TOP CYBER NEWS MAGAZINE

2023 SPECIAL EDITION

TOP PERFORMERS IN CYBERSECURITY 2023 FROM FIVE CONTINENTS, WORKING FOR A SAFER AND RESILIENT DIGITAL FUTURE

Fore*Word*

Own Your Future!

"We, In Security, Protect Hope."
~ Troels Oerting, Expert Member Of Interpol,
Global Cybercrime Expert Group

ONLY talent! NO ranking here!

With the global cyber-skills shortage, it is crucial to encourage talent who dedicate their energy and career to cybersecurity.

This special edition spotlights remarkable cybersecurity and digital industries professionals. Top Cyber News MAGAZINE is pleased to unveil this list of young and devoted professionals: ambassadors, advocates, and influencers.

All are part of the inspiring force behind the global Cybersecurity Awareness movement. These talented experts and brilliant minds come from 21 countries and five continents.

I invite you to discover these wonderful professionals. See the light in others and you will be stunned about how this light comes back to you! Enjoy reading! Share! Learn!

Yours most sincerely,
Top Cyber News MAGAZINE Team

Season's Greetings From

Capitol Technology University!

Season's Greetings from Capitol Technology University! As we plan for the holidays ahead, we reflect on progress over the past year. Capitol Tech has been busy expanding programs for cyber professionals. And we have exciting plans for professional development webinars and activities for the new year.

As a leader in STEM education since 1927, Capitol Technology University continues to develop cutting-edge degree programs. Located just outside of Washington D.C. and accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools. We were recently ranked the top 10 Best Master's Online Programs by Master's Programs Guide, with programs such as Cybersecurity, Cyberpsychology, Cyber Analytics, Aviation Cyber, Critical Infrastructure and more .

Capitol Tech offers online doctoral programs to meet the needs of busy cyber professionals. The growing need to more advanced and specialized research is reflected in the program options- Cyber Leadership, Cyberpsychology, Cybersecurity, Financial Cybersecurity, Healthcare Cybersecurity, Human Factors, Offensive Cyber Engineering and more.

In our ongoing commitment to provide education, information and support for the cyber professional fields, we offer monthly webinars on important topics in the industry. Join us for our Cap Tech Talks or visit our page to view a previous session. Some of our recent presentations include- "Practical Understanding of the OSINT Practices and Tools" and "Infrastructure: Critical Challenges and Differences between the Private and Public Sectors."

We are happy to announce our new Center for Women in Cyber. Capitol Tech's Center for Women in Cyber (CWC) is focused on empowering women of all ages to pursue careers in cyber. This Center seeks to address the growing need for women professionals and leaders in cyber-related fields. The CWC provides the resources, direction, and positive support needed for success in achieving professional and educational goals through presentations, hands-on activities, partnerships, and mentoring. The CWC is passionate in its quest to develop the next generation of diverse cyber leaders.

The CWC is led by Dr. Diane M. Janosek, Executive Director. Dr. Diane M. Janosek is an international award-winning, well-known cybersecurity leader and author. She is dedicated to giving back to the community and increasing diversity in the cybersecurity, national security and technology domains. Having both her law degree (J.D.) and Ph.D. (from Capitol Technology University in Cybersecurity Leadership), she focuses on the intersection of law and policy with technology.

Wishing You A Happy And Healthy Holiday Season And An Exciting New Year!

40 under 40 in Cybersecurity

Is A Recognition To Live Up To

2022 has been a big year for many of us, we have all started to head back into the world, withdraw from the virtual world and back into the physical world. It has been tough; it has been challenging but it has been rewarding on so many levels. As one of the Top Cyber News 2022 "40 under 40" Alumni, I was honoured but also inspired to do more.

Some of my fellow 2022 alumni will likely know that feeling, on the one hand, we have been included in a global list of amazing cybersecurity professionals, people who individually do amazing things that make a deep difference to the industry. They are the game changers, the people who walk the walk, not just talk the talk. They do what they say and drive positive change however they can in an industry that can be just with the day job be quite challenging and onerous on one's time but to then commit a large amount of their spare time to help make that difference.

I know I felt a renewed call to action, a responsibility to meet those internal expectations, to be the person who deserved to be among that list, to be the best version of myself I could be. Did I achieve that goal? Honestly, I think I have. By no means does that mean I am done, that is all I can achieve, no way, that just means I have worked hard, I have written some books, mentored some amazing people, and helped grow my local cyber community. Yes, I have kicked some goals and I have helped some people.

That's a good start. There is so much more to be done and as an inaugural winner of the 40 under 40 by Top Cyber News Magazine in 2022, I want to throw out a gauntlet for you all. The members of the "40 under 40" 2023 Top Cyber News MAGAZINE new alumni,

I want you to take this moment of pride, the satisfaction of being recognized for what you have been able to achieve up until this moment. **Take that moment you have earned it but once you have let the dust settle, I want you to look at your achievements, look at your fellow "40 under 40" member's achievements and consider what you could do to go beyond that level.** Could you make a bigger difference in what you are doing, could you help one of the other members achieve what they have been trying to do, could you expand their reach and just be that missing piece that could really make a difference?

Take this recognition, this honour and make it a stepping stone to greatness. Yes, that's right cease your moment, help others cease theirs and let us make the Top Cyber News "40 under 40" alumni members forever remembered as the shakers and movers of our industries, the ones who didn't sit silently on our victories but continued to charge, continued to take ground.

You are all, what this industry needs, heroes, people to aspire to. Go be that person.

Yours sincerely, **Craig Ford**

Global "40 under 40 in Cybersecurity" by Top Cyber News MAGAZINE 2022

From Buddy Poppy Queen

to Science, Quantum and Cybersecurity Empress

Dr. Keeper L. SHARKEY, USA

Dr. Keeper L. Sharkey is the founder and CEO of ODE, L3C, a social enterprise the serves through quantum science, technology, and research. She is the Lead-author of a recently released book titled: Quantum Chemistry and Computing for the Curious: Illustrated with Python and Qiskit® code, published by Packt. She serves as the Chair of Quantum Applied Chemistry at Quantum Security Alliance, Vice-Chair of Cyber Security in Quantum Computing and Quantum's Effect on Current Architectures in the group Cyber Security for Next-Generation Connectivity Systems with IEEE, is a civilian member friend of US Quantum Industry Coalition, point of contact for ODE's co-founding membership of the Quantum Economic Development Consortium (QED-C), and is a member of both American Chemical Society and American Physical Society.

She is also a Research Associate at University of Arizona, Department of Chemistry & Biochemistry with the Adamowicz Group as well as the Entrepreneurial lead for National Science Foundation Innovation-Corps (I-Corps) program Team QLEAN and Market Research Affiliate at Tech Launch Arizona. Dr. Sharkey received her PhD in Chemistry and her BS in Mathematics and Chemistry; both from the University of Arizona and attended Telluride Science Research Center summer school on Theoretical Chemistry followed by a Postdoctoral Faculty position at Washington State University, Department of Physics and Astronomy. Her honors and awards include: the National Science Foundation (NSF) Graduate Research Fellowship DGE1-1143953, and NSF I-Corps program participation - 1547749. She has authored over 30 publications in high impact peers-reviewed journals regarding non-Born-Oppenheimer quantum mechanical finite-nuclear mass variational algorithms with over 400 citations. She moderated the panel session on END USER APPLICATIONS (CHEMISTRY / PHARMA) Session at Quantum Business Europe and served on a panel for the Department of the Air Force Information Technology conference (DAFITC) about quantum and cybersecurity.

Steps to Build a Modern

Vulnerability Management System

Trishneet ARORA, INDIA & USA

Trishneet Arora is exceptionally passionate about securing cyberspace and started his entrepreneurial journey in 2013 at 19 when he founded TAC Security. From there, under his leadership, TAC Security has been securing the world's top brands and governments across the globe while disrupting cyberspace. He is a part of the Forbes Business Council, an Invitation-Only Organization for Successful Business Owners, and the Forbes Technology Council, an invitation-only organization comprised of leading technology executives.

Trishneet is a part of Forbes 30 Under 30 List (2018), 50 Most Influential Young Indians by GQ Magazine, Fortune's 40 Under 40 List twice (2019 & 2021), being the youngest one on it both times, Top 200 "Leaders of Tomorrow" by St. Gallen Symposium (2018 & 2022), a two-time list maker (2020 & 2021) for "The Top 100 Great People Managers List" by Great Managers Institute in association with Forbes and many more. In 2017, 25th August was proclaimed "Trishneet Arora Day" by the Late Javier Gonzales, Mayor of the City of Santa Fe, New Mexico.

With the current ever-evolving and solution-oriented market, it can be overwhelming to narrow down and build an appropriate and robust Vulnerability Management System. Here's a guide to building a vulnerability management system that matches all your needs to ease the confusion.

What is Vulnerability Management? Vulnerability Management is the continuous process of identifying, assessing, prioritizing, mitigating, and remediating the vulnerabilities across the complete IT infrastructure of the organization. Cybersecurity needs to be monitored in real-time and remediated as soon as possible to avoid attacks, and this activity is often overseen by organizations through vulnerability management tools or products.

Assign Roles and Responsibilities to the team –

- A VP or Director to design, monitor, and modify the operation as per the requirement
- A Senior Manager or Project Lead is in charge of the whole operation
- A Security team to discover, identify and prioritize
- An IT team to Remediate the vulnerabilities

Build a Robust CyberSecurity Process – One must understand what every organization has to offer as solutions vary from one to another and the organization's requirements. A robust system includes the ability to discover, assess, prioritize, and remediate all vulnerabilities in the IT infrastructure.

Discover an account of your attack surface – To be sure of your robust cybersecurity process, one must know every weakness, vulnerability, and asset present in your system.

Discover, Measure, Prioritize and Remediate your Vulnerabilities – Discover the vulnerabilities across your entire IT stack and measure the criticality of the vulnerabilities found and remediate them immediately to reduce the possible attack bracket time.

Know your cyber score – By 2025, the cyber score will be the de facto of cybersecurity, like a credit score in the fiscal world. An organization will have to achieve a certain number to be compliant. This also helps to know the exact cybersecurity levels and converse easily across your organization.

Conclusion - An organization's attack surface changes and expands daily as it introduces new employees, assets, partners, servers, etc., to the system, making it vulnerable. To monitor and protect your organization, a Vulnerability Management system that gives real-time cyber securing abilities is a need of the hour and a boardroom conversation.

Cybersecurity Strategy
in Organizations

Fatimah ADELODUN, NIGERIA

Fatimah Adelodun is the Special Assistant to the Director General of the National Information Technology Development Agency, Nigeria where she advises the DG on matters relating to National Cybersecurity.

Prior to this role, she worked as the Information Security Manager at the Nigerian Bulk Electricity Trading Plc, the foremost electricity trading company in Nigeria and one of the largest Energy companies in Sub-Saharan Africa.

As a strategic cybersecurity leader, Fatimah is leading the chart in encouraging women to pursue careers in the STEM fields, particularly, cybersecurity. She is the founder of SheLovesCyber- an online (Instagram) platform that educates people on practical tips to be safer online and guidance to people that want to pursue careers in Tech & Cybersecurity.

Fatimah holds a Bachelor of Science in Computer Science and a Master of Business Administration (MBA) with a specialization in Global Leadership from Edhec Business School, Nice, France. She is a Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), Project Management Professional (PMP), AWS Solutions Architect, among others.

The concept of cybersecurity has gone beyond implementing security controls to prevent breaches, especially with the growth in the number of attack vectors on a daily basis. While technological solutions are certainly an essential piece of the defense puzzle, developing a cybersecurity strategy is essential in the protection of organizations against cyberattacks.

What exactly is a cybersecurity strategy?

A cyber security strategy is a plan that involves selecting and implementing best practices to protect a business from internal and external threats. This strategy also establishes a baseline for a company's security program which allows it to continuously adapt to emerging threats and risks.

Typically, cybersecurity strategies are high-level blueprints that are developed with a three-to-five-year outlook but should be updated as frequently as possible. It is imperative that the Management of every organization champion a cybersecurity strategy that is robust enough to repel the vast majority of attacks, and ensures the organization is resilient enough to quickly recover from any that succeed.

A proactive approach is better than a reactive one. Effective cybersecurity requires a sustained effort that encompasses not only application security, penetration testing, and incident management but also employee behavior, third-party risks, and many other potential vulnerabilities.

As organizations are putting their cybersecurity strategies together, they should consider three critical elements to maximize the impact of these leading practices. These elements include: Governance, Technology and Operations.

1. Governance is how an organization directs and controls IT security.
2. Technology refers to the organization's infrastructure to withstand cybersecurity threats over time as users interact with it.
3. Operations are how an organization exercises security by putting the governance and technical elements into action.

Conclusion

When planning a cybersecurity strategy, it is critical to have conversations with key business and IT stakeholders about the governance, technical, and operational elements. Considering all three of these will improve your organization's ability to address and mitigate risks as well as increase its cyber-resilience. This is what it takes to withstand, respond, and recover from a cyber-attack.

We Are Stronger Together

Cooperation in Cybersecurity

Adrien CHERQUI, FRANCE

The digital growth of our economies has rapidly increased over the last two decades. But with new technologies come new threats. Actually, Cybersecurity is not only digital but it relies on existing criminal patterns, trends and networks. The Cybercriminality is the expression of a global context. It is the expression of our modern world. Cybersecurity is not only digital but deeply rooted in the real world politics. To better understand the cybercriminal ecosystem, trends and the overall cybersecurity activity, we often have to step back and look at the big picture to perceive the underlying threats.

Threats are now global and to help reducing the risk, we must cooperate. Cooperation in Cybersecurity has many faces and takes places at different level. It can be technical, operational and strategical.

The most well-known communities gathering incident response teams are the FIRST and the TF-CSIRT respectively created in 1990 and 2000. Through these organizations numerous teams have been able to share information and work together for a common objective: Cybersecurity. The work of these communities is tremendous as they shape rules and norms for the classification of threats (e.g. taxonomy), the sharing of information (e.g. the Traffic Light Protocol) and to raise awareness amongst board members and policy makers.

We have also seen the development of sectoral CSIRTs and ISACs (Information Sharing and Analyzing Centers) over the years. A sectoral approach does also make sense to fight common enemies targeting a specific sector of the economy. Cooperating between sectors through official, structured and unofficial networks of CSIRTs (Computer Security Incident Response Team), SOCs (Security Operation Centers), ISACs and between Governments, helps reducing the risk by sharing information such as IOCs. In fact, creating sectoral and regional CSIRTs and ISACs can improve the cyber resilience.

These last years, we saw the increase of information sharing in France, thanks to ANSSI, and at the European Union level through the Network and Information Systems (NIS) Directive community. As the Cybercriminal Ecosystem is getting more complex and skillful, cooperation becomes a powerful tool for defenders. In France, ANSSI has incubated a network of private CSIRTs called InterCERT-France that has demonstrated its added value in mitigating threats thanks to its contributors. In Europe, the NIS Directive has set up a strong cooperation framework with the creation of the EU CSIRTs Network and the NIS Cooperation Group that gather national CSIRTs and national authorities. **We do no longer have to face threats alone. Together we can get stronger.**

Head of Cybersecurity Performance, Thales.

Expert, Ad Hoc Working Group on SOCs (ENISA)

Expert, European Cyber Agora

Adrien Cherqui is a Cybersecurity leader focused on Strategy and International Relations. Currently Head of the Cybersecurity Performance at Thales, he is also an expert for a working group on Security Operation Centers of the European Network and Information Security Agency, and the European Cyber Agora, a multistakeholders initiative for a digital Europe facilitated by Microsoft, the EU Cyber Direct and the German Marshall Fund of the United States.

He also worked for the French National Cybersecurity Agency, ANSSI, as an International Affairs Officer and published several articles and co-edited books on Cybersecurity, Policy, International Affairs and Intelligence in France and Taiwan.

My Cybersecurity Journey

Is Not A Destination

Noureen NJOROGE, USA

Executive Advisory Board Member | Director of Global Cyber Threat Intelligence | Cybersecurity Mentor | President of Women in Cybersecurity NC

Noureen Njoroge is a Cybersecurity Executive with vast experience in multi-faceted, complex, fast-paced environments in both public and private sector. She is a strategic thinker with proven leadership experience on issues concerning Cybersecurity, Data Privacy, Blockchain security, IoT, Cloud Security, Metaverse digital wallet Identity and Security.

Noureen is a Global Keynote Speaker, a people leader who is passionate about mentoring others. She is ranked amongst the Top 50 Cybersecurity Influencers & Ambassador in the industry today by Engatica Global leaders' platform, Europe IFSEC & Rocheston. Noureen holds a bachelor's degree in Information Technology & Cybersecurity from University of Massachusetts & MIT.

"In the ever-changing landscape of Cybersecurity, one thing is for sure that we are never done learning. As a lifelong learner, I am constantly challenging my mentees to do the same. It's one thing to learn however what's more effective is sharing the knowledge gained with others. I practice the same by mentoring others in this industry after all "We rise by lifting others". In addition to finding a community that supports learning and fosters inclusivity, such as WiCyS (Women in Cybersecurity) and many others out there. "

Featured Podcasts:

- The importance of mentors in your cybersecurity careers | ZeroHour Podcast.
- Diversity and Mentorship in Cybersecurity | Securitymetrics.com
- An Infosec Life | ITSP Magazine
- Creating more opportunities for others in Cybersecurity industry | Cisco Security.
- The impact of a diverse cybersecurity team | Cisco Security.

President and Co-founder:

- North Carolina Women in Cybersecurity
- Global Cybersecurity Mentoring (cybersecmentorship.org)

Advisory Board Member at:

- WiCyS.org
- Cyber leadership Institute
- United Cybersecurity Alliance
- Spark Mindset
- Africa Cyber Defense

Notable Speaking Engagements

- Canada SiberXchange
- Cisco Live, SecCon
- UK Cyber Senate
- International Women's Day
- Caltec Cyber Bootcamp
- WiCyS
- ISSA
- Africa Cyber Defense Forum
- InfoSec girl summit
- ISACA
- Sparkmindset & CyberHER
- BWiSTEM

Join a community of other Mentors & Mentees in Cybersecurity!

Hacking Humans

Dr. Fatemah ALHARBI, SAUDI ARABIA

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 is the CEO of the Cybersecurity Awareness Month Initiative, Member of the Applied Science Research Center Council and 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.

Educating Underprivileged Youth

On Cyber Security

Praveen SINGH, INDIA

Co-Founder & Chief Information Security Advisor at CyberPWN Technologies Pvt Ltd, young and talented Cybersecurity Influencer and Blogger, Praveen Singh is internationally known for his passion for Technology, Cybersecurity Research and Cybersecurity Community Building worldwide.

Cyber Security enthusiast and strategist with more than 15+ years of proven track record in Cyber Security Consulting and Strategic business management, Praveen offers advisory and mentoring for upcoming CISOs while running many CISOs communities across India. He has demonstrated success-devising information security strategy, setting operational standards and governance frameworks.

Praveen has recently become certified Cybercrime Intervention Officer (CCIO) under the National Security Database (volunteer) which highlights his inclination towards Cybersecurity.

Cyber Leaders - Call for Action

At the age of 18, when I was in college, realized that there were a few underprivileged children who were deprived of access to quality education. With India taking a giant leap in education initiatives, I and a few of my classmates came together to address this issue by volunteering ourselves and spending some quality time teaching these children.

Then, I realised that volunteering for a good cause can provide a healthy boost to our self-confidence, self-esteem, and life satisfaction. I truly felt that the role as a volunteer to help someone can also give you a sense of pride and identity while benefiting the underprivilege youth.

In this digital era with "growing demand for cybersecurity professionals", what I believe is that Cybersecurity education can be a powerful tool which empowers communities to turn around their lives. But unfortunately, underprivileged youth do not have the resources to acquire quality education. Therefore we, the cybersecurity leaders, should come together to educate these underprivileged children and shape their future in our spare time.

When we start , we could face practical difficulties like we cannot give enough time but when it comes to volunteering, it is not all about time. Even the most minor acts of volunteering matter a lot. This Initiative - volunteering for Cybersecurity education for Underprivileged Youth, cannot be done by yourself alone. You being just one person cannot be in multiple places at once. The best path is to encourage others to be community-minded, attend meet-ups, speak, write, and innovate.

I would request all cybersecurity leaders to contribute some of their time towards "Volunteering for Cybersecurity education for Underprivilege youth", Trust me, We can change life of millions…!!!

We, Cyber leaders, should use our knowledge, skills and expertise to help underprivileged youth develop their resilience to be motivated to learn cybersecurity over time, through various initiatives such as support, training or awareness programmes, and national policy improvements.

To sum-up, it would be great initiative if cybersecurity leaders reach out to their local underprivilege community to engage them on career option available in cybersecurity domain and give them pointers how to build career path in cybersecurity for themselves. All we need as cybersecurity leaders is spirit of giving back to society, a sense of altruism by sparing our time, expertise and focusing on uplifting underprivilege youth so that they will be able to thrive in life.

Next-Generation

Chiefs Information Security Officer

Dr. Yosra BARBIER, FRANCE

Dr. Yosra Barbier is a passionate cybersecurity professional who focuses on emerging and innovative cybersecurity concepts and solutions aimed to mitigate the evolving threat landscape.

Dr. Barbier is determined to use her cybersecurity expertise, experience and skills to disrupt the myths and often outdated cyber practices. She has been harnessing the interest of business and technical teams alike through influences in her public speaking assignments at renowned Cybersecurity Forums and conferences.

Dr. Barbier believes that to succeed as a cybersecurity leader, a technical background is a must besides being a strategic thinker and influencer. Yosra is a dynamic and determined, who relies on her Security Engineering and management skills to transform the Security posture for organisations.

By 2025, a single, centralized cybersecurity function will not be agile enough to meet the needs of a digital organization." Gartner for IT Leaders, Top Trends in Cybersecurity 2022.

Such statement might be surprising for Company leaders who used to have one single CISO (Chief Information Security Officer) responsible for implementing and controlling the Information Security controls and enhancing the Cybersecurity posture of the company. In addition to that, CISOs reporting to CEO (Chief Executive Officer) might feel privileged compared to other CISOs. Indeed, this hierarchical position of the CISO is still not standardized. Some CISOs are still reporting to the IT directors or to CTO (Chief Technology Officer).

In such organizational setup, security team is "isolated" (think about it from a roadmap point of view) from other teams (IT Development, Cloud, Customer Success teams, etc), even if the collaboration exists between them.

The immediate consequence of this isolation is the non-agility of the security controls deployment. In a world where the business is increasingly digitized, this isolation is a real obstacle to cybersecurity integration with every layer of the company.

It is also challenging to meet compliance requirements and customers expectations. Therefore, and to remediate to this situation, we noticed some initiatives like the definition of Security Champions or Cybersecurity relays roles to integrate Security in different teams. These initiatives can be considered as the first steps toward distributed cybersecurity function along with the company' functions. Think about it like an organizational matrix focused on Cybersecurity.

Cybersecurity is everyone's business!

Within every team, we will have security experts reporting to what I call Next-Generation Chiefs Information Security Office but performing within a "non-security" team. The best example I can mention would be Cloud and DevOps team. Usually, those teams are composed of Cloud Architect experts, DevOps Engineer, Automation Experts with a solid background on how to manage the cloud instances/environments, a solid expertise on micro-services, a good understanding of the CSP (Cloud Service Provider). Enforcing this team with dedicated Cloud Security Expert(s) is a game changer to integrate security within the roadmap and projects managed by the Cloud Team.

Bringing Cybersecurity Hiring

Out from Behind the Firewall

Travis DEFORGE, USA

The pandemic forced many companies to embrace remote work. You might think that access to a global talent pool would alleviate the shortage of qualified candidates, but that has not proven to be true. Now more than ever, jobs in cybersecurity are in high demand. The situation looks serious when considering that ISC² estimates that the total cybersecurity workforce needs to grow by 65% to meet emerging threats . This has transformed the industry into a candidate's market in which there is tremendous competition for those few candidates with the perfect combination of experience and certification.

Organizations filling vacancies in their cybersecurity departments must get more creative in the types of candidates that they seek. Identifying highly motivated people with strong soft skills, a genuine passion for the subject matter, and a willingness to learn will often produce a better ROI over the long term. Technical skills can be taught, but work ethic, intrinsic motivation, and communication skills are far more challenging to influence.

According to a recent survey in the Hays Cyber Security Talent Report, 61% of employers found it difficult or very difficult to recruit cybersecurity talent . Survey respondents attributed the challenges to a lack of technical skills and soft skills. Soft skills cited in the study were adaptability, interpersonal and communication skills, passion, being curious and inquisitive, and having general business acumen .

A combination of technical domain knowledge and these soft skills is ideal for cybersecurity practitioners. An engineer who can conduct a penetration test, effectively communicate the findings in writing and verbally, all while translating the real-world, top-line and bottom-line business impact to clients sounds like the perfect candidate. While individuals like that certainly are out there, finding them is a challenge.

But there is another option. Hard skills such as specific technologies, analytics, and incident response techniques, can all be taught, but I've yet to see an effective method of teaching somebody to be passionate and inquisitive. Instead, focus on identifying candidates who have demonstrated adaptability (perhaps by training to switch industries into cybersecurity), have well-honed communication skills, and are passionate about learning the hard skills.

Travis DeForge is the Security Engineering Manager of GoVanguard Security, a US-based boutique cybersecurity firm that provides high-quality penetration testing, malicious adversary simulation, threat intelligence, and cybersecurity strategy services. In this role, he routinely conducts network and web application penetration tests, social engineering engagements, and cloud security assessments for multibillion-dollar global organizations.

Before joining GoVanguard Security, he served as a Military Intelligence Officer in the United States Army for several years. During this tenure, he held several positions related to signals intelligence (SIGINT), open-source intelligence (OSINT), electronic warfare (EW), and information operations at both the tactical and operational levels.

Travis is passionate about cybersecurity and training others. He regularly publishes open-sourced content to help motivated professionals transition into the industry and cohosts a free weekly cybersecurity training session for the community.

Building Cybersecurity

First Things First

Asmae EL MORABIT, MOROCCO

Asmae EL MORABIT - Regional IT & Cyber Risk and Permanent Control Officer at a multinational financial group- is a driven security minded and business oriented professional. She credits more than 10 years in IT, Education and Financial Industries, and has cumulatively represented internal control functions within multinationals in IT and Cyber Risk Oversight and Supervision, Compliance and Data Protection. Her knowledge and expertise are recognized on an international scale around her peers through her work and projects in area of IT & Cybersecurity Audit and Risk Management. Asmae believes strongly that technology and innovation can push Africa to the next level of economic growth, especially with the rise of FinTech, a growth that would stay dependent on a resilient and sustainable Cybersecurity Framework.

In recent years, we witnessed a paradigm shift in the way IT systems are implemented to serve businesses and allow organizations to remain competitive. The race to adopt new disruptive technologies such as cloud computing, RPA & AI, Machine Learning and IoT is driving tremendous changes in many industries, in a post pandemic era where working from home became the new normal.

Consequently, the focus on cybersecurity has never been sharper. Disruptive Information Technologies start to reflect on disruptive cyberdefense and cybercrime mechanisms dynamically evolving. Hackers and cybercriminal providers are vying to outsmart each other, getting more and more innovative, while on the other, cybersecurity topics are starting to move from the IT department to the board room and becoming a vital matter, giving the rise of losses in terms of consumer trust, regulatory penalties and decrease of revenues. The sheer volume of digital assets, across different environments, that we collect, produce, distribute, manage and share have extraordinary value to individuals, businesses, and governments. And while IT environment are growing more complex, organizations fail to safeguard and protect their valuable assets.

This is where Cybersecurity Management Frameworks come into play to effectively prevent, detect and react to threats and attacks. The proper deployment of the latter and its continuous improvement, with focus on data as the core digital and business asset, remains challenging. In fact, delivering effective enterprise cybersecurity is not only about acquiring and deploying the top latest cyber security tools, it starts by defining a business integrated cyberrisk strategy and governance, aligned with business objectives and regulatory requirements, while providing a balance between performance and conformance to deliver value.

This can be incorporated with agility across the organization by focusing on maturity attributes that can be measured and controlled permanently. It can include (1) the definition of clear goals and key performance & risk measurements; (2) the deployment of cybersecurity policies and procedures; endorsed by (3) setting up clear responsibility and accountability involving business functions; while (4) ensuring that security positions are filled and that skills and expertise stay sharpened; (5) using tools for process automation and, last but not least (6) spreading awareness and cybersecurity culture across all organization. Finally, any cybersecurity initiative would be doomed to failure if not placed at the heart of the business, and sponsored by top management.

Cyber Security

And Outer Space Security

Tawhidur RAHMAN, BANGLADESH

The functioning of a large portion of the world's essential infrastructure depends substantially on space, more especially, space-based assets. Communication, air travel, maritime trade, financial services, weather monitoring, and defense are just a few of the critical systems that significantly rely on space infrastructure, which includes satellites, ground stations, and data links at the national, regional, and global levels. This dependence presents critical infrastructure providers and policymakers with a significant, but largely ignored, security challenge, particularly in the context of cyber attacks.

Satellites and other space-based assets are susceptible to cyberattacks, much like any other increasingly digitalized essential infrastructure. These cyber vulnerabilities seriously endanger important infrastructure on the ground as well as space-based assets. These dangers could obstruct the expansion of the world economy and, consequently, compromise international security if they are not eliminated. Furthermore, these worries are no longer just conjecture. More nations and commercial entities have acquired and used counter-space capabilities in cutting-edge applications during the past ten years, posing a larger existential danger to crucial space assets.

Why are space systems vulnerable?

Many space systems date back to a time before cybersecurity was given primary consideration by policymakers. They feature flaws like hardcoded credentials, which are employed by military, commercial aircraft, and ships and make access by knowledgeable actors relatively simple. We are seeing the transition of spaceflight from a publicly funded activity to a for-profit sector. The range and scale of activity in this field will grow as more business actors can access space through commercial service providers and offer a variety of services there. By demonstrating that space exploration is no longer the exclusive purview of affluent spacefaring nations' governments and their academic affiliates, NASA's SpaceX Demo-2 mission, which was successfully completed on August 2, 2020, created history. NASA will no longer need to use Roscosmos exclusively to carry its astronauts to the International Space Station (ISS), which will save the agency more than $30 million per astronaut every trip….

https://fintechbd.com/cyber-security-and-outer-space/

Tawhidur Rahman is a security professional with over 17 years of experience in Cyber security consultancy, Digital forensic, Framework Design, Policy Making, project development and execution, integration of various technologies, lawful interception system, Telecommunication network interrogation & active tracking system, command control and communication, critical infrastructure security, tactical & intelligence solutions etc. Currently he is working with Government of Bangladesh E-Government Computer Incident Response Team as Senior Technical Specialist (Digital Security & Diplomacy). His previous experience includes consultancy for Government Joint Defense Intelligence organization on different cyber-security issues. His research focuses on cybersecurity governance, and incident response. He holds a PGd in Digital Forensic from University of Leicester and Cyber Threat Intelligence from Carnegie Mellon University and a BSc in Computer Science & MIS from the Independent University, Bangladesh.

Shamane's Three Keys

Shamane TAN, AUSTRALIA

Chief Growth Officer at Sekuro, Shamane Tan is an award-winning global cybersecurity influencer who works with the C-Suite and Executives on their strategy in uplifting their corporate security posture..

Shamane enjoys using her commercial mindset coupled with her technical background, to help bridge business gaps. Throughout her career, Shamane has partnered directly with CISOs, CIOs, CTOs and Global Heads to help both enterprises and smaller companies in APAC with their growth strategy. 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.

Shamane is the author of three books: 'Building a Cyber Resilient Business: a handbook for Executives and Boards'. 'Cyber Mayday & the Day After' & 'Cyber Risk Leaders: Global C-Suite Insights – Leadership and Influence in the Cyber Age', all business guidebooks and stories containing rich leadership insights from 100+ CxOs across industries.

As a TEDx speaker, podcaster and founder of an international Cyber Risk Meetup which has 3,000 members across six different cities, her Mega C-Suite Stories conversations with top industry C-level leaders offer a platform for security enthusiasts and executives to impart and exchange innovative insights.

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.

Remediation

For Social Engineering

Dorota KOZLOWSKA, POLAND

We continuously work towards improving security hygiene within companies by introducing new policies, security controls and other defences to increase the business resiliency to security incidents. However, as the reliance on technology advances, so do the ripple effects of attacks such as supply chain attacks, ransomware and other incidents. It is a scary environment for businesses, but as a Penetration Tester, it is a great environment to be in as I can help companies improve their security hygiene with the skills and knowledge I possess.

We need to focus more on the cultural aspect within businesses and highlight the human element of security. For example, emotions are often a target of social engineering attacks: trust, kindness, and anger can all allow for social engineering attacks to be successful. In addition, well-formed social engineering attacks can significantly impact the business. The 'hacking-the-human' or social engineering trend is a result of criminals realising that it is difficult to breakthrough sophisticated security technology, whereas it is very simple to trick someone to open up a malicious attachment, click on a link or share sensitive information. Traditional awareness training needs to be better, and we must arm employees to improve personal security hygiene, which will translate to better business hygiene.

The threat within the business is also something that needs to be taken seriously, such as policy violations, vindictive employees, and poor processes are examples of internal threats that can undermine the business's security posture. Visibility is critical to allow security teams to perform the due diligence to identify and protect the company from these threats. Social engineering is the path of least resistance for criminals; security controls such as firewalls, host protection, and many others create a defence-in-depth environment in which the easiest way in is through the human. The awareness training should give employees the right skills and knowledge to help them identify threats and highlight reporting lines where they can get assistance from professionals within the business. On the other hand, the company should deploy controls to reduce the impact of social engineering attacks because the risk of human error and social engineering is never zero. Security awareness needs to be continuous, measured, and flexible; it needs to be engaging and exciting. Investing time and resources in building a security culture is a powerful thing for business leaders to consider.

Dorota Kozlowska - Skilled Penetration Tester, One-Woman-Army, doer, and a self-starter with a growth mindset - often takes initiative on things and leads the rest of the group. Previously experienced in QA, Test Automation and Project Management with personal passion for CTFs, and Red Teaming and degrees in: Economics, Management and Marketing, and Computer science.

Dorota has made a few career switches from being a local government official into QA, Test Engineering, and Security Analyst to Penetration Testing - her dream job. She is continuously building her knowledge base and displays lots of grit, adaptability, fast learning capabilities, and personal strength. She seems to be unstoppable.

"I am a true Wonder Woman. I have finally made my dream of becoming a Penetration Tester come true. I am a Winner. What have I won? My own life."

~ Dorota Kozlowska

Cybersecurity
in the SaaS Industry

Ludovic LECOMTE, FRANCE

Ludovic Lecomte began his role as CISO at Inova in February 2022. After spending 10 years in Cybersecurity consulting and audit roles, Ludovic built a certified Information Security Management System from scratch for Inova, leveraging his communication skills, risk engineering and passion for new technologies to take cybersecurity to the next level.

In addition to adopting a rigorous risk-based approach to cybersecurity, he is committed to building a digital trust space for both customers and internal users. Ludovic is always ready to share his expertise with the broader CISO community and with students training to be future Cybersecurity engineers at a French university.

With the rise of the Software as a Service (SaaS) business model and explosion of data externalization, companies have increased their exposure to data leak. By making an investment in a "Security by design" project, SaaS companies can stay one step ahead of the competition, prevent the impacts of a cyberattack for their customers, and save money by not having to fix vulnerabilities later in production. All SaaS companies should demonstrate that cybersecurity is a key component of their development processes and that they are taking aggressive steps to integrate security into their everyday operations.

"Security is all about Trust." Placing cybersecurity at the center of a SaaS product delivers a confidence boost for customers who adopt it and establishes trust in the software and its capabilities to protect the data. There are famous certifications like SOCII or ISO27001 that go a long way in providing customers with evidence that best practices are applied and audited, but compliance is not enough. We need to continuously improve security by renewing risk assessments, tracking new threats and monitoring security solutions.

"We know the incident will happen, we just don't know when." Security by Design is a concept that pushes SaaS companies to build their software and hosting platform around a secure foundational principle. It is a proactive approach that aims to avoid and limit the impact of a successful cyberattack. This approach also means minimizing the cyberthreats exposition surface by identifying risks scenarios and implementing organizational or technical security controls. To do so, my strategy at Inova was to follow these steps: Conduct a cyberthreat modelling exercise. Formalize and share a Secure Software Development Lifecycle Policy. Train Security Champions who are the eyes of the security at all steps of the DevOps process. Finally, integrate security tools into the DevOps pipeline to automate vulnerability and cyberthreat detection.

"Do remember to protect your Forgery!" In addition to training people on cybersecurity, evaluate risks on the internal Information System of the company. The latest cybersecurity news confirms this. SaaS companies are being directly attacked from their internal Information System through social engineering or malicious code directly injected in the development framework. Finally, cybersecurity is more about people. Organization and trainings are the best investments a SaaS company can make to begin its security by design project. Particularly when it is not that complicated to find magic tools that automate security scans and provide alerts on vulnerabilities. At the end of the day, you still need people able to react quickly. Therefore… can we say/think that Cybersecurity is an infinite human loop?

The Cyber Talent

Conundrum We Must Solve

Confidence STAVELEY, NIGERIA

Founder and Executive Director of CyberSafe Foundation, a leading non-Governmental organization dedicated to improving inclusive and safe digital access in Africa,

Confidence Staveley is Africa's most celebrated female Cybersecurity Leader, Talent Developer, Global Speaker, blockchain security professional, and Inclusion advocate. She has achieved numerous professional certifications and industry recognitions.

Confidence is an official member of the Forbes Technology Council, an invitation-only community for world-class CIOs, CTOs, and technology executives.

Winner of the Cybersecurity Woman of the Year Award in 2021 and 2022, IFSEC Global Top Influencer in Security & Fire 2021, Top 50 women in Cybersecurity Africa, Confidence has spoken at over 30 international conferences, a testament to her global thought leadership and influence. She is an alumnus of some of the most prestigious fellowships across the world such as: Obama Foundation African Leaders, International Visitors Leadership Program (IVLP).

In recent years, there's been plenty banter about the millions of unfilled roles in cybersecurity, something we have come to describe as the cybersecurity skills gap. There's however, a school of thought which believes that this skills gap epidemic is a self-inflicted wound, one we are not doing enough to heal. Just like money, talent does not grow on trees and the much-needed diversity in our industry will not be achieved without taking radical steps and throwing away the box within which we have limited our thinking to. Here are three thought-provoking ideas.

Internships, the kitchen we forgot to build into the house: Its common knowledge that one of the major challenges with breaking into cybersecurity is getting a first job. As an industry, we dread creating real entry level roles and then cry big ugly tears when we are unable to fill mid-level to senior positions. We have created a funnel with a very narrow entry point. We can change that by creating more simulated virtual internships, where cybersecurity enthusiasts get work experience and grow their skill set. Just as we are currently incentivizing industry mentorship using CPE credits, certification bodies and governments could also create policies to incentivize paid and unpaid internships in the private and public sector.

Is it time to look to Africa for Talents? Africa currently has the youngest population in the world with 70% of sub-Saharan Africa being under the age of 30. Such a high number of young people is a well of opportunity to tap from. Interestingly, Africa's youth population have over the years, shown high interest in building cybersecurity careers albeit all the challenges they face. Given that cybersecurity is a global practice, why isn't geographic talent mobility made easy for talents at all career levels if we are in dire need of a skilled cyber workforce? With a good vetting and ranking system, the rest of the world could benefit from developing countries in Africa, producing more passionate cyber talents than the available work opportunities locally.

Microwaved talent or disruptive talent development: Cyber talent building interventions have become necessary to augment the number of cybersecurity graduates, our traditional learning institutions are producing. There is also a conversation on the structure of bootcamps being better positioned to quickly churn out graduands with hands-on skills the industry currently needs. However, these bootcamps need to be supported with funding and training content especially for minority & underrepresented populations and developing countries. The industry also needs to work with universities to improve curriculums.

Citizen Cyber Awareness

'The Pivot To Cyber Security'

Natalia SPÎNU, MOLDOVA

I have devoted my recent professional career to cybersecurity.

With more information flow and numerous communication technologies and devices at interplay of human interaction, the more complex has been the evolution and manifestation of cyber threats. The emergence of cyber threats is pervasive to humanity and the growth of emerging technologies such as artificial intelligence and blockchain has increasingly made 'awareness' about cybersecurity more complex.

The global standards such as the ISO are good for private sector enterprises, but there is much dearth of standardised civic practices at making citizens understand the threat and countermeasures via-a-vis cybersecurity.

Raising awareness about cyber-attacks for citizens must become part of all national strategies; especially for low- and middle-income countries (LMICs) who do not have adequate resources and cyber infrastructure to deal with manifesting cyber-threats.

Citizen cyber awareness effort should solicit simple communication regarding cyber-attacks such as awareness raising regarding chatbots, acts of denial-of-service attacks on websites, and attacks that target individuals (at work or at home); as these are significantly more common and arguably much effective.

Phishing, for instance, is widely regarded as the most dangerous threat to everyday users of communication tools such as mobile phones and emails as it accounts for up to 90% of all security breaches. Awareness raising for 'human-error' must become centric to citizenship awareness in cybersecurity and efforts must focus on avoiding small mistakes which have far-reaching impacts.

Cyber citizen awareness must become a leading area of practice and research to focus on the human aspects in security. In addition, understanding as how awareness is reflected in citizen action is important to and good metrics must be devised to adequately measure cyber citizen hygiene and behaviour. For example, does directed reading, posters, or online or in-class training really raise the level of cyber citizen awareness?

And if yes, how does one measure it? Cyber awareness must build a foundation of cognitive cyber intelligence and incorporate methods that not only protect the citizen; but also make them resilient against cyber influences.

Director at European Institute for Political Studies in Moldova, Ms. Natalia Spinu is the Internationally renowned thought leader and influencer, with high expertise in ICT project management; ICT strategy development; Information security implementation and audit; ICT security policy development.

Former Chief of the Government Cyber Security Center (CERT-Gov), she has managed cybersecurity projects for the government with responsibility for strategic planning, international and intergovernmental cooperation and capacity building.

Published author, genuine contributor to the cybersecurity community, promoting collaboration via knowledge sharing, organizing various cybersecurity-related workshops, events, and meetups, Natalia is often engaged as a speaker in various national, regional, and international forums, conferences and seminars in cybersecurity.

Cybersecurity
In The Internet Era

Rushabh Pinesh MEHTA, INDIA

Rushabh Pinesh MEHTA, PGP-ITBM, Bengaluru (also called Bangalore) is the capital of India's southern Karnataka state. The center of India's high-tech industry).

Rushabh Pinesh MEHTA is currently working as an IT Audit Manager at Amazon.

Mr. Mehta carries 7 years of work experience in InfoSec. He has worked with IBM, PwC, Deloitte, BNP Paribas and Infosys in the past. He was fortunate enough to serve clients from various industry sectors such as BFSI, ITeS, Oil & Energy, and Consulting. He has pursued Post Graduate Programme in Information Technology Business Management from Symbiosis Centre for Information Technology; Advanced Program in Cyber Law from Asian School of Cyber Laws; and Bachelor of Engineering in Electronics and Communication.

Mr. Mehta holds the following significant information security professional credentials such as CISM, CDPSE, ISO 27001 ISMS LA, ISO 22301 BCMS LA, ISO 27701 PIMS LI, CRisP, NIST CSF, CSA STAR, ISO 27017, AZ-500, AZ-900, OCI Foundations, Alibaba Cloud Security, etc.

Mr. Mehta has expertise in below mentioned information security skills:

- GRC (NIST, COSO, COBIT, PCI-DSS, HIPAA, HITRUST)
- Information Risk Assessment / Risk & Controls Self Assessment (RCSA)
- ISMS - ISO 27001:2013 internal audits
- IT Auditing skills - ITGC, ITAC, S-Ox controls testing, SOC 1 and SOC 2 report attestation.
- Gap analysis & Cybersecurity Maturity assessments
- Third Party Risk Mangement
- Cloud Security reviews
- IT Infrastructure reviews
- Data Privacy & GDPR
- BCP / IT-DR

Rushabh has hands-on experience in below mentioned core IT Audit skills:

- General IT Controls (GITC) testing for ERP applications, Operating Systems, Databases and Network components
- IT Automated Controls (ITAC) testing
- Business Cycle Controls (BCC) testing for business processes such as P2P, O2C, R2R, Depreciation, Inventory Management - BOM / Back flushing, Payroll and Treasury
- Information Produced/Provided by Entity (IPE) testing for completeness and accuracy of the customized reports
- Sarbanes Oxley (S-Ox) Act - Section 404 reviews
- Segregation of Duties (SoD) conflicts testing
- Service Auditor Report (SAR) attestation: SOC 1 (SSAE 18/ISAE 3402) and SOC 2 (Trust Services Criteria) - Both Type I & Type II

He is enthusiastic, always keen to learn and capable of solving complex problems by applying analytical and logical understanding. In his free time, Mr. Mehta likes following cricket, playing chess and listening music.

"Cybersecurity is basic hygiene for all individuals in the era of internet; and is helmet / seat belt for organizations' data in their journey of digital exploration."

How To Stay On Top Of Cybersecurity

Dasha DIAZ, SPAIN

For over a decade, Dasha Diaz, founder and CEO of itrainsec has been organising top-class IT security conferences and training for leading cybersecurity professionals around the world. Her unparalleled experience has enabled her to build a network with the best and brightest experts and trainers the industry has to offer.

Before founding itrainsec, she spent nearly 12 years at one of the world's top cybersecurity companies, Kaspersky, where she began her career as a PR manager, then joined the Global Research and Analysis Team (GReAT) as Senior Research Communications manager. Her standing in the industry also led Dasha to be appointed co-director of the Cyber Security Programme at Harbour. Space University in Barcelona, where she creates a brilliant master's program to nurture cybersecurity talents.

For any individual, keeping cyber security skills up-to-date and relevant in a threat landscape that is evolving so rapidly is a challenge. Threats are growing increasingly complex and sophisticated, and adversaries are more well-funded and determined than ever.

The bottom line? If you want to stay in the cyber security game and remain on top of it, You need to be continually learning, researching, and practicing. To be clear, this isn't about certifications alone, because while these form the basis of any cyber security professional's knowledge, you must learn about the new techniques and procedures that can help you stay abreast of the trends that are affecting the industry.

Anyone who watches the news will have seen a spike in the number of data breaches and ransomware attacks. Bad actors are looking for every possible weakness in security defences, and are finding more as the world becomes increasingly connected. This means that cyber security professionals need to understand the vulnerabilities in newer technologies and how attackers can exploit them.

Developing new skills helps you to stay relevant, and boost your skill set to ensure you are armed with the knowledge and expertise you need to fight today's threats. There are a number of ways to do this. The first step is staying up to date with the latest happenings in the world of cyber security. This can be done by signing up for the most interesting and relevant newsletters, attending forums, and becoming actively involved in a professional community that caters to professionals in the cybersecurity arena.

This will facilitate the exchange of relevant experience, ideas, and approaches to security between a wide range of experts and businesses. Even consider starting your own events that can involve your peers and other practitioners in the cybersecurity field. Remember that identifying and sharing information about potential and attempted breaches with other invested parties can strengthen security measures.

Finally, attend specialised training. By keeping up to date with the goings on in the cybersecurity industry, you can identify any gaps in your skills or knowledge, then devote time to enhancing or growing these skills. We all know that cybersecurity threats change every day, and as we find new ways to connect, exchange, and secure information, malefactors discover new ways to get their hands on it. For cybersecurity professionals, ongoing learning and skill development are more than a priority, they are the key to overcoming current and future industry-wide hurdles.

Security Analytics

Clemens SCHWARZ, GERMANY

In the context of globalization, the human lifeworld has changed away from an analog to a digital one on all levels. Companies as well as cyber security experts are therefore confronted with unexplained manifestations (phenomena) of security-relevant facts in the context of digitalization on a daily basis, such as cybercrime, cyberterrorism, cyber espionage and cyber sabotage. Other requirements such as those imposed by security laws, security by design, data protection and other country-specific legal regulations must also be observed by companies. In companies, IT security officers are, therefore, often perceived by the business as disruptive to business development and even as a hindrance to new and flexible ways of working because of the establishment of necessary standards and technical-organizational measures for IT risks. It is therefore essential that security strategies leave behind classic thought patterns and embrace the need for the dynamics of digitization. Instead of rigid protective walls and castles, open buildings for flexible use are required.

Security analytics is a strategic option here, enabling new paths to be taken in the conception and operationalization of digital transformation in a secure and compliant manner.

Answering questions about the phenomenon and the outlook on future possibilities are essential. In the daily work of IT security managers such as CISOs and top management, the core of this is real-time fact-based decision-making. Gathering information, verifying, and falsifying knowledge enables the formation of the necessary template for decision-making. This ability to decide and to trust in the decision in turn requires real-time analytics, which per se will lead in the short term to the requirement for predictive analytics. Metadata provides the basis for so-called expert systems. These systems are based on distributed IT architectures on the one hand and on algorithms and data structures or data models on the other.

To establish a strategy of trust (Zero Trust) thus illustrates how necessary it is approaches to develop further strategic techniques and methods for finding, securing, and evaluating evidence (facts) for correct management decisions. It will be all the more important that further interdisciplinary expertise for medium- to long-term goal-oriented systematics or methods for problem solving be introduced into the decision-making process. In this way, by investing in security analytics, companies can exploit new potential as a competitive advantage for the further development of their core business in the future and generate added value at the same time.

Clemens Schwarz is a certified Senior IT Security Officer (CISM, CISA, TÜV Lead Auditor ISO/IEC 27001) and experienced Group CISO at Messe München.

Clemens has proven his security analytics expertise in 12 years of implementing security strategies in international projects for German SMEs, automotive manufacturers, security authorities and law enforcement agencies.

He is the author of several scientific publications (NextGen fact-based decision making in real-time) and has been involved in education and training (Chamber of Industry and Commerce), association and committee work (ISACA, German Society of Criminalistics, AFCEA Intelligence) and international (IT) security research (traces and patterns of cyber-extremist-ideological threat phenomena of a globalized world) for more than 10 years.

Protect Your Assets
and Critical Infrastructure

Saltanat **MASHIROVA,** KAZAKHSTAN & UAE

Experienced Advanced Cybersecurity Architect/Engineer at Honeywell, President of ISACA Astana Chapter, founder of Women in Cybersecurity Kazakhstan, Presidential Scholarship awardee (Kazakhstan) for the University of California's Master's program focusing on networked systems and certified in CISSP, GICSP, GRID, CISM, CISA, TOGAF, ISA 62443, ISO 27001, Saltanat Mashirova is an extraordinarily talented influencer, mentor, and a role model in the cybersecurity community.

Saltanat is currently deep into industrial cybersecurity and benefiting the community through innovation, secure architecture development, consulting, training, and onsite deployment of cybersecurity solutions in critical infrastructure. To help others succeed, Saltanat mentors young girls in rural Kazakhstan and worldwide, volunteers at many local communities related to cybersecurity.

The level of digitalization in ICS continues to grow across almost all industries. Today the development of digital technologies has made the market for automation and advanced business solutions available for not only large corporations, but also small and medium-sized industries. At the same time, high demand for digital solutions has also attracted more opportunists who are well-prepared and capable of multi-stage cybersecurity attacks. All attacks on critical infrastructure can be conditionally divided into 2 large groups based on the technical complexity of attackers. First, well-planned attacks that aim to implement a high-quality, covert presence and the ability to control critical production at Level 1, Level 0. Usually, these types of attacks have a long timeline, which includes collecting data about the target company, developing remote access tactics, corporate-level infection, obtaining data on control systems for developing a suitable exploit, and directly introducing a rootkit, reverse-shell. The motives of attacks are usually at causing real damage to the critical infrastructure of the object – distributed control systems (DCS), safety instrumented systems (SIS), or emergency shutdown (ESD) systems.

The second type of attack refers to fast attack, aimed at Level 2 and Level 3 infrastructure. The technical targets of the attack are high-level OS-based systems with known vulnerabilities which are often not patched by the victim. Often, attackers use a ransomware attack to disable the server with technological data so that the business and planning systems are inoperable. The aim of attack can be the extortion of a large money in exchange for a decryption key. The future of production management systems and, in particular, critical infrastructure will be aimed at deepening the symbiosis of the classical process control system with new virtualization technologies (Software Defined Network, CPU Programmable Logic Controller (PLC) virtualization, etc.), various analytical decision support systems, which in turn will increase the number of attack vectors and the extent of damage to business. Changes in the technology and architecture of process control and management systems will require changes in the approach to maintaining this infrastructure and improving its physical and cyber security. Therefore, it should start first with holistic risk management approach by utilizing best practice frameworks, identifying of "mission critical systems," integrating cybersecurity risk assessment in early project design stage, integrating cybersecurity risk assessment into traditional process hazard analysis, then creating resilient architecture with redundancy and high visibility. Last and most importantly, train your people who are responsible for OT Cybersecurity by collaborating with vendors and trusted certification authority program.

To The Stars...

Securely

Chris MCDONALD, AUSTRALIA

The space industry is growing rapidly and with this growth, comes a larger threat profile and associated cyber security risks. It is important, particularly now with a large number of significant cyber breaches occurring and attracting worldwide media attention, to focus on embedding cyber security into your business from the get-go.

The space sector is heavily start up focused, and often cybersecurity is either not considered, or has its funding reallocated to quick win profit focused activities.

This is because often boards and investors want to see a quick return on investment, and to achieve this, organisations cut corners or take short cuts, with cyber security one of the first items to go. There are two main reasons this occurs, 1. Cybersecurity can be perceived as expensive, 2. There is a lack of understanding and skills in cyber within the business, and its importance.

However, getting cyber security right from the start, or even getting a certification such as ISO27001 has proven to contribute to profits for a number of organisations, in some instances even doubling or tripling revenue. A conversation I have regularly is, if you think cyber is expensive, wait until something happens because it wasn't prioritised.

Several key space initiatives are starting to gain momentum, with services being offered to multiple sectors including defence/government, transport, and emergency services. It is imperative as space technology begins to enable new services, particularly services that will support critical functions, for cybersecurity to be a priority.

Understandably, space technology, in particular satellites pose a different technology landscape for cyber security specialists, as it is something that is considered emerging or innovative, and with that, a lot of solutions need to be customised or tailored, but its not impossible, and its important. This is where security by design comes in.

I am looking forward to seeing how this industry continues to grow, and contributing to how we can secure critical space assets. The threat landscape changes completely when we start to think about space and how technology will enhance our services on earth, and enable our expansion and exploration into space.

Chris McDonald is currently a Director of Cyber Security, focusing on Space Technology, based out of Brisbane, Australia. Chris started his career in cyber security working in incident response and forensics, later moving into penetration testing and now strategy and GRC.

Chris has always had a passion for cyber security, and endeavours to bring technical knowledge of cyber to all levels of a business and be a voice and champion of cyber to boards. Now, Chris brings this knowledge to space technology companies, helping them secure critical assets, and enabling them to demonstrate to their customers that their technology is secure.

'Anthro-centric Security'

Lianne POTTER, ENGLAND, UK

As the Head of SecOps for the largest greenfield technology transformation project in Europe, Lianne Potter is building a leading-edge security team to meet the needs of a modern retail organisation, prioritising innovation, and aiming to create new standards in best practices. Lianne has delivered talks worldwide, sharing her vision for a new type of human-centric security function.

Drawing upon her expertise as a cyber-anthropologist (through her consultancy, The Anthrosecurist), and her practical experience as a security-focused software developer and as a security practitioner; Lianne combines the human and the technical aspects of security to evangelise a cultural security transformation.

The cybersecurity industry needs to hire more anthropologists. Why? Because cyber criminals are using what makes us human against us. They are already acting like anthropologists, psychologists, and behavioural scientists, and we should be too. Or at least hiring them!

Many organisations are talk about embedding a 'strong culture' at their workplace, do they know what it really means?

Culture is shared. Culture is learned. Culture is adaptive.

Culture arises out of our need for meaning, our desire to build for social forms, culture is about behaviours which are learned from those around us. Technology continues to change but the human element is the only constant. So if you want a new approach to security culture that works for your organisation to help you face new threats, then you might do well to consider hiring from the humanities (the clue is in the name) or social sciences. To build an intrinsic security culture however, we need to know what we are working with first.

We use terms like 'insider threat', 'least privilege' and 'zero trust' in relation to our colleagues. Not very endearing, is it? But when we do share information, our favourite ingredients are FUD - Fear, Uncertainty and Doubt. Now fear has been recognised as a motivator to influence a change in behaviour, but if that's all you are drawing upon, it can cease to be impactful. The very people we are trying to protect are fatigued by our interventions and it's causing them to switch off. Once we lose our ability to face threats as a collective, then we are weaker as a culture. Then when that early warning system is gone, something is going to go wrong somewhere.

So next time when you're looking for your next hire, remember that 95% of cybersecurity breaches are caused by human interventions.

We need to do better to create a culture that enables all of us to build up our resilience against these cyber threats. We must cater for a wide breadth of expertise, capabilities, experiences, cultural norms, along with equalities and disparities that frame these individuals. Think to yourself 'what decisions can I make to ensure we are building an anthro-centric security culture?

Why should the cybersecurity industry hire more anthropologists? Because when you follow the cables, behind every piece of tech is a person, consumer, creator, and even hacker, and we should never lose sight of this.

Light The Way

For The Next Generation Of Cybersecurity Professionals

Alexandra MERCZ, SINGAPORE

Precious stones go through tremendous pressure and heat in order to transform into polished gems. Young cybersecurity talents go through the same self-cultivation process to discover their unique potential, which is not without its hardships. In this refinement process, challenges generate resilience and develop inner fortitude in order to fulfil their purpose to make the world a better and safer place.

Being at the forefront of the cybersecurity industry comes with the natural responsibility to mentor and advance young talents, who will then become the leaders of tomorrow. In this sense, all experienced cybersecurity professionals are mentors, either through a defined and dedicated program, or by everyday interactions. Mentoring is the work of building bridges for the mentee, "human bridges" when it comes to connecting with people and "knowledge bridges" to connect the dots and help the mentee realize their potential.

A good cybersecurity mentor wears many hats. A role model who sets an example for the breadth and depth of achievements the mentee can consider pursuing; a trail-blazer who supports growth and innovation; a trusted guide and ally who serves as a source of knowledge and offers encouragement. A good mentor acts as a lighthouse that provides direction and shines light on possible pathways for the mentee.

When paving the way for the next generation, we must be considerate to the different needs of the multitude of diversity. This sensitivity provides a great ground for targeted support, taking into account one's values, gender, cultural, physical and neurodiversity.

It is a scientifically proven fact that diversity results in enhanced decision making, increased innovation and better business growth. With such a wide range of benefits, it is not a question anymore for businesses to create and maintain a diverse workforce, not only in junior levels but also in senior and board director roles.

Yet the cybersecurity industry still struggles finding the right balance and providing opportunities for a diverse workforce, including enhancing women representation in all levels of roles. Senior cybersecurity leadership needs to be the driving force to change this situation and to provide the development venues for the next cybersecurity generation.

An avid public speaker, renowned wide-reaching influencer and role model, Alexandra Mercz is the Cybersecurity Chief of Staff of Gojek and GoTo Financial, the largest technology group in Indonesia. In her career, Alexandra developed a strong track record in the global financial industry and held multiple senior positions at COO and CISO offices.

Recognized with the award of Singapore 100 Women in Tech, IFSEC Global Influencer in Security and Top Woman in Cybersecurity in Singapore and ASEAN, Alexandra is a leading voice being the Chapter Ambassador for ISC2 Singapore, and member of the European Women on Boards organization. Mrs Mercz plays an active role in achieving diversity in technology and cybersecurity worldwide.

Cybersecurity

Education and Training

Fortune E. ONWUZURUIKE, USA

Fortune E. Onwuzuruike is a Cybersecurity Program Manager at Microsoft and serves as the Career Development Lead for Blacks at Microsoft Atlanta Chapter. He is also a Part-Time College Professor and on the Industry Advisor Board at Georgia State University. A Doctoral Cybersecurity Candidate at Marymount University, Fortune has a successful track record of managing complex programs with the nation's largest companies around the cybersecurity domain. Lastly, Fortune is the manager of 'Tech Is The Wave', which feeds his passion for revolutionizing and uplifting the ecosystem of those who want to do more to advance their career, business, and themselves.

Cybersecurity is constantly evolving, and cybersecurity professionals gain expertise over time with practice. However, it is no secret that cyber threats are growing exponentially as the field lags behind due to the lack of skilled cybersecurity professionals. Reducing the gap starts with building professionals from the ground up. Being in the connected technology era, cybercriminals are getting more sophisticated and taking advantage of the cybersecurity field's talent gaps. Thus, every organization must ensure security is a top priority. Cybersecurity education and training are essential in the cybersecurity workforce. This provides students, recent graduates, and those interested in breaking into this space with information on finding the right path. Paths include formal education from universities and institutions that provide programs to better equip the student who desires to be a cybersecurity professional (e.g., bachelor's, master's and doctoral degrees) and cybersecurity training such as boot camps, certifications preps, and certificate programs.

As more cybersecurity programs are developed, it is paramount to ensure all domains within security are covered and taught correctly. Newly created cybersecurity programs now provide students with technical security skills, business strategies and processes knowledge, and a clear understanding of the governance, risk management, and regulatory compliance associated with cybersecurity. Cybersecurity programs teach students foundational skills to prepare them for the workforce. Students explore operating systems and focus on programming languages, software development, and various techniques and methods for testing computer system security. Students could also pursue management coursework to prepare for upper-level careers. Hands-on cybersecurity experience remains the primary factor in determining whether a candidate is considered for an open position. However, cybersecurity certification credentials are also a meaningful way to break into the field as hiring managers struggle to find potential candidates with a well-rounded body of work who have hands-on experience in the cybersecurity field. Cybersecurity certifications help increase candidates' expertise, and some employers view it as a must-have. The certification type depends on the role, as different positions require different skills. While this is necessary, it has also led to a gap in how cybersecurity roles compare across academia, government, healthcare, and the private sector. The US National Institute of Standards and Technology (NIST) and National Initiative for Cybersecurity Education (NICE) Framework helps close the cybersecurity gap by providing a common framework, a reference taxonomy for those individuals who carry out this type of work.

Cybersecurity

The Great Human Challenge

Antonio DELGADO ALONSO, SPAIN

The digitalization of our society has represented a fundamental change in our lifestyle, creating a hyperconnected, globalized and highly dependent world of telecommunications technologies. The increasing dependence on new technologies is accompanied by inherent threats called "cyberattacks", which can materialize in various forms: theft of money, leakage of sensitive information and even disruption of essential services such as electricity or water. We are all exposed to these attacks: from ordinary citizens to national governments, meaning that they can affect our social well-being and even the stability of our nations.

For all these reasons, cybersecurity is emerging as one of the pillars that will sustain modern societies as we know them today and will be one of the most sought-after professions in the labor market in the coming years. It will be as essential to society as law enforcement, medical or engineering services.

Companies and organizations will therefore need to design cybersecurity master plans and dedicated budgets, as well as technologies and personnel to support them. The figure of the CISO will be increasingly important in the boards of directors of all companies in the world, and their work will be as important as that of a CFO or a legal director. Cybersecurity training and awareness will be another aspect that will need to be covered both by major companies and SMEs, even by ordinary citizens, as this challenge must be transversal to the whole society and labor market.

After all the years that I have dedicated as cybersecurity professional, for which I am extremely grateful, I have been able to discover how the demand for cybersecurity projects and professionals has only grown and its market is more in need of talent than ever. We are living in a time of great opportunity for the cybersecurity industry and I am sure that the sun will shine brighter in the next few years.

Publications such as Top Cyber News MAGAZINE serve as a testimonial of the exponential growth of this vibrant sector and, above all, to demonstrate how cybersecurity talent crosses cultural and national borders.

The 40 under 40 initiative is a perfect example of the great international talent currently available in the cybersecurity market and how age is no barrier to excellence. In a market with a great need for professionals, knowing how to foster and attract young talent is essential. People must become their own bulwark against cyberthreats to ensure a safer digital world.

Antonio Delgado Alonso is a Cybersecurity Manager with more than 9 years of experience working in the main consulting firms: Capgemini, Deloitte and EY. He has been responsible for the development and implementation of multiple Cybersecurity projects for clients in the aerospace, financial, insurance, energy, automotive and public sectors, among others.

His main lines of work include the definition of strategic cybersecurity plans, supervision of security operations, regulatory compliance, technology risk management, managing business continuity and disaster recovery or promoting cybersecurity culture. He holds the following certifications: CISSP, CCSP, ISO 27001 and ISO 22301.

Raising Public Awareness

of The Importance of Cybersecurity

Mousam KHATRI, INDIA

Mousam Khatri is a Counsellor at Confederation of Indian Industry (CII). He is committed to empowering the Indian industry to secure their digital journey. He has a proven track record of leading and executing cyber security projects with multinational companies.

Mousam volunteers widely to increase cybersecurity awareness across the globe with a keen focus on India and he is the Founder of Cyber Safe Season. Mentor of WiCSP - Women in Cyber Security & Privacy and Member of CII Cyber Security Task Force. He holds a Master of Science degree in Cyber Law and Information Security from the National Law Institute University, Bhopal.

The development of digital technologies is growing at a fast pace. With the increasing use of digital technologies in society, cybercrimes have become a major concern. The Internet has come to be one of the integral elements of our day-to-day life. It has transformed the way we communicate, make friends, share updates, play games, and shop. They are impacting most elements of our everyday lifestyles. Cybercrimes are a growing problem globally that is vital for every individual to be aware of and to implement measures against them. It is more important than ever before to promote cybersecurity awareness. Cybersecurity awareness for the public is one of the most important things we can deliver in the fight against cybercrime and help protect their digital world.

As digital technologies continue to evolve and become used in most aspects of peoples' personal and professional lives. The adoption of digital payment applications in society has grown. UPI (Unified Payments Interface)-based transactions in India, have witnessed exponential growth both in volume and value terms post-pandemic, as well as an increase in the number of cybercrimes through illegal lending apps.

Cybercrimes against persons such as social engineering attacks, phishing, vishing, smishing, online payment fraud, online dating fraud, online job fraud, cyber extortion, cyberstalking, cyberbullying, cyber pornography, and identity theft are rising globally. Cybercriminals become more sophisticated all the time and often find new and improved ways to find vulnerabilities and weaknesses that they can exploit to get access to credentials, data, and money. Additionally, they look to exploit human behavior and emotions. When new threats emerge such as ransomware, it is important that we let society know about them as they occur.

Do not make cybersecurity awareness a one-time deal. Cybersecurity awareness must be a continuous activity for society through various platforms. To educate individuals and organizations about the role they play in improving cybersecurity and the steps they can take to be more secure in the digital world. We conduct cybersecurity awareness programs every week for our citizens for a secure world for everyone. Cybersecurity is a shared responsibility, which means every one of us must maintain proper cyber hygiene. There are many reasons why cybercrimes go unreported, however, the most basic motive is social stigma. Statistics of successful data breaches in recent years indicate that there is still room for improvement in cyber awareness.

Every nation must prioritize its focus on cyber security awareness for the online safety of its citizens for a secure world. To live securely within the online world, it is vital to comply with some cyber-safe practices.

Cybersecurity

‘Bottom-Up Leadership’

Cat CONTILLO, USA

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 (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.

The Asymmetric
Security Landscape

Henrik PARKKINEN, SWEDEN

Henrik Parkkinen is a security professional from Sweden with +20 years of career experience. He holds several highly ranked industry credentials, e.g. CISM, CRISC, CISA, CCSK.

Henrik has a broad and deep understanding of today's digital ecosystem, emerging technologies, security universe, and threat landscape. The knowledge he holds is a product of experience collected from both a defensive and offensive security perspective through technical hands-on assignments to management and leadership roles.

Henrik has experience from medium sized organizations to international enterprises spanning over the globe within multiple different industry verticals. He also shares his experience and knowledge through his website, www.HenrikParkkinen.com.

Our world is going through an evolutionary transformation. Societies, humans, and organizations have grown into a new substrate. Digital. The transformation is irreversible, the pace is faster than ever, and we are just at the beginning of this era. The pace will get even faster.

One of the reasons behind this prediction is that IoT, machine learning, quantum computing, AI, and other emerging technologies are still in their early evolutionary cycles. The real power of these capabilities and technologies is far from fully realized as progress and advancement are made every day. And the digital evolution, from a macro perspective, is still also in its early phases.

"Defending organizations have to defend against every kind of attack, while the attackers just need to identify one weakness to exploit."

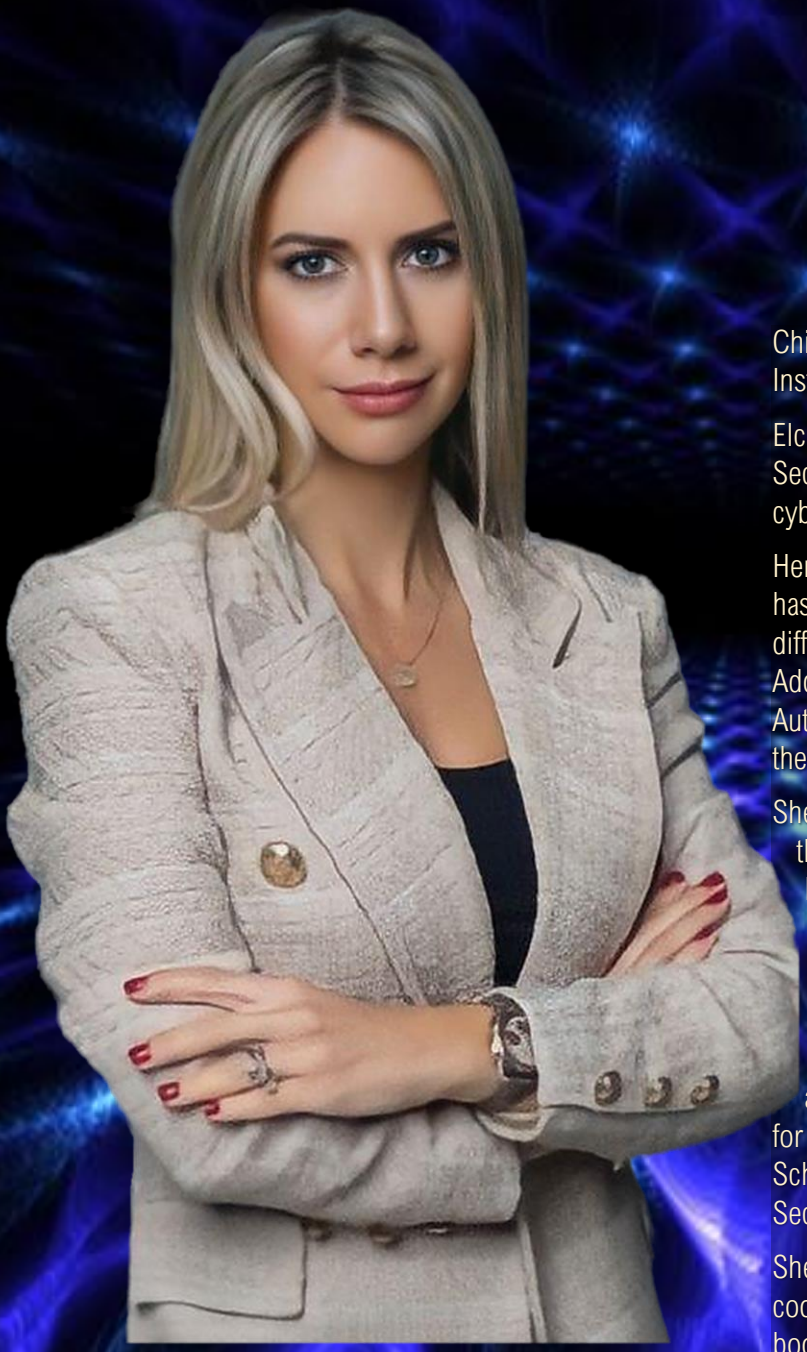
For an organization to stay resilient and protective, in today's digital landscape adequate security capabilities need to be established. Security is about three perspectives. Humans, Processes, and Technologies. The security posture of an organization is a composition built up from these three perspectives.

And it is not enough for an organization to only make sure security is providing resilience and protection to an organization. Security investments need to be aligned towards the organization's mission, vision, and objectives. Security does not exist in a vacuum. It is there to support the organization to reduce risks and increase success. To achieve this, security needs to be approached as a team sport. There is no one, not a single person within an organization that can make sure resilience and protection is created alone. This is something that everyone in the organization needs to pitch in to, all the way from the executive leaders to each individual employee.

I believe that together, since security is something involving and a concern for everyone, we need to help each other to achieve a more resilient digital ecosystem against cyber security threats and attacks. The security landscape is highly asymmetric, the attackers do not have the same requirements as defending organizations. They do not need to focus on generating business value, competitive edge, staying compliant towards regulations and so forth. The security game is something that we all, together, can help each other with. By sharing our experience and knowledge. The way forward is by doing it together and by helping each other. Security is a team sport.

She Leads Tech!

Elcin **BIREN**, SWITZERLAND



I'm passionate about protecting the world from hackers. But if you want to know my real dopamine hit, it's my involvement in our Women in Tech initiatives!

Chief Information Security Office UBS | Chair Swiss Cyber Institute | ISACA SheLeadsTech Ambassador

Elcin Biren is an Industrial Engineer specialized in Cyber Security. She has worked in distinctive roles across cybersecurity spectrum since 2006.

Her passion is to save the world through cyber security and has been working in at UBS Zurich Switzerland undertaking different global Cyber Security roles for over 7 years. Additionally to her main role at UBS, Elcin is an UBS CISO Authorized Speaker at conferences and webinars to increase the awareness about Cyber Security.

She is currently the Chairwoman of Banking and Finance at the Swiss Cyber Institute and IDC CISO Summit Board Member, SheLeadsTech Ambassador at ISACA, along with being the UBS Women in Technology Regional.

Lead for the Switzerland, and has volunteered in Global Cyber Communities where she focuses on the diversity topic to inspire young girls to enrol into this industry. She also had opportunity to be a guest speaker, adjunct faculty for various academic platforms such as "IMD Business School" where she talks about "Digital and Information Security Risk Management".

She loves travelling, hiking, surfing, snowboarding and cooking with her family. She is a bookworm, an amateur kids book writer about Cyber and Information Security Awareness, and she likes playing battery drums.

She is the Chairwoman of Women Working Groups at the Swiss Cyber Forum and SheLeadsTech Ambassador at ISACA, along with being the UBS Women in Technology External Stream Lead for the Swiss Region, and has volunteered in Global Cyber Communities where she focuses on the diversity topic to inspire young girls.

The Board's
Cyber Understanding

Alon NACHMANY, USA

Alon Nachmany is a cybersecurity expert currently working as the CISO and Principal Consultant at AZEN Consulting. His experience in leadership roles across industries from small start-ups to established enterprises and from both side of the Cyber Security table enables him to help bridge the gap between Cyber Security Vendors and Cyber Security Customers.

In the past Alon has served as the Director of IT and Information Security for WeWork, the CISO for National Securities Corporation and the Field CISO for AppViewX uniquely positioning him to understand and address the mounting security challenges of the modern-day enterprise.

The Board of Directors are individuals appointed by shareholders to a supervisory role, overseeing the company's activities and assessing performance. Their scope is supposed to be from a bird's eye view and ensure the long-term sustainability of the company. Being a director on a board comes with many responsibilities and duties, including Fiduciary Duty. That Fiduciary duty means that the directors must act in the best interests of the shareholders and the company, despite their personal interests. Much emphasis has been placed on the responsibility and accountability of the board when it comes to the company's financial health, but what about the cyber health of the company?

It's no secret that corporate boards are comprised of individuals who are often retired and join a board as a hobby. Often these board members are successful individuals from the financial sector or are individuals who specialized in the type of work the company does, such as scientists or doctors, leaving a gap in cyber security knowledge.

Many CISOs know the challenges of presenting to the board all the risks and how to counter them with technology or even giving a snapshot of the company's cyber health. Although most board members are extremely knowledgeable in finance and operations, they have little or no understanding of the ongoing and ever-changing requirements to secure a company's data, making explaining to the board about a breach often a painstaking experience.

One recommendation would be to present the risk figures in financial terms and explain how a solution can provide a positive ROI to mitigate the risk. Another would be mandatory cyber security education to help improve the board's cyber literacy and understand the importance of investing in data protection.

It is becoming clear that soon many boards will have to have a director with actual cyber experience and understanding. For companies to continue to grow and function in our ever-changing world, this requirement will help ensure a healthy future. This is similar to how it became mandatory for boards to have a basic understanding of a company's financial health. Once this requirement is fully set, accountability will follow. No longer will the excuse of "we didn't know better" be acceptable to shareholders or even judicial systems. We are already seeing the accountability of CISOs take place in the courts, and the buck will eventually stop with the board.

The Customer is King

Josh Darby MACLELLAN, CANADA

Josh Darby MacLellan is a Cyber Threat Intelligence specialist with experience in the financial, tech, and cybersecurity sectors. He currently works at Feedly as a Sr CTI Customer Success Manager. After his second Masters in Security and conflict, Josh started his career in physical threat intelligence before pivoting to cyber.

Josh enjoys contributing to the intelligence community and mentoring. He sits on the Board for the Threat Intelligence Exchange Roundtable and for CyberToronto, holding previous positions with (ISC)2 Toronto Chapter. Josh holds the CISSP and CCSP, and was awarded Canadian Security's Emerging Leader Award and IFSEC Global's One-to-Watch Award in 2020.

In recent years, there's been plenty banter about the millions Whether you realize it or not, if you're in Cyber Threat Intelligence (CTI), you're in the customer service industry.

When I first joined Feedly's CTI Customer Success team, a friend working for a cybersecurity vendor said welcome to the customer-facing side. But when I reflected on it, I realized I've been on the customer-facing side the entire time, just less consciously and with internal clients.

There is a lot of prestige with working in CTI that people like to indulge in. Sometimes, this leads us to resist the idea that we are in service to others, but we are. At its core, intelligence informs decision-makers so they can make better decisions; we are fundamentally hired to help people. We owe our jobs to revenue generated by the business and can't be employed without organizations to protect.

When I worked as a CTI Analyst for a Canadian bank, a shift in my mindset came when I stopped thinking of recipients of my intelligence products as stakeholders, but instead as customers. A stakeholder has an interest in your intelligence so should instinctively read your reports. Whereas you must win over a customer, build a relationship with them, provide a tailored service, and outcompete others for that customer's attention.

Anyone who knows me will know I enjoy a good conversation, often at great length. Simply put, coffee chats are essential for building relationships. One of the most effective ways to understand your customer is by making time to speak to them in a relaxed setting.

Many of us shy away from reaching out to strangers for a conversation, but it's a vital skillset that I recommend everyone practice. Find one person a week on LinkedIn who has a cool-sounding job and ask to learn more about their career over a virtual coffee. At the very least, you'll expand your knowledge of career paths, understand other people, and gain insights from their experiences.

If I can leave you with one final thought, it's that you can spend 10 hours producing the best intelligence report 2023 has seen, but if no one reads it, it's pointless. To increase the chance of people reading your work, get to know them, and treat them like a customer that you must win over. We are all in the customer service industry.

Preventing Privacy by Design
from Becoming a Privilege

Muneeb Imran SHAIKH, PAKISTAN

Privacy is a theme that has remained consistent throughout history across all human societies regardless of culture, religion, or ethnicities. It has been an area that is professed by religious scriptures and by the human intelligentsia.

However, with an increased transformation of societies alongside digital sphere, we are observing increased privacy risks caused by the overcollection and processing of personal data. The privacy subject matter experts have advocated the need to bake privacy into the design as a fundamental ingredient rather than dressing it up on an established product or service. However, organizations are still battling with the challenges to adequately embed privacy into the design aspects of the developed product or service.

The real issues creep up with the lack of substantial and objective controls to be implemented within product or service. The abstract nature of the privacy principles allows escape routes to the product or service designers to interpret these principles in their own manner and claim to have adequately baked privacy within their services or products.

In a quest to make personal data not linkable with reasonable efforts by the threat actors, it becomes necessary to alter the architecture by moving away from centralized service architectures to partially or fully decentralized service architecture. As we decentralize, there becomes an increased need for computational resources, human resources to manage additional service domains which ultimately adds to the overall product or service cost.

Such challenges impair the smaller organizations capabilities to commit themselves to privacy by design in their products or services. Additionally, organizations also rely on the off the shelf software and the underlying architecture in terms of database and applications is a completely black box to them and therefore the privacy risks cannot be adequately ascertained or addressed unless the products have been certified against international privacy standards. Currently we are collectively standing at crossroads where the abstract nature of controls and principles create cushion for threat actors to circumvent the privacy. There is therefore a dire need to add more nuance to the privacy controls which are verifiable and capable of being objectively assessed otherwise we may run into a territory where Privacy by Design may be reduced to a privilege.

Muneeb Imran Shaikh is an Information Security & Privacy Consultant with a forte in Strategy, Program development, Governance, risk, and compliance. Based in Middle East region, he has worked with different clients from financial, governmental and telecommunication sector to help them in developing and implementing Cybersecurity and Privacy program in accordance with their regulatory, legal and compliance requirements.

An avid reader with an eagerness to help people and networking with other energetic professionals who value diversity, inclusion and the importance of emotional intelligence in the work environment. Strong Proponent of creating healthy culture that values Stakeholder Engagement, Mutual Respect, and Emotional Intelligence.

He has contributed with his knowledge and expertise through various writings, podcasts, policy reviews, conference appearances. Some of his major contributions include Review of Pakistan's Cybersecurity policy 2021 and his two papers on cyber threat intelligence.

Driving Effective
Cyber Communication

Yehudah SUNSHINE, ISRAEL

Bringing together his diverse professional cyber know-how, intellectual fascination with history and culture, and eclectic academic background focusing on diplomacy and the cultures of Central Asia, Yehudah Sunshine keenly blends his deep understanding of the global tech ecosystem with a nuanced worldview of the underlying socio-economic and political forces which drive policy and impact innovation in the cyber sectors.

Yehudah's current work focuses on how to create and enhance marketing strategies and cyber-driven thought leadership for Cyfleuncer, the cybersecurity thought-leadership platform. Sunshine has written and researched extensively within cybersecurity, the service sectors, international criminal accountability, Israel's economy, diplomatic inroads, innovation, and technology, as well as Chinese economic policy.

Effective communication is the cornerstone of meaningful conversations and the prerequisite when conveying complex ideas to non-technical audiences. In an era of infinite distractions and even greater cyber risks, today's security leaders must use their voice and humor, wit, and ability to connect with a broad spectrum of individuals to make any sustainable impact on cyber hygiene and approach to cyber threats.

What drives conversations that keep people thinking?

Is it a strategy of how you intend to convey a pressure point or maybe it's an understanding of your audience? In truth, effective technical communicators have the desire to bring clarity specifically to their audience, break down the consistent points of confusion into simple terms and avoid sales or marketing-driven language which often leaves the reader without any real value for their hard-earned time.

In cybersecurity, the shortage of effective communicators has left many with the impression that the risks and applicable solutions are just too technical or difficult for them to execute. Fortunately, with a few strategic adjustments, security leaders can alter the trajectory of their language and make more impact on their peer's approach to cyber risk management.

Effective cyber communication entails:

Minimize jargon. While the technical specificity of an attack, risk vector, or product might provide some value, for many the complexity of technical language induces fear. The solution lies in blending an understanding of pressure points and the value of technical solutions while not overly focusing on the technical nuances or endless data points.

Think Big Picture. While the minutia might get your audience to the problem at hand, more often than not they are looking for direct value or an understanding of how the solution at hand will help them manage a strategic risk on the near horizon. Effective cyber communicators can frame technologies and risk areas with clear problems and solutions without being bogged down with too much of the process or an overly technical discourse.

Know your audience. Effective communication is never about the speaker and should be entirely focused on the partner on the other side of the table. If you intend to give over technical problems or complex solutions, the key is the understand who your speaking to. What their risk profile is, their level of technical expertise, and their role in the implantation hierarchy. By investing in understanding your audience, your message can be razor focused and hyper-effective.

Human Factors Of
Cyber Security

Shira RUBINOFF, USA

When it comes to cybersecurity, Humans Are The Problem and the Solution. Human factors and cybersecurity go hand-in-hand. First, to be cyber-secure, the elements of security technology must be addressed. While you're executing this monumental task, remember that human factors have to be a fundamental consideration in formulating your protocol. How humans are approached when implementing security compliance will ultimately determine the level of security within a given organization.

The human is the weakest link in the cybersecurity chain; Make them part of the solution, not the problem. I believe this is the most powerful sentence to consider when thinking about the overall cybersecurity of an organization. The human is always the weakest link in the security chain on both ends. While security is built to protect humans, humans build security and humans break down security. Therefore, humans are the common thread and are always the centerpiece of both the security problem and the solution.

Given that there are humans involved in every step of the way, an organization can decide to take the view that humans are the problem and govern from that perspective. Alternatively, they can flip their vantage point and take the position that humans are the solution. With that in mind, they can implement proper cyber hygiene in the organization, while simultaneously unifying their team, as humans take center-stage as the solution.

Making humans the linchpin of your solutions to security issues in your organization will empower your employees. It will also help lay the groundwork for a loyal and cohesive workforce that is bound together and working in concert toward ensuring your company is secure from the inside out.

Following this philosophy you'll be much more likely to create an environment with proper cyber hygiene, which is crucial in today's ever more dangerous world.

Cyber hygiene will be pivotal in curtailing threats from all four vectors: the oblivious insider threat, the negligent insider threat, the malicious insider threat, and the professional insider threat. Additionally, you'll also create a culture of buy-in where employees form a cohesive, dedicated and loyal collective. With this mindset, they'll be much more likely to deliver effective security that solidifies the organization's cyber safety every day.

Shira Rubinoff is a recognized Cybersecurity Executive, Advisor, Global Keynote Speaker, Influencer and Author, who has built two Cybersecurity product companies, and both incepted and led multiple Women-in-Technology initiatives. She is a sought-after International Global Keynote Speaker and Presenter, and Expert Media Commentator on topics surrounding The Human Factors of Technology & Cybersecurity who has also been Calculated by leading industry analysts to be the Top Female Cybersecurity Influencer Globally on social media.

Ms. Rubinoff provides guidance to numerous Fortune 100 companies in areas related to cybersecurity and company thought leadership and consults to various organizations in areas of business development and organizational dynamics.

“Crime-as-a-Service” CaaS

Pooja SHIMPI, SINGAPORE

Pooja Shimpi, a passionate Information & Cybersecurity expert in leading projects and strategies at reputed international banks believes in doing things differently. She wears multiple hats across several domains of Information Security and Technology Governance, Risks & Compliance (GRC).

She has inspired many aspirants globally to join the world of Cybersecurity by leading “Global Mentoring for Cybersecurity” and “Protégé for Cybersecurity” programs. Her interviews & articles are published in reputed magazines and she actively participates as a speaker on ongoing topics in Cybersecurity. She holds a Master’s degree in Computer Science including prestigious certifications such as CISSP & Certified Data Steward.

Looking back at 2022, it was a year of many firsts. Working remotely became a norm for many organizations around the world. In fact, most of the top firms globally stopped adding office infrastructure to cater to the new norm. Geopolitical instability and conflicts grabbed headlines on news channels. Towards the end of 2022, economic headwinds started blowing in the direction of a global recession. To top it all, cybersecurity space reported a record number of ransomware attacks.

So, what will be the top trend for Cybersecurity in 2023?

With the access to internet almost everywhere in the world, it is no longer a surprise to see the gaining popularity of CaaS i.e. Crime-as-a-Service!

Yes, CaaS has become as simple as booking a cab or ordering pizza. Cyber criminals are taking advantage of every new capability for their growth & success. CaaS is basically, offering a readymade user-friendly product such as phishing kits, malware, DDoS attack, command & control infrastructures, etc. for launching attacks with few steps and clicks. These reasonable, easy to use and simple products are attracting and enabling new & novice threat actors. The overall CaaS model is turning out to be very dangerous and also challenging from law enforcement perspective.

Cybercrime is one of the most profitable forms of crime and it’s affecting almost ~1 million people every day! Data is the new commodity & critical data is more precious than gold & diamonds. Cybercrime is for here to stay and will only rise in the future. Having a defense strategy and system in place is the need of the hour.

How do we tackle cybercrime challenges?

Fortunately, many countries are taking the lead and establishing various cybersecurity related initiatives and programs. Without a strong cybersecurity program, it is nearly impossible for an organization to keep up with all the changes from intensifying complex threats and risks every day. To build an effective cybersecurity framework requires a multi-layered approach, that includes implementing controls based on three main pillars: people, processes and technology (PPT) with a strong synergy & collaboration amongst these pillars.

For cybersecurity related topics and knowledge, I strongly recommend reading **Top Cyber News Magazine 2022**, where many veteran Cybersecurity leaders shared their knowledge and provided valuable insights.

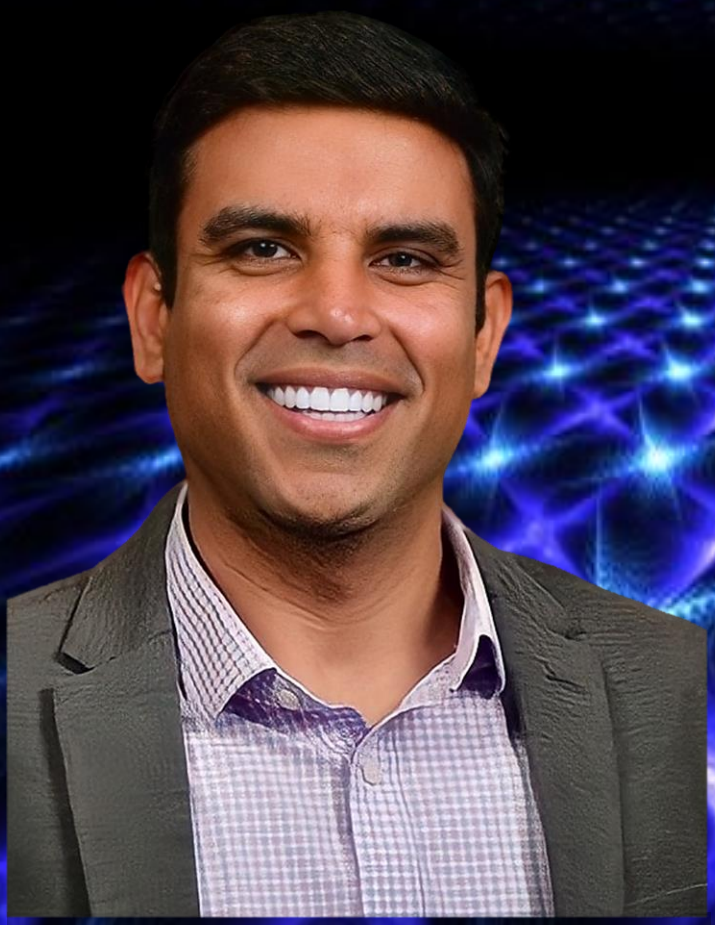
Cybersecurity is everybody’s responsibility and everyone should play their part effectively.

Converged IAM

The Future of Identity

Kapil BAREJA, USA

Kapil Bareja is a Global Technology Leader as part of the Digital and Governance capability at Saviynt. Advises multiple security startups on Product Strategy, Alliances and Integrations and Sits on multiple Customer Advisory Boards helping to improving digital and cybersecurity risk oversight. As a professional, he has advised, managed and delivered projects related to innovation, enterprise resiliency and Cloud security programs including controls, enterprise-wide assessments and audits, policy and technology reviews, documentation and workflow/process creation, architecture and implementation, technology review, and organizational cost savings.



Kapil is serving as co-chair with DevSecOps working group with Cloud Security Alliance, Strategic Chair for Multi-Cloud working group at Advanced Technology Academic Research Center and author, his works have been published in industry leading and award-winning publications, including International Security Journal, Harvard Business Review, International Association of Privacy Professionals, Security Intelligence and many high audience blogs.

Converged IAM can be defined as an IAM solution that brings all the different dimensions of identity and access management into a single platform. Access Management, Identity Governance and Administration, Privileged Access Management, and in some cases even CIAM, all converging in a single solution and is touted to be the future of enterprise security infrastructure.

Most of the leading players in the IAM industry have been strong in only one dimension of IAM and customers always had to purchase an Access Management solution from one vendor, and an IGA solution from another, maybe an add on PAM too. What if there was a need for risk analytics? Maybe another set of solutions.

This fragmented approach left customers with-

- Large bills
- Long implementation cycles
- Complicated vendor management.
- No common ground to manage the data of identities from these various solutions

The solution to this predicament – Converged IAM

Converged Identity and Access Management is an IAM solution that is equipped with the functionalities that can enable organizations to be secure and productive without exhausting their resources in managing the solution itself.

Converged IAM is indeed the future of IAM. It's only a matter of realizing this importance and educating stakeholders to ensure organizations are better equipped to handle today's sophisticated threat landscape. Forward-thinking CISOs and CSOs are now looking more broadly at security and how to not only mitigate risk but also how they can make their departments more efficient. These leaders are looking at how they connect the IAM solution to other parts of the organization such as physical access control as a more centralized process as well as ensuring that there is a single record of truth on individual access. These CISOs expect access control solutions to integrate their IAM solutions with their physical credentialing and access control. Ultimately, by doing this, their teams save time and effort, by utilizing a single source of truth for access (physical and virtual), automatically eliminating access upon offboarding. The adoption of risk-based IAM will not be easy or quick. For most companies, it will be a transformative, multi-year journey. But in today's IT landscape, identity and risk can no longer be considered autonomous of each other. There is no greater example of that synergy than the risks that are being exposed every day by organizations that have been breached because of their failure to effectively manage non-employee access.

Back to the Future

CISO Outlook in 2023

Malini RAO, INDIA

Malini Rao is a proven cybersecurity leader with 2 decades of global experience in cybersecurity industry.

Malini Rao is a CISSP, CISM, CCISO, CCSK certified security professional and an international speaker. Malini is currently with Wipro Technologies as Global Head of Cyber Defense, Engineering, Data Protection & Investigations.

Malini brings in extensive global experience and expertise while she has been working with Fortune 500 clients in various areas of cybersecurity with key focus on Cyber security engineering, operations, cyber defense, application security, infrastructure security, cloud/digital security, DevSecOps, Identity & Access Management, Governance Risk & Compliance, Cyber risk management, IOT Security, AI/ML Innovations in cyber security and access management. Ms. Rao has won many awards and recognitions for her contributions to the cybersecurity industry. Malini is also a Women in Cybersecurity, Inclusion & Diversity influencer.

Let's look at what will continue in 2023 and what we can expect as increasing trend in 2023 which CISO's need to focus upon.

Ransomware attacks & Protection will continue to increase in 2023, threat actors will divulge into seemingly legitimate phishing attacks, lateral movement. CISO's need to focus on updating their playbooks, MITRE attack frameworks, threat intel use cases.

Educating everyone about security, security awareness as culture in your organization — no matter their role or job title — is critical to operating securely. This includes everyone from software developers to customer representatives to the C-suite.

Automation across cybersecurity will increase, Automation helps focus on solving high-value problems for enterprises as well as their customers. Technologies like automated reasoning, risk monitoring, risk remediation, automated playbooks, anomaly detection and machine learning/deep learning not only save time but can also quickly surface unknown security risks to help organizations better protect their data, infrastructure, applications, and customers environment. As ransomware and automated attacks increases, AI/ML has a huge potential in the cyber defense area specifically into threat intel, anomaly detection, finding and stopping the attackers quickly, before they can achieve their motive or objectives.

Getting visibility into the cloud security posture, investments in cloud security controls and its implementation will see a increasing trend as most the organizations move their data and/or infrastructure to the cloud (Public/Private/Hybrid). As digital transformation implementation continues, getting visibility into cloud security posture has become critical.

Data Security/Data Protection & Privacy investments will see an increasing trend as the work from home and hybrid work environment continues to evolve and remain in 2023 as well. Data is the new oil and data security controls such as encryption of data in the cloud, Data leakage prevention solutions for cloud, Cloud access security broker, cloud security posture management solutions investments will increase

Increase in spends in zero trust architecture and controls over the next 12 months. As per the recent survey by cloud security alliance 77% of C-Suite executives are increasing their spend on Zero Trust over the next 12 months and 94% are already in process of implementing zero trust architecture in their organization.

Cybersecurity
and Digital Gold

Samuel NG, HONG KONG

Passion fuelled cybersecurity professional with leadership trained by Armed Forces, Capt. (R) Samuel Ng has extensive experience in all cybersecurity domains from both technical and management perspective with executive presence working alongside senior management in various corporate industries, government & military sectors.

He brought value to organisations by orientating governance, controls, risks and business strategies ultimately upholding the CIA Triad (Confidentiality, Integrity, Availability) at highest standards to risk appetite accordingly. As a Malaysian Army veteran with master's degree and multiple infosec-recognised certifications, he is now contributing to various sectors in Hong Kong including: banking and financial industries, cloud, IT infrastructures, virtual banks, crypto, digital assets, R&D etc.

While paper-currencies are slowly being phased out, future monetary value is likely to lie in cryptocurrencies and digital assets with decentralizing technology to promote trust system. That's also where future organized crime is heading predictively. Cybercrime will not be only geeks under the basement anymore. Undeniably the blockchain do have its own problems keeping pace with rapid-evolving quantum computers. Recent research shows a 1.9 billion qubits quantum computer could possibly crack the encryption safeguarding Bitcoin roughly within 10 minutes.

This sounds like a Y2K event-like catastrophe. Fortunately for the defenders, it's still many years away before deployment of quantum computers with these capabilities. Blockchain developers is on the high ground at the moment to defend against these known threats by increasing number of digits in cryptographic keys to safeguard the chain, fending off brute force attacks for the foreseeable future, but the crystal ball tells us it's a fallacy to believe that zero-day attack won't likely ever exist. With rapid evolution in cryptocurrencies globally, comes associated risks. As the security cat & mouse game will never end as we all know it, we are constantly required to be vigilant while juggling between cyber risks & business priorities. Managing cybersecurity risks & frauds from technical & management level varies significantly from one industry to another.

These are some common cybersecurity risks associated with specific crypto industries you are involved in or investing in.

1. Cyber-attacks towards Unregulated Cryptocurrency Exchanges
2. Scammers Piggybacking regulated crypto trading platform targeting users
3. Mobile Application Impersonation
4. Impersonating Law Enforcements & Legal Bodies targeting crypto firm
5. Fake Websites/Social Media, Phishing Domains

Fraud tactics can be similar occasionally, but techniques used are diverse. From the examples above and our experience dealing with them, we know that the fundamental elements of malicious effort typically exploits:

1. Sense of Urgency
2. Sense of Fear
3. Greed

Ultimately if it's too good to be true, it probably is! Or If we don't pay for a product, we are the product! These 2 "configurations" are probably the best "hardening" deployment for your "Human Firewall" in your organization.

Cyber Security Trends

That Needs Great Focus in 2023

Sourish DATTA, AUSTRALIA

Sourish Datta is a strategic, result-oriented Security & Risk Management leader with almost two decades of global experience in leading security transformation for organizations.

Mr. Datta has a proven track record of leading cybersecurity resilience strategy, security service delivery and security architecture for organizations aimed to deliver best-in-breed security capabilities to protect against adversaries. Sourish specializes in setting enterprise security vision which has a demonstrable result of improving the ROI besides driving value & consistency of security outcomes across the business domains.

Sourish is also entrusted by organizations to lead governance, compliance and audit programs which includes working with industry & government regulatory bodies to inform them about the organization's adoption of regulatory requirements, obligations, risk posture and remediation / maturity uplift roadmap besides periodically reporting on any breaches, risks, and incidents on critical infrastructure.

Organizations are struggling to be as good as the emboldened adversaries in the cyber space who have access to seemingly endless intelligence, compute power and tools, sometimes along with state sponsorship.

The threat that organizations face is not only limited to their systems and data; they extend to the value of their brand and trusted relationships in marketplace.

In recent years we have seen the topic of cyber security move from being a technology problem to the board room and hence here's a look at some of the key cyber security trends for organizations and the board members to focus in 2023:

- IoT devices possess a new cybersecurity threat paradigm
- Adoption of Zero trust is a must for organisations
- Edge computing and data at the edge presents a new threat
- Couple Biometric Authentication with Continuous Contextualized Authentication
- Quantum computing threats are looming large
- Secure Access Service Edge (SASE) is emerging
- 5G led data breaches is becoming a reality
- Focus on Nation state actors targeting critical infrastructure
- Cognitive Artificial Intelligence (CAI) to play a prominent role in cybersecurity
- Cloud security needs more attention
- Threat Intel Sharing is necessary for contextualisation
- Build a Robust Incident Response capability
- Security of remote workforce is at the focal point post pandemic
- Build a strong security-aware culture
- Cyber Insurance needs to be done right with Annual Loss Expectancy (ALE) considerations

While we focus on security trends, it is also important to maintain basic security hygiene. There is no silver bullet solution with cyber security, a layered defence is the only defence to protect data and critical infrastructure. As cybersecurity leaders, we also have to influence building a strong security culture and ensure that the business and its people be a part of that culture.

Cybersecurity In 2040!

Hafiz SHEIKH ADNAN AHMED, AUSTRALIA

Cybercrime is on the rise. With the advent of quantum computers, drones, the IoT, and AI, humans might not even be needed to perpetrate it. It is believed cybercrime could end up costing billions of dollars of damage, which only stresses the need for stronger security systems and better education to those connected to the internet. It also stresses the need for consequences for hackers who create security breaches.

Currently, most cyber-attacks are easily avoided by taking preventive measures such as: not clicking on unknown links, using anti-virus, keeping software up to date, not visiting suspicious or illegal websites etc. but this is not the case anymore.

The rise of Quantum Computers and AI have enabled to perform brute force calculations much faster than modern computers. This implies that quantum computers can break into modern security systems and thus threaten the entire cyber world.

Future AIs may not be dependent on any machine and if one such system was powerful enough it may use hundreds of machines to act as redundant systems so that shutting down one machine does not stop the AI from working and making the AI harder to track.

Another area that is even more dangerous is the IoT (Internet of Things). Drones and robotic vehicles are becoming increasingly common. The world is approaching to remotely controlled drones that could be used as explosive delivery systems. The chances are there will be ways for a hacker to gain control of such a device and they could decide to turn the robot around and do real damage.

So, the question is where would Cybersecurity be in 2040? The answer lies in flipping the side of the coin. If a device can be made to hack systems more easily, then such systems can be used to create more effective security measures. We may find that once quantum computers become a consumer reality, most devices connected to the internet will need to contain a quantum security chip.

Governments are already working on legislations regarding the creation of learning AI systems and their uses. It is most likely that AI systems will rely on large computer systems and so the average home user may not have the means to develop such a system. It will likely come down to the ever-developing cyber security industry to help build safeguards for the everyday people whose lives are increasingly tied to the internet.

Hafiz Sheikh Adnan Ahmed is an analytical thinker, writer, certified trainer, global mentor, and advisor with proven leadership and organizational skills in information and communications technology (ICT) governance, Information and Cybersecurity, business continuity and organizational resilience, data privacy and protection, risk management, enterprise excellence and innovation, and digital and strategic transformation. He is a certified data protection officer and won chief information security officer (CISO) of the Year awards in 2021 and 2022. He is the Co-Founder and CIO of AZAAN Cybertech Consulting.

To know more about AZAAN Cybertech consulting, log on to: https://azaan.net.au Hafiz can be contacted through email at hafiz.ahmed@azaanbiservices.com

TOP CYBER NEWS MAGAZINE

2022 SPECIAL EDITION

INDIVIDUAL CYBER SECURITY PROFESSIONALS - OUTSTANDING PERFORMERS IN THE FIELD OF CYBERSECURITY AND DIGITAL INDUSTRIES - TALENTED EXPERTS FROM ALL CONTINENTS, WORKING FOR A SAFER AND RESILIENT DIGITAL FUTURE

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, USA

«Thank you for making us all a true global Cyber Community! Our Cyber Community, as exemplified in Top Cyber News MAGAZINE is the ENVY of all other industries! We celebrate each other, and do so across continents and language barriers. Today we celebrate Top Cyber News MAGAZINE, Ludmila Morozova-Buss!»

Dr. Diane M JANOSEK, JD, CISSP, LPEC, Deputy Director of Compliance at National Security Agency, USA

AN AWARD-WINNING DIGITAL MAGAZINE

ABOUT PEOPLE, BY PEOPLE, FOR PEOPLE

Ludmila Morozova-Buss

Editor-In-Chief

Doctoral Student at

Capitol Technology University