BE THE VOICE - CHANGE THE WORLD

RAISE THE CYBERSECURITY CURTAIN

CYBERSECURITY LEADERS QUOTES

Global thought leaders for cybersecurity awareness
Scale-up thinking and strategy for a safer digital world.

By Ludmila Morozova-Buss

FORE WORD

LUDMILA
MORZOVA-BUSS

BE THE VOICE

By their very nature, the privacy and security domains have always maintained a culture of “non-disclosure.” We need to find the right balance between protecting corporate sensitive information and individual data privacy while sharing knowledge and expertise within the cybersecurity community. Knowledge and awareness are vital for businesses to operate securely.

With the profound passion for knowledge in the security domain, I developed the competence and passion of a communication catalyst in the field of cybersecurity - one of the main pillars in the digital economy. As my knowledge increases, my awareness increases.

In the current environment characterized by change and agility; being the voice, standing for new ideas, and sharing expertise is more crucial than ever. I state firmly that this is an important and value-creating mission for a knowledgeable cybersecurity influencer.

Ludmila Morozova-Buss

International Cybersecurity Woman Influencer of the Year 2020.
Ph.D in Technology at Capitol Technology University Researcher, Student.

https://www.linkedin.com/in/ludmilamorozova/

Search no for ranking, search for thinking here. Cybersecurity needs cooperation more than competition.

RAISE THE CYBERSECURITY CURTAIN

Carmen MARSH
CEO Inteligenca

We need more women in cybersecurity.

Not only because we look at things differently, but also because we are the ones that make light out of the darkness.

We are the creators of life we bring into this world to thrive and survive.

We are also the subtle but strong protectors of our families, our communities, and each other.

The world needs us – perhaps now more than ever!

What is your "why" for being in the cybersecurity or privacy field?

Stéphane NAPPO
VP & CISO Groupe SEB

In a boardroom or at a 'nuke proof' data center, a Chief Information Security Officer – CISO 2.0 - participates in creating and protecting digital assets value.

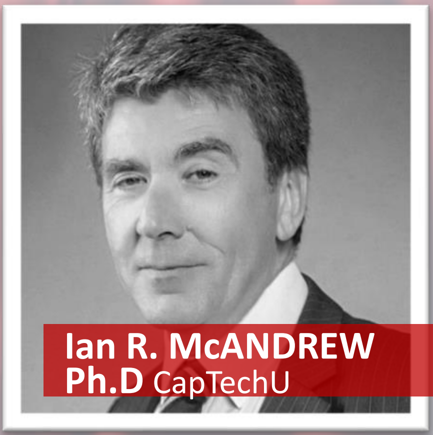
For success in digital transformation, turn comprehensive risk management, and cybersecurity into key business differentiators.

Rather than fearing or ignoring cyber-attacks, ensure your cyber resilience to them.

Chuck D. BROOKS
CEO Brooks Consulting Int.

Cybersecurity is a team effort, and everyone needs to be involved. It starts with basic cyber-hygiene and understanding the threat landscape.

A risk management strategy to meet growing cyber-threat challenges needs to be both comprehensive and adaptive. It involves people, processes, and technologies.



Ian R. McANDREW
Ph.D CapTechU

Cybersecurity is a subject that requires logic, knowledge, thought and commitment. It can be applied or research based.

It is a true leveller for all to enter, be successful and lead the future of cybersecurity.

The modern world is a dangerous cyber world for the innocent now and cyber experts are needed more than ever.

The education of the next generation of Cyber experts must start now, include all those that have historically been limited to be part of this defence of our ways of life.

RAISE THE CYBERSECURITY CURTAIN

Thomas HARRER
IBM Systems EMEA

Increased cyber risks and threats are the backside of increased opportunity of digital innovation.

Companies need to balance both, investment into innovation and focus on cyber risk mitigation.

Tina GRAVEL
SVP AppGate

The faster we run (or Zoom) into Digital Transformation, the more potential we have for digital threats.

Protecting yourself and your company is no longer a "nice to have" but a "have to have" in our current climate of 2020.

Troels OERTING
World Economic Forum

Fighting cybercrime remained an uphill battle. This is not a static number. It will increase unfortunately.

We can still cope but the criminals have more resources and they do not have obstacles. They are driven by greed and profit and they produce malware at a speed that we have difficulties catching up with.

Gary HAYSLIP
CISO SoftBank

Each of us walks our own road during our professional careers, sometimes this road is smooth and straight, but many times it's full of accidents and traffic jams.

What is vital to remember for all of us is we are members of a community, and even with the best career plan, it helps to have friends and peers to speak to and mentors to hold us accountable.

RAISE THE CYBERSECURITY CURTAIN

Samir SARAN, Ph.D
President ORF

Encryption is an idea that is grounded in the principles of data integrity and data ownership. The right to encrypt communications is central to the autonomy that we offer all citizens over their own data and who can use, analyze, and access that data and under what conditions.

This right automatically grants them the opportunity of determining who can commercially exploit their data.

Encryption is perhaps the centerpiece of the falsely dichotomous conversation around security and human rights. Encryption, however, must fundamentally be about human rights.

Cecile MAYE
CEO Megaverse

In our increasingly complex cyber world, humans have never been as powerful and as vulnerable at the same time.

Cyber awareness is essential to ensure long term cyber serenity for all.

Can you imagine driving a car or flying a plane without a licence? It has become impossible to safely surf the world wide web without learning basic behaviours!

Eugene KASPERSKY
CEO Kaspersky LAB

We live in a world that is dependent on digits, which live in digit and which is not protected from hostile penetration.

Aghiath CHBIB
CEO SEECRA

Artificial intelligence (AI) offers tremendous opportunities for the world in general and for the development of national cybersecurity strategies in particular.

It has led to the development of a whole array of different in-app solutions towards fostering growth in productivity, increasing efficiency and, above of it all, providing essential tools to smoothen processes up within Governments and its public institutions.

RAISE THE CYBERSECURITY CURTAIN

Brad SIMS, Ph.D, FRAeS
President CapTechU

Capitol Technology University is focused on providing students great careers in areas needed by industry to drive national economies.

Our award-winning cybersecurity programs are one of our top focus areas. Let us help you today.

Shawn TUMA
Spencer Fane LLP

There is no such thing as being “secure.”

There are always vulnerabilities that could have been found or remediated.

There are always more things that a business could have done to protect its networks and secure its data—and the data of its customers, clients, patients, and consumers—if only it would have devoted more time, money, and resources to cybersecurity.

Christiane WUILLAMIE OBE
CEO PYXIS

Unless you help individual employee to secure their home, mobile environment, their partners, children and elder relatives, you cannot expect them to keep the company's asset secure.

Culture and collaboration is key to reduce data and cyber security breaches.

When will you start leveraging your culture for positive outcomes for customers, employees and scaling your business?

Mikko HYPPONEN
F-Secure Corporation

I see beauty in the future of the Internet, but I'm worried that we might not see that.

I'm worried that we are running into problems because of online crime.

Online crime is the one thing that might take these things away from us.

Andrea MARTIN
IBM Distinguished Engineer

Creating trustworthy AI solutions requires paying attention to a couple of important attributes: Fairness and Anti-bias belong in this list, explainability and transparency, too.

And among several other attributes it's also about robustness and security - we need to ensure no one can tamper with the data and the results, manipulate them or even steal them.

Kris® K.
InfoSec Professional

The ‘effectiveness’ of the ‘efficient’ cybersecurity tools, standards, procedures, and frameworks we pick and choose from, depends on people who we work with.

To ensure that efficiency is followed by effectiveness we ought to respect relationships and value ‘people first’.

Roland LEINS
IBM

"We Live In A Data-Driven World."

More than ever before, data protection and cyber resilience for vital data assets is on the minds and the agendas of business and IT professionals.

Gabrielle BOTBOL
Pentester OKIOK Data

Awareness is no longer an option. Cybersecurity as a popular culture is essential to become a lifestyle.

To achieve this long-term goal, we will need everyone:

- Cybercommunity, already so generous in sharing knowledge, will double its efforts to popularize it;
- Companies by applying privacy and security by design policies;
- Public services by training young people in computer hygiene from early age and by launching national advertising campaigns «Stay safe online».

Chris VELTSOS
Cyber Risk Strategist, Author

CISOs Are Key to Enabling the Cognitive Enterprise!

The cognitive enterprise is an organization with an unprecedented level of convergence between technology, business processes and human capabilities, designed to achieve competitive advantage and differentiation.

Isabel María GOMEZ
Continuity Transformation Lead

In crisis times, where your company's strengths will test your resistance, tenacity, and decisions, always remember that we will have a huge opportunity to protect and transform your IT processes.

Take the lead and change the traditional business continuity model for a new neuronal network resilience model that enforce cybersecurity improving from BAU activities to cybersecurity goals for the business.

This is a “must have” for achieving an efficient transformation of your processes, reducing costs, and improving availability and usability for our own teams, stakeholders and technological providers in collaboration with our third parties, looking to exceed our customers’ expectations.

Claudia Mendes SILVA
Project Manager Siemens

Parents and educators are powerful role models for children.

By giving them chances to experiment all fields, learn from failures, accept the risks and embrace diversity, you will be contributing to more equal and balanced world.

Create the awareness of safety online and educate your children about the importance of safeguarding their personal information.

Ginni ROMETTY
IBM

We believe that data is the phenomenon of our time. It is the world’s new natural resource.

It is the new basis of competitive advantage, and it is transforming every profession and industry.

If all of this is true—even inevitable—then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world.

Emilio IASIELLO
Cyber Intelligence

As air traffic management systems become increasingly sophisticated and reliable, they also become more vulnerable to cyber attack from bad actors.

As we develop more and more tools to increase our interconnectivity, we must also develop the methods to protect them.

Steven C. MORGAN
Founder Cybercrime Magazine

Cybercriminal activity is one of the biggest challenges that humanity will face in 2021.

Global cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

Marilise de VILLIERS
Founder CEO Author

My motto is: Work hard, play hard and be kind.

I believe that an organisation can only become truly successful by investing heavily in its people and creating safe and inclusive environments where everyone can thrive – be at their best – and make their organisations more resilient.

People have to become the strongest defence against cyber-attacks. I developed a proven approach that helps organisations tangibly reduce human risk and embed secure mindsets and habits into their cultures.

Jiwat RAM, Ph.D
Professor La Rochelle BS

The next big thing in technological evolution is not what AI can do, but it is what women can do to define the journey of that evolution.

Cyber-security is a mantra for survival in today's information age. A lax approach towards cyber-security could not only result in loss of data, but could well put someone's personal life in undesirable hands.

RAISE THE CYBERSECURITY CURTAIN

Heinz V. HOENEN
Credit Suisse

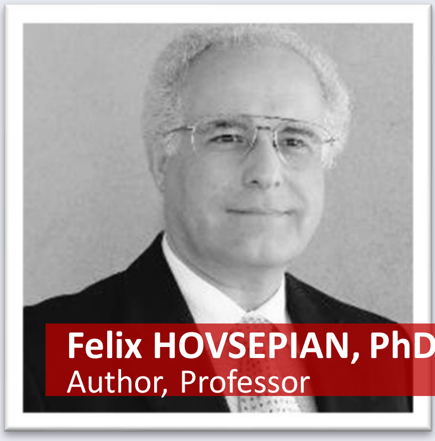
Businesses face an arduous task, from the discovery of a data breach to forensic investigation to notifying customers and the public about the attack.

The task becomes less arduous with the help of incident response planning.

Victoria BECKMAN
Privacy & Data Security

Safety comes when people have their needs met and do not feel threatened.

If societies elevated their approach of an individual's digital identity to be treated with as much care, respect and tolerance as their physical one, we would all be in a much safer world.



Felix HOVSEPIAN, PhD
Author, Professor

Some are aware that Alan Turing was involved in cyber security during WWII, some have even heard of Joan Clarke, but how many are aware that a significant portion of the workforce involved in this effort were women?

Kevin MITNIK
CEO "White Hat" Hacker

The key to social engineering is influencing a person to do something that allows the hacker to gain access to information or your network.

Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business.

Dawn KRISTY
VP Cyber Solutions

The combination of lucrative business for hackers and fraudsters, increased use of internet-connected devices, and remote work cybersecurity vulnerabilities create a “perfect cyber storm”.

Holistic cyber risk management including cybersecurity, cyber risk awareness training to decrease human error, and cyber insurance will help businesses weather the storm.

Scott SCHOBER
CEO Berkeley VS

Most females are not encouraged to ever consider a path in engineering. Within my own company, there have only been a handful of female engineers over the years that we have employed.

I recently posted a job for a Senior Software Engineer on http://LinkedIn.com & http://Monster.com and received over 50 resumes. Out of those 50 resumes, there was not a single woman that applied for the job.

This anecdotally tells me there is a real shortage of women in the job market for software engineering and the broader tech industry too.

Anzar HASAN
Founder LTESecurity

Compliance is not Security and do not assume PCI-DSS covers HIPAA, CCPA and GDPR!

It is your illusion that security tool will solve all your problems.

Right tool and right configuration are the key for the successful deployment based on your environment.

Copycat approach never works in security.

Steliyan PETKOV
CISO iCard

One of the most talented, dedicated and inspiring cybersecurity professionals that I know are women.

Therefore it is unacceptable that the cybersecurity field is mainly dominated by men.

Dear women, the barriers to achieving what we want are mostly within ourselves!

Just take the path of cybersecurity and you will have all our support!

RAISE THE CYBERSECURITY CURTAIN

Stewart SKOMRA
CEO Vanderplaats R&D

Cybersecurity is maintaining the sanctity of the individual. We Humans love to create our own illusions such as 'Government', 'Corporation', 'Organization' when these are all simply people - individuals choosing to apply their industry - their diligence - as one.

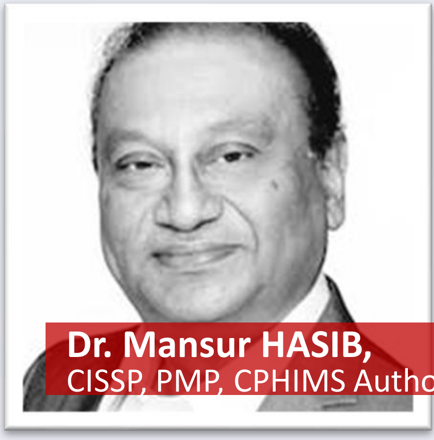
Cybersecurity needs individuals with the perspective of Emily Dickinson: 'If you take care of the small things, the big things take care of themselves. You can gain more control over your life by paying closer attention to the little things.' ~ Emily Dickinson, 1830 – 1886"

Anna ABKOWICZ, PhD, EMBA Société Générale

Technology touches every part of our lives, and as a result cyber threats are present in every aspect our daily lives.

We must make cybersecurity education an integral part of our culture, taught and evangelized at all ages.

Only through this comprehensive effort will we burn cybersecurity into our DNA and create a true global culture of security.



Dr. Mansur HASIB,
CISSP, PMP, CPHIMS Author

Cybersecurity is people powered perpetual innovation.

Do not play someone else’s game that is already rigged against you! Instead, change the game.

Vishva VAGHELA
Penetration Tester, Researcher

To excel in the task and secure the deal, in cybersecurity (digital forensics) you always got to dig in deep. For profound is the power of self-confidence based on knowledge and expertise!

Being a digital forensic enthusiast, I am focused on learning and exploring the magic of cybersecurity. Significant is simply the force certainty dependent on information and aptitude!

RAISE THE CYBERSECURITY CURTAIN

Natalia OROPEZA
CCSO and CDO Siemens

"I have often been the only woman on the board, or in meetings."

"I think we need the female perspective in technology."

"The skills shortage is due to the requirement for cybersecurity to grow very quickly, because digitalization is increasing very fast"

"I think universities are not yet aware or prepared to develop the type of professionals we need in cybersecurity."

"We need complete professionals, meaning people who can communicate and work in teams, and are able to influence and lead others..." "These are the kind of cybersecurity professionals we need." Natalia Oropeza for Bloomberg.com

Gergana (KIRYAKOVA) WINZER Unisys

Saving cost and rationalizing while mitigating the cyber risks will make the difference between the successful and wanted CISOs/ CSOs and the rest.

There will be the need to 'know what they do not know' today in order for them to protect the future reputation, financial exposure and the critical assets.

That need may mean deeper conversations, more time spent in understanding the people, the culture, the business holistically, the risks associated with cyber threats (or threat actors) exploiting vulnerabilities.

Jochen POETTER
IBM

Nearly 20% of all cyber-attacks hit small businesses with 250 or fewer employees.

Roughly 60% of small businesses close within six months of a cyber-attack.

Disaster Recovery is no longer just traditional backup of data, in today's world, it embraces more modern concepts such as data reuse, security, air gap, multi-cloud and cyber-resilience.

Protect data to stay alive.

Denae BROOKS
USAA Senior Risk Analyst

In a world where no organization is immune to potentially devastating events like data breaches and ransomware, leaders must commit to doing more to educate, empower, and arm its people against phishing and other social engineering threats that could result in high impact situations.

One way organizations can do this is through implementing strategically targeted security awareness programs driven primarily by the organization's most valuable data, its internal threat intelligence.

RAISE THE CYBERSECURITY CURTAIN

Vincent ROMNEY
Enterprise Security Architect

While Security Operations Centers (SOCs) will continue to leverage algorithmic approaches to anomaly-detection and response actions, cybercriminals will continue to leverage advanced mathematics so move more stealthily through a compromised network.

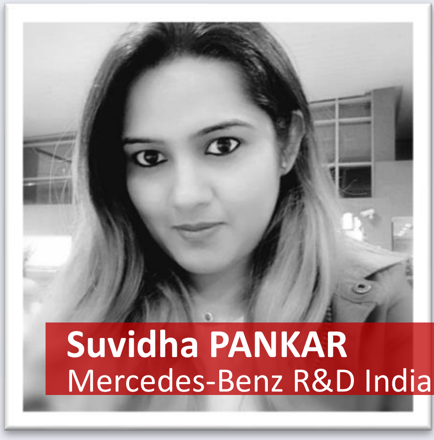
Legitimate business will only win this arms-race with the direct involvement of governments around the world providing increased funding to drive defensive innovation and literally out-spend the criminals.

Paul de SOUZA, CSFI
Cybersecurity Forum Initiative

A new paradigm shift occurs in the cybersecurity industry, with an apparent convergence from node protection at the edge to in-depth data protection buried deep inside our networks.

The separation between cyber and other elements, such as electronic warfare and information operations, has created multiple stovepipes.

The challenge is to more effectively integrate those capabilities to produce information warfare outcomes.



Suvidha PANKAR
Mercedes-Benz R&D India

For me cybersecurity is like spectrum that is not specific to one set of output from the experience you have, it varies across the continuum.

It's true leveller through continuous learning and getting deeper in order to see the light of logic, knowledge, thought and commitment from the Prism.

Ken MUIR
vCISO LCM Security Inc.

We are Losing the Cyber War.

My experience has taught me that there is a significant disconnect between industry recommendations and what is being practiced.

2021 will see a three-fold increase in security breaches, so building a security strategy following industry standards such NIST, will reduce your risk and increase your security, and may just save your business.

Sailaja VADLAMUDI
SAP Labs India

Cybersecurity is not just technological it is more existential.

Cyber Security is one profession where we have all roles in it. Technical, Legal, Process, Program management, Insurance, Audit so on...

Patience, Passion and Purpose are the key driving forces and success mantras for any of the profession in this role.

With over 560 million internet users, India is the second-largest online the market in the world, this shows the volume of the challenge we have In front of us. Cyber attacks are on a quantum leap.

Ilana BIDERMAN
Tech PM DigitalOne

Cybersecurity is like a clock on the wall you don't pay much attention to until it's broken.

Take it out of the system, and the data, events, projects, money, assets, people, all you care about become a disaster.

Work on prevention, have a recovery plan, update your tools, strategies, and methodologies.

It will give your company a peace of mind and value many years to come.

Monte MASSEY
Director MARSOC SOCP

A second generation of cyber security products made by a second generation of thinkers are on the horizon to change everything we know about cyberspace.

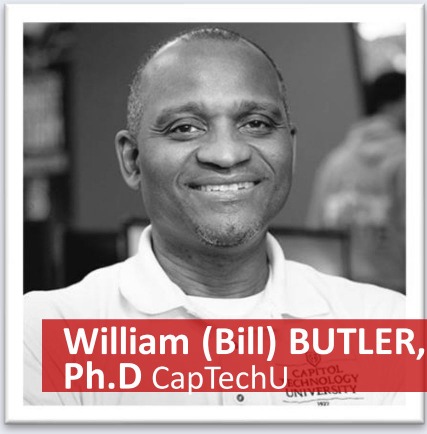
We could think outside of the norm and find new approaches.

Software/ hardware architecture should be inspired to solve problems.

Aaron BISHOP
CEO Eigenspace

What if Cybersecurity teams shifted from reacting to regulation and known threats and focused their spending on true Cybersecurity protections (where compliance is a byproduct, not the focus) and because a true holistic Cybersecurity posture is in place, it transcends specific attacks rather than chasing to protect the known attacks?

RAISE THE CYBERSECURITY CURTAIN



William (Bill) BUTLER, Ph.D CapTechU

This is truly the 911 moment for the current generation (Can anyone recall what life was like prior to March 2020?).

The pandemic has long term implications both for our economy and our very way of life.

The way we view cybersecurity must change in these times as the virtual boundaries of our enterprise networks now extend into the bedrooms and home offices in millions of homes across our nation.

Diana KELLEY
CTO SecurityCurve

Attackers are getting better at targeting at-risk industries and critical infrastructure. We saw this happening during the early days of COVID when health systems and aid organizations were targeted by human-operated ransomware gangs.

Unfortunately, I expect this trend to continue into 2021 resulting in an increase in ransomware and malware being used to interrupt activity in industries like healthcare, government, and energy.

Mike HAROUNOFF
Unisys

Every Public Sector organisation is under pressure to protect its citizens' data from GDPR, FOI and most potently, cyber attack.

It is not a question of if, but when?

Prevention is not the answer, it is normally too late.

It is now about how quickly you can respond and how resilient your organisation can be.

A Zero Trust approach with dynamic isolation will help save taxpayers' money, avoid reputational damage and give confidence as the custodians of protecting valuable citizen data.

Philip MURRAY
Consultant DigitalXRAID Ltd

We face an uncertain future.

The good news is that we have the power to inspire this and future generations to being safe.

This starts at the top, from Politicians through to CEO's these are the people who can inspire change and increase the awareness needed to help create a safer future.

Vincenzo AQUARO
United Nations Digital Gvt.

When we deal with cybersecurity in public sector, sometimes we put too much attention to build resilient and secure infrastructures, forgetting the importance to build - at the same time - a trustworthy and accountable public governance.

These two aspects go hand to hand and have to be seen as the two sides of the same coin.

Stijn Van IMPE
Unisys

Are there rightfully more important things to worry about today than internet security?

Or are we at risk of collectively casting a blind eye over the sophisticated multi-layered attacks that are only set to increase?

And when COVID-19 caused the majority of us to work from home, did we simply assume our corporate security would stretch out?

Linda F. MARTIN, Ph.D
Capitol Technology University

Occupational health and safety professionals need to incorporate a strong working knowledge of cybersecurity protective measures into their facility management plans, construction sites, recordkeeping, and other aspects of safety management systems.

Lack of cybersecurity awareness and the related cutting-edge protections at the operational and project levels can result in massive critical infrastructure and financial damages.

Louis COLUMBUS
Principal Dassault Systemes

Cybersecurity's fastest-growing skill areas reflect the high priority organizations place on building secure digital infrastructures that can scale.

Cybersecurity professionals with cloud security skills can gain a $15,025 salary premium by capitalizing on strong market demand for their skills in 2021.

DevOps and Application Development Security professionals can expect to earn a $12,266 salary premium based on their unique, in-demand skills.

413,687 job postings for Health Information Security professionals were posted between October 2019 to September 2020, leading all skill areas in demand.

RAISE THE CYBERSECURITY CURTAIN

Bill STANKIEWICZ
CEO Savannah Supply

I have seen many small city governments get hacked in 2020. For 2021 we can see more bad guys going beyond the individual targeting to many more businesses.

If you have a weak authentication process and limp verification practices, you can expect social media based assaults to be successful.

María ISIDRO
1600 Avenue & 1600 Cyber GmbH

In order to inspire more girls and women to join Cyber, we need to create spaces where they feel safe and adjust the messaging, so they feel comfortable and supported.

The narrative used about the lack of women in the field should be reconsidered.

Andrea ANDERNACH
IBM

Life is a continuous learning journey. The same applies to Cybersecurity - so constant adoption, learning and resilience is key to stay ahead of the threat!

Since Covid-19 more and more children are exposed to the Internet due to home schooling and thus it is more than ever important to explain and educate them on the danger of the cyber world to ultimately protect them of exposure and to chaperon them navigating safely and comfortably thru this cyber jungle.

Sarah-Jayne GRATTON, Ph.D Influencer Author

Information is the beating heart of industry and the data encapsulating it, its soul.

If you respect this fact, then you'll embrace cybersecurity as the guardian of your businesses heart and soul.

Patricia LEWIS
Sales Executive F5 Networks

The front line in cyber is shifting, this shift is driven by attractive economics for the attackers.

An explosion of available stolen credentials, new advanced attacker toolkits, and cheap global botnets to rent have all contributed to making large-scale, automated attacks against web & mobile applications very inexpensive, fast and easy to launch, and potentially quite lucrative.

The need for innovation in fraud prevention becomes more urgent when you factor in the accelerated shift to online channels driven by the current global health situation.

Debbie BLACK
Independent Advisor

As an International Chief Executive and a woman, cyber security has been a top priority for me over the past 30 years.

From educating and ensuring my daughters could not be identified on social media, through to protecting the companies I influence.

That means ensuring that cyber security strategies are listed as a top risk mitigation priority for governance controls at the board level. Staff get busy and distracted, to rely on them to protect the company by not clicking on certain emails will not happen.

Cyber security is a systems issue which needs professional controls and professional people hired in, to protect the staff, company and shareholders.

Diane GANDARA
VP Sales ioSENTRIX

Passionate, trailblazing cybersecurity professional leader, strategic thinker, community leader, educator, mentor with a vision that all people of diversity will be respected and included, as we orchestrate security across the nation during the digital transformation age.

We will do this TOGETHER and without borders, cause we are BETTER TOGETHER.

Ruth HOUBERTZ, Ph.D
Senator of Economy Europe

Each challenge in life delivers new opportunities for professional and personal lives, the ways how we interact on all levels.

Aside of all negative impact, Covid-19 has led to a significant speed in digitization, a different way of how companies present and do their businesses, the creation of new business models, among many other achievements. The employment of novel technologies such as AI, Neural Networks, and Quantum Computing becomes more and more important.

People are aware of fast changes in these technologies, with a huge portion of fear, particularly from people which are no techies. We need to supply a framework of Cyber Security and transparent and understandable communication for all people on all levels to foster these changes we are facing in the next years.

Margaret MORTON
Forbes Technology Council

Cybersecurity is edifying, as a culture and a career, and it is thrilling to see a focus on educating both professionals and our children - as young as kindergarten.

In a direct response to the growing impact of computing and data in an ever-changing digital world, universities across the nation are opening schools, forming research centers and offering new data-driven majors to meet the demands of the workforce. And they are betting that students will follow.

Roman V. Yampolskiy, Ph.D

On Controllability of Artificial Intelligence

Roman V. Yampolskiy
Computer Science and Engineering
University of Louisville
roman.yampolskiy@louisville.edu

Invention of artificial general intelligence is predicted to cause a shift in the trajectory of human civilization. In order to reap the benefits and avoid pitfalls of such powerful technology it is important to be able to control it. However, possibility of controlling artificial general intelligence and its more advanced version, superintelligence, has not been formally established. In this paper, we present arguments as well as supporting evidence from multiple domains indicating that advanced AI can't be fully controlled.

Consequences of uncontrollability of AI are discussed with respect to future of humanity and research on AI, and **AI safety and security**. This paper can serve as a comprehensive reference for the topic of uncontrollability.

Christophe AUBERGER
CTO, CISO Fortinet

As 2021 approaches, it is obvious that the cyber threat will be more present, more sophisticated and more efficient at the same time as the attack surface of companies will be increasing.

In order to have a more proactive approach to this risk, a trend will be the implementation of fusion center, it is an entity merging the functions of SOC, CERT and cyber threat intelligence.

One of the major challenges for these entities will be the ability to sort, store and process a huge and growing mass of data.

Mani Keerthi NAGOTHU
Ballard Power Systems

The uniqueness of cybersecurity is that there is something new every day and something new to learn. There is so much to learn from the past, in the present, and the future.

We need to adapt ourselves to the changing risk landscapes and innovate new solutions for the evolving challenges and threats. Keeping ourselves prepared and updated is a way to address emerging trends.

From a proactive perspective, focusing on what do we know, why there is a gap, how we can address it, where we need to improve, what we need to do better is a step in that direction.

Dan GOLDBERG
Principal Partner Cybza

Cybersecurity is a constant battle where only all together we win!

Cyber Security has never been as important as now!
Globally business was forced-migrated to digitally transformed working without planning.
Uncertainty in our normal way of life has opened opportunity to phishing and scams.
Home infrastructure and adaptions integrated into business networks, unpatched and unknown.
Situations open and unremedied ripe with risk, vulnerability and open to exploit.
How we beat this is by growing community knowledge and action.
By diversity of people and culture our ideas grow.
Cybersecurity is a constant battle where only all together we win!

Zoe BRAITERMAN
PurePoint International

Building YOUR cybersecurity career starts with YOUR decisions to feed your curiosity and build upon your knowledge base and skill set, or step up as a security champion within your current organization or profession.

For example, software developers may want to start exploring application security (AppSec), and network engineers may want to start exploring network security.

It’s important to simultaneously seek mentorship and mentor others, at any given point in your career.

JP Cavanna
Cybersecurity Strategy Lead Unisys

We need to adopt a new approach to security that is focused on shifting business culture, mindset and trust to provide optimised outcomes and durability.

Resilience accepts shocks will occur and the organisation’s power of response is as important as its power of control because, after all, it’s every bit as much about cyber resilience as it is cyber security today.

Rizwan AFSHAR
CEO Business In Motion

Anything & Everything that is digital is hackable.

Cyber, Electronic & Digital Assets security is paramount in today's World of Digital Transformation.

And awareness, constant applied knowledge, education & action staying ahead of the threats is imperative.

RAISE THE CYBERSECURITY CURTAIN

Diane M JANOSEK
Training Director NSA

Cybersecurity is a chain link fence.

Each connection must endure.

Each link needs the others as it only takes one crack to break the defenses of all.

Cybersecurity professionals help each other to not be the weakest link.

Let’s celebrate the amazing solidarity of Cybersecurity community!

Frank FEATHER
CEO Quantum AI Future

Quantum Computing will transform Artificial Intelligence into Advanced Intelligence, superior to humans.

Quantum Advanced Intelligence or QAI will ensure Quantum Advanced Cybersecurity, as it must in order to preserve privacy in every dimension.

That is the future I see this decade.

And the ethics of that future will be driven by women and men together.

Nathan CHUNG
Security Architect EY

Women in cybersecurity represent our wives, our mothers, our daughters, our sisters, our nieces, our cousins, and our friends.

Girls in school and young women entering the workforce today will become the future leaders of tomorrow.

Men and women need to work together to solve the world’s cybersecurity problems of today and prepare for the security challenges in future technologies yet to come.

Richard LANDER STOW
Security Solution Architect Unisys

With malicious agencies and ever advanced malware targeting big business to make an "easy buck" with ransomware, what can you do by focussing your time and budget to significantly reduce the risk that you are a headline news story tomorrow for all the wrong reasons?

The Zero Trust approach can be implemented tactically as you build towards a practical solution to many of your security problems.

John WALKER
Nottingham Trent University

2021 will see an increase in Ransomware attacks, and more in depth State Sponsored activities out international adversaries.

Successful Cyber Attacks will continue with more high profile companies falling to compromise.

Sadly, 2021 will not be the year we see real steps taken toward Cyber Resilience - but it will be the year in which we encounter a more serious mindset toward addressing the aspect of Cyber Security.

We may have to wait for 2022 and beyond to see those thoughts formulate into tangible action.

Bonnie BUTLIN
World Economic Forum

Despite the current issues regarding inequality for women within security, we must continue to address this imbalance through the provision of more recognition and opportunities for women currently working in security, in order to show that there is indeed a successful career path available during these extraordinary times.

Denis PUKINOV
CISA EuroChem Group

We get eternity in our kids and they depend on us, please, be kind, open, curious, smart and think about their privacy.

Frank SATTERWHITE
Founder & CEO, 1600 Cyber

It’s time we embed social consciousness into organizational strategies.

Communities have caught great attention from businesses in 2020, related to systemic racism, mental health, human rights…it’s time we fully align businesses to support our communities.

By creating more positive role models, providing more opportunities, and generating safe spaces, we can truly inspire underrepresented groups to join cyber security, fostering inclusion, and equality.

RAISE THE CYBERSECURITY CURTAIN

Anastasios ARAMPATZIS
European IT Certification Institute

As cybersecurity professionals we have spent countless hours "preaching" about security policies, best practices, frameworks and controls.

Despite our rigorous and heartfelt efforts, I have the feeling that we are failing.

We are failing because there is a security awareness gap in our societies.

Our message fails to reach the most vulnerable groups, our kids and our elders.

Collectively, government and private educational institutes should embark on a mission to provide engaging, motivating training programs for all – kindergarten kids to grandparents.

We all use technology. It is time to learn to use it safely and wisely.

Chloé MESSDAGHI
VP of Strategy Point3 Security, Inc

Misinformation, apathy, and burnout places security at risk for companies.

When security is comprised, companies lose the trust of their customers.

Without customers, you do not have a product and or a company.

Thus, it's critical to understand the importance of security and invest in it.

George Platsis
Director, Cybersecurity FTI Consulting

We Didn't Consider the Security Risks!

We were — understandably — looking to move online at the speed of business. Or perhaps, more appropriately nowadays, it is better to say at the speed of convenience.

Business and innovation forced us to look for efficiencies in order to gain an edge. We moved from wanting it fast to wanting it instantly.

Kris RIDES
CEO Tiro Security

I've seen some of the most technically gifted cyber security individuals struggle to get a job or achieve the career path they want.

Within security, the most important skill to develop is communication. Written and verbal communication holds the key to not only getting a job, but also to creating a fast moving career path.

Even if this is something that does not come naturally to you, it can be worked on and improved. For some, it will take courage and effort. I've seen it done, and trust me, you can do it.

RAISE THE CYBERSECURITY CURTAIN

Victor van der KWAST
Supervisory BM Anadolubank N.V.

This current perfect storm, with dropping revenues, COVID 19, rising costs and increasing digital business and consumer traffic will force companies to rethink their strategic models of delivery, products and profitability that embraces more digital and AI mechanisms.

It creates a sense of urgency amongst leaders to step up their efforts to change business models, office space and people agenda.

Chase CUNNINGHAM, Ph.D
Principal Analyst Forrester

What exactly is Zero Trust?

For those of you who've been hiding away in a cave for the past decade, Zero Trust (ZT) is a concept founded by Forrester alum John Kindervag in 2009 that centers on the belief that trust is a vulnerability, and security must be designed with the strategy, "Never trust, always verify."

Andy JENKINSON
Group CEO CIP Cryptography

From hand combat to keyboards, the cyberwar is raging all around us. The basics can secure you or be used to attack you.

An easy guide to cyber security and encryption...

Depending on which side you stand, a door can be an exit, or an entry point. A door can provide secure access, or secure the contents inside.
In the digital world, every connected organisation has dozens or hundreds of doors, known as domains or websites. Every one relies upon a digital certificate to be secure. These domains allow secure access, both in and out, typically for trade.
The challenge occurs when the digital certificates expire or are non matched with the domain meaning there is no encryption. It is also at this stage, a metaphorical flashing beacon alerts every cyber criminal to the fact and that there is unencrypted data fest to be had.

Kimberly MENTZELL
Adjunct Professor Cybersecurity

In the digital landscape, cybersecurity education is essential to the success of future generations.

We need to not only convey current concepts and techniques, but to inspire students to think beyond current conventions and cultivate new ideas.

RAISE THE CYBERSECURITY CURTAIN

Andre MEYER
Security Lead Accenture

Technology in security is important. It helps to minimize the potential for human error by facilitating and automating complex, recurring tasks.

But in the end, all technology is developed by humans, configured by humans and operated by humans. Your employees are the most crucial, single point of failure in any operation.

Neglecting the human factor can have the most dooming consequences.

Jan BARBOSA
Global Brand Ambassador beBee Inc.

Hacking attacks have been in a frenzy lately, the Sony Hack, PlayStation Network Hack, Icloud leaks of celebrity photos and even the wearable health-oriented device "Fitbit" have been hacked providing information on the wearer daily habits.

Cybersecurity evolves rapidly to foil these daily attempts to erase, steal or ransom data every day, but sometimes the hackers win and precious information becomes part of the open markets.

So here goes the question, if the biggest names in the business like Microsoft, Sony and Apple can be hacked, how secure can I be? More so when our common devices like cars, televisions, and refrigerators are becoming "smart"?

Michael HOFFMANN
Digital Strategist

While the digital transformation is advancing rapidly, companies around the world are generally, and in particular, being forced to adapt to a variety of challenges.

Given financial constraints, increasing work from home, fewer staff and more frequent interruptions in the supply chains for IT equipment in addition, new risks for IT security exist already.

An important role for future-oriented security in information technology plays, for example, the increased use of artificial intelligence (AI).

The use of AI can potentially increase the precision and efficiency of cyber analysts.

Alexandre BLANC
IT & CyberSecurity Director

Our generation, and next generations, deserve common sense and understanding.

Cybersecurity awareness, and privacy protection is our duty, to give a chance to defend freedom.

Freedom of thinking, moving, and speaking.

I started the connected=hacked and cloud=leak communication, in order for decision makers to ask questions about security when they initiate project.

My hope, through my growing audience, is to get privacy and security better integrated in the processes, from the get go.

Security by design, instead of bolted on (post incident) security.

We should not be the product.

RAISE THE CYBERSECURITY CURTAIN

Prince Albert of Monaco

"Today, we live in a world where digital is everywhere and is impacting everything from business to education and from health to government.

It is an absolute priority for me and my government that the Principality be on the front line of the digital world."

Prince Albert of Monaco for Forbes

Pascal ANDREI, Ph.D
CSO Airbus

System limitations and flaws can result in the intentional or unintentional destruction, interruption, degradation or exploitation of the data, systems and networks that are critical for safety of an airplane.

As such, cybersecurity represents a fundamental element of cyber resilience that, in turn, contributes to business resilience.

Kirk BORNE, Ph.D
Booz Allen Hamilton

The two greatest applications of emerging digital technologies, such as AI and Blockchain, are healthcare and cybersecurity.

As we are seeing this year, the convergence of concerns around health data security has forced a convergence of attention on this challenge across all organizations and sectors.

Cybersecurity never should have been only one department's responsibility.

It must also be a corporate culture, a way of thinking, a part of all training, and top of mind for everyone.

Only with multiple diverse perspectives on the cybersecurity challenge will we see our way forward in addressing it.

Joris den BRUINEN
The Hague Security Delta

Cyber Security is about technologies, process and people. All people included: man and women, young and old and whatever sexual orientation, cultural background or religious beliefs.

We need to educate the people to make our world more cyber resilient and have the cyber talent for this market.

To be successful we need all the necessary and available talent. We simply could not ignore women, because this way we leave 50% of the labour market talent behind.

I commit to give these (female) talents a podium now, in 2021 and towards the future.

After WORD

With a clear grasp of systems theory and revelation of pervasive, persistent, and resilient interconnectedness, I set out on the journey to interact with 100 "best of the best" Cybersecurity / Information Security professionals to learn about their own EXPERIENCES and gain INSIGHTS from their personal perspectives.

I was truly blessed to have had a wide variety of insightful conversations with leaders who are serving their organizations at various levels.

I sincerely wanted to expand the impact of the lessons I learned from these interactions by sharing them with Cybersecurity enthusiasts around the globe - people who are paving their own way towards a successful Cybersecurity career.

I hope readers will gain insights into how they can guide their career path to the success they desire and benefit the global security community through their unique contributions.

I am thankful to all who have contributed towards this effort and wish all incoming aspirants striving for success in the cybersecurity world, my very best.

To all those who voted for me in the International ‘Cybersecurity Woman Influencer of the Year' 2020, my heartfelt and sincerest gratitude to you all. You have helped to further my goal of generating the interest needed to encourage more women to join us in this field.

Thank you!