorship programme, Community and Development board member for BBWIC, an active member of WITS Ireland (Women in Technology and Science Ireland), WomenTech Community and WiCyS Global (Women in Cyber Security) and works hard to insure diversity and inclusion within her industry.

Uma RAJAGOPAL

What is Governance?... Governance is Accountability in Action.

Enterprise governance is a set of responsibilities and practices exercised with the goal of providing strategic direction, ensuring that objectives are achieved, risks are managed appropriately and verifying that the enterprise's resources are used responsibly. Critical Components to the success of the enterprise are Security, Transparency & Accountability. These three components together define the enterprise integrity to shape the enterprise policies and standards, and set the corporate culture.

Cybersecurity and Ethical culture both have direct correlation. Since ethics is a moral philosophy or code practiced by a person or group make sure that cybersecurity is EVERYONE'S business no matter what your role is within the organization. All individuals in the organization share the responsibility for the state of its ethical culture and security.

Next RISK MANAGEMENT is the keystone of governance. Accurate information is required to correctly understand the various threats and subsequent risk being faced and how the enterprise chooses to respond. Effective risk management assists in maximizing opportunities. For example, a risk decision may consider the potential benefits that may accrue if opportunities are taken, versus missed benefits if those same opportunities are forgone. The dual nature of risk is a result of its use in different contexts by business and IT, and it is not always easy to draw the distinction.

Governance is not just for senior management and the board of directors; it is applicable to all departments and individuals within an enterprise. However, a well-managed enterprise that lacks proper governance is not aligned with the enterprise's strategic visions and goals and does not create any value. It is therefore conclusive that an effective Governance strategy helps ensure that risk management practices are embedded in the enterprise's business strategy, enabling it to secure optimal risk-adjusted returns.

Uma RAJAGOPAL, United States

Uma Rajagopal is a dynamic leader with 20+ years IT industry experience committed to enabling the business to achieve success in the Security and Resiliency of their technology foundation. What makes her unique is her ability to be results-driven.

She is a collaborative and future-minded leader with extensive experience in building security strategies & risk management program. Her superpower is in building high performing teams with diverse views.

Complementing work life, she serves on several Advisory boards. Not only she enjoys the rigors of Board oversight, but the opportunity to share this rewarding passion with her peers is invaluable.

Dr. K
ROYAL, JD

Protecting Health Data: GDPR v. HIPAA

These past two years have been rampant in requirements related to the privacy of health information. Whereas most countries with privacy law include health /medical information, the United States does not have an omnibus privacy law, albeit one proposed law seems promising now.* However, that is not to say that the US does not have strong laws around health data. The Health Insurance Portability and Accountability Act (along with subsequent amendments, "HIPAA") is quite strong. As is the European Union's Gen eral Data Protection Act ("GDPR") - also the United Kingdom's GDPR where they currently match. But…. HIPAA compliance does not equate to GDPR compliance and vice versa.

Let's look closely at the similarities and differences between the GDPR and HIPAA. Clearly, HIPAA applies to certain protected health information, generally patient data, and GDPR encompasses all personal data, holding medical data as a special category of data…

Read the Full Article Here! Top Cyber News MAGAZINE. July 2022

As you can see, although it is easy to see where a company accustomed to the tight regulatory oversight of HIPAA might think there is no room for improvement, but that would be wrong. The GDPR is much broader and has higher penalties, although not discussed here. So if you are a covered entity or a business associate and you believe that you are good to go under GDPR, please re-evaluate. You need to make some tweaks.

And if you are GDPR-compliant and find yourself a business associate through a customer… you also have a lot of work to do before being HIPAA-compliant.

Dr. K ROYAL, JD, United States

Dr. K Royal, JD is a global data protection lawyer, certified as FIP, CIPP/US /E, CIPM, and CDPSE. She is a tech columnist for the Association of Corporate Counsel, a frequent speaker, and co-host of the top-ranked Serious Privac y podcast. From everyday operational issues to strategic efforts, K meets professionals where they are.

K is a vibrant and passionate personality, with creative approaches to intense compliance areas, backed by expertise and elbow grease. She often mentors new professionals, students, and peers involving topics from career transition to Life-Work balance to managing disabilities. She sits on the board for several non-profits, is in-house at Outschool, and teaches privacy / data protection at ASU.

Lynn DOHM

That moment in time...

It's that moment when your beliefs, passion and career align that you feel complete. As the Women in CyberSecurity (WiCyS) executive director, that's me. Being a part of the WiCyS team for years, I've been grateful to be connected to a community that, with each and every action, continues to support the recruitment, retention and advancement of women into the fantastically ever-evolving and engaging field of cybersecurity.

I joined the WiCyS leadership team from the Chicagoland area where, since 2012, being a solution-oriented strategist with over 20 years of experience aligning businesses, nonprofits and grants with their initiatives and business outcomes. I'm so grateful that over the last 14 years, I've worked intensely within the cybersecurity education sector, having active roles in grant-funded programs and nonprofits that assist in providing educational solutions to the cybersecurity workforce.

The energy of women, allies and advocates making such a commitment to themselves and others by joining the WiCyS organization is contagious. Now with over 5.7K members and having representation in 70+ countries, the WiCyS strength in numbers extends from 50 professional affiliates and 170 student chapters around the globe. Specialty affiliates focus on niche areas such as artificial intelligence, BISO, cloud security, critical infrastructure, data privacy/law, military, LGBTQ+ pride, neurodiversity, and more. Training programs, initiatives, mentoring cohorts, internships, apprenticeships, leadership series, conferences, and more opportunities in the workforce to many. Together, industry professionals, government, and academia are expanding to create inclusive spaces and have the powerful and much-needed diversity of thought brought to the cybersecurity workforce. I love working each day to show up and create more opportunities for tomorrow. My favorites in life are laughing with my family, being a midwesterner, drinking delicious coffee, listening to bluegrass music (or any LIVE music), and sitting on my front porch.

Lynn DOHM, United States

Lynn Dohm brings 20+ years of organizational and leadership experience to the WiCyS team.

She has collaborated with businesses, nonprofits and grants to produce outcomes aligned with their cybersecurity business goals. Lynn is passionate about the need for diverse mindsets, skill sets and perspectives to solve problems that never previously existed and facilitates opportunities for WiCyS members led by inclusion, equity and allyship. Lynn lives each day fulfilled as she continues to crusade on bridging the cybersecurity workforce gap and improving women's recruitment, retention and advancement in cybersecurity. Follow Lynn on Twitter at @lynn_dohm and Linkedin at www.linkedin.com/in/lynndohm/

Simbiat
SADIQ

Cybersecurity as a Business Enabler

Technology has become essential in achieving business growth and maximising revenue. Businesses are leveraging technology to build solutions, provide services and enable business growth. However, the adoption of technology and its evolving nature has opened businesses to cyber risks and attacks as large amount of data has been generated and shared which contains sensitive and valuable information's.

Malicious actors/cyber criminals are devising new method to steal this information which could cause reputational damage to businesses among others. Being able to clearly show that you take cybersecurity seriously is increasingly important as more and more organisations do their business online. Businesses needs cybersecurity to defend itself against cyber threats thereby minimising risk. Cybersecurity is not a tool but a set of procedures businesses should carry out to protect their computer systems and data.

Cybersecurity enables your business by:

1. **Building customer confidence and loyalty;** With data security breaches are becoming more alarming than ever, consumers of products and services are more conscious of security. Businesses needs to let customers know their data is safe and businesses that invest in security while continuously updating their security can prevent customer experience disruptions, protect their brand reputation, and maintain the trust and confidence of their customers.
2. **Reducing cost by detecting risks early;** Businesses who function with cybersecurity as one of its core elements can detect threats and vulnerabilities that might be exploited which may result to a cyber-attack. Detecting these risks early reduces the cost of dealing with a security breach or a cyber-attack.
3. **Increasing brand equity;** Security breach will result in negative publicity which reduces equity of a brand. Building businesses with a cybersecurity mindset will give an opportunity to respond adequately to security breaches and this can increase brand equity. It is therefore important for business to ensure there is a cybersecurity strategy in as this will boast productivity among others.

Simbiat SADIQ, Nigeria

Simbiat Sadiq is a cybersecurity professional with over 4 years of experience. As someone who first learnt about cybersecurity out of curiosity, she has constantly inspired, mentored, and volunteered for initiatives that enable her give back to the community.

She is a digital security advocate who is passionate about creating social impact in Africa's cyber security space. Simbiat has lead Pan-African projects in the cybersecurity space. One of her favourite volunteering so far is the CyberGirls, an Initiative of Cybersafe foundation. She has constantly driven cybersecurity awareness and shared her opinion on various cybersecurity issues via various means including blogs, articles, and social media.

Dr. Fatemah ALHARBI

Hacking Humans

Today, most cybercriminals shift their interest from attacking systems and networks into hacking humans. In the context of cybersecurity, this type of act is referred to as social engineering which is an act used by adversaries to psychologically manipulate their victims to sacrifice their privacy and divulge confidential information.

Social engineering cyberattacks come in a variety of forms: phishing, smishing, vishing, dumpster diving, USB drops, impersonation, and tailgating. The weakest link in all these attacks is the user. By looking back at 2020, we see how all these attacks have evolved during the COVID-19 pandemic and how it's developing in 2022. Sadly, as the crisis evolved, cybercriminals compromised key companies and organizations through social engineering and activated numerous ransomware attacks on critical infrastructures such as healthcare, manufacturing, transport, government, and educational institutions.

During pandemic, many companies survived from economic crisis by adopting a new "normal" working environment and allowed employees to work from home. This increased digitization and has brought new cybersecurity risks specially to non-IT employees. Unsurprisingly, according to the last FBI Internet Crime Complaint Center (IC3) 2021 Internet Crime Report, the older the user is, the more vulnerable he/she would be to social engineering attacks.

As for companies and organizations, it is highly recommended that they change their security practices. Conducting social engineering penetration testing on users should be their default approach. To perform a successful penetrating test, users need to be selected carefully, basically those who would be easily tricked. The tests are typically done remotely by ethical hackers conducting social engineering attacks, reporting the vulnerabilities, and providing recommendations to mitigate these vulnerabilities to the intended audience, e.g., senior cybersecurity managers.

All companies and organizations, across every sector and of all sizes, must ask, how can we make sure that not only our data is safe but also how aware our employees are to cyberthreats? Social engineering penetration testing is a great way to measure the security posture. **This assessment process is about security governance and control with a view to the prevention of social engineering cyberattacks.**

Dr. Fatemah ALHARBI, Saudi Arabia

Dr. Fatemah Alharbi is an Assistant Professor in the Computer Science Department at Taibah University, Yanbu, Saudi Arabia. She received her Ph.D. in Computer Science in 2020 from University of California, Riverside. Dr. Alharbi is selected as one of the 15 remarkable Arab Female Scientists…

Cybersecurity researcher and consultant Fatemah has been involved in many research projects that were published in prestigious conferences (e.g., USENIX, CCS, and INFOCOM) and journals (e.g., IEEE TDSC). A seasoned public speaker having spoken in many prestigious and International conferences such as AtHack by BlackHat, Dr. Alharbi successfully presented a cyberattack on the Domain Name System (DNS) infrastructure targeting Apple macOS, Linux Ubuntu, and Microsoft Windows.

Karla REFFOLD

Cybersecurity's Relationship With Entrepreneurship

Entrepreneurship plays a huge role in how the cybersecurity industry progresses. We are faced with complex organizations to secure, against a variety of motivated, adaptable, and well-resourced threat actors. For the most part, the industry has been on the back foot. We secure legacy systems, responding as new threats emerge. While resources have increased significantly, many organizations struggle to respond to the issues they face.

While there can be some tension between cybersecurity vendors and the customers they serve (mostly sales related) entrepreneurs and vendors essential to how we respond. We need vendors to provide the tools and solutions for organizations to implement. And we need to support those same vendors to improve their tools and find innovative solutions to the issues that we face.

The passion of entrepreneurs allows them to develop solutions to niche problems, with great success. Where would we be if Tenable hadn't developed Nessus? And some great solutions are emerging. Risk Ledger has a fantastic way of understanding where risk is concentred in the supply chain. Orpheus Cyber has a more accurate and responsive way of prioritizing vulnerabilities. Appgate is helping organizations create a zero-trust environment.

Yet as important as entrepreneurship is for the industry, it has never been harder to support them. We are overwhelmed with solutions and our tech stacks are already large enough that it can be hard to manage new products. Those with the largest marketing budgets get our attention but that doesn't ensure innovation or efficiency. I'd encourage those with purchasing power to consider if they are supporting our entrepreneurs. And while speaking to all of them isn't likely to be possible, consider taking part in reviewing one of the many innovation awards, competitions, or accelerators. Finding ways to support them today may just help us be more secure tomorrow.

Karla REFFOLD, United States

Karla Reffold is an experienced entrepreneur with two successful exits from cybersecurity-related businesses. She is currently the COO of Orpheus Cyber, a threat-led cybersecurity company providing attack surface management, vulnerability management, and third-party risk. Karla is an industry awards judge, the host of the Capital Tea podcast, and an experienced speaker on the topic of cybersecurity and women in technology.

Karla is also a non-exec director and enjoys helping businesses grow, using her own experience and passion for people-centric businesses to enable them to succeed.

Shamane
TAN

Shamane's Three Keys

1. Surround yourself with the right voices, and watch the ones in your head
Being in a community can make all the difference. Networking with mentors and meeting other visionary women who demonstrated great ambition, was one of the factors which gave me the much-needed boost to make the switch to cybersecurity mid-career.

Also, watch the narrative you're telling yourself. Your identity can be shaped by what you speak of yourself – if your inner voice keeps calling you out as courageous, you will eventually start living out more bold achievements. Use any dissuasions as fuel into personal growth and development.

2. Embrace big dreams
I have always been someone with big aspirations and it is important who you share this with. There are the other big dreamers who can also be great encouragers giving practical ideas on how you can be better, whilst advocating for you.

Surround yourself with mentors, and a community of healthy and positively minded people who will inspire you for greatness. Together, we can be fearlessly vocal of our achievements, while cheering each other on at the same time.

Whenever any limiting beliefs start to rise, just ask if you are willing to be your own roadblock, or are you going to back yourself?

3. Invest in strong, deep, and authentic relationships
These friendships ended up carrying me really far and helped me navigate the corporate landscape in the years to come. Let's also value different thinking, perspective, and experiences. The more colourful our industry is (in terms of skills, passion, personality, and backgrounds), the more everyone grows in new ways. Let's authentically own our uniqueness; see our differences in the way we approach/think/ see things as a complementary value-add to the current way things are being done in organisations.

Shamane TAN, Australia

Shamane Tan is the Chief Growth Officer at Sekuro, leading the security outreach strategy with the C-Suite.

Featured in World's Leaders as the world's 10 most influential business leaders in cybersecurity, she serves on the advisory board for Black Hat Asia Executive Summit.

The TEDx speaker and 'Cyber Mayday and the Day After' best-selling author is also the founder of Cyber Risk Meetup, an international community for executives to exchange learnings. Shamane is listed in 40-under-40 most influential Asian-Australians.

Courtney H. JACKSON

The Evolution of Women in Cybersecurity

I have been working in the Information Technology (IT) field for over 20 years. After serving as an Information Systems Technician (IT) in the Navy, I accepted a helpdesk role and worked my way up to the C-Suite, before exiting the Corporate space to pursue my entrepreneurial endeavors full-time.

I did not get here overnight. My first cybersecurity job was a Security Operations Center (SOC) analyst in 2008. I was the only female on my team of 14+ individuals and required to work night shift as the newbie.

I used that night job as an opportunity to gain as much hands on experience as possible from working firewall ticket requests to responding to Intrusion Detection System (IDS) alerts. I also studied for, and passed, my Certified Information System Security Professional (CISSP) certification. In 2010, I landed a job as a Security Control Assessor (SCA) and worked in a group of over 20 people, four of us were woman.

Fast forward to present day and women are still underrepresented in this field. However, as I attend meetings and events, I see more women emerging! Anywhere from newbies to Senior Level Executive / Founders. The progress is refreshing, although we still have a long way to go.

There are many mentorship and apprenticeship programs available now that did not exist when I was learning this field. Recently, the Department of Commerce and Department of Labor launched a joint effort to initiate a 120-day Cybersecurity Apprenticeship Sprint to promote registered apprenticeships. Opportunities exist for those willing to put in the necessary work to gain the required experience to help fill the nation's cybersecurity workforce gap.

There is no replacement for experience or shortcut to success!

Source: U.S. Department of Labor Website

Courtney H. Jackson, United States

Courtney H. Jackson, MSISA, CISSP, CISM, CEH, CHFI is the Founder and CEO of Paragon Cyber Solutions, LLC, a veteran, woman, minority-owned, Florida-based company, specializing in information security and assurance. Courtney has over 20 years of certified hands-on experience, encompassing both executive leadership and entrepreneurship.

After serving active duty in the U.S. Navy, she took an entry-level position as an IT Help Desk Representative, impressively working her way up to the C-Suite in the span of her career before exiting the Corporate space to pursue her entrepreneurial endeavours full-time. Courtney's unique journey has positioned her to mentor women in cybersecurity by helping them shatter the glass ceiling that stands in the way of their career advancement to executive leadership roles.

Cat CONTILLO

Cybersecurity: Bottom-Up Leadership

In most high risked problems in the cybersecurity industry, the decisions for everything are given to the higher-ups, for example, executive level. When things go wrong, it is typically the executives who must answer. This is known as a top-down approach instead of a bottom-up approach. Keep in mind, having diversity creates innovation in the organization. Sometimes we must change up what is often typical, to change up the way it works and take the risk that we might get a better option.

Cybersecurity organizations need to want and need the desired results, no matter what. There are new designs that are enabling a new breed of handling your organization in cybersecurity. It is elevating employees in the bottom-up approach where the analysts, engineers, and developers in the cybersecurity space configure, and flag vulnerabilities before the addition to the application or code is pushed to being produced.

It tends to be hard to give up control especially when it has been yours the whole time. But think about different minds, and other teams being able to non-traditionally approach this lifecycle when adding a new application, or tool to your current stack. The organizations cybersecurity standard is applied by that people who are working in that space and doing that day in and day out.

Think about the experience individuals in this field of cybersecurity and information systems who can use their knowledge and familiarity to guarantee the design and production of a highly secure and profitable product, approach, or task at hand. **Button up leader in cybersecurity can be a non-traditional and successful approach to organizations and their products.**

Cat CONTILLO, United States

Cat Contillo (she/they) is a formidable force. Despite hardship, disability and exclusion, Cat has made great strides in her professional life, and now thrives in a career in Cybersecurity.

Cat is employed as a Threat Operations Analyst Team Lead at Huntress and battles cybercriminals who seek to attack and exploit businesses. This interest in defending is a theme mirrored in her personal life, where Cat advocates for Diversity Equity, Inclusion, and Accessibility, providing needed education to others about gender equality, autism, and chronic illness. Cat also serves on the Board of the Women in Cybersecurity (WiCys) Neurodiversity Affiliate, where she provides guidance on effective inclusion practices and procedures.

Cat is a fighter and is just getting started.

Rupali DASH

Getting Started With Kubernetes Cluster Pentest

Kubernetes is an open-source container-orchestration system for automating computer application deployment, scaling, and management. The next generation IT is moving towards Docker and Kubernetes because it supports the automation and scalability of every aspect of app deployment. Despite of the convenience, secure implementation of containers is still a raising problem. Hence comes the role of a pentester to identify the security pitfalls and monitor the secure deployment. Though there are currently not much of structured training in this specific area , the course by offensive labs, which is called Hacking and Securing Kubernetes Cluster, is a great resource to start of with kubernetes pentest.

Kubernetes Cluster Security Issues and How to Overcome Them

Kubernetes deployment consists of many different components (including: the Kubernetes' master and nodes, the server that hosts Kubernetes, the container runtime used Kubernetes, networking layers within the cluster and the applications that run inside containers hosted on Kubernetes), securing Kubernetes requires you to address the security challenges associated with each of these components.

Authorization: Kubernetes provides four authorization modes called Node, Attribute-based access control (ABAC) , Role-based access control (RBAC) ,webHook. The two most popular our of these four are ABAC and RBAC.Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.Attribute-based access control (ABAC) defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. Read the Full Article Here!
at https://rupali-rupalidash.medium.com

Rupali DASH, Singapore

Rupali Dash - a pen-tester by profession and a Hacker by heart, Rupali is currently expanding her expertise into cloud security. Coming from an offensive security background Rupali has earned some distinguished certifications as OSCP, OSWE, OSWP, CRTP, CRTE, AWS security specialist etc.

Experience gained while working with top notch organisations like: Synopsis, Goldman Sachs, JPMorgan, United Technologies, BNP leads the young and talented cybersecurity professional and passionate researcher to the staged of multiple international conferences like Devseccon , BlackHat Asia, Cocon, as well as participation in many bug bounty programs and live Hacking challenges by Hcker one and Cobalt.io.

Iretioluwa AKERELE

The Future Of Diverse Cybersecurity Talent

Diversity is the practice or quality of including or involving people from a range of different social and ethnic backgrounds and of different genders, sexual orientations.

The cybersecurity ecosystem has advanced in over a decade. Cyber-attacks are increasing, and sevral organisations have recorded different types of cyber-attacks and data breach in recent times. In response to these attacks and the evolving cybersecurity ecosystem, diversity is important in the industry. Recently, the cybersecurity industry has opened opportunities to females using skill acquisition programs. For example, Cybersafe Foundation is currently training 300 women in 6 African countries in Cybersecurity. Other women specific skilled programs exist to give women more opportunities.

The high demand for cybersecurity professionals globally has led to the immigration of people from different countries to take opportunities in some developed countries in Europe, Australia, and Canada. Cybersecurity professionals will continue to be in demand due to the increase in cyber attacks and the importance of organisations securing their people, processes, infrastructure and enhancing their security posture. Organisations have put in effort to attract and retain a diverse workforce. One of the ways by which these organisations have achieved diversity is by having a wider pool of talent irrespective of their gender, background, and country of residence.

Previous research has shown that ethnic and gender diversity has directly translated to an improvement in performance. To address the current cybersecurity skills shortage, diversity is important. **A more diverse cybersecurity team is an improved cybersecurity team. Having diverse cybersecurity talent in the workplace is achievable. Retaining such talents are important. Organisations can achieve this by creating an inclusive environment for all employees. This can be achieved by ensuring equal pay and prioritising skills over background or location.**

Iretioluwa AKERELE, United Kingdom

Iretioluwa Akerele is an award-winning cybersecurity professional who has expertise as a cybersecurity consultant and industry practitioner. An Advisory Board member of Cybersafe Foundation, Iretioluwa is a career coach and mentor who has given direction to over 500 cybersecurity beginners and enthusiasts.

Iretioluwa is the founder of Cybarik Limited, an organisation that provides world-class information security consulting and training to organisations and individuals. Iretioluwa is excellent, has integrity and is passionate about supporting people starting their career in Cybersecurity. Recently Iretioluwa co-founded a cybersecurity community that supports African students in Europe.

Elizabeth WHARTON, J.D.

Go Beyond With Scythe

SCYTHE moves beyond just assessing vulnerabilities. It facilitates the evolution from Common Vulnerabilities and Exposures (CVE) to Tactics, Techniques, and Procedures (TTPs).

Organizations know they will be breached and should focus on assessing detective and alerting controls. Campaigns are mapped to the MITRE ATT&CK framework, the industry standard and common language between Cyber Threat Intelligence, Blue Teams, and Red Teams.

FEATURES

MULTIPLE COMMAND AND CONTROL CHANNELS
Adversaries leverage multiple communication channels to communicate with compromised systems in your environment. SCYTHE allows you to test detective and preventive controls for these various channels: HTTP, HTTPS, DNS, SMB, Google Sheets, Twitter, and Steganography or easily integrate your own.

MAPPED to MITRE ATT&CK & Atomic Red Team Integration
SCYTHE emulates behaviors that can be mapped directly to MITRE ATT&CK. Each action performed can be tagged for better reporting. Full integration with Atomic Red Team so operators just click on which test case to perform in the given campaign.

LEVERAGE CYBER THREAT INTELLIGENCE
Creating campaigns from Cyber Threat Intelligence could not be easier for analysts or operators. You can export and share your custom threats in the SCYTHE Community Threats Github or import threats with two clicks.

AUTOMATE ADVERSARY BEHAVIORS & TTPs
Leverage SCYTHE's threat automation language to automate adversary behaviors and TTPs for reliable and consistent execution every time. SCYTHE can make decisions based on previously executed modules and leverage the results for the next instruction…

Elizabeth WHARTON, J.D., United States

Elizabeth (Liz) Wharton, J.D. leverages almost two decades of legal, public policy, and business experience to build and scale cybersecurity and threat intelligence focused companies.

She currently is VP, Operations at SCYTHE, an adversary emulation platform. Prior experience includes helping lead Atlanta's ransomware immediate incident response team as the senior attorney responsible for technology projects and policy at Atlanta and its airport. She received her J.D. from Georgia State University College of Law and her B.A. from Virginia Tech.

Alexandra MERCZ

Shared Fate in Cloud Security

Security is everyone's responsibility and hence the approach of shared fate is becoming more and more common. Whether we talk about the shared responsibility of every employee to protect the organisation; or the complex interdependencies between cybersecurity service providers and their clients; every side is equally important.

The fast-paced evolution of the security landscape requires close-knit partnerships, especially when it comes to managing security in the cloud. Moving away from traditional physical infrastructures (on-prem) to full migrations to the cloud or to utilise a hybrid model, can be perceived as loss of control over security. This insecurity over security can be mitigated by disciplined migration frameworks that provide the required reliability and even better cloud security controls; and cater for various use cases from Infrastructure-As-A-Service to Software-As-A-Service.

Shared fate in cloud security is intentional and works best when it clearly outlines the responsibilities of each parties for both technical and procedural controls. The model intends to structure and direct focused cloud security domain expertise and competency, to allow for effective management, which in return reduces cloud security risk. Additionally, shared responsibility enables better ability to more accurately measure the current cyber risk of the company, which drives the complex underwriting process for cyber insurance.

The resilience and business continuity of organisations these days relies on layered and complex solutions to properly secure their cloud environment. Defense in depth is not anymore an option but the only way to effectively protect organisations from real-world cyber threats.

By sharing the concept of shared fate in cloud security, where everyone assumes specific responsibilities for their respective area, the approach of "the whole is greater than the sum of its parts" comes into practical application to create better security and more trust for everyone.

Alexandra MERCZ, Singapore

Alexandra Mercz is the Information Security Chief of Staff of Gojek and GoTo Financial, the largest technology group in Indonesia.

Alexandra's strong track record in the global banking domain enables her to marry together business acumen and technology expertise. Mrs. Mercz held senior positions at several CISO and COO offices and she achieved multiple certifications in Cybersecurity, Cloud Security, NIST and agile implementation.

She is a seasoned public speaker and an avid volunteer in the Cybersecurity space. Alexandra is at the forefront of the industry and leading the way for better diversity and inclusion, along with very strong advocacy for self-development and breaking barriers.

Jessica GOTTSLEBEN

The Power Of "Acting As If" For Women: Magic Words And Microphones

In my recent podcast interview with Susannah Wellford, founder and director of Running Start, I learned some magic words. And weirdly, just by saying these words out loud or even silently in my head, I get an instant confidence boost.

But first, a word about the very neat work of Running Start. At Running Start, Susannah and her team inspire and prepare girls and young women to get involved in political life. And a big part of that work is helping women imagine themselves in a powerful political role, especially when they don't see a lot of role models in political institutions. And of course, this lack of visibility is worse for women and girls of color, or who come from poor families, or who are LGBTQ. So confidence building is a critical task in all the programs they offer. And that's where the "magic words" come in.

"My name is ….and I am running for…."

Running Start encourages the girls and young women in their many programs to get comfortable saying these words: "My name is … and I am running for….". Susannah says the impact of that sentence is immediate. "You can see it right away. They stand up a little taller - they just feel more confident." It's the power of those words - even it they are not true (yet.) The the young women are asked to hold that statement in their heads and mentally rehearse it whenever possible.

Your turn!

So why don't you try it - right now! "My name is … and I am running for…. "   Don't stress about what you're running for - pick anything (but it's fun to use "Congress!"). And the best part is, you don't have to actually run for anything to get the benefit! (although you can!)

My name is Jessica Gottsleben and I am running for ..." #CSWY2022!

Read the Full Article Here! At womenspeakup.org

Jessica GOTTSLEBEN, United States

Jessica Gottsleben is a globally recognized policy advisor and strategist, security scholar and researcher, human and civil rights defender and advocate, consultant, survivor expert, and subject matter expert.

Heaviest areas of expertise: cybersecurity, cyber policy, climate security, climate policy, energy security, climate science, human security, human trafficking, slavery, intelligence, national security, foreign policy, abuse, violence, terrorism, exploitation, environmental and economic justice and transformative and restorative justice, sustainable development, harm reduction, peacebuilding, healthy relationships, transnational organized crime, femicide. Strategic foresight, ethics, and resiliency across Just Transition, Fair Trade, Clean Energy, Regenerative, Circular and Solidarity Economies, for the Fourth Industrial Revolution, the Digital Age, and Public Diplomacy 2.0. Calling for a Just Recovery.

Polly GITAU

Rating an Organization’s Cybersecurity Posture

Cyber Maturity assessments are executed to help organizations gauge how prepared they are to: identify, prevent, detect, respond, and contain threats to their cybersecurity posture. In these assessments, organizations can expect to obtain a holistic view of the current state of their posture, the target state, and what improvement opportunities exist to aid them achieving the desired target state. To better provide a benchmark comparison of the current and target state of the cybersecurity posture, a maturity rating can be allocated. The Capability Maturity Model Integration (CMMI) by Carnegie Mellon University can be considered as it has five maturity levels ranging from level 1 being the lowest to level 5 being the highest.

For maturity level 1 **Initial,** cybersecurity capabilities are unpredictable, poorly controlled, and reactive. In Level 2 **Managed**, capabilities are conducted as projects that are planned, performed, measured, and controlled though frequently reactive. Level 3 is **Defined** as capabilities shift from being reactive to proactive. At this point, policies and standards defined by the organization provide guidance across the different cyber capabilities.

Progressing to level 4 **Quantitatively Managed**, the cyber capabilities incorporate data driven activities hence predictable and more aligned to meet different stakeholders’ needs in the organization. Lastly, in level 5 **Optimizing**, the organization is stable and flexible in delivering the different cyber capabilities while working towards continuous improvement and adapting to changes and opportunities.

With these ratings in place, an organization can better understand what they need to incorporate in their cyber capabilities to improve their maturity levels. For example, from a defined posture to an optimized one. While an organization focuses on attaining the maturity level of 5 in their cybersecurity posture, it is crucial to have a reference point that informs the organization where they are now and where they want to go next.

Polly GITAU, Germany

Passionate about making the digital space secure and trustworthy, Polly Gitau has made great strides in the cybersecurity space. She has enabled organizations gain visibility of their cybersecurity posture and their compliance levels to cybersecurity and data privacy regulations.

She has been recognized as “One To watch” Top influencers in Security 2021 as well as Top 50 Women in Cybersecurity Africa 2020. Polly is a mentor for the CyberGirls fellowship and a member of VigiTrust Global Advisory Board plus Women in Cybersecurity (WiCys).

Currently, she is an Afrika Kommt! Fellow at SAP supporting cybersecurity and data privacy compliance related activities.

Saman FATIMA

Technology Education in my Country

Science and Technology in the Indian subcontinent date back to the Indus Valley Civilisation, about 2600 BCE. A civilization that maneuvered sophisticated irrigation and sewage systems thousands of years ago can only describe the pinnacle of technology my country and my heritage was since the beginning of humankind.

India has been the pivot of technology since time memorial. Being one of the oldest civilizations in the world, historically and culturally rich, we have a long scientific and technological tradition. It is no surprise that many significant inventions have come out of India. The Zero, Yoga, wireless communication, the USB (Universal Serial Bus), Board Games, Cataract surgery, and many more are all Indian inventions, giving us a glimpse of the technological advancement, we were then and the relentless progress that is not new to us.

The tech education in India is highly exhaustive with the curriculum following the changing times. The Indian Institutes of Technology (IITs) and National Institute of Information Technology (NIIT) are some of the pioneer institutes that have given birth to genius minds like Sundar Pichai, N. R Narayan Murthy, Raghuram Rajan, Deepinder Goyal, Arvind Kejriwal, etc., to name a few. We have some of the most amazing research going on in these pioneer institutions that have proved to be a game changer in the field of technology.

Interestingly, India has the largest number of engineers and engineering infrastructure in the world. As per 2021 data, India produces fifteen lakh engineering graduates every year. With budding young minds, India's technical education infrastructure includes 2500 engineering colleges, 1400 polytechnics, and 200 schools of planning and architecture.

India today is at the cutting edge of technology. With the latest advancements in Information Technology, Gaming, Data Science, Artificial Intelligence, Virtual Reality, and Blockchain technology, to name a few, India is making a mark on the face of the world.

Saman FATIMA, India

Data Engineer at Macquarie Group with comprehensive experience in software development and Cybersecurity, Saman Fatima is the rising star of the industry! Trained extensively in Identity and Access Management, she has always been a Cybersecurity Enthusiast and is an active member and young leader, instructor, ambassador and advisor, mentor, and encouraging participant of professional discussions at OWASP - Women in AppSec, CyberPreserve Community, Women in Cybersecurity (WiCyS), Women In Cloud , Snyk Ambassador, as well as the Management Lead & Vice Chair of Board at BBWIC Foundation. Saman has been a speaker at conferences like SANS New2cyber Summit 2022, OWASP Appsec 2021, DevSecCon 2021, c0c0n 2021, Rainbow Secure Cyber Symposium 2021, Tech(k)now Day 2021 & 2022, The Hackers Meetup, and various local and virtual meetups.

Lisa ROTHFIELD-KIRSCHNER

How We Got Cyber Smart

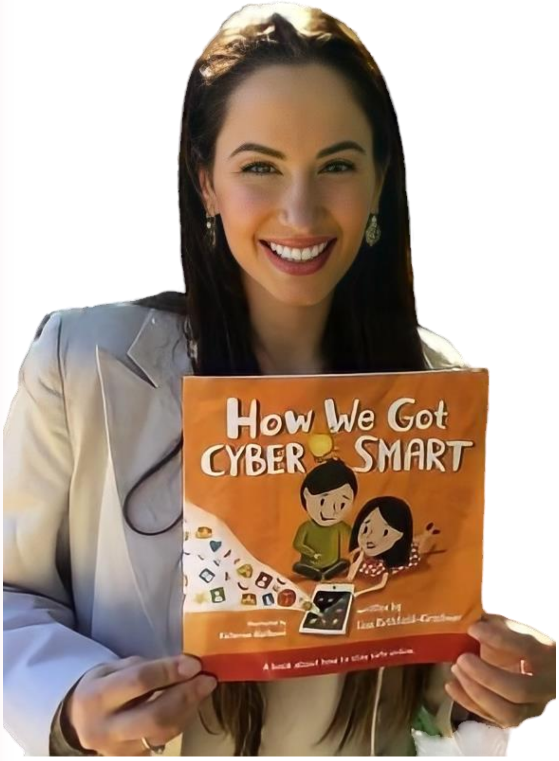
When I was growing up, discussion about children's safety was usually focused on stranger danger and bullying was dealt with by parents telling kids to 'just ignore them'. 'Screen time' was mostly limited to what was on the TV in the living room.

Nowadays, it's much harder for parents to keep up with dangers facing their children in today's rapidly expanding world of online gaming, social media, video streaming and more. Kids are getting online earlier, and there are predators online that can connect to your children without you knowing about it. This is more serious than many people think, and the rate of cyberbullying, stalking and harassment against children is alarming, which is why It's more important than ever to keep our children safe online.

As a mother of two young boys, I needed to ensure they knew how to stay safe online. I also learnt that it's not always an easy topic to discuss with your kids. That's why it was incredibly important to me to write How We Got Cyber Smart, so that my children and other children can learn how to stay safe online and families can use it as a resource to help start the conversation about online safety together.

How We Got Cyber Smart is aimed at elementary school-aged children and follows twins Olivia and Jack who encounter a cyberbully when they're playing on their tablet. The story is realistic and models positive parental behaviour to children whilst showing the emotions felt by Olivia and Jack when they encountered the cyberbully. It's also a terrific story for educators to read to their students to help facilitate the discussion about online safety in the classroom.

You can purchase your copy of How We Got Cyber Smart through Amazon - https://www.amazon.com/dp/0648727513/ or visit https://howwegotcybersmart.com



Lisa ROTHFIELD-KIRSCHNER, Australia

Lisa Rothfield-Kirschner is the author of the celebrated children's book 'How We Got Cyber Smart' which deals with online safety and cyberbullying.

As a concerned mother of two young boys, Lisa creates resources to help parents, caregivers and educators have conversations with elementary school-aged children about staying safe online.

Lisa's focus is on making learning about online safety accessible for younger children in a relatable way. This passion has seen her develop content for ySafe, Australia's leading Cyber Safety education provider, the Australian Women in Security Magazine, and the Australian Department of Education "Cybermarvel" Program.

Confidence STAVELEY

Breaking News from the CyberGirls Linux Party

We don't miss an opportunity to infuse fun into #cybersecurity at CyberSafe Foundation ; so for this cohort of CyberGirls, we introduced an in-person event called the CyberGirls Linux Party.

This event is scheduled to hold in 3 cities on 3 dates and is exclusive to our community but with the requirement for each fellow to complete reading Linux For Hackers. While we'll have really fun games like Cybersecurity themed charades, CyberGirls Got Talent (CGT) our custom-made find-your-command game; we'll also have a CTF to test our fellows Linux skills. The winner will go home with a cash price and other beautiful gifts.

In Nairobi, the talented Catherine Kamau came first position and I can't wait to both meet our CyberGirls based in Lagos for the first time and see who takes home the $100 cash price in Nigeria.

Our dress code was 90's themed, to allow us play dress up and have fun while learning.

It's my opinion that if we are to succeed at attracting many more women into #cybersecurity we must get innovative and enrich the learning experience.

CyberGirls is a 1-year fellowship, designed to equip girls with globally sought-after cybersecurity skills to improve their socio-economic wellbeing, by providing world-class free cybersecurity training, mentorship and job placement.

Confidence STAVELEY, Nigeria

Confidence Staveley is a multi-award-winning Cybersecurity Professional, Cybersecurity, Awareness Advocate, Cyber Talent Developer and Global Speaker.

Confidence has achieved numerous professional certifications and industry recognitions including but not limited to; Cybersecurity Woman of the Year 2021 Award, IFSEC Global Top Influencer in Security & Fire 2021, Top 50 women in Cybersecurity Africa 2020, 2021 African Obama Leader, etc, an acknowledgment of her professionalism and expertise globally. She is the Founder and Executive Director of CyberSafe Foundation, a leading non-Governmental organization dedicated to improving inclusive and safe digital access in Africa.

Gabrielle BOTBOL

Pentesting as an Action for Cyberpeace

In the hyper-connected world, Cybersecurity must be at the heart of a company's IT strategy. An intrusion in the information system or a data leak can jeopardize a company's viability. The penetration test is an effective asset in terms of security.

Pentesting is a technical, proactive security measure that aims to identify vulnerabilities in a system by attacking it. Also, the role of a pentester within a company or an organization, invites them to question the protection of the democratic values of our societies. Unlike a cybercriminal, an ethical hacker acts for the common good and in the interest of Cyberpeace.

State cyber attacks have increased significantly, and cybersecurity must be tackled in a global manner. It is not just a technical matter anymore, but everyone's concern. In an unstable geopolitical world, a resilient cyber strategy with a systemic approach becomes urgent based on cyber governance, cyber hygiene culture, and risk and crisis management. Collaborating with all cyber teams is essential to provide continuous security to all societal actors.

Some companies, NGOs, universities, local governments, or hospitals do not have the budget or the expert teams to protect themselves. Money and priorities for the security of all must become a central issue in our societies. Several associations like Hackers Without Borders and Cyberpeace Institute are actively involved, but it is still challenging.

I particularly praise the need for private and public actors to come together and provide solutions like massive training on cyber hygiene habits and training to all cyber enthusiasts in cybersecurity professions. Democratization and education from an early age would make our societies more resilient. Moreover, including all citizens with cyber experts in securing the society would allow taking into account the different backgrounds, genders, and profiles for better robustness in cyberspace.

Gabrielle BOTBOL, Canada

Gabrielle Botbol is a professional actress who became an ethical hacker!

A self-study program for ethical hackers, created and led by Gabrielle gave professionals the chance to democratize information security.

Gabrielle is the heart and the voice of cyber communities, and she promotes the values of equality and justice, acting her best in “Action for Cyberpeace.”

She shares her knowledge through talks and workshops for international conferences and local organizations.

Mrs Botbol has been honored for her accomplishments and contributions by multiple awards like Top 20 women in cybersecurity in Canada 2020 and Educator of the year 2022.

TOP CYBER NEWS MAGAZINE

BRING TECHNOLOGY TO THE FRONT OF THE BUSINESS

Human Centered Communication Of Technology, Innovation, and Cybersecurity

«Top Cyber News MAGAZINE continues to highlight those leaders of cybersecurity that others may not know and at the same time inspiring many others to become our future leaders in a cyber career that is so desperately in need of additional employees»

Dr. Bradford SIMS, FRAeS, President at Capitol Technology University

«Top Cyber News MAGAZINE has been an invaluable resource in getting the message about the unique issues of control system cyber security to the mainstream cyber security community.»

Joe WEISS, Managing Partner Applied Control Solutions

«Amazing read Ludmila, you have my full support. I especially love and appreciate how many women are highlighted in your publications. There's a definite need to equal the playing field in tech.»

Dhafir FULLER, Director of Sales and Marketing Development at Format Cyber

«Thank you for these profiles. It's helpful to many to see the dreams and struggles with obstacles and celebrating wins others experienced on their journey to career seniority and success. DEI and A stories are especially critical since many people once rarely saw and talked to people like them or felt uncomfortable taking a risk raising the challenges they face and the personal impact the barriers and blows had on them. How people overcome and how they felt is as critical as seeing someone like us sitting at a dais or standing on a stage.»

Kawika DAGUIO, MBA/MPM, vCxO and PA Constable (Chief)

TOP CYBER NEWS MAGAZINE

Human Centered Communication Of Technology, Innovation, and Cybersecurity

AN AWARD-WINNING DIGITAL MAGAZINE

ABOUT PEOPLE, BY PEOPLE, FOR PEOPLE

Ludmila Morozova-Buss

Doctoral Student at

Capitol Technology University

Editor-In-Chief