TOP CYBER NEWS MAGAZINE

FEBRUARY 2022

Chuck D. BROOKS

BROOKS CONSULTING INTERNATIONAL

CHANGING the CYBERSECURITY AWARENESS

May THE Techs Be With You

Exclusive article by

June R. KLEIN

CEO at Technology & Marketing Ventures Inc.

Co Executive Producer "*4 Days to Save the World*" TV Series

HOW CHUCK D. BROOKS IS CHANGING CYBERSECURITY AWARENESS REACHING THE RIGHT MIND AT THE RIGHT TIME. STEP BY STEP. RAISING UNDERSTANDING OF THREATS IN CYBER REALM


The Evolving
Industrial Metaverse Stirs
New
Strategic Challenges
for
Cybersecurity
Initiatives

We Do Not Have The High Ground Against Our Adversaries

Editorial by Ken MUIR

Information Technology And Cybersecurity Leader

"In Sun Tzu's The Art of War, military leaders are advised to take the high ground and let the enemy try to attack from a lower position."

Well, we do not have the high ground against our adversaries. We have never had the high ground. Companies have been losing $100Ms since the 1990s and we are on course for losses in the $trillions. The only thing that is different now is the level of awareness, and more importantly, the level of acceptance that we are in a war for the very survival of our industries, economies and way of life.

In Canada, as an example, we lost a one-hundred-year-old company because of IP theft from a nation-state that ultimately cost the jobs of almost 95,000 people worldwide. While we continually charge up that hill trying to gain the high ground, the casualties keep mounting. Various government bodies have designed aggressive legislation to fine companies for lack of adherence to good security practices, but this is clearly not working.

We have created solutions too complicated for an average business to understand. Every day, there is a new widget or service that is designed to solve this problem. However, as we keep seeing, more and more organizations are falling victim, and the perpetrators by and large are getting away with impunity despite all of these innovations. Part of the solution is that organizations should take basic steps that are not expensive or complicated. More importantly, we need international cooperation to punish those countries that are sponsoring cybercriminal organizations. We have precedence for this in other areas, so why not here.

"By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemies must be divided." ~ Sun Tzu

We are going through a cyber-specific Darwinian period in our evolution where only the strong will survive through adaptation. It is time to stop saying, "let us sit down and figure this out!". It has already been figured out! We have tools, techniques and proven methodology.

"Cyber Security Is No Longer Enough. Businesses Need Cyber Resilience."

Ken MUIR

Technologist since 1993, globally recognized information technology and ybersecurity leader, Graduate of an Electronics and Electrical Engineering program, vCISO to a multitude of organizations.

Chuck D. BROOKS

United States of America

Chuck D. BROOKS, President of Brooks Consulting International

Mr. Brooks is a globally recognized thought leader and subject matter expert Cybersecurity and Emerging Technologies. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named by Thompson Reuters as a "Top 50 Global Influencer in Risk, Compliance," and by IFSEC as the "#2 Global Cybersecurity Influencer." He was featured in the 2020 Onalytica "Who's Who in Cybersecurity" – as one of the top Influencers for cybersecurity issues. He was also named one of the Top 5 Executives to Follow on Cybersecurity by Executive Mosaic. He is also a Cybersecurity Expert for "The Network" at the Washington Post, Visiting Editor at Homeland Security Today, Expert for Executive Mosaic/GovCon, and a Contributor to FORBES.

In government, Chuck has received two senior Presidential appointments. Under President George W. Bush Chuck was appointed to The Department of Homeland Security (DHS) as the first Legislative Director of The Science & Technology Directorate at the Department of Homeland Security. He also was appointed as Special Assistant to the Director of Voice of America under President Reagan. He served as a top Advisor to the late Senator Arlen Specter on Capitol Hill covering security and technology issues on Capitol Hill.

In industry, Chuck has served in senior executive roles for General Dynamics as the Principal Market Growth Strategist for Cyber Systems, at Xerox as Vice President & Client Executive for Homeland Security, for Rapiscan and Vice President of R & D, for SRA as Vice President of Government Relations, and for Sutherland as Vice President of Marketing and Government Relations. He currently sits on several corporate and not-for-profit Boards in advisory roles.

In academia, Chuck is Adjunct Faculty at Georgetown University's Graduate Applied Intelligence Program and the Graduate Cybersecurity Programs where he teaches courses on risk management, homeland security, and cybersecurity. He was an Adjunct Faculty Member at Johns Hopkins University where he taught a graduate course on homeland security for two years. He has an MA in International relations from the University of Chicago, a BA in Political Science from DePauw University, and a Certificate in International Law from The Hague Academy of International Law.

In media, Chuck has been a featured speaker at dozens of conferences and webinars (Recently, Chuck briefed the G-20 Energy Conference on operating systems cybersecurity). and has published more than 200 articles and blogs on cybersecurity, homeland security and technology issues. His writings have appeared on AT&T, IBM, Microsoft, General Dynamics, Xerox, Cylance, Checkpoint, and many other blogs.

Changing Cybersecurity Awareness Step by Step

This interview is courtesy of **Ludmila M-B**, Doctoral Student at Capitol Technology University & Founder, Editor-In-Chief at Top Cyber News MAGAZINE and **Chuck D. Brooks**, President of Brooks Consulting International.

[Ludmila M-B] In our chaotic world, where in unison, the media contributes to the culture of fear, a mysterious mistress - the cybersecurity is, in reality, more spoken about than understood.

Overwhelming flow of capital, technologies, and skills into the field of security, including the cyber security attract 'white' and 'black' players – 'Lords of Order' and 'Lords of Chaos'. Multiplied by wild ambitions of the world's military superpowers, here we are, standing in front of the Apocalypses at its best!

More often than not – undetectable; unseen and invisible for a non-professional; indistinguishable; hidden; unknown, cybersecurity is a force just like electricity and gravitation and must therefore be considered as the fact rather than the fiction.

While the idea is somewhat extreme, there is no disagreement that it is happening. The condensing of the artificial intelligence worldwide that affects lives of billions of people around the globe can also mean the rapid increase of cyber threats.

In the industrial metaverse era, a sensitive place of the worldwide integration of current and future emerging technologies, aim to regain control of your cyber ecosystem, then cybersecurity will serve as your business enabler.

"Thinking About Tomorrow, Think How To Create Value For The Future Of Industry And Society"

Cybersecurity. What it is not?

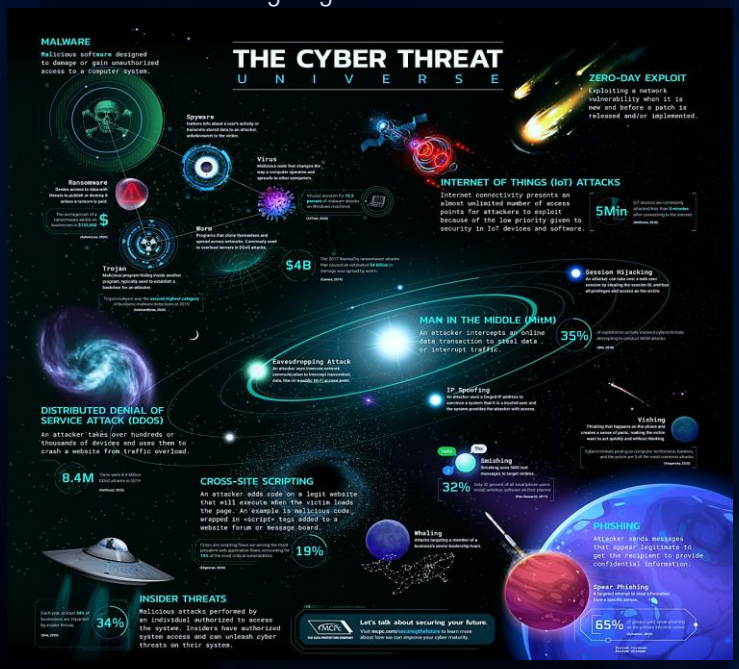
With this and a few more questions I am proud and honoured to invite Mr. Chuck D. Brooks – one of the world's renowned experts and the industry guru to the February 2022 edition of Top Cyber News MAGAZINE. Chuck D. Brooks – the person-legend and reference for the topic's most competent and comprehensive quests and analysis.

[Chuck D. BROOKS] Thanking Ludmila for this wonderful honor of being featured on the Cover Page of her new innovative people-centered magazine. I want to commend for publishing and editing Top Cyber News Magazine. It is an indispensable resource for those of us in the cybersecurity profession!

[Ludmila M-B] Why is Cyber Awareness so important in today's changing world?

[Chuck D. BROOKS] The underlying problem is that the Internet was not built for security at its inception; it was built for connectivity and sharing communications. Therefore, anytime you are online, you are facing peril. It is important for business and individuals to understand the risk. The best defense in cybersecurity is to be knowledgeable. There are a variety of components to being knowledgeable.

You need to know the threats, know the risk management policies, know the technologies, and know the resources available to assist in making yourself more cyber-secure. I have made a dedicated effort over the last several years to bring content and cyber-awareness through writing and speaking on those components. In that sense I am a cybersecurity advocate and change agent.



[Ludmila M-B] What do government and industry perceive to be the main cybersecurity threats and required responses?

[Chuck D. BROOKS] We live in a world of X & O algorithms where we are all vulnerable to cyber-attacks. In particular, protecting our critical infrastructure, including the electric grid, transportation networks, and financial networks is an imperative. Cybersecurity capabilities must keep pace to fortify against the increasingly sophisticated threats aimed at both industries and governments.

Detecting, identifying, and responding to those threats is a significant security challenge of our increasingly interconnected digital world.

Recently, I wrote an article in FORBES highlighting what as I see as some of the biggest cyber- threats. They include (excerpts from y article) 4 Beckoning Cyber-Threat Challenges (forbes.com) :

[Chuck D. BROOKS] 1. Critical Infrastructure Attacks (Via Ransomware and Malware) Will Heighten in Numbers and Intensity: Numerous reports suggest that the cyberattacks, including ransomware and malware, have expedited by more than 200 billion this year. A Verizon report points out that 71% of security breaches are financially motivated, whereas 25% takes place with a motivation of espionage. The 52% breaches feature hacking, 28% involves malware, whereas 32-33% are performed through phishing and social engineering.

Critical infrastructure can also include the third-party risk of the supply chain. The need for better supply chain protection, called to attention by the SolarWinds breach has brought supply chain security to the forefront of consideration in both government and the private sector. Supply chain cyber-attacks can be perpetrated from nation state adversaries, espionage operators, criminals or hacktivists. Their goals are to breach contractors, systems, companies, and suppliers via the weakest links in the chain.

2. Expect Continued and Elevated Sophistication of Cyber-attacks: The assault on remote workers will not stop any time soon. Working from outside the office has changed the paradigm of cybersecurity by expanding the attack surface area. Phishing attacks are up 600% targeting remote works. "Cybercriminals are always ready to launch attacks that exploit users' behaviors, even if inadvertent. This was never more apparent than in 2020 & 2021, when employees forced to comply with stay-at-home orders became remote workers scrambling to adapt to new technologies and devices.

Artificial Intelligence & Machine Intelligence spreading malicious software will be used to automate target selection, check infected environments before deploying subsequent stages of attack and avoid detection. "Threat actors often misuse advanced technologies to create new kinds of malicious operations. According to research from the United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol, and cybersecurity firm Trend Micro, cybercriminals are rampantly leveraging AI to spread a wide range of digital threats for ill purposes. It is said that AI systems are being developed to enhance the effectiveness of malware and disrupt anti-malware and facial recognition systems."

Botnet attacks on smart phones to launch Denial of Service (DDoS) attacks to the organization – Smart, mobile devices are a primary target to gain access to the organization. Example, attacks to industrial control systems and supply chain partners through IoT devices. The expanded use of social media platforms to spread misinformation about any type of entity, in the form of bots and effective amplification, with a story to spur debate, threaten a brand, manipulate public perception. Social media is also a growing vehicle for deep fakes and a resource for gathering info for identity theft.

3. Greater Collaboration Among Cybercriminals

Trends show that cybercriminals are leveraging the underground market, while purchasing and sharing tools such as hacking-as-a-service, re-usable hacking kits. Also, there is visible sharing of tools on dark web websites and forums. The hidden hacker forums and access to the underground vulnerabilities database are enabling cyber criminals of various levels of expertise to coordinate and launch sizable attacks. Consolidation of smaller hacker affiliates into larger hacker criminal families for a wide mix of attacks, including exploit kits, and malware, as well as other services such as money laundering and making malware undetectable. With cryptocurrency and ransomware available, small hacker groups will go where the money is and often share and coordinate opportunities.

4. Internet of Things Devices Presents Special Security Challenges:

There are an estimated 44 billion IoT endpoints today (and that number is expected to triple by 2025) and trillions of sensors connected to those endpoints. Hackers have many attack options and entries for inserting malware into such a large attack surface. They can also employ DDoS (distributed denial of service) attacks to devastating effects.

IoT complexity (that often includes a lack of standards) magnifies cyber risk. Most IoT devices differ from conventional computers as they are highly specialized and are small, both in physical size and computing capacity. Lack of visibility and the lack of ability to determine if a device has been compromised and not performing as intended. IoT devices including wearables, TVs in the boardroom, and security cameras are all easy targets for kill-chain intruders.

[Ludmila M-B] What would be on your own master list of cybersecurity challenges, priorities, applications, and emerging trends?

[Chuck D. BROOKS] Great question, there are so many aspects to cover that I composed the list below with summations as a sort of cheat sheet.

Challenges:

- Increased cyber-attack surface (*the expansion of the Internet of Things and the large impact from remote work)*
- Modernization of IT legacy systems (it is a cumbersome and slow process, especially in government).
- Growing complexity, sophistication, and intensity of cyberattacks from social engineering. ransomware, phishing, and DDOS attacks.
- Supply chain security. (Third Party access, insider threats, and misconfigured code pose continuing
- As government is moving toward cloud and hybrid clouds, a challenge is how to best optimize and secure applications.
- Lack of cybersecurity expertise in the C-Suite (*industry need to see security and an investment in reputation and survival and have SMEs involved in leadership*)
- Lack of qualified cybersecurity workers (*an ongoing global issue).*

Emerging Technology Areas:

- Artificial intelligence and Machine learning *(will have huge impact on detection, analytics, and automation)*
- Internet of Things *(new verge of exponential interconnectivity)*
- *5G (will greatly increase transmission speeds of data and communications)*
- Med Tech Security (large impact for medical monitoring via wearables and telemedicine. Securing medical tech devices, and associated life sciences data is a top priority)
- Drones and Robots (for manufacturing, security, production)
- Smart Cities (the future mesh of technologies, systems, and platforms)
- Blockchain (*decentralized peer-to peer network)*
- Quantum Technologies *(cryptography, encryption, decryption, the dawn of a new era of supercomputing*
- Neuromorphic human computer interface (*machines are already capable of transcribing human thoughts)*

Technology Applications:

- Protecting critical infrastructure (*OT-IT fusion, advanced sensor monitoring, automated incident mitigation and response*)
- Identity Management (*multifactor authentication, biometrics*)
- Automated network-security correcting systems (*self-encrypting drives*)
- Technologies for "real time" horizon scanning and monitoring of networks
- Diagnostics and forensics (*network traffic analysis, payload analysis, and endpoint behavior analysis)*
- Advanced defense for framework layers (*network, payload, endpoint, firewalls, and anti-virus)*
- Mobility and BYOD security

Trends:

- Informed risk management and industry-specific security frameworks (i.e., *NIST, MITRE)*
- Zero Trust, defense in depth, and security by design (*three pillars of security*)
- Emergence of stronger Public/Private sector partnerships to include more information sharing, collaboration, and shared R & D spending between the public and private sectors
- Increased spending for cloud and hybrid cloud computing
- Expansion and training of cybersecurity workforce
- Cybersecurity insurance
- As government is moving toward cloud and hybrid clouds, a challenge is how to best optimize and secure applications.
- Lack of cybersecurity expertise in the C-Suite (*industry need to see security and an investment in reputation and survival and have SMEs involved in leadership*)
- Lack of qualified cybersecurity workers (*an ongoing global issue).*

Emerging Technology Areas:

- Artificial intelligence and Machine learning (will have huge impact on detection, analytics, and automation)
- Internet of Things *(new verge of exponential interconnectivity)*
- *5G (will greatly increase transmission speeds of data and communications)*
- Med Tech Security *(large impact for medical monitoring via wearables and telemedicine. Securing medical tech devices, and associated life sciences data is a top priority)*
- Drones and Robots *(for manufacturing, security, production)*
- Smart Cities *(the future mesh of technologies, systems, and platforms)*
- Blockchain (*decentralized peer-to peer network)*
- Quantum Technologies *(cryptography, encryption, decryption, the dawn of a new era of supercomputing*
- Neuromorphic human computer interface (*machines are already capable of transcribing human thoughts)*

[Ludmila M-B] What advice would you impart on careers in cybersecurity and in tech?

[Chuck D. BROOKS] In reflecting over the span of my career in government (and in the private sector) I have come to a recognition that are several valuable elements for reaching you career goals.

These include: 1) being able to network and build relationships; 2) having to the ability to effectively write and speak; and 3) to be able to dedicate yourself to learning and developing an expertise on key issues, concepts, and policies encompassing your work. Networking, communications, and developing subject matter expertise are all key ingredients for the pursuit of any career path.

Also, being willing to participate in the global ecosystem of experts and leaders is very important. It really is a small world, and the security community is very interconnected. Having a strong understanding of international relations and cultural mores of a variety of countries is important to thrive in business and security.

I received my master's degree at the University of Chicago in International Relations, and also studied International at The Hague Academy of International Law. That academic training and networking laid the groundwork for being able to think, analyze, and learn from lessons of history.

I am now reciprocating my passion for learning to students at Georgetown University. I serve as Adjunct Faculty at Georgetown University's Graduate Applied Intelligence Program and the Graduate Cybersecurity Programs and teach courses on risk management, homeland security, and cybersecurity.

In my faculty role I developed content, designed, and teach graduate course called "Disruptive Technologies and Organizational Management now in its third year. I also helped design a certificate course on Blockchain technologies. I particularly enjoy and represent the University at speaking events on topic of cybersecurity, intelligence, and emerging technologies.

[Ludmila M-B] A more in-depth bio and where Mr. Brooks can be reached is below.

Chuck Brooks LinkedIn Profile:
https://www.linkedin.com/in/chuckbrooks/

Chuck Brooks on Twitter: @ChuckDBrooks

Considerations for an Augmented World

Author: George PLATSIS

"In the year 2032 it is quite possible there will be a merged physical and digital world."

An article by Chuck Brooks in FORBES, Welcome To 2032: A Merged Physical/Digital World. provides excellent insights on the potential of emerging tech and its impact on our future society.

What we call that future world is still yet to be determined and you may have noticed the shifting names over the last few years. It started with Virtual Reality (VR), then Augmented Reality (AR) and now we see Extended Reality (XR) entering the lexicon.

Regardless, whatever we call it, this much is true: there is a meshing of the physical and digital world that may become so entangled over the next decade, without serious discussion and consideration today, we may end up somewhere we do not want. New cures for diseases, integrated use of artificial intelligence, flying cars, and connected smart cities all sound nice, but we should be cautious before we push the pedal to the floor.

"The rose-colored glasses view of the future has a dark underbelly and there is a historical reference warning us to slow down: the Internet."

Inherent Vulnerabilities Must be Addressed

Many decades ago a decision was made: should the Internet be designed to be secure or should the Internet designed to be free?

The latter won out the argument at the time and, at least for the first few decades, this decision seemed like the prudent course of action. More recently though, over the last decade, we increasingly have to pay the piper for that decision. The inherent vulnerabilities of the Internet are continually exploited, which has forced us to take the "when we get breached…" approach versus the more preferable, but highly unlikely, "if we get breached…" approach.

The cost on our ledger of these attacks have generally been financial, with secondary and tertiary effects. For example, the lives of employees have been ruined because a cybersecurity incident has resulted in financial ruin for the company. The downstream impact is the company closing its doors, leaving people unemployed. Similarly, an attack on critical infrastructure has downstream impact by cutting water or electrical supply to everyday people.

But few of today's cybersecurity incidents directly target an individual, or a group of individuals, as the primary target. Short of information warfare and social engineering, both that have roots in psychology, it is not feasible to "technically hack" somebody's mind. Any "hacking" requires psychology. The augmented world changes that.

"Current trends indicate that we want to impose or merge an inherently vulnerable system (the Internet) onto a likely fragile system (the human mind)."

What Does The Individual Look Like in 2032?

Throughout civilization, even during its darkest times, humans have still had the ability to maintain an absolute firewall on their individuality. Granted, under totalitarian regimes minds have been broken (think forced confessions) but individuality remained intact.

The augmented world is on a collision course to shatter that barrier. Today, if you have a technical issue with your home internet or phone line, a customer service representative, halfway across the world, can connect into your technical infrastructure via the Internet and troubleshoot the issue. Are you – are we – ready for that same operating model if we "technical infrastructure" with "brain" or "mind"? If we are suffering from some sort of medical ailment, are we ready to allow somebody halfway across the world to "upload a patch" into our "individual operating system" and look at that as a cure?

The technical possibilities are incredible, much like how they were when the Internet came online. But the more ethical and moral implications were not discussed, such as the erosion of privacy and the door opening into full coverage surveillance.

The Time to Ask Questions is Today

As we barrel forward into the metaverse and augmented worlds, these types of questions need to be asked today:

- What does the individual look like in an augmented world?
- What are privacy expectations in the augmented world?
- Can you opt out from a fully augmented society and what does that life look like?
- Can you undo mistakes, such as "installing" the wrong medical patch?
- What is considered legal? Does a stray thought out of frustration trigger a pre-crime alert on some dashboard?
- What is real and what is not?

Perhaps the most human question of all: are you allowed to make a mistake? So many of life's greatest moments are children of mistakes. The definition of "a mistake" even comes into play. If there is an orthodoxy of permitted thought, does anything outside of that confined thought matrix constitute "a mistake" and if so, what is the penalty for such a mistake? Mistakes, while still bearing a penalty, also open the door to opportunity.

Rose-colored glasses paint a picture of futuristic marvel and wonder, and hopefully we can reach that pinnacle, but sober thought and deep considerations can paint a very different picture, one where society more closely resembles The Borg of Star Trek lore.

"Like all decisions in life, there is a risk consideration that needs to be addressed. The responses to the questions above will help us determine our personal and societal risk tolerances. The piper will be paid, it is just a matter of how much and when. Best to therefore have these discussions as soon as possible before we pass a point of no return."

George PLATSIS

George PLATSIS has worked with private, public, and non-profit organizations to address their strategic, operational, training, reputational, and compliance needs. He has worked in the United States, Canada, Europe, and Asia. Currently, he is a Senior Lead Technologist as part of the Proactive Incident Response & Resiliency capability at Booz Allen Hamilton.

Specific areas of expertise include: enterprise and organizational resiliency, enterprise incident response, business continuity, disaster recovery, governance/risk/compliance, digital forensics and incident response, expert reports and testimony, social engineering, insider threats, psychological warfare, data manipulation and integrity, and information dominance.

As a professional, he has advised, managed and delivered projects related to: enterprise resiliency and incident response programs including remediation, insider threat investigations, enterprise-wide assessments and audits, forensic investigations, policy and technology reviews, documentation and workflow/process creation, critical infrastructure hardening, framework development and implementation, technology review, and organizational cost savings.

As an author, his works have been published in industry-leading and award winning publications, including: IBM's Security Intelligence, Bloomberg Law: Privacy & Data Security, Tripwire's State of Security, Homeland Security Today, Security InfoWatch, Nextgov, BRINK News, Ethical Boardroom, ITSP Magazine, BizCatalyst360, Fifth Domain, and many high audience blogs. His works maintain a Top 5 ranking for page views, organic traffic, and social traffic on IBM Security Intelligence.

He holds a bachelor's degree in business administration and has graduate degrees in business administration, disaster and emergency management, law and cybersecurity. He has completed executive education in national/international security and cybersecurity at Harvard University, Syracuse University and the Canadian Forces College.

George is a founding member of The #CyberAvengers, a group of seven cybersecurity professionals and influencers who collectively have tens of thousands of followers on various social media platforms. The views expressed by this author on Top Cyber News MAGAZINE are those of the author and not necessarily the views of Booz Allen Hamilton, its management, its subsidiaries, its affiliates or its other professionals.

May THE Techs Be with You as We Go Where Others Have Not Gone Before

Author: June R. KLEIN

"Universe Cybersecurity is about 'having your head above the clouds,' rolling up your sleeves, not looking through rose-colored glasses, having an algorithmic method to find the intersection of 4 pillars, and knowing THE Chuck Brooks featured on the magazine cover." ~ June R. Klein

Backstory.

In the GoldenEye spy film, James Bond fights to prevent a rogue ex-M16 agent from using a satellite weapon against London to cause a global financial meltdown.

In 1996, the producers brought in Judi Dench, to take over as the role of M, James Bond's boss, and the first woman to portray M in the series.

Fast forward to the reality/docu TV series, Mr. Knight, Chairman of GIA4, asks AnalystX, "June, are the satellites ready?" Prior to answering, June does the TMVi™ Impact analysis below and contacts her colleague, Chuck Brooks who she has worked with on and off for over a decade. We met in our roles as tech advisors for the Gates Foundation where we practiced Ubuntu humanity philosophy, "I am because WE are."

Then a cybersecurity board level issue analysis using TMVi framework, followed by collaborations via Linkedin's Group - Emerging and Futuristic Technologies, a NYC cyber executives panel with Darktrace - UK's cyber startup, Lockheed Martin team aligned with merchant bank and government-funded incubator, Board of directors of an IOT firm, a NIST standards effort, a World Economic Forum speech, and Who's Who for 2021 Cybersecurity Awareness Week.

Drumroll please…

I then sat in on Chuck's masterclass with William Jeffrey PhD CEO of SRI and Director of National Institute of Standards and Technology and Dr. David Bray, who is one of the foremost experts on both the technologies and geopolitics on anything satellite related… now how I got to my answer. ***"Mr. Knight, Satellites operational, GIA4 signing out."***

Assumptions: Adversaries are eager to exploit cybersecurity vulnerabilities in space systems. There is a renewed focus about cyberattacks on infrastructure assets like water treatment plants. Satellites could be used as a weapon impacting the built environment.

Problem: If hackers took control of private industry satellites, they could spoof signals creating havoc for critical infrastructure like water networks.

Process: ***How does each of 4 PILLARS relate to satellites, cybersecurity, ESG, humans, built environment, water-related climate change, investment decisions?***

Technology insights:

(a) Space systems are interconnected so attacks spread from a ground station vulnerability to the satellites. One weak link could impact 100s of satellites. The key points of access that exist for a potential satellite cyberattack are the extended land-based infrastructure (ground stations etc.), the satellites themselves, and the supply chain.

(b) The digital twin concept synchronizes a physical object with a cyber form. This enables testing of different scenarios to find vulnerabilities and create protection solutions.

(c) Next generation of satellites need complex designs and thus are even more vulnerable to cyber threats.

(d) Desalination solutions should be important to built-environment practitioners where ocean salt water can collapse buildings reinforced with concrete rebar support.

(e) All cloud companies will become space cloud companies.

Marketing observations:

(a) Space race has moved from the ideas of visionary engineers into enablement via wealth entrepreneurs and ideally human betterment.

(b) Some re-thinking about link between built environment and social value needs before and after cybersecurity attacks and water disasters.

Ventures pop-up:

(a) While cybersecurity has been viewed as a technology issue, it is now also regarded as a key environmental, social, and corporate governance (ESG) concern, falling under the "Social" pillar.

(b) Corporate community is getting on board with ESG thinking. Environment and social impact are becoming a growth strategy begging for direction on ESG reporting.

(c) Private equity firms, public markets, government agencies, and special-purpose-acquisition-companies are continuing to buy and raise money for space-related firms.

(d) Government has best practice cyber standards for space, but commercial needs to develop appropriate standards to be secure and resilient.

"inc." pulls together:

(a) Encryption and authentication of the data sent to and from spacecraft is the first line of defense inside a space system.

As we see in the Mr. Knight-June trailer, https://vimeo.com/620955556 it allows private communications that are only visible to others with the cryptographic key. [The integrity algorithm GIA4 computes a Message Authentication Code (MAC) on an input message under an integrity key IK128. The input message may be between 1 and 65536 octets long. For ease of implementation the algorithm is based on the same block cipher (KASUMI) as is used by the confidentiality algorithm GEA4.]

(b) A cyber-resilient spacecraft needs a robust Intrusion Detection System (IDS).

(c) Cyberattack resilience testing for spacecraft software needs to be designed and checked for cyber resilience before launch – not in orbits with no viable recovery option – not after third-party software is operational.

(d) Cyberattack insurance policies are challenging for satellites since this is a new class of risk and no historical data.

(e) Cybersecurity as an "ESG" metric is a new stance, but all evidence points to continued interest across the board.

(f) Elevating the "Social" on agenda brings us closer to a holistic understanding of VALUE.

Like my career and proven TMVi™ Framework, the integration of "Environmental" the universe-built environment into "Social" human cybersecurity impact via "Governance" is a journey, not a destination. Governance, investment decision-making, and management is a dynamic process which evolves and changes.

Contact: https://linkedin.com/in/juneklein
or you@EmpowerNatorJune.com
https://dellaleaders.com/v3/profile/june-klein

June R. KLEIN

June R. KLEIN, MBA is CEO of Technology & Marketing Ventures, Inc., venture development, management consultancy. She transforms tech, innovation and methodology into empowerment, resilience, and wealth.

Prior to starting her own firm, she evolved from being math educator into Federal Reserve Bank programmer, to Merrill Lynch systems research analyst, to IBM Region Manager, to Citigroup Global Marketing FinTech Executive, to JPMorgan Government Banking Investor Services Lead, to public and private company board member, to global awards recipient. Mrs. Klein is an Honorable Member, Della Leaders Club, NYC Transformation Committee.

Her stakeholder focus is on compiling best practices resilience solutions for built infrastructure impacted by floods and hurricanes catapulted by climate change. As Executive Producer and top talent on a social movement docu-series she leverages TV to impact humanity at scale.

Impact Leaders hire TMVi to navigate them through uncharted water. Because some need assistance with implementing soft skills of adaptability, resilience, and recovery and most do not have a framework to manage constant change, complexity, and risk. So, June shares and customizes her proven algorithm with executives.

The outcome for leaders is being seen as innovative ecosystem builders driving scalable, sustainable, profitable businesses. In this article, I use the TMVi™ Framework to tackle space -satellites, cyber-risk, and digital-twins.

Combating Cyber Threats
Sprint vs Marathon Approach

Author: Angelique "Q" NAPOLEON

"Against the backdrop of a complex and growing cyber threat landscape, where 57% of businesses now assume their IT security will become compromised, businesses are also waking up to the fact that one of the biggest chinks in their armor against cyberattack is their own employees." ~ Kaspersky Daily

The Front Lines

Cyber criminals and threat actors have escalated attack campaigns on a continuous rhythm exploiting the various vulnerabilities and exploits within hardware and software and businesses both large and small have had their cyber shortcomings turned into one public embarrassment after another. Breaches, network misconfigurations, shoddy coding practices, and insider threats continue to cripple businesses and government organizations with no end in sight.

The pandemic forced organizations to remote work options with little to no preparation or adequate protections in place to combat the onslaught of attacks. Strains in the IT supply chain have complicated the tech refreshment cycles and the defense posture is a lack of qualified Cyber and IT professionals.

Battling Burnout & Lack of Qualified Candidates

IT and Cyber teams are stretched to the limits with many teams facing burnout from junior to CISO ranks and support has slowly trickled in due to a battle for talent regardless of the experience level.

The battle rhythm for cyber-attacks has not slowed and over the course of the pandemic it has only increased putting a strain on human and IT resources.

Human Resource Professionals struggle to fill open IT and Cyber positions with the ripple effects being felt throughout organizations and the challenge to find qualified candidates is forcing greater creativity in recruiting methods to include bonuses, work-life flexibility, and generous salaries.

These professionals have worked tirelessly on the front lines of the IT and Cyber labor shortage, and they too feel the strains of burnout and frustration with finding qualified talent.

The labor pools which have traditionally provided highly qualified IT and Cyber talent are shrinking with more and more professionals leaving the work force.

by Angelique "Q" NAPOLEON

Running the Race

Cyber and IT teams began the race in a full-on sprint coming together at the start of the pandemic and quickly deploying remote work solutions and putting their organizations back to work while continuing to migrate their businesses to meet the challenges of working in a completely new environment.

These teams worked around the clock to address the daily business challenges of providing support to their user base and continue to fight the cyber-attacks, educate their work forces on Cyber vulnerabilities, and evaluate and integrate new technologies.

Running at this pace for long periods of time begins to take a toll on teams and is unsustainable for any organization as burnout and critical mistakes begin to become more common. People, like machines, aren't designed to run at sprint speeds for an indefinite period.

This pandemic has turned the race from a sprint into a marathon and it has become a balancing act for organizations trying to defend against ever-evolving cyber-attacks and sustaining a battle tested workforce.

The race, no matter the speed, has brought management and technical teams closer together as they work to recruit, educate, defend, and integrate new technologies.

The Technical C-Suite have been instrumental in building and leading the IT and Cyber teams required to finish this race.

No matter how your organization has run the race, whether it's been a full sprint comprised of agile processes and highly tuned resources, or a carefully calculated marathon with trained teams integrating and sustaining tomorrow's technologies, the key to staying ahead of tomorrow's cyber attacks are your people.

Invest in their education, training, and mental wellbeing so that they have the right tools to defend the organization against the cyber-attacks, vulnerabilities, and insider threats that can cripple any organization.

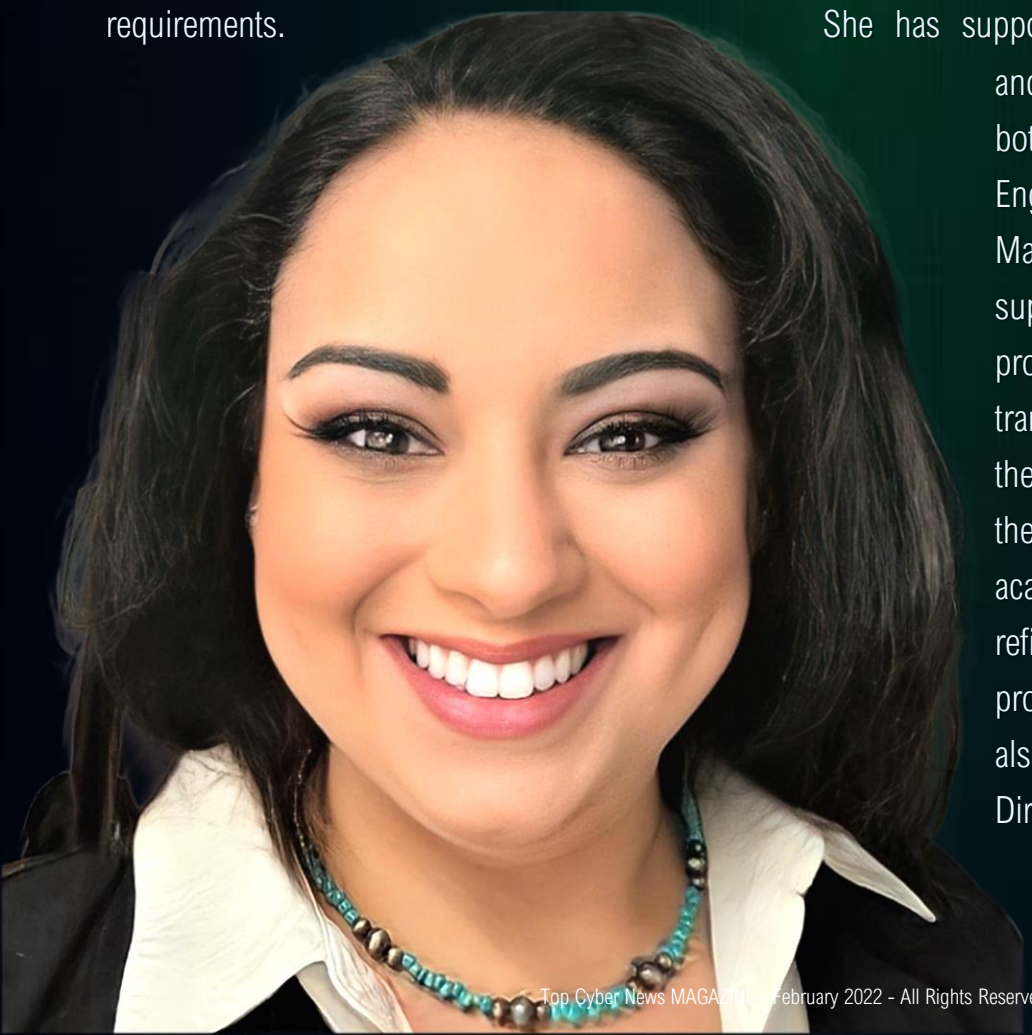
"The race isn't over, and we need everyone on the team to finish and win! Recognize the signs of burnout and be creative when looking for talent! "

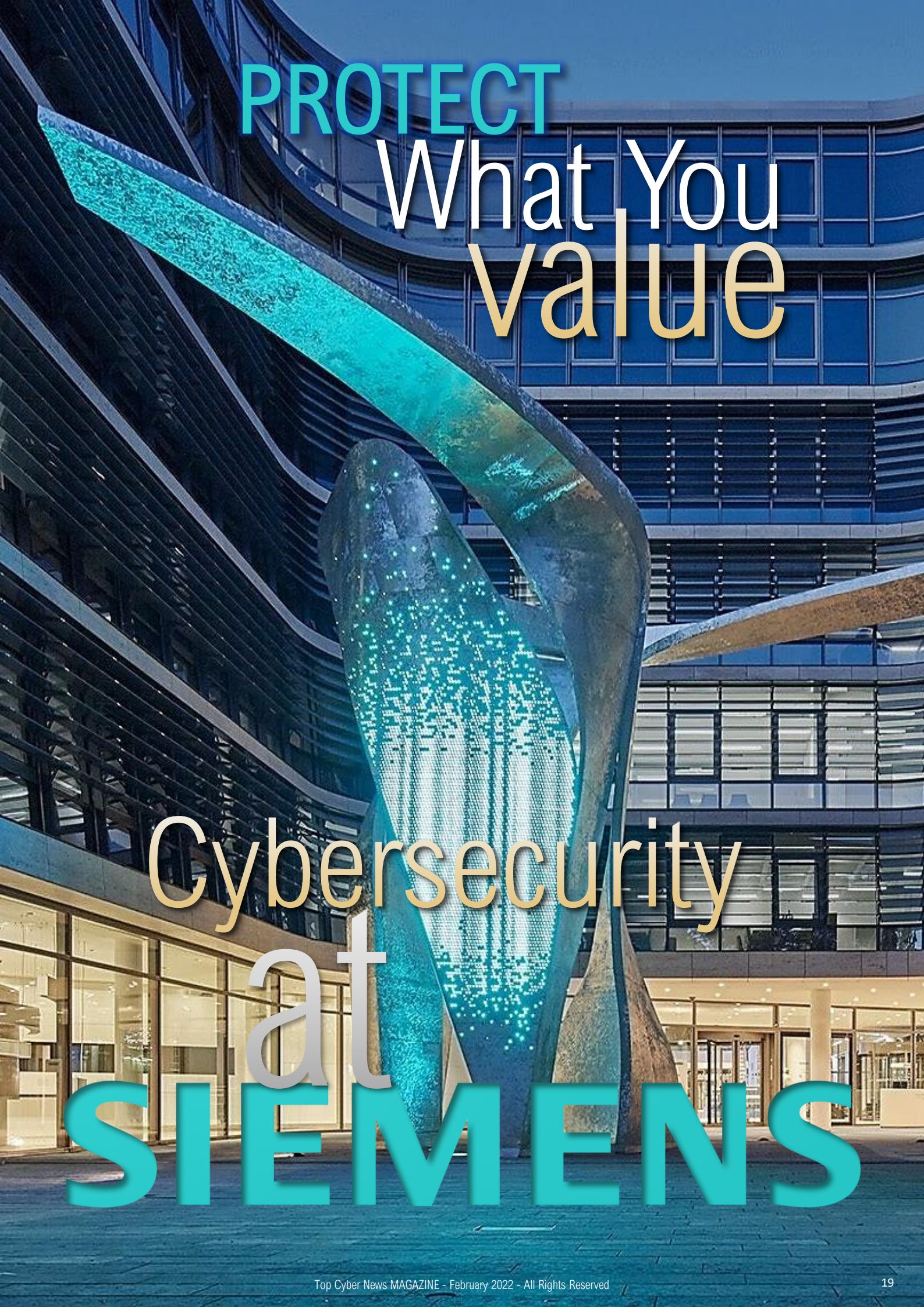
Angelique “Q” NAPOLEON

Angelique “Q” NAPOLEON, Washington, D.C. is a Principle Cybersecurity Subject Matter Expert for the Department of Defense in Washington, D.C.

As a Principle she is responsible for various cyber activities which build on the foundation for Cyber Resiliency for her assigned programs which she supports as well as her Defense Industrial Base (DIB) clientele who rely on her expertise as their virtual Chief Information Security Officer to protect their networks and employees from adversaries and cyber criminals. She has developed highly specialized cyber capabilities, frameworks and services from Penetration Testing, System Security Engineering (Cloud/On-Prem) and development of Cyber Threat Intelligence products to both commercial and defense clients.

She has also established the Price Forensics Lab for IntellecTechs and is a Fellow to the Lab Director where she handles all of the Digital Forensics and Incident Response activities to include formalized reporting and coordination with US Government & Federal Law Enforcement organizations. She produces Cyber Threat Intelligence products and hosts Cyber Awareness & Compliance training sessions aimed at increasing awareness and affordability. She works with small to medium sized businesses in establishing tailored Cybersecurity programs which target DOD and US Government cyber compliance requirements (CMMC, NIST, ISO) that are affordable and sustainable which meet the organizations contractual requirements. She has supported US Government programs and projects for over 25 years in both Intelligence and Cybersecurity Engineering & Executive Management capacities. She supports various mentorship programs and initiatives for transitioning Military members and their families looking to enter into the Cybersecurity field and supports academia in development and refinement of cyber education products and services. Angelique also serves on several Board of Directors.




PROTECT
What You
value
Cybersecurity
at
SIEMENS

Cybersecurity at SIEMENS

Multifaceted and Values Driven

Author: Natalia OROPEZA

"Cybersecurity teams need to be diverse – not just with respect to gender, but also e.g. with respect to nationalities, age, or the ways of thinking."

Successful cybersecurity teams have to be something more than a collection of individuals who are just as diverse and multifaceted as the attackers whom they must vanquish every day. They should also be a community of shared values. This is the only way that they can successfully fend off the multiplying number of menaces they confront in cyberspace.

Cyberattacks are launched from everywhere – and this frequently means from unexpected directions. The attackers range from teenage hackers and criminal syndicates to government-sponsored strike forces that have unlimited resources at their disposal.

Their methods are multidimensional: denial-of-service attacks, ransomware smuggled into supply chains and phishing e-mails that lure users into clicking links or documents that appear to be ever so innocent. Their aims are just as multidimensional: sabotage, espionage and blackmail. The damage caused by these hackers costs companies billions and billions of dollars.

Companies that are determined to defend themselves need teams of cybersecurity experts who are not cut from the same cloth. They must have an array of experiences, talents, perspectives, mindsets and résumés. The reason is simple: It is this diversity of ideas and recommendations that produce the solutions that can counter today's threats.

"Cyber-attacks know no borders - they come from different regions of the world. That's why attackers' approaches are correspondingly diverse."

A number of studies have confirmed that cognitively diverse teams are more successful. A McKinsey report analysed the data of 366 companies and concluded that companies that have a higher degree of ethnic and gender diversity perform significantly better in commercial terms.

On the other hand, teams consisting of motley assortments of individuals run the risk of remaining in a constant state of disagreement. This is why these teams must share the same values, a quality that is just as important as diversity.

It is a principle that applies in many places. Individuals who care for the elderly should share a commitment to helping fellow human beings. Employees at a technology company should be motivated by innovation – and society as a whole should promote equal opportunity and inclusion along with diversity.

"A good team is always a community of shared values," says **Natalia Oropeza,** Chief Cybersecurity and Chief Diversity Equity & Inclusion Officer at Siemens AG.

Siemens – a company with about 300,000 employees and hundreds of factories – registers around 1,000 cyberattacks each month.

Tough fight for the most talented people

Siemens achieves both goals in its cybersecurity department. Diversity touches on something much more than gender here (see the information box) – it also applies to age, ethnic background, sexual orientation, social background and nationality. Siemens operates five major cybersecurity locations around the world, and they are staffed by employees who come from more than 25 different nations. Natalia's team consists of a range of different mindsets that foster innovation, creative thinking and fast problem resolution.

At the same time, such values as equal opportunity and inclusion play a key role in Siemens' corporate culture along with diversity. The result: a powerful global team. It is a team that is certainly needed: Siemens – a company with about 300,000 employees and hundreds of factories – registers around 1,000 cyberattacks each month. To make matters worse, the number is growing. Each attack must be successfully blunted in the shortest amount of time.

The team also develops innovative security solutions designed to keep it one step ahead of the attackers. It works to ensure that all employees in the Group understand just how important cybersecurity is to the jobs they perform everyday.

"Good teams are diverse, as they deliver better results. Furthermore the feeling of belonging is very important for every Community. Thus also for the Cybersecurity Community of Siemens. All of this boosts innovation and creative thinking and problem-solving. "

A team's diversity also acts as a calling card that piques the interest of greater numbers of job candidates in the company. A survey conducted among users of Glassdoor – a website where employers are rated – found that 67 percent of respondents view diversity as an important job-selection criterion. Such considerations play an even greater role in cybersecurity. The reason is quite simple: This area faces an ever-shrinking pool of experts and has to fight tooth and nail to hire the most talented individuals as a result.

It is a situation that also affects the entire cybersecurity industry: The industry's culture must be changed from top to bottom in order to remain attractive. Such change extends all the way to the type of words that the industry uses. In the past, the term "master/slave" was used to describe data-transmission hierarchies in networks. But the term is now falling out of fashion as the industry moves forward.

Questions are also being raised today about AI programs that have been trained with data sets that were selected only by a homogeneous group of individuals. *"The male-dominated world of hacking assumed for years that there was a technological solution for everything,"* says the cybersecurity expert **Mirko Ross.** *"But that is not true. We need cultural change to address many social problems. Companies can help fuel this change."*

Intensified employee commitment

Job seekers are interested in something more than a diverse culture. They are also looking for something that could be described as a home. And why shouldn't they? They spend much of their lives at and with work. This means that an employee must be able to identify with the values of an organization. These are values that may not be particularly noticeable from the outside. Instead, they are the values that employees experience on the job every day and that ultimately determine whether they identify with the company.

Equal opportunity means flexible work conditions for employees who have children at home or have to care for elderly individuals. It also means that every employee has access to the same information and receives equal pay for doing the same job. Inclusion ensures that every voice in a company is heard, including those expressing uncomfortable truths.

It all pays off for companies in the end: A study conducted by Deloitte found that inclusive work cultures and diversity resulted in increased employee commitment. This approach *"helps people find meaning in their work – and to commit themselves accordingly,"* **Oropeza** says. *"It is a situation from which companies and employees profit equally. Siemens has two goals for its cybersecurity teams: They should not only be diverse, but also make employees feel at home. This is good. But there is certainly much more to do."*

Women on the rise

When it comes to diversity, the most-talked-about issue is gender diversity. By tradition, men dominate technical jobs. Around the world, women make up less than one-third of individuals with jobs related to the four STEM subjects (science, technology, engineering and mathematics). The level is even lower in cybersecurity, where the average total is just 20 percent. Global technology companies like Siemens are now working to systematically increase the number of women in these jobs.

As part of this effort, Siemens has teamed up with institutions of higher learning to methodically support women who are studying STEM subjects. Networks have also been created within the company itself to give women a voice and career opportunities like those enjoyed by men. Employees are also undergoing training that will help them recognize their unconscious biases. An implicit association test developed by Harvard University found that more than 70 percent of respondents associated men with careers and women with families.

During the recruiting process at Siemens, the company makes sure that job candidates speak with the widest range of interviewers. The results are encouraging: At Siemens, women make up nearly 30 percent of managers on the first and second levels in cybersecurity – even though men compose 74 percent of the company's workforce.

Natalia OROPEZA, Chief Cybersecurity Officer & Chief Diversity Officer of Siemens AG

Natalia OROPEZA, Chief Cybersecurity Officer & Chief Diversity Officer of Siemens AG. Born and studied in Puebla, Mexico, Natalia has about 30 years of experience in the area of Information Technology with international experiences in Mexico, USA and Germany. She holds several academic qualifications and IT certifications and is a founding member of "Women4Cyber", an initiative of the European Cyber Security Organisation (ECSO). Before she started her engagement at Siemens in 2018, she worked as Chief Information Security Officer and Head of the largest IT Transformation Program at Volkswagen Group.

Cybersecurity at SIEMENS

Subscribe to Siemens Newsletter

Mark your calendars!

As part of the Munich Security Conference 2022, the Charter of Trust is pleased to invite you to its insightful executive event on building resiliency through community, taking place online on 18 February.

It is clear that no one can face cyber threats alone – and that is why the Charter of Trust is so relevant, pushing for stronger Cybersecurity since 2018.

Editor-In-Chief

TOP CYBER NEWS MAGAZINE

and

RAISE THE CYBERSECURITY CURTAIN!

Ludmila Morozova-Buss

Doctoral Student at

Capitol Technology University

«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.»

Shawn TUMA, Co-Chair, Data Privacy & Cybersecurity Practice at Spencer Fane, LLP

«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.»

Gary HAYSLIP, Global CISO for SoftBank Investment Advisers

«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.»

Dr. Pascal ANDREI, Chief Security Officer at Airbus, France