

TOP CYBER NEWS MAGAZINE

About people, by people, for people

NOVEMBER 2022

Pooja SHIMPI

VICE PRESIDENT, REGIONAL INFORMATION
SECURITY OFFICER APAC at Citi

A CYBER SMART
NATION
SINGAPORE



Securing the Smart Nation

Exclusive article by

Edward MILLINGTON

Founder and Managing Director of CariSec Global Inc.

HOW POOJA SHIMPI, A PASSIONATE INFORMATION & CYBERSECURITY EXPERT LEADS THE TEAMS AND STRATEGIES AT REPUTED INTERNATIONAL BANKS. HOW SHE HAS ESTABLISHED AND LEADS THE GLOBAL MENTORING FOR CYBERSECURITY (GMFC) AND PROTÉGÉ FOR CYBERSECURITY

Foreword

An increasingly digital world is no longer an abstract concept; it is a reality. A great example of a digital society coming to life is the Smart Nation – Singapore. In our November cover story, Pooja Shimpi of the Citi demonstrates what is possible when all pillars of society work together for a common goal; how the Singapore government protects the data and safeguards the system. She talks about Singapore as a shining example how an enterprise, a government, a nation must strive to synchronize its digital transformation strategy with a cybersecurity strategy.

A panel of international experts contributes each month their valuable opinions to help shape the content for your Top Cyber News MAGAZINE edition's major theme: Treasa Dovander, Chris Kubecka, Scott Schober, Dr. Ofer Alon, Mr. Daniel Ehrenreich, Edward Millington, Christian Scott, Travis DeForge and Luc Chrétien.

Rather than spending months and years finding genuine cybersecurity talent, read the Top Cyber News MAGAZINE. This is where knowledge is shared, trust is built, equity is realized, diversity is celebrated, and inclusion is valued.

2022 European 'Woman in Cyber' Trophy in Cybersecurity Supporting Professions Awardee

Ludmila Morozova-Buss, Top Cyber News MAGAZINE



European Cyber Women Day

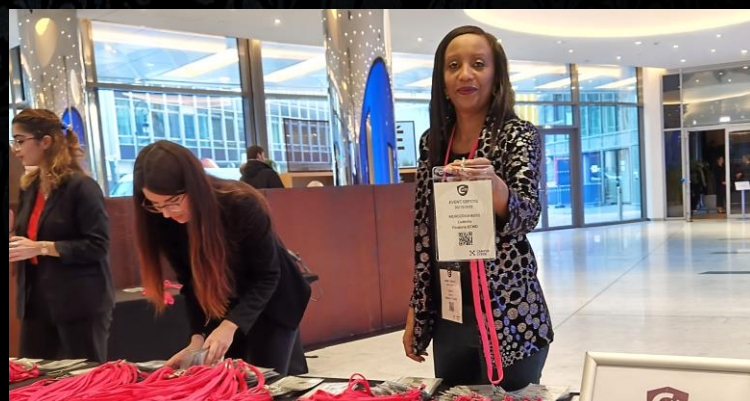
October 20, 2022 - Paris - France



CEFCYS

Cercle des Femmes de la CyberSécurité

Dr. Nacira Guerroudji-Salvan
Fondatrice et Présidente du CEFCYS



European Women in Cyber Trophy Winners 2022

Paris - France



Brunessen Bertrand
Jury's favorite



Anabelle Masclet
Nuno Filipe Award
CEFCYS's favorite



Dr. Hakima Kadri Dahmani
Professional in Cybersecurity France



Capitaine De Corvette Louise Leroy
Cyber Defense and Security France



Delphine Streichenberger
Cyber Supporting Professions France



Clémentine Maurice
Researcher in Cybersecurity France



Valéria Santamato
France Woman Cyber hope



Cristiana Santos
Researcher in Cybersecurity Europe



Lou-Anne Ducos
Student in Cybersecurity France



Livia Tibirna
Europe Woman Cyber hope



Wiem Tounsi
Professional in Cybersecurity Europe



Charlotte Couallier
Leader or CEO in Cybersecurity France



Phedra Clouner
Leader or CEO in Cybersecurity Europe



Ludmila Morozova-Buss
Cybersecurity Supporting Professions Europe



On US National STEM Day

Representation Matters

Editorial by **Treasa Dovander**, Ericsson Digital Services, Stockholm, Sweden

"It can't be done" – this is a sure-fire way to get me going. I'm Treasa, and I love creating, problem-solving and building.

Today scrolling through LinkedIn, I came across three different stories that got me thinking about the actual level of advancement of women's involvement in politics, industry, science, technology and engineering. Because my concern is if we are not sitting at the table, who represents our voices, perspectives and insights?

1. COP27: On today's major international forum the COP27 ("United Nations Climate Change Conference of the Parties") event where the world's leadership are on stage taking a picture for prosperity it was shocking to see a sea of suits and ties. Male leaders. At a location where life-altering decisions for the future sustainability of our planet is being made – global decisions that will impact the world's people, industries and society at large - women are sadly under-represented.

2. Crash-test dummies: Reports show that women are more likely to die in a car crash as crash-test dummies since the beginning of crash-testing dummies have always been fashioned after the male anatomy. Today, the first female crash test dummy is in use to help car manufacturers better support women if faced with a driving accident. It's a testament I think that technology and engineering are primarily male-dominated careers and thus the role-modelling of crash test dummies was lopsided. Guess who is leading the research into this area? Correct a female - **Dr. Astrid Linder**

3. Meanwhile, yesterday, **Marie Skłodowska-Curie, the first woman to win the #NobelPrize twice**, was born November 7 in 1876. She remains the only individual to receive the prize in two different science categories. Even though it's 155 years ago, she still serves as an important

reminder that even today the world needs more women in science and technology - not only that she serves to remind us that in 2022, we are still under-represented in senior roles still in politics, in business and in many industries.

So it's not lost on me that today, November 8 is considered National #STEM Day in the US, a time to appreciate the value of careers in science, technology, engineering and mathematics.

Because without diversity - how much unknown talent, perspective, insights and life-altering inventions lie untapped that have the possibility to fundamentally re-shape society, build in new insights and perspectives that might just be life saving for us?



Treasa Dovander is currently Head of Executive Communications and Influencer Marketing at Ericsson for a business area. She is passionate about advancing the role of women in STEM so that women are being recognized for their contributions in the sciences. A former journalist she is keen to highlight why representation matters.

by Chris Kubecka - A Prominent Keynote Speaker at CyberTech New York!

We are surrounded by billions of Internet connected tech. The digital world has permeated our homes, workplaces, public spaces. Winning hearts and minds, forcing change good or bad in our society. We might not be cyborgs, yet. But we depend on bits and bytes for our global economy and survival. Clean water, manufacturing, electricity, railway systems, maritime, aviation and space are almost all digital and much of connected to the internet.

With the embrace of this digital world, there has understandably been a darker side. Crime syndicates have turned various internet frauds and internet of things malicious bots into billions in illicit gains. In 2021, digital theft is now more common than physical theft. The growth of IOT has outstripped the supply of existing cybersecurity professionals. There are little to no regulations on the safety and security of IOT devices, allowing our own technology to be used against us in various cyber grift.

What can be done to turn the tide? Many of the various cybercrimes we don't hear about occur on a smaller scale and not considered newsworthy. Small businesses and NGO's who cannot afford full time tech departments much less basic cyber security are at most risk. They are the backbone of most economies or form part of a social safety net for those in immediate need. Focusing on those easily targeted by both cyber professionals and those trying to gain real world experience in the field can benefit from helping, especially NGO's. The picture doesn't have to be bleak when we consider our digital future and the burden on uncontrolled risk. We as technologists can take a village perspective to provide assistance and give back to our own communities, making them stringer for everyone.



CYBERTECH NEW YORK

November 15-16, 2022

The Javits Convention Center // New York



Speakers of CyberTech NYC 2022

<https://nyc.cybertechconference.com/speakers>



POOJA SHIMPI, SINGAPORE

Pooja Shimpi, a passionate Information & Cybersecurity expert in leading projects and strategies at reputed international banks believes in doing things differently. Curious by nature, she is raring to take on new projects that are outside of her comfort zone. She wears multiple hats across several domains of Information Security and Technology Governance, Risks & Compliance (GRC), and emerging technologies such as Blockchain and IoT.

She has inspired many aspirants globally to join & grow in the world of Cybersecurity by designing and leading **“Global Mentoring for Cybersecurity (GMFC)”** and **“Protégé for Cybersecurity”** programs in 2022. Her interviews & articles are published in reputed magazines/forums and she actively participates as a speaker on ongoing topics in Cybersecurity. She holds a Master’s degree in Computer Science along with prestigious certifications such as CISSP (Certified Information Security System Professional), Certified Data Steward (MDM, Data Quality, Stewardship Core), ITIL v3 and COBIT.



TOP CYBER NEWS MAGAZINE

About people, by people, for people

NOVEMBER 2022

Pooja SHIMPI
VICE PRESIDENT, REGIONAL INFORMATION
SECURITY OFFICER APAC at Citi

**A CYBER SMART
NATION
SINGAPORE**

HOW POOJA SHIMPI, A PASSIONATE INFORMATION & CYBERSECURITY EXPERT LEADS Citi
BANKS, HOW SHE HAS ESTABLISHED AND LEADS THE GLOBAL MENTORING PROGRAM



Securing the
Edward

TO INTERNATIONAL
CYBERSECURITY

“PROTÉGÉ FOR WOMEN IN CYBERSECURITY”

by Pooja SHIMPI

“Everybody Needs Somebody!”

Global Mentoring for Cybersecurity Program

Mentoring is one of the most important things a person can do, to enhance their career and professional life. It takes time and commitment, but it is well worth the effort. Whether you are the mentor or the mentee, it's a win-win for both. The opportunity to be both a mentor and a mentee, provides an invaluable retro and forward perspective experience.

The world of cybersecurity is on the move, and with the start of 2022 it's moving faster than ever. Cyber criminals are getting progressively sophisticated in their cyber-attacks, making it imperative for organizations to beef up their defences. Needless to state, there is a supply-demand gap in terms of the need for cybersecurity professionals, to the tune of approximately 2.7 million worldwide.

Many countries and organizations have a roadmap to increase skilled staffing but is it enough? It's been proven that gender diversity in any field results in higher productivity and better profits. While the number of women is gradually increasing in this niche space of Information Security, are we firing up all cylinders to encourage more women to join the cybersecurity work force?

Do you have any self – doubts, such as:

“How can I get into cybersecurity?” “What can I do to make the internet a safer place?”

“Why can't I have a career in cybersecurity?”

“When would be the right time to enter cybersecurity?”

If these thoughts ever crossed your mind, you are not alone!

Many individuals, think of this and are missing a great opportunity to join the cybersecurity field. The **Global Mentorship for Cybersecurity (GMFC)** program is established by Pooja Shimpi in partnership with Cyber Risk Meetup group in February 2022 with the **mission** to bring together highly skilled cybersecurity professionals from diverse background as mentors, along with individual enthusiasts (as mentees) who want to join / grow in the cybersecurity field, from all over the world.

This is a 6 weeks guided program and there is no fee to participate in the program for any participants. The efforts are in place to establish a strong mentor-mentee partnership with a goal to uplift and guide the mentees to meet their cybersecurity related goals. **The overall aim of this program is to help bridge the gap of cybersecurity workforce talent.**

We have received an overwhelming response, and with laser-focused diversity & inclusion approach we have successfully enrolled 39 individuals in our 1st GMFC cohort, The participants are from 9 countries and 19 different cities with a whopping 51% women representation.

Out of total 20 women who are participating, 13 are mentees and 7 mentors. Most of the mentees are freshers or experienced professionals with no or few months/years of experience in Cybersecurity field. All the mentors are united by one common goal, i.e., to share knowledge, provide the right guidance & spark passion among the mentees for the ever-changing world of cybersecurity.

The mentors come from diverse cybersecurity backgrounds, carrying a balanced combo of cybersecurity knowledge and expertise and required skills to guide the

mentees in correct direction to achieve their goals to break in or grow in cybersecurity industry.

While there is no silver bullet, a good mentorship program & volunteering by leading experts in cybersecurity can be the simple solution that we are looking for. Additionally, it can help address the huge supply-demand gap in cybersecurity workforce. While many organizations are struggling to improve their overall gender diversity, their Human Resources team could start focusing on returning women, as one of the key levers for their hiring.

This way they would end up hiring not just a rejuvenated woman who is eager to join the workforce, but also someone who is more motivated, has obtained a fresh perspective, and eager to perform.

Mentorship can also help bust several myths, such as:

- You need to be very technical to join cybersecurity
- Cybersecurity is a very stressful field
- Certification/cybersecurity course will help you secure a high paying job immediately
- Previous experience will be devalued

"Life's most persistent and urgent question is 'What are you doing for others?'" - Dr. Martin Luther King Jr.

"Protégé for Women in Cybersecurity"

In Cybersecurity field, the % of women applying for cybersecurity roles is incredibly low and 25% of women representation in Cybersecurity field is not impressive.

Women need examples of other successful women role models or influencers in "sustained and upward trending" leadership roles to be able to visualize themselves in one.

Hence, Pooja Shimpi has started an initiative **"Protégé for Women in Cybersecurity"**, where she publishes Inspirational stories of amazing mentors and mentees across the globe in medium.

Cyber security is an evolving field and limited number of role models and female mentors, but this trend is changing and there is an encouraging sign that women are aspiring for doing higher studies in Cyber security. With this initiative, the young female enthusiast is getting inspiration through the interviews from those talented women role models who are making in the top or on the pathway of breaking the ceiling! In their interview, the mentors provide a great knowledge about Cybersecurity field, their journey, challenges they have faced and guidance to mentees along with best resources to refer to break in Cybersecurity field.

Check her medium.com blogs "Protégé for Cybersecurity" for the amazing stories from the cybersecurity leaders and young professionals. Participate and share your mentorship in Cybersecurity story through this initiative and it will have an amplifying effect inspiring other.

It's time to pay it forward...





International
Cybersecurity Forum



International Cybersecurity Forum - #1 European
Event on Cybersecurity launched the FIC North
America in Montréal, Canada on November 1st & 2nd





UNIQUE LEARNING OPPORTUNITIES

Capitol's faculty are working professionals in the field.



LAUNCHING INTO SPACE

Our students have launched 6 payloads into space in the last 5 years!



MILITARY FRIENDLY

Tuition discounts for active duty military and their spouses.

1927

Capitol Radio Engineering Institute was founded by Eugene H. Rietzke, a radio operator and Navy veteran.



THE CAPITOL COMMITMENT

Up to 36 additional undergrad credits for FREE if you are not employed within 90 days of graduation.



PROFESSIONAL EDUCATION

Capitol provides cybersecurity training to participants in the NSA's SEED program.

16:1

Student to Faculty Ratio

AWARD-WINNING CYBER PROGRAM

Capitol Tech won SC Media's Best Cybersecurity Higher Education Program in 2020.

WHY CAPITOL?

As Washington D.C.'s premier STEM University, Capitol Technology University produces graduates that are highly sought-after by America's most technologically advanced government agencies and their private sector partners. With "hands on" curricula focused purely on STEM careers, Capitol Technology University positions its students for top roles in the region's booming tech hub.

POOJA SHIMPI

Vice President, Regional Information Security Officer APAC at Citi

This interview is conducted by **Scott Schober**,
President and CEO of Berkeley Varitronics Systems

[Scott Schober] I am delighted to have a chance to interview Pooja Shimpi. She is an Information Security Officer at CitiBank and has a wealth of experience in cyber security technologies and risk & compliance. She is based out of Singapore which is considered one of the world's greenest cities. Her tireless work keeps global banks and financial institutions safe from cyber threats. Pooja is passionate in making out digital lives more secure and safe.

[Scott Schober] Can you tell us about Singapore's journey to being a Smart Nation?

[Pooja Shimpi] Singapore aims to be the world's first Smart Nation, to use technology in improving the quality of life, strengthening businesses, and helping government agencies serve citizens better. This is also due to increasing urban density and aging population.

On 24th November 2014, Singapore's Prime Minister, Lee Hsien Loong launched

the Smart Nation initiative to harness technology to make life better for Singaporeans. He highlighted the mission and vision of the Smart Nation respectively.

"The Smart Nation Programme seeks to harness ICT, networks and data to support better living, create more opportunities, and to support stronger communities."

"A nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all."

The Singapore government sees the need to take "a whole-of-Government, whole-of-nation approach to building a Smart Nation". To do this, it has set up a Smart Nation Programme Office to plan, coordinate and execute with various initiatives such as multi-billion annual research and development, cultivating fast growing startups, engaging with multi-national corporates to cofound laboratories.



[Scott Schober] Your move to Singapore coincided with major initiatives in Singapore to being a Smart Nation. What changes have you seen?

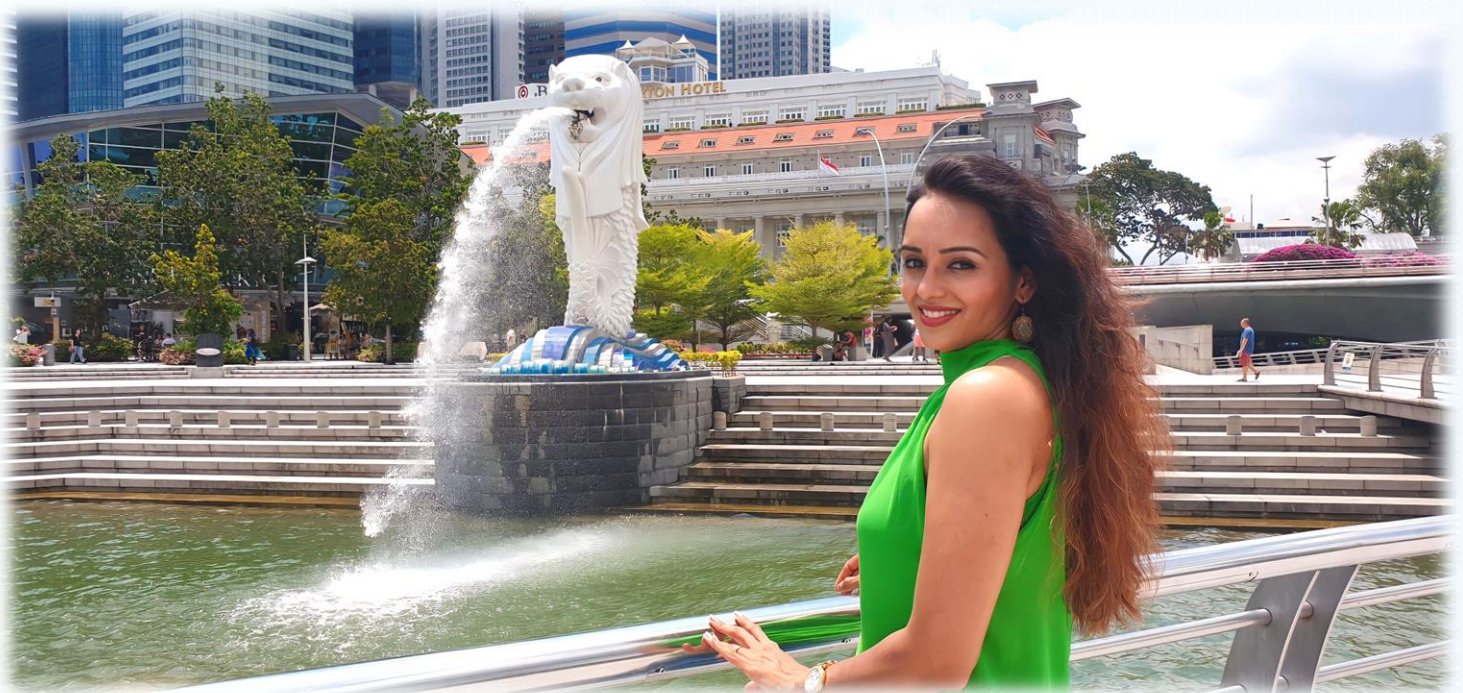
[Pooja Shimpi] Being a Smart Nation is a continuous improvement journey. There are many aspects of truly defining a smart nation, and digitalization is one of them. Since I moved here in 2014, I have seen the digital landscape changing really fast. As of 2022, more than 90% of the population of its ~5.9 million uses a smartphone, indicating that it is a leading country for the use and engagement of smartphones. Singapore has the fastest download speed of any country in the world averaging ~239 MBPS. Moreover, it was the first country in the world to achieve country-wide 5G coverage. Investment in digital transformation of its economy has been a long-term strategy that has led to steady GDP growth. And, this transformation has not happened over night. Since the inception of broadband internet, Singapore has been on the cutting edge. In 1998, it completed the first nationwide broadband network in the world, called Singapore ONE (One Network for Everyone),

providing access to the majority of the country. In comparison, only 3% of American households could get broadband in 2000, when 34% of the country was still using dial-up.

Since 2010, Singapore turned its attention to fiber, spending billions of dollars to upgrade its infrastructure, called the Next Generation Nationwide Broadband Network, and which promises gigabyte speeds across the city-state. Also, digitalization of public sector operations and services, together with development of digital industries and jobs has helped drive socio-economic development in Singapore.

Presently, Singapore has a mobile penetration rate of ~152%, with about 8.3m active mobile subscriptions. About 93% of Singaporeans use internet every day, averaging about seven hours and nine minutes, and there are ~4 connected devices with smartphones being the most used device. Smart cities will not be possible without the infocomm infrastructure to support IOT and Cyber Physical Systems.

No wonder Singapore is a world leader in strategizing & adapting digital technologies.



[Scott Schober] What would Singapore look like as a Smart Nation? Perhaps you can break it down and paint a digital portrait for us to get a better glimpse....

[Pooja Shimpi] As a city-state, Singapore was the first to earn the “**smart nation**” title. It’s a 721-square-kilometre (278 square mile) hub where new traffic control systems, data analytics models, and centers specialized in everything from health to digital commerce are tested out daily. This all happens in a context where sustainable transport is the primary motor for keeping both people and the economy moving.

Singapore is relying on digitalization and developing an efficient public transport network with a goal of traffic free country. If the government’s plan come to fruition, by 2025 all cars on the city streets will be self-driving. Experiments are underway on the island to enable vehicle-to-vehicle and vehicle-to-infrastructure communication. In addition to car-to-car dialogue, traffic light dialogue, for example, will keep drivers informed more quickly.

The evolution of the transportation system, combined with the benefits of artificial intelligence, is just one facet of Singapore’s ongoing progressive changes. Futuristic projects are in the pipeline such as creation of multi-route, aerial network for drones tasked with carrying packages, advance facial recognition systems to identify customers and many more.

Big Data and Internet of Things contributes to the realization of Singapore’s dream of becoming a Smart Nation. For Example, the smart watch of your is recording all your physical activities, heart rate and can be connected to a hospital and have access to your past medical history constituting to a big data.

A Smart Nation can be imagined as all devices having the ability to talk to each other and be seamlessly controlled. Imagine a day, where your self-driving car is taking you home, upon reaching through smart parking system your car is auto-parked, your elevator is waiting for you and as you enter the home the smart lighting system adjusts to your mood, the aircon is already at your preferred optimal level, your favorite play list is being streamed as you enter. Your smart refrigerator has placed an order to the closest grocery shop for the food items, and the list goes on. The intelligence of things is made up of Sensors + Internet + AI (Artificial intelligence) + Big data. Such smart technologies are getting used to collect data that is designed to help improve operational efficiency, drive economic growth and improve quality of life for residents. With more such information coming into the picture, we will need to have more in-deep thoughts of protecting these data. Information is critical. It can bring an organization or nation to halt; information likes customer data, or patient records, patents, military secrets and the list goes on.



[Scott Schober] What role does cyber security play in a Smart Nation? Who is involved in, and why is it so important to have a plan....

[Pooja Shimpi] Cyber security is an enormously important aspect of a Smart Nation. It is vital that smart cities have trusted secure systems, not just preventing stolen credit card numbers or identity theft, but protecting from malicious attacks, hacking or Distributed Denial of Service attacks. Security issues are critical on new and stored data that are collected for future use.

This is intensified by heterogeneous networks and applications and wireless communications. To become a smart city, investment alone is not enough. It takes human resources and, above all, talent and many modern smart cities are promoting cyber hack competition and offer prizes.

From Cyber security stand point, it's crucial to spread awareness across the nation, as Protection will never be 100% guaranteed. If your system has got DOS (Denial of Service) attack or phishing attack, the smart systems may not function and might turn around and create issues for users.

Having a strong password and changing it frequently is a good start. It's always a good idea to have basic cyber hygiene and then slowly build up the layered defense to protect the network. Strict cyber policies of cyber security of critical infrastructures including financial institutions, transportation systems and hospitals are essential to ensure continuance. Cybersecurity is a team sport, and everyone has a part to play.

For any smart nation a national cyber security masterplan is crucial, to provide strategic directions to guide national efforts to enhance cyber security for the government, businesses, public and private sectors. As more and more smart devices are getting produced, this could lure even more cyber criminals to scouring the weakness in the technology. Small devices mostly don't have any encryption and authentication capabilities and it can be easily targeted. It's been speculated that armies of "Smart" devices like web cameras could become a rising force of disruption especially when IoT devices has less or no regulations over their security standards. "The lack of consideration for security controls within those smart devices is giving hackers the ability and privilege to take ownership of them".



Chaos and confusion could be caused if critical infrastructure & systems were fall in wrong hands.

It's crucial to know what you have, because you cannot protect what you don't know! Smart cities can go a long way in bettering citizen services with increased convenience, but their risks should not be overlooked. With the help of tech like AI, cybersecurity can become smarter alongside cities to ensure citizens remain protected from cyber threats. Apart from building in multiple layers of defense strategies, there is a need to promote national resiliency so when any attack strike, the country can swiftly bounce back and return to normalcy.

[Scott Schober] Who do you feel are the most vulnerable when it comes to cyber attacks & what is Singapore doing to address that?

[Pooja Shimpi] Globally, the latest figures show an increasing number of smartphone users year after year. In 2022, the number of global smartphone users is ~6.6 billion, marking a 4.9 percent annual increase. It is also 2.9 billion, or 79 percent, more than the number of smartphone users there were in 2016, just six years ago! In Singapore, smartphones are the most used devices for browsing the Internet, used by 92% of the population. Singaporeans embrace social media, with ~80% of the population having an account on a social media platform.

With the advent of IOT (Internet of Things), many more devices are connected to the internet even at homes, for example – Amazon Alexa, white goods, smartphones, tablet computers, cameras and security systems. And in a post COVID world, work-from-home users are also connected to the same network devices using their work laptops. Hence, a simple phishing attack on any of the home devices could lead to unexpected threats. There have been instances globally of attackers hacking home cameras or CCTV systems leading to privacy thefts. Moreover, sharing of smartphones with children and even toddlers is quite rampant not just in Singapore but globally. Similarly, a growing population of senior citizens using smartphones in Singapore makes them more vulnerable as usually they are late adopters of technology. While on the surface, it might not seem like a big threat when you compare cyber risks associated with banks, financial organizations and public utilities, however this age group could be most vulnerable in the future.

With the advent of IOT (Internet of Things), many more devices are connected to the internet even at homes, for example – Amazon Alexa, white goods, smartphones, tablet computers, cameras and security systems.



And in a post COVID world, work-from-home users are also connected to the same network devices using their work laptops. Hence, a simple phishing attack on any of the home devices could lead to unexpected threats. There have been instances globally of attackers hacking home cameras or CCTV systems leading to privacy thefts.

Senior citizens were the most vulnerable group when the COVID19 induced circuit breaker was in effect, as they had no means to socialize and instead consume content on the internet for entertainment or use video calling for chatting with friends and family over mobile or web cameras. It was the same case with children who couldn't go to school and had to attend classes online using their parent's smartphones or laptops. Hence it is of utmost importance to spread cyber safety awareness among this age group at all levels.

Additionally, cyber scams have been on the rise, and in 2021 alone Singapore lost SGD 633.33 million which is 2.5 times more than the previous year. About 90% of the scams originated from overseas where the scammers were syndicated, well-resourced and technologically sophisticated. Such cases are difficult to investigate and prosecute as the local efforts will be dependent on the level of cooperation from overseas law enforcement agencies. Investment scams accounted for the most amount of money stolen, with victims losing \$190.9 million in total. The largest amount taken in a single case was \$6.4 million.


To encourage more people to adopt better cyber practices and be more aware of the threats, CSA (Singapore's Cyber Security Agency) has regularly launched the "Better Cyber Safe than Sorry" national cybersecurity awareness campaign.

The national campaign augments concurrent efforts by CSA to target students and seniors respectively under the SG Cyber Safe Students Programme and SG Cyber Safe Seniors Programme. In collaboration with various government agencies, such as the Ministry of Education, GovTech, SPF and IMDA, these initiatives enable CSA to reach out to students and seniors with relevant cybersecurity messages through platforms – such as roadshows and webinars – to raise awareness and adoption of good cyber practices. Initiatives such as the Go Safe Online Pop-up and Go Safe Online Drama Skit under the SG Cyber Safe Students Programme have reached more than 160 schools, libraries, and community spaces, while CSA has engaged more than 45,000 seniors under the SG Cyber Safe Seniors Programme since the launch of both programmes in 2021.

“Cyberspace transcends borders. We therefore need to mobilize a global response to address systemic cybersecurity challenges.”

[Scott Schober] Pooja, thank you so much for all you do in fighting the cyber criminals and keeping the financial institutions and global banks safe.



A portrait of Scott Schober, a man with short dark hair, wearing a grey suit, white shirt, and a patterned tie. He is smiling and has his arms crossed. The background is a nighttime city skyline with illuminated skyscrapers, including one with an 'HSBC' sign.

About the interviewer:

SCOTT SCHOBBER, UNITED STATES

Scott Schober is the President and CEO of Berkeley Varitronics Systems, a 50-year-old, New Jersey-based provider of advanced, world-class wireless test and security solutions. He is the author of three best-selling security books: *Hacked Again*, *Cybersecurity is Everybody's Business*, and *Senior Cyber*.

Scott is a highly sought-after author and expert for live security events, media appearances, and commentary on the topics of ransomware, wireless threats, drone surveillance and hacking, cybersecurity for consumers, and small business. He is often seen on **ABC News, Bloomberg TV, Al Jazeera America, CBS This Morning News, CNN, Fox Business**, and many more networks. Scott also serves sits on several cyber advisory boards for various companies.

TOP CYBER NEWS MAGAZINE



CYBERTECH

MEDIA PARTNER

CYBERTECH NEW YORK



CYBERTECH IN THE BIG APPLE

Event Registration:



<https://nyc.cybertechconference.com/registration>

 CYBERTECH NEW YORK

November 15-16, 2022

Javits Center // New York City



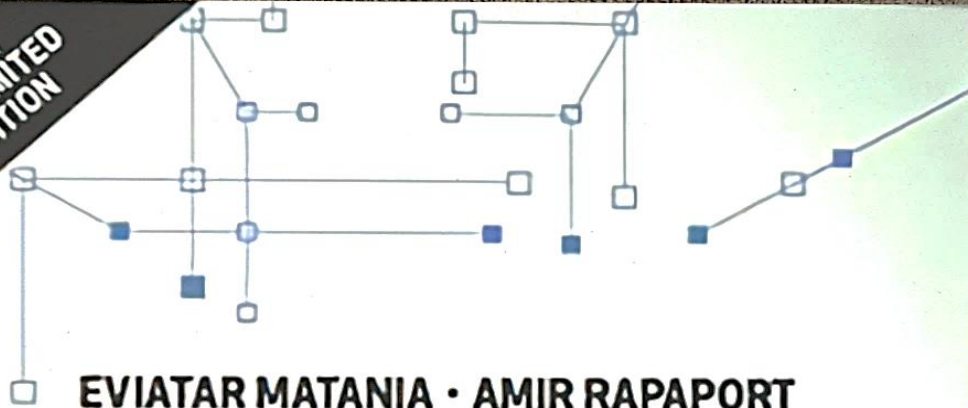
Biggest startup pavilion in America

80+ Exhibitors



CYBERTECH

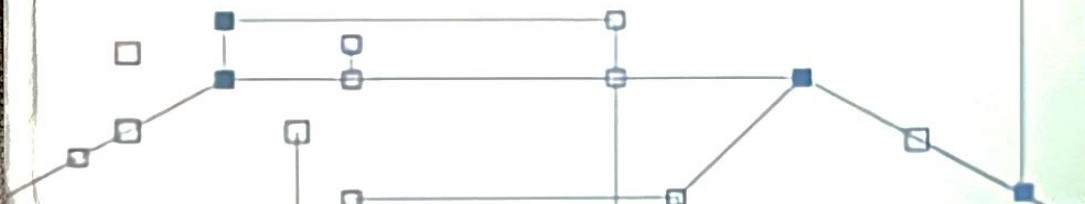
**EARLY
AND LIMITED
EDITION**



EVIATAR MATANIA • AMIR RAPAPORT

CYBER MANIA

**HOW ISRAEL BECAME A GLOBAL POWERHOUSE
IN THE DOMAIN THAT IS REVOLUTIONIZING
THE FUTURE OF HUMANITY**



THE TOP 5 TIPS

FOR LAUNCHING AN INFOSEC PROGRAM FOR YOUR SMALL BUSINESS

by Travis Deforge & Christian Scott of GoVanguard Security



“Plans are worthless, but planning is everything.”

When President Dwight D. Eisenhower said this in 1957, he certainly wasn't referring to an Information Security (InfoSec) program. The principle, however, is applicable to preparing your small business to contend with modern hacking groups. Assessing your organization's cybersecurity posture, identifying its vulnerabilities, and formulating a plan to defend your digital assets are often-overlooked necessities for small businesses.

Some small-business owners believe that their size renders them invisible to malicious actors. Unfortunately, recent cybercrime statistics suggest that small businesses are in fact easy, often-exploited targets. According to Verizon's 2021 Data Breach Investigations Report, small businesses accounted for about 46% of all breaches tracked by the communications company. External actors launched 57% of these attacks, and 93% of malicious actors had financial motives.

While creating a robust InfoSec program may seem intimidating and expensive, the truth is that it doesn't have to be. Based on my observations as a penetration tester, the most difficult businesses to compromise are not those with multi-million-dollar security budgets, but those that have a solid understanding of their own risks and systematic processes for mitigating them. While the former can require a robust staff and suite of tooling, the latter simply requires planning and consistent due diligence.

To begin planning and maintaining an InfoSec program for your small business, focus on these five areas:

Understand your environment

To determine where you're going, you must first determine where you are. In InfoSec, determining where you are translates to mapping your InfoSec environment. Only after you've mapped your InfoSec environment should you begin making extensive InfoSec plans.

First, let's define InfoSec 'environment.' Your InfoSec environment is your network and attack surface and how both relate to your current and future business objectives. Understanding your environment is critical because business environments are always changing.

For example, five years ago, you might have used on-premises servers. Now, you're in the cloud, with a hybrid workforce, and federating all your authentication needs through a third party like Okta or Duo. Each change that is made to your environment inherently changes the organization's risk posture, hopefully for the better, but not always.

Once you understand your current InfoSec environment, you must also understand where it's going. For example, are you planning to add another location? Expanding your workforce? Shifting to a hybrid work arrangement? The good news is that none of these changes happen overnight. As you're charting your business trajectory, include InfoSec in your planning. The key is ensuring that your approach to InfoSec is proactive and preventative rather than reactive. Gathering the operations, IT, and security teams together to brainstorm future initiatives now may save you from exercising your disaster recovery plan later. (You've got a disaster recovery plan, right?)

Understand your attack surface

Once you understand your InfoSec environment, you can begin to get granular about mapping your attack surface. Your attack surface constitutes every way a malicious actor could breach your company. It includes every web server that a malicious actor could access on the internet as well as individual devices, such as laptops, tablets, and phones. To put it simply, if it's part of your network or a service that your organization uses, then it's part of your attack surface.

If your small business uses a managed service provider, your provider should be able to supply a comprehensive list of servers and devices easily. However, it is easy to overestimate one's familiarity with the true attack surface, especially if it is a complex environment that has not recently had a penetration test.

For example, if your business has security cameras, can they be accessed from an external IP address by any internet user? Is your HVAC system accessible from the open internet, and when was the last time it was patched? Do you have smart thermostats or TVs that aren't protected within your network? Do any of these devices retain their default credentials, which a malicious actor could simply Google?

Creating a comprehensive map of your attack surface provides valuable insights as to how a malicious actor could gain a foothold in your IT architecture and begin moving from device to device within your network. This is where a defence in depth approach becomes critical. Defence in depth includes endpoint security, like antivirus software, patch management tools that keep your systems and applications up to date, network security controls, such as VPNs, systems that detect intrusions by malicious actors, and access management solutions, such as multi-factor authentication and impossible travel alerts.

However, no matter how security-hardened your external perimeter is, a malicious actor

eventually will find a way in. At that point, it becomes essential from an incident response standpoint to be intimately familiar with the internal attack surface to ensure the threat is detected, contained, and mitigated.

Set clear and concise policies

Every business, regardless of size, needs a Written Information Security Program (WISP). In fact, businesses operating in certain industries, such as healthcare, are legally required to have WISPs. While your WISP does not need to be long and complex, it should at a minimum outline:

- **Administrative safeguards**
- **Physical safeguards**
- **Technical safeguards**

If your business does not have a WISP, basing one off the Center of Internet Safety (CIS) Critical Security Controls Version 8 is a good place to start. CISv8 is a practical, prioritized set of safeguards to get you started.

CIS also provides a policy guide that includes WISP templates. While templates offer sound starting points, they often contain a lot of boilerplate language and irrelevant information. Cut out anything that doesn't apply to your small business; otherwise, you may end up with a monstrous document that no one reads.

Finally, policies and procedures in your WISP should reflect your small business as it's currently configured – not future initiatives and features. Update your WISP once you've rolled out new business elements.

Define and test a disaster recovery plan

What steps will your small business take to recover from an attack? These steps constitute your Disaster Recovery Plan (DRP).

DRPs are only useful if they evolve with your small business. Any time your InfoSec environment and/or attack surface changes, revisit your DRP. Conduct tabletop exercises to simulate attacks on valuable company assets.

For example: Your head of marketing falls victim to a spear-phishing attack, which compromises your client list. During the tabletop exercise, your team reviews hypothetical responses while others challenge those responses. The exercise may go something like this:

CEO: Sally from marketing's email was compromised. What's the impact?

Analyst 1: She has a master list of all our clients. The malicious actor could socially engineer the clients by sending an email as Sally.

CEO: How do we stop this?

Analyst 1: We lock down her email account.

Analyst 2: How about we create a fake email account, replicate this attack, see what the malicious actor could obtain, and see if locking down her email account addresses the issue?

The goal of these exercises is to reach a point where your DRP breaks down. Once you identify the point of failure, update your DRP to eliminate it. To get started, the CIS has a great white paper laying out six scenarios for these types of exercises. And the best part is, that they're all mapped to the applicable CIS controls to help refine your WISP.

Set quarterly and annual reviews and objectives

The point of creating quarterly and annual reviews along with objectives is to mature your InfoSec program. If your InfoSec posture constantly lags the growth of your small business, you're constantly vulnerable. The antithesis is to establish your InfoSec baseline by following the tips mentioned in this post, forecasting your growth, creating a plan to co-evolve your InfoSec posture, then repeating the process by establishing a new baseline.

Create quarterly, annual, three-year, and five-year goals for your InfoSec posture that reflect where your small business is headed. Your progression toward those objectives can include smaller milestones, such as cybersecurity awareness

training for your employees, running phishing and social engineering testing, or even simply preparing a short presentation on common InfoSec threats in your industry. KnowBe4 is also a great training resource. A little time spent on Google, IBM X-Force Exchange, or VirusTotal will reveal threats specific to your industry and business size.

This type of research and employee education is free, except for the cost of time and planning. The key is to emphasize continuous refinement, continuous improvement, and continuous re-evaluation. Complacency kills.

This type of research and employee education is free, except for the cost of time and planning. The key is to emphasize continuous refinement, continuous improvement, and continuous re-evaluation. Complacency kills.



Moving forward with a plan

Small businesses are not immune to malicious actors. Fortunately, they are agile enough to implement these simple, low- or no-cost tips, which can form the basis of your InfoSec plan. Planning does not need to be complicated, time-consuming, or expensive. However, it does require a commitment to setting goals, monitoring progress, and updating your InfoSec plans and priorities as your small business grows.

This work is as essential to the health and sustainability of your small business as paying your bills and balancing your books. And while it's true that no plan survives first contact, having no plan at all jeopardizes your small business' chances of surviving first contact. And believe us: If it hasn't happened yet, contact is coming.



TRAVIS DEFORGE, UNITED STATES

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..



CHRISTIAN SCOTT, UNITED STATES

Christian Scott is an extremely passionate, self-made technology & cybersecurity leader. Christian initially matriculated from the domain of software development and then moved into network & systems engineering before finally settling into cybersecurity by performing penetration testing & building security programs for numerous Fortune 1000 companies. Currently, Christian serves as the COO & CISO at GoVanguard Security.

GoVanguard Security is a boutique cybersecurity firm based out of Manhattan, focused on providing high-quality penetration testing, malicious adversary simulation, and cybersecurity strategy services. In his free time, Christian enjoys teaching & mentoring others in the areas of cybersecurity, business development, and leadership. Currently, Christian cohosts free weekly cybersecurity training sessions with Travis Deforge. Christian's latest community contributions can be found at enclave-regenerous.com, which he hosts with his business partner Blake Shalem.



SECURING THE SMART NATION

by Edward MILLINGTON, CISSP, ISSA, MCIIS, MIET, PAN-ACE), the Founder and Managing Director of CariSec Global Inc.

The digital revolution is driving sustainability to new and achievable levels and with the help of COVID-19, the digital transformation program for the private and public sector has exploded exponentially, thereby creating an environment for a true digital culture. In addition, with digital accessibility to communications and the Internet of Things (IoT), the realization of a Smart Nation is very much viable and is occurring at an evolving rate over the last 10yrs.

The Smart Nation ideology is a great concept in the advancement of mankind and his habitat. But while the Smart Nation will implement

many concepts in achieving balance systems, its digital nature makes it a prime target for cyber-criminals and other cyber risks; affecting people, process, technology, and service.

Securing the Smart Nations involves creating security strategies for the protection of its many systems, functions, and services; in the observance of confidentiality, integrity, availability, and safety.

Governance

Designing, implementing, operating, maintaining, and monitoring the Smart Nation will involve effective and efficient policies, legislations, laws, standards, and frameworks in creating the environment for security and secured operations; data protection and privacy; secure technologies; human diversity and inclusiveness. Additionally, great efforts in program development bridging private and public partnerships for the common good of mankind in the delivery of goods and services should also be a benefit in this phase – a precursor to the Smart Nation lifecycle.

In essence, a security strategy should be well developed by all stakeholders before any further development occurs in the lifecycle of the Smart Nation.

People

The lifecycle of the Smart Nation in its current evolution is dependent on the human element. The human element should be highly trained and competent, and be part of a continuous educational program, keeping them up-to-date on technology changes and cyber risks. Such persons should possess the skills, knowledge, and abilities to function effectively



and efficiently in their roles as they deliver a culture of security and security culture to their peers, third parties, and other partnerships. The inability to achieve high standards and capabilities with the human element can result in greater cyber risks when it comes to data losses, misconfigurations, vulnerabilities, cyber-defence, etc.

In addition to the culture of security, public (service) users should also be aware of cyber risks in everyday life and through awareness campaigns report anomalies, disinformation, and misinformation by systems, functions, and services.

Process

Smart Nation operations should be process driven at a high maturity level where procedures and practices making up its programs, should be inherently written with security by default - by design. Documents should document risk-based cyber asset management; access and control methods to data, systems, and services; procurement procedures; service delivery agreements; data management; security controls auditing methods; configuration and change

management; security testing procedures; privacy management; risk management; third-party risk management, etc.

Technology

All procured technologies should have security-by-design and security-by-default in the operations of the Smart Nation. It is very important that the risk profile for all technologies utilised are known and continually assess for vulnerability and patch management programs. In addition, technology management is strategic when it comes to Information Technology, Operation Technology, and IoT management and operations. Each technology has specific needs when it comes to the design and implementation of risk-based security controls. To note, some controls can be DLP, process verification, device identity management, etc.

Service

A Smart Nation provides a range of services for sustainability. The integrity, availability, and safety of these services are crucial in the development, operations, and functions of the Smart Nation. It is very important these services are very well trusted and provide the confidentiality needed through demonstrated security features like AAA, monitoring, anomalies detection, notification, etc.

“A Smart Nation processes and stores large volumes of data for effective and efficient operations in the provision and management of services and functions. It is therefore very important that all systems are highly secured and protected from unauthorized access; unauthorized changes to data, systems, functions, and services; cyber-attacks, etc.”



PREVENTING DATA BREACHES

RISK MANAGING ORGANISATIONS' VULNERABLE CYBER ASSETS

by Edward MILLINGTON, CISSP, ISSA, MCIIS, MIET, PAN-ACE),
Founder and Managing Director of CariSec Global Inc.

Cyber-attacks against organisations continue to be prevalent over the last few years and while there is no shortage of such awareness as reported daily by the global media, cybercrime and its associated multidimensional effects are costing organisations millions of dollars per year in Incident Management activities and cyber-resilience capacity building. Cybercrime is a Global Security problem and continues to be listed in Global Threat Reports like the World Economic Forum (WEF) The Global Risks Report – 2021 & 2022. This implies the need for Global to National to Local Cybersecurity Strategies in the cyber-defence against cybercrime.

Justifiably, no business is safe, and reducing business exposure is very important. The script for compromised and breached businesses are almost always the same and that is, vulnerabilities in the organisation's governance structures affect its people, process, technology, and service - thereby affecting businesses' cyber-resilience capacity.

When one talks about reducing organisation's exposure in the security (cyber) sense, it really refers to reducing the administrative, technical, and physical surface areas (also known as attack surfaces) where an organisation can be attacked by a cyber-criminal - placing data and other critical assets at risk - affecting their confidentiality, integrity, availability, and safety. In essence, the organisation must understand its operating industry's Threat Landscape which may comprise the following: Email threats,

Ransomware attacks, Supply Chain threats, Exploitation of vulnerabilities of applications, databases, networks, etc., just to name a few. For businesses to improve and develop higher security operating postures in the cyber-defence of assets, the vulnerability profile of assets must be known through risk management activities, where cyber-threats can be appropriately risk-treated by the implementation of risk-based security controls in the administrative, technical and physical domains of the business. The inability to do so could mean cyber-criminals gaining entry into (compromising) the business to install a device(s) and or software, encrypting, damaging, and or exfiltrating data for financial gain (ransom). In fact, in the latter half of 2021 and more so in 2022, cyber-criminals started the criminal profile of shaming businesses to cause reputational and other forms of organisational damages when the ransom is not paid - especially in heavily regulated or high-profile industries. These are some of the well-known activities of cyber-criminals.

The first venture for a business in the application of securing and protecting its assets is to implement a Risk-based Cybersecurity Asset Management Program, where the discovery of all assets is one of its major activities. This employs prodigious collaborative efforts at all levels of the organisation to gather, identify and document all assets that can be at risk due to threats that can cause organisational damages. The asset can be classified as

organisational, people, process, technology, and service. **It must be noted for the program to be risk-based; all activities are led by a comprehensive Automated Cyber & IT Risk Management Program (C/ITRMP).**

Secondly, once all assets have been discovered and classified, the risk impact on the business should be well understood and known by all stakeholders. This clarity can only be gained by understanding each asset's vulnerability profile and associated threats pertaining to the operating industry - attained from threat intelligence reports. Reaffirming, all derivatives from the C/ITRMP.

Lastly, knowing the risks to your business implies a great level of understanding of your attack surfaces for risk management. Explaining carefully, the controls put in place to reduce cyber-risks can be more of cybersecurity awareness training; designing and implementing effective and efficient policies; frequent penetration testing on applications and networking infrastructures; red team ethical hacking on the organisation, people, process, and service; certified training of personnel, etc.

Cybersecurity is an Organisation Strategy owned and operated by the executive teams and it is not an IT Strategy IT is responsible for.

In conclusion, once the organisation understands its assets' vulnerability profile, it will be in a better position (risk-aware) to strategically secure and protect those assets (the organisation, its people, process, technology, and service) from cyber threats due to its high operating security posture. This optimised security maturity level also implies that the organization will have a high cyber resilience against sophisticated cyber-attacks from cyber-criminals, due to the institution of risk-based security controls operating at high capabilities levels.

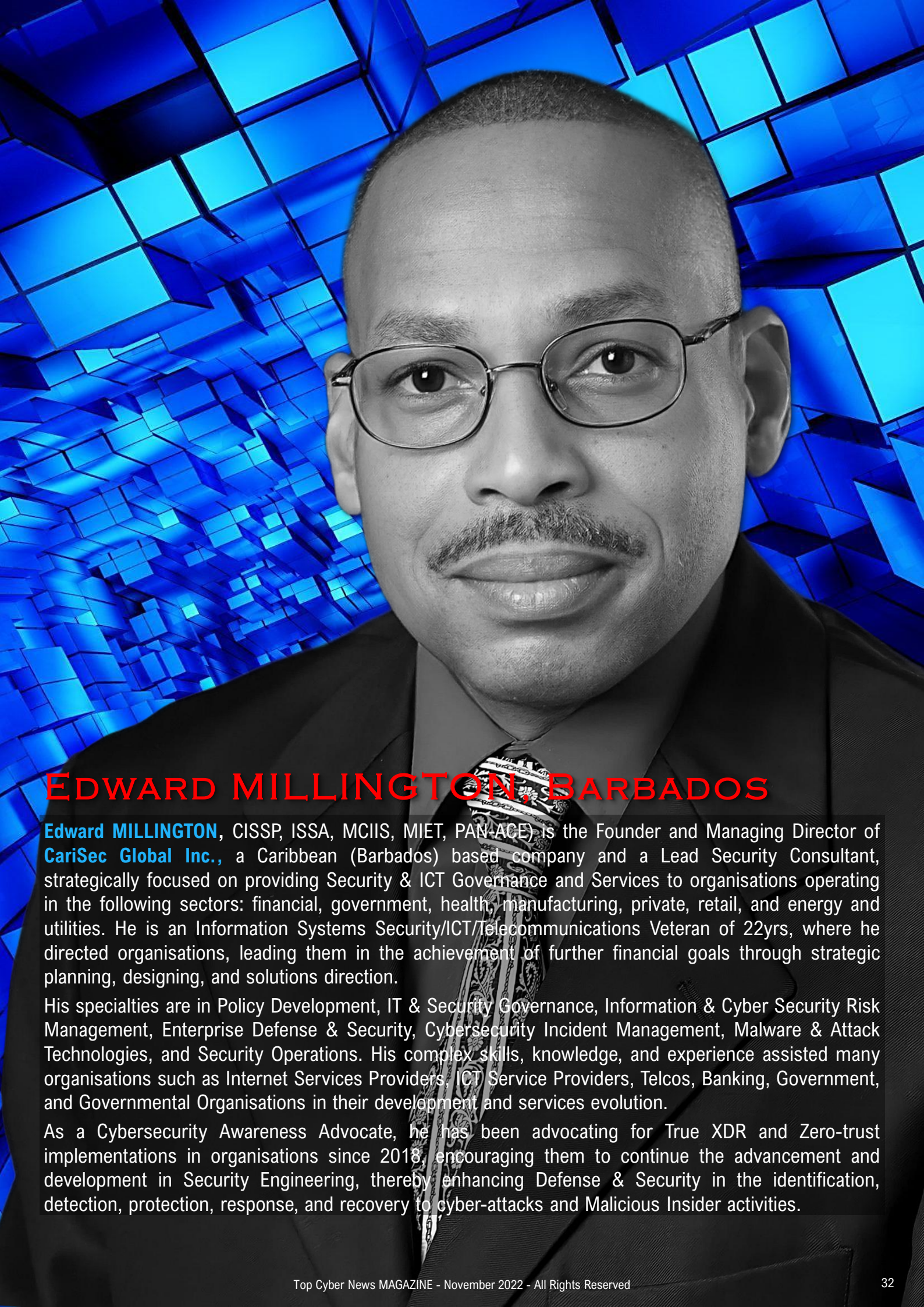


CariSec Global, a leading Next-Generation Managed Service Provider – providing Risk-Integrated Cybersecurity & ICT Managed Strategic Services, protects Businesses and their Data by integrating International Standards and Frameworks into the organisations' strategies and goals; meeting obligations to laws, regulations, and industry compliance(s), while providing business operational safety, integrity, trust and resilience to Institutions: financial, government, health, manufacturing, private, retail, and energy and utilities.

This is achieved through our globally recognised team, which brings 22+ years of high-level skills, knowledge, and a wealth of experience in the areas of Information & Cyber Security, Capacity Planning, Business Continuity & Disaster Recovery Planning, Risk Management, ICT, Telecommunications, and Technology Project Management.

As an MSP, CariSec Global provides industry-leading Managed Services through Managed Consultations.

CariSec Global Creates Partnerships in the Development of Organizations Information Security and ICT Programs.
<https://carisec.global>



EDWARD MILLINGTON, BARBADOS

Edward MILLINGTON, CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of **CariSec Global Inc.**, a Caribbean (Barbados) based company and a Lead Security Consultant, strategically focused on providing Security & ICT Governance and Services to organisations operating in the following sectors: financial, government, health, manufacturing, private, retail, and energy and utilities. He is an Information Systems Security/ICT/Telecommunications Veteran of 22yrs, where he directed organisations, leading them in the achievement of further financial goals through strategic planning, designing, and solutions direction.

His specialties are in Policy Development, IT & Security Governance, Information & Cyber Security Risk Management, Enterprise Defense & Security, Cybersecurity Incident Management, Malware & Attack Technologies, and Security Operations. His complex skills, knowledge, and experience assisted many organisations such as Internet Services Providers, ICT Service Providers, Telcos, Banking, Government, and Governmental Organisations in their development and services evolution.

As a Cybersecurity Awareness Advocate, he has been advocating for True XDR and Zero-trust implementations in organisations since 2018, encouraging them to continue the advancement and development in Security Engineering, thereby enhancing Defense & Security in the identification, detection, protection, response, and recovery to cyber-attacks and Malicious Insider activities.

SMART CITIES REQUIRE ENERGY EFFICIENCY AND CYBER-SECURED DATA COMMUNICATIONS

by Dr. Ofer Alon and Daniel Ehrenreich

Introduction

The transition from traditional city operation to Smart City configuration is already happening at an unprecedented rate. Considering the significant changes happening worldwide, city authorities and operators must adapt their operation mode to higher energy efficiency. They will have to introduce state-of-the-art control systems for managing energy resources, enforcement of efficient energy consumption, remote control for smart lighting poles, deployment of display screens on streets, and providing information on public transportation, news, and more.

The rapid pace of these new developments also poses significant challenges for policymakers in introducing adapted processes. The modernized services required for smart cities are expected to consume a significant amount of electric energy at many locations across the city. Smart Cities operators will obligate the regional power utilities to ensure an adequate level of electric power also delivered at high peak periods. They will have to deploy efficient high-power distribution grids and add alternative and backup solutions. The supplied energy may be available at variable tariffs to control the demand, especially for not-time-critical power consumers.



The deployment of modernized services across the city will require the availability of high-speed, reliable, low latency, and cyber-secured data communications. These networks shall be suitable for transferring a large amount of critical and sensitive data via strongly protected private and public networks. Furthermore, deploying Internet of Things (IoT) endpoints which will be integrated into modern architectures, will increase the cyber-attack surface and consequently increase the risks of attacks against critical operations. Creating an integrated architecture requires combined expertise in the fields of power generation and distribution, energy efficiency and data communications, wireless networks, and cyber security.

Targeted technology solutions

As already mentioned above, the modern technology solutions provided for Smart City operations must include the following:

- a)** Electric power must be delivered effectively, reliably, and safely to all endpoints. It means that the power grid shall include a connection to the main grid of the power utility, including onsite generating facilities, UPS, photovoltaic systems, and more. The operation of these facilities shall be monitored according to the defined programs and controlled by dedicated supervisory Control and Data Acquisition (SCADA) system.
- b)** The end-to-end data communication network must include a combination of fiber optic networks, Copper cable Ethernet, Coaxial cables, Wireless data networks, and cellular media. These media shall be seamlessly interconnected to assure the highest possible data rate, low latency, operation reliability, and capability to secure interfacing to a broad range of appliances operated by manufacturing facilities, commercial organizations, and private entities.
- c)** Assurance of cyber-secured data communication is critical to minimize the risk of Man in the Middle (MitM) attacks, Distributed Denial of Service (DDoS) attacks, and include adapted solutions for Data Leak Prevention (DLP). The defense shall minimize the risk of attacks against cloud-based databases and prevent hostile encryption of computers, and databases for purpose of collecting ransom payments.

These cyber defense goals can be achieved by deploying encryption and authentication processes, intrusion detection systems (IDS), Security Information and Event Management (SIEM), deployment of sophisticated deception systems, and managing the operation through Security Operation Centers (SOC).



Applicable Verticals

As mentioned above, Smart Cities are required to integrate a broad range of vertical applications and each one has distinct characteristics and different demands related to power consumption, data communications, and cyber security.

#	Description of the Vertical	Power Consumption	Communications Performance	Cyber Security
1	Charging of electrical vehicles in a parking	Remarkably high	Low	Medium
2	Operation of Street lighting systems	Medium	Very Low	Medium
3	Display screen for information to the public	Medium	High	Critical
4	Public transportation information displays	Low	Incredibly low	Important
5	Real-time synchronization of traffic lights	Low	Incredibly low	Critical
6	Private point-to-point data links	Low	Very High	Very High
7	City-wide Wi-Fi Access points for visitors	Low	High	Low
8	Deployment of electrical rail transportation	Very high	Low	High

Summary and conclusions

While in the past, the industrial, utility, and public safety-related networks were segregated from the Information Technology (IT) network, the operation of these independent systems must be coordinated through secure integration.

The design deployment, integration and commissioning of advanced Smart City operations requires experience and expertise in specific vertical applications, process control, data communications, and cyber security.





DR. OFER ALON, ISRAEL

Dr. Ofer Alon – Acting as a strategist and expert in business and technological efficiency for buildings, energy solutions, and climate control and periodically delivering lectures and guiding organizations and local authorities in upgrading infrastructure and control systems, smart cities, and energy efficiency, energy saving, and green construction. Service in Israel and abroad (Strategic consultant, Expert in Business & Technological Efficiency) initiated, planned, developed, and managed a wide variety of unique projects, solutions, and patents that led to significant savings in energy consumption.



DANIEL EHRENREICH, ISRAEL

Daniel Ehrenreich, BSc. is an expert in the field of Industrial Control System and Operation Technology (ICS/OT), acting as a consultant for industrial cyber security lecturer at Secure Communications and Control Experts (SCCE) and periodically conducting workshops and presenting at industry conferences on the integration of cyber defense with industrial control systems; Daniel has over 32 years of engineering experience with ICS and OT systems for electricity, water, gas, and power plants and cyber security for these systems. Re-selected as **Chairperson for the 7th ICS CyberSec 2022 in Israel** on 20-11-2022.

THE SIDESTEP THAT ENABLED ME TO RENEW CYBERSECURITY EXPERTS TRAINING

by Luc Chrétien, CEO of Propulsar Cyber Academia

As a training professional, in this article, I explain step by step how I approached the training of cybersecurity experts. With my fresh eyes, I had the privilege of making some extremely enriching observations about cybersecurity and its actors. From these insights, I combined relevant pedagogical concepts with my training experience. Here is my "discovery report".

The Three Pillars of Cybersecurity. I was immensely dissatisfied with the mountain of knowledge that cybersecurity requires. It's like describing an elephant, one describes the trunk, one describes a leg, the next describes the flank, etc. With lots of acronyms like CERT, CISSP, DDoS, EDR, GRC, IAM, OSINT and many more! In this context, it was difficult for me to access a simple and comprehensive understanding of cybersecurity. Fortunately, while preparing a publication in LinkedIn (I also started to do it) on the reconciliation of the Aviation Safety Management System (SMS) and the Cybersecurity Management System (CMS), I came across a synthetic diagram that finally gave me the vision and the global understanding of cybersecurity that I was hoping for. From then on, everything became simpler with an easily memorable overview of cybersecurity. Indeed, this diagram or tree structure of categories and subcategories, makes it easier to learn, prioritize and make decisions. Exactly what every CISO and cybersecurity expert needs to do.

How I landed in the unknown land of cybersecurity. It all started in February 2020 when Covid-19 hit the world. And on my professional world, that of human performance improvement. With group workshops or individual coaching that engaged the body, the mind, and the emotions, I quickly understood that my professional activity was done for a long time!

Luckily, a few days before the confinement, I met the European manager of the Israeli company Pilat Loctel Group (since bought by the British Career Star Group). Specialized in online training in digital technologies, this company works for all the world tech in America, Europe and in Asia. We negotiated and signed commercial agreements to develop the French market for digital technology training: Telecom, Hardware Design Training, Computer Technology Skills, Internet of Object (IoT), Data Science & AI and finally Cyber Security.

After a few months, I realized that in life, I liked to innovate, work on the product-service and master the price. I was then ready to launch myself into the marketing vertical of cybersecurity expert training. The cybersecurity market seemed more affordable than the vastness of IT development. Plus, with the cybercrime that everyone was talking about more and more, the choice was easy to make.

Having the desire to be an entrepreneur is good. But starting with solid training concepts is better. With more than thirty years of experience in training, all I had to do was draw on my experiences and observations.

Project-Based Learning. In the 90's (I agree with you, I'm really going back in time) I was working for HEC Executive Education (France) and I liked to accompany small groups of executives to realize action projects.



PROPULSAR

Cyber Academia

The Project-Based Learning approach was so effective that at the end of the general management programs, the participants retained the action projects that had allowed them to make the link between the training program and their activities in companies. I have facilitated a variety of projects in banking, industry, and services. The projects touched on different areas of business management: marketing, organization, financial portfolio restructuring, performance indicators, etc. I also practiced action projects with university leaders in Latin America, for the University of Monterrey (Mexico).

Online training. From the very first steps of the Internet, I was working with the directors of French higher education institutions on how to develop online training. We had "la vista": everything we had conceived about learning via the Internet saw the light of day in the years that followed. Only the tools evolved! At the beginning of 2000, I founded one of the first training organizations in France that specialized in customized e-learning. This is how I developed the first e-learning programs for the Alcatel technology group (now Alcatel-Lucent). This pioneering experience has left its mark on me.

Training for executives. At Arcelor's corporate university, which later became ArcelorMittal, I set up a blended MBA executive part-time program, I developed programs with the best professors from the most prestigious universities such as MIT, Penn State University, London Business School, Insead, HEC, etc. It was a very rich experience with a target group of executives. These high-level activities, these intense exchanges on program design and pedagogical practices have given me a lot of insight on how to do it.

Progress in cybersecurity. A network like LinkedIn allows you to discover cybersecurity experts who do not hesitate to share their experiences by publishing inspiring content. This is how I discovered the three fundamental rules to progress in cybersecurity, whatever the profile: CISO, Pentester, ISO 27001 Auditor, SOC Analyst, etc. These three rules are: (1) cultivate your network, (2) collaborate with a mentor and (3) excel in at least one area. Propulsar's offer is precisely in line with these three rules! In fact, the training design had been developed before, but it always feels good to confirm afterwards that the road traced is the right one!

Why am I so involved in the training of cybersecurity experts? The digital economy drives today's society and facilitates the creation of wealth. By accelerating the training of cybersecurity experts, I am helping to better protect the digital assets of businesses and organizations from cybercrime. In addition, I have found that cybersecurity experts are severely time poor, this is due to an unreasonably high workload. This overload is caused by a recurring worldwide shortage of cybersecurity professionals, resulting in vacancies in companies and hospitals for months at a time. Under these conditions, for experts to continue training, their skills development must be integrated into the workflow.

Do not hesitate to ask me any questions you may have. To do so, contact me by email: luc.chretien@pro-pulsar.com . I will answer each of you, with great pleasure!



LUC CHRÉTIEN, FRANCE

Luc Chrétien is the **CEO of Propulsar Cyber Academia**. A graduate of the University of Paris Nanterre (France) and Harvard University (USA), Mr. Chrétien has long been involved in the training of professionals and business leaders. He loves the effectiveness of collaborative online learning and workplace training.

TOP CYBER NEWS MAGAZINE

Human Centered Communication Of Technology, Innovation, and Cybersecurity



AN AWARD-WINNING DIGITAL MAGAZINE
ABOUT PEOPLE, BY PEOPLE, FOR PEOPLE

Ludmila Morozova-Buss

Doctoral Student at
Capitol Technology University
Editor-In-Chief

TOP CYBER NEWS MAGAZINE

BRING TECHNOLOGY TO THE FRONT OF THE BUSINESS

Human Centered Communication Of Technology, Innovation, and Cybersecurity



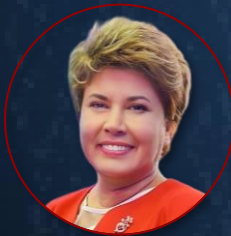
«Top Cyber News MAGAZINE continues to highlight those leaders of cybersecurity that others may not know and at the same time inspiring many others to become our future leaders in a cyber career that is so desperately in need of additional employees»

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



«Thank you Ludmila Morozova-Buss Top Cyber News MAGAZINE for bringing the smile on our faces after long debate hours.»

Liliana MUSETAN, Head of Unit at Council of the European Union. Brussels, Belgium



«Thanks for publishing your MAGAZINE It helps big companies as well as SME and citizens to beware of cyber threats!»

Prof. Dr. Annita Larissa SCIACOVELLI, Professor of International law, Cybersecurity Specialist. Italy



«Ludmila Morozova-Buss fantastic work and keep it up! I love reading about the people in your articles and looking forward in reading more in the future. All the best Ludmila.»

James CASTLE, Chairperson (CEO), Cyber Security Global Alliance & CSGA Cyber Accelerator | CEO/CISO/CSO, Terranova Defense Solutions & Terranova Cyber Solutions | CSO, Terranova Health Network, Canada