CYBERSECURITY: WHY YOU SHOULD CARE

RAISE THE CYBERSECURITY CURTAIN

2021
PREDICTIONS BY CYBERSECURITY LEADERS

Le Retour à la Raison. The Return to Reason.
Scale-up strategic thinking for a safer digital world.

by Ludmila Morozova-Buss

FORE SEE

LUDMILA MOROZOVA-BUSS

BE THE VOICE

Operational space of digital (r)evolution requires an instantaneous reaction. Seeking knowledge has brought me far beyond my personal horizons of discernment.

With hope to create and scale globally an inclusive 'authors-publisher-readers' circle of wisdom and expertise; with channeled determination to gain understanding by carefully selecting the best information sources (Dis moi où cherche! Mais où?) and reading between the lines, I invited the Cyber Warriors 'Men and Women on the Arena' with hope to "Raise the Cybersecurity Curtain".

A central topic of these thoughts is cybersecurity. A fundamental and delicate question at the heart of my work is: how to inspire readers` thirst for knowledge, for learning.

I advocate a Systems Thinking approach in informing our readers, followers, friends, business associates on digital transformation, emerging technologies and cybersecurity. Systems thinking forever changed the way I think about the world and approach issues. Imagine an open immeasurable non-linear system - the Cyber Space, where cyber threats and cybersecurity are two of many (to be defined) elements of this system… to be continued.

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/

The Hon. Troels Oerting
Expert Member INTERPOL

Chairman of the Board
of **World Economic Forum**
Centre for Cybersecurity (C4C)

'We, in security, should not promote fear – but protect hope'.

Before the global pandemic hit the World in spring 2020, the digital transformation increased speed and magnitude. Fuelled by super-drivers like mobile/5G, IoT, Cloud and AI the number of users, applications, storage, connections and algorithms outpaced what we had seen before. The huge possibilities provided by the Internet created a 'tech' environment attracting the best brains the World could produce and geopolitical tensions between China, Russia, EU and US intensified the regional competition on 'who controls the Internet' and the subsequent influence, growth and wealth.

The global Covid Pandemic forced us to move approximately 1.2 BN workers from their offices to work from homes in order to keep the wheels spinning. Internet enabled communication tools substituted physical meetings, teaching, marketing, trading, reading, accounting, watching and demand for online services surged and Accenture has estimated that globally we went through 3 years normal speedy digital transformation in just 3 months. This will continue. We will not go back to the 'old days' even after we get a vaccine. We will continue to work remotely – not necessarily from home but from anywhere. Both employers and employees have seen the benefits of this new flexible work-regime providing support from working both from offices and from anywhere.

In the future everything will be connected, everything will be sensing, everything will be stored and everything will be used, sold or utilised in other ways.

The future will provide more positive opportunities for the global, and connected, citizen – for businesses, education, healthcare, sustainability, climate, transparency and democracy. But it will also present challenges to security, privacy, integrity and trust. Trust between the citizen and consumer on one side and governments and corporations on the other side. Who can we entrust with our digital footprints and other assets, will our data become a commodity including face recognition and other tracking and can we believe what we read or see? Will someone 'hack' opinions in the future and influence elections and public debate negatively?

The National State normally regulate the level of domestic crime through the 3 P's. Prevention, Protection and Prosecution. Due to the current lack of trust between states and governments – it is not possible for global law enforcement to cooperate when fighting cybercrime. In reality cybercrime is presently a risk-free crime. Secondly, we have not been able to agree on the 'rules of the game' for State Actors covert operations on the Internet and in reality no written or unwritten rules regulate these operations. We have no cyber Geneva Convention.

>>>

The Hon. Troels Oerting
Expert Member INTERPOL

Chairman of the Board
of **World Economic Forum**
Centre for Cybersecurity (C4C)

'The World gets more hyper-connected at pace, but the governance around this development does not move.'

Based on this – we, as citizens, corporations, administration and users need to engage more actively in securing the Internet from crime and regulating rules around privacy and integrity.

A few areas of importance come to mind:

- The starting point must be a coalition of the willing who understand that sharing is caring.
- Security staff should stop talking a 'tribal language' and engage in a real discussion with the public, the C-level and decision makers. If they do not understand what we say, we speak the wrong language.
- As in many other areas the biggest improvement is always based on hygiene. Back to basic. We need to focus on basic defence and risk based graduation of our overall security posture.
- If you are not a VIP or your company is not in the hair-cross of foreign intelligence, the biggest threat to your cybersecurity is from cybercriminals. Cybercriminals do not hack for fun and will not invest 1 dollar to steal 50 cents. They might use advanced tools but they will be automated and if they do not find the anticipated weaknesses - they will move on to the next target. The trick is to have a security level above the criminal threshold.
- The tone from the top is important. We are all dependent of the Internet and security and privacy should be part of our personal and corporate DNA.
- Create alliances, work together, share best practice, develop and innovate responsible and with security, privacy and integrity in mind.
- Start prevention early and realise it is a long lasting effort.

Humanity will survive the Internet. It will be a bumpy road. We better buckle up and get started.

'I am a born optimist and wish us all good luck.'

Stephane NAPPO
VP Global CISO Groupe SEB

2018 Global CISO of the Year
Strategist, Technologist, Board Advisor, International Keynote Speaker, Key Opinion Leader

"One of the main cyber-risks is to think they don't exist - The other is to try to treat all potential risks."

The digital world is in constant transformation and there is no way of predicting what the world will look like in five years and who the new conquerors of the digital space will be. Cybercrime and cybersecurity follow ineluctably this trend, therefore, ***"if you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you."***

The dependence of the physical world to the digital one will increase with an extension of the cyber risks impact to environment and people; the adjustment of industry to the structural change generated by digital technologies and the transformation of society.

Acting both as cyber warrior and profit enabler, the CISO 2021 will have to meet unexpected challenges and meet the boards' expectations to secure the value chains beyond the company boundaries and the technical dimension.

What will the 2021 bring?

- Boosted by the pandemic, the direct-to-consumer shift 'from offline to online' will increase attack surface of the retail realm.
- Data sovereignty will become a major concern for nations and their economies.
- Large number of Internet of Things (IoT) devices will turn into Internet of Threats after being hijacked in public areas, at home or at enterprise.
- Classical cryptography will lose the ground in front of quantum computing weaponization.
- Post quantum cryptography will emerge (from theory to reality) as a necessary solution.

"Technology trust is a good thing, but control is a better one".

Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation. And do remember:

"Threat is mainly the reflection of our weaknesses"

Rather than fearing or ignoring cyber-attacks, ensure your cyber resilience to them. In times of hyperconverged infrastructure platforms and technologies, hyperconverged problems, strive to create hyperconverged solutions!

"Security, like life, has the colors that you give it."

Diane M. JANOSEK, Esq.
NSA Training Director

'Seize the Moment: Now is the Time for Women in Cybersecurity'

We live in interesting times. While 2020 was completed unexpected, likewise I predict additional, significant unexpected events in 2021. This will apply to the field of cybersecurity. In this increasing age of digital connectedness, bad actors come in many forms. Unsophisticated hackers can cause disruptions with ransomware, such as we have seen with attacks on soft targets such as libraries and school districts, and major disruptions from coordinated cyber criminal activity costing millions in losses.

Cyber criminals do not sleep, and this sleep deprivation will continue in 2021! During the global pandemic, they thrived! A 2020 report released by the cybersecurity company Mimecast revealed that cybercrime definitively increased significantly during the pandemic. The 48-page report "100 Days of Coronavirus (COVID-19)," released in May 2020, reported an overall increase in cyber-attacks by 33%. Breaking it down even further, the cybersecurity company said it saw the monthly volume of all detection categories increase by at least 26%, with:

- spam/opportunistic detections increased by 26.3%;
- impersonation detections increased by 30.3%;
- malware detections increased by 35.16%; and
- blocking of URL clicks increased by 55.8%.

Cybercriminals will continue to take advantage of dire situations and wreak havoc on people and businesses in times of uncertainty and economic pressure.

The field of cybersecurity needs talent to address these complex and increasingly sophisticated threats. That talent must come from all genders. Currently, women only make up 20-25% of the global cybersecurity workforce.

Together we must embrace this opportunity to not only make a difference to this much-valued field of data protection, privacy, and information security, we must encourage women to go into the field and to stay in the field. Women in cybersecurity must now seize the moment- our moment! We can change the trajectory to not just moving the needle, but to owning the needle and dominating the cyber industry.

We have the power to solidify our future by creating business partners and networks with women-owned businesses. Cyber needs leaders who possess and reflect the core strengths of collaboration, innovation, and intelligence. With the exponential growth in cybersecurity, let us re-imagine in 2021, the trajectory for greater female representation and leadership. In 2021, I predict, we will change our mindset and we can achieve it.

'This is our moment! Let's seize it in 2021!'

Founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine

GLOBAL CYBERCRIME

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

RANSOMWARE

A 2017 report from Cybersecurity Ventures predicted ransomware damages would cost the world $5 billion in 2017, up from $325 million in 2015 — a 15X increase in just two years. The damages for 2018 were estimated at $8 billion, and for 2019 the figure rose to $11.5 billion.

The latest forecast is for global ransomware damage costs to reach $20 billion by 2021 — which is 57X more than it was in 2015. We predict there will be a ransomware attack on businesses every 11 seconds by 2021, up from every 40 seconds in 2016.

CYBERSECURITY SPENDING

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was worth more than $120 billion. The cybersecurity market grew by roughly 35X during that 13-year period — prior to the latest market sizing by Cybersecurity Ventures.

Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021.

Cybersecurity Ventures anticipates 12-15 percent year-over-year cybersecurity market growth through 2025. While that may be a respectable increase, it pales in comparison to the cybercrime costs incurred.

The Tick

Fictional short story of our digital reality

by Wesley A. Whittaker

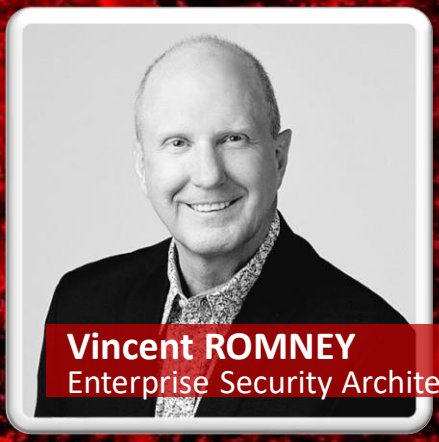
It had been an innocent mistake. Elaine Malveux, the Executive Assistant for Dr Charles Bolland, was working late. Bolland had asked her to type of the minutes of the Project Status meeting from the afternoon and send it to the Directors at Corporate as soon as possible. He was the head of Research and Development for Aquaxon Corporation. A breakthrough had happened with their atomizer technology on the chlorine dioxide project and it was a game changer in the fight against viruses and airborne pathogens. As soon as they brought the product to market, it was going to transform Aquaxon's financial status exponentially.

Elaine was happy for the good news, but she was going to get home too late to make dinner for her three children. She logged off the corporate network and brought up her personal contacts list. Clicking on the Angelo's Pizza website, she ordered a pizza to be delivered to her home and paid with her personal credit card. As she waited for the confirmation, a message box appeared asking her to confirm her ZIP Code. She did and the confirmation appeared. Elaine closed out the Windows app and attempted to log back on to the corporate network. A pop-up window appeared informing her that her session had timed out and she needed to reboot her workstation. She did, texted her oldest child about the pizza delivery, and then returned to finishing her report.

In a non-descript building across the street from the Amar Jyothi Electric Substation in Bangalore, India, a red light on the monitoring console signaled the desk agent that an unprotected internet access had been made from one of the targeted URLs. Although identified as "Far East Trading Ltd" on a faded sign by the front door, the building was really a server farm owned by a front company for the Ministry of State Security. Its purpose was to electronically monitor and attempt penetration of several high-tech companies in the West. With a few keystrokes, the agent determined the high-level nature of the target and initiated the penetration program called "The Tick." As soon as the target entered a random five digit number, the malware downloaded in to the root directory and awaited a reboot to proliferate through the network.

Elaine finished her report, logged off, and went home for the night. Later that evening, the Aquaxon server received a command for an unscheduled system backup. Within hours, a copy of every single file on the Aquaxon server was being analyzed in Shanghai.

Wesley A. Whittaker



Vincent ROMNEY
Enterprise Security Architect

2021 will provide a large number of interesting cybersecurity events, no doubt. But it should also see a few things shifting, and not necessarily in the right direction.

Application Programming Interfaces (APIs) present an environment that the cyber criminals have not fully exploited in the past, but I believe they will take additional, focused interest in 2021. To date, hackers have made some inroads leveraging flawed business logic or poor API implementation to do things like validating stolen credit cards, but there's not been a concerted effort by the cyber criminal world to fully compromise APIs at scale. 2021 may be the year.

The application of mathematical algorithms at scale (otherwise referred to as Artificial Intelligence/Machine Learning) will continue to be utilized on both the offensive and defensive fronts, but the use of this approach to gain the upper-hand in the cyberwar will gain huge momentum this coming year in what will be akin to a true arms-race.

Security Operations Centers (SOCs) will continue to leverage algorithmic approaches to anomaly-detection and response actions. The human interaction will move further up the response flow as AI begins to learn what is and isn't an attack. Lessening the need for lower-level human interaction will free up the time (and minds) of analysts and other SOC staff to respond more aggressively and accurately to true attacks.

Similarly, the criminals will continue to evolve their use of AI to allow their malware to move more stealthily through a network once a foothold is achieved. This AI "arms race" is likely going to be won only by the side that spends the most money evolving their technology.

COVID-19 has shaped many aspects of life on a global scale, but the economic impact of the pandemic on both local and national economies may open unforeseen opportunities for cybercriminals to exploit government organizations more than ever before. Economies around the glove have declined heavily, and tax-bases will be correspondingly reduced, forcing layoffs in the government sector.

With reduced staffing comes the reduced ability to identify phishing, block attacks, or respond adequately to successful penetrations. Essentially, governments are going to get hit more frequently and harder due to their own responses to the pandemic.

'Let us hope 2021 shows us all meeting, and beating the threat!'

Julie CULLIVAN
CTO & CPO ForeScout

As much as **COVID-19 changed everything**, it has changed very little for all the cyber-warriors in the world.

My predictions for security in 2021, are essentially the same as they have been for the last five years.

Organizations need to focus on three areas:

Building a **Culture** of Security, Gaining **Visibility** & Situational Awareness, Practicing **Basic Security Hygiene**, and Processes. And remember your work is never done.

As cyber leaders, we must continue to be the champions that **enable innovation and growth while minimizing risks.** It can be lonely and takes incredible courage, but it is what we do!

And it is because of these challenges that the **cyber community** is so important. We empathize with each other, support each other, and cheer each other like few other professional communities do.

Thank you for including me in your tribe.

Chris WINDLEY
Cyber Security Valley UK

2020 was the year of the cyber virus, **2021 will be the year of the Cyber Virus and Cyber War**.

Governments will go on the offensive (eg GCHQ) but criminals will fight back hard. What they have learnt in skirmishes will be applied in an all out war to protect and extend their ill gotten gains.

One challenge is that Cyber Security solutions were built for and priced for Enterprise structures that no longer exist.

The HQ Citadel is now much smaller and there are thousands of vulnerable nodes (people) to protect.

There will be **massive acquisition activity as solutions** cannot be adapted or developed fast enough.

We may just have invested in young talent early enough but will leaders drive change fast enough? Maybe.

In the UK there is innovative and co-ordinated activity to improve policing effectiveness (Cyber Resilience Centres).

The **UK Cyber Security Council will ensure professional standards and qualifications are improved**.

The NCSC and the WCIT and others will start the training of our young people in primary and secondary education with the Cyberfirst and Cyber Girls First Programs.

Christiane WUILLAMIE OBE
CEO PYXIS

Successful cyber security is the result of **an alignment between people, processes and technology.** Technology alone is not sufficient in the war against cyber-crime. **A strong cyber security culture, joined up cyber and risk processes, and cross-functional teamwork are mandatory.** Unfortunately, most organisations lack joined up risk and business processes. In fact, most companies have strong, independent functions acting like disconnected silos. The result is a weak cyber security culture, making it easier for external hackers and cyber-criminals.

Cyber security must become the responsibility of the entire organisation and no longer simply seen as a cyber security department or information technology issue. More and more sophisticated attackers are targeting individuals at all levels inside the company rather than attempting brute-force penetration through firewalls and modern technology defences. The entire organisation must work together to share information and issues concerning cyber security. It is the job of the modern CISO to help break down the functional silos and build a strong, enterprise-wide cyber security culture.

The successful CISO must have the ability, courage and authority to integrate all the business units and functions into an aligned, enterprise-focused cyber security team. It is imperative that the CISO report directly to the CEO and have regular access to the Board of Directors.

Dr. Kirk BORNE
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 increasing concerns around health data security and remote work security have forced a convergence of attention on the information security challenge across all organizations and sectors.

Data security is a fundamental requirement in a digitally transformed world, where **data is the fuel**, **the connector,** and **the knowledge conduit** that enables business, government, consumer, and personal transactions everywhere. Beyond data, **the networks** through which proprietary knowledge and private information flow **must also be kept secure and must be provably secure.**

The ubiquitous proliferation of sensors within the internet of things further magnifies the flows of data and the corresponding data security challenges.

Cybersecurity (including data security and network security) **is not only an enterprise-wide requirement, but a worldwide requirement**. 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.

Margaret MORTON
Mutual of America Fin. Group

Cybersecurity, 2020-forward, will see **a rise in international cooperation and public-private cooperation**, initiatives strongly emphasized in 2016.

Speaking in Tel Aviv in 2016, then DHS Deputy Secretary Alejandro Mayorkas offered that "one of the lessons…we have experienced in the cyber world is to go it alone is a very precarious endeavour, but to **work together makes us all stronger and creates an ecosystem** that will best protect us."

2016 also saw examples, which will ideally be renewed, of public-private partnership efforts bolstering cybersecurity skill advancement for students.

One example, through the Army Cyber Institute at West Point, benefited two female cadets-speaking of the program, Retired Major General Dan Balough, a Vidder (sponsoring Silicon Valley firm) board member and a graduate of West Point, described the internship as "…a door opener -- it will broaden the ability of the Academy to get people out here to what I consider the heartbeat of the 21st century." And also **a door opener for women**.

'A door opener for women.'

James CASTLE
Terranova Defense Solutions

James Castle, President, Terranova Defense Solutions predicts into the '***World of Cyber Security, will span into the balance of Cyber Detection, Cyber Defense, Cyber Warfare, and the misuse of technology.'***

The world will be politically challenged with opposing persons who use technology for the good of all or well-intended purpose in intelligence, surveillance, as well as for attacking people, corporations, and institutions. Drones will increase the threat in this stage, it will be through this technology that **terrorism will bring new cyber conflicts**. We are working together, creating Cyber Security defense strategies and solutions to defend against this evolving threat. We will see people and radical groups trying to take power, using advance technologies to try to achieve absolute control.

We are seeing drones themselves becoming smaller, quieter, enhancing in video and audio surveillance recording quality. We will see other applications emerge as technologies evolves through **artificial intelligence and quantum advancements**. Our Cyber Security companies have developed and continue to invest in the evolution of a ground-breaking combative post-quantum bi-symmetric hybrid software system to combat cyber-attacks. This will become the **forefront on cyber defense** in our constantly evolving digital world to test the integrity, as well as vulnerabilities to protect our digital planet protecting us from harm.

RAISE THE CYBERSECURITY CURTAIN

Dawn KRISTY
VP Cyber Solutions

In 2021, **we will see a "perfect cyber storm"** allowing ransomware gangs to pummel businesses of all types and sizes with lucrative ransomware attacks demanding higher ransom payments.

In Q32020, the average ransom payment increased to $233,817, up 31% from Q2 2020.

The same cybersecurity vulnerabilities that exist during the COVID-19 Pandemic (**remote work, emotional distress, distractions, human error or mistakes**) will continue into next year, which means one can predict a similar 31% increase in ransom payments for Q4 2020 and Q1 2021.

'You need not weather the storm alone. You need to bring cyber risk expertise onto your team', offer cybersecurity awareness training to your employees, and invest in cyber insurance to cover some of the financial losses (ransom payments, business interruption, data recovery, and data restoration).

'A failure in cyber risk management could mean a failure of your business.'

Ashwin PAL
Director Cybersecurity Unisys

Cyber security is no longer a standalone function. It is a key business risk that needs to be managed in a manner similar to other business risks. It is key that it is part of the Enterprise Risk Framework and has Board visibility.

Cyber security can no longer be about protection only. Breaches will occur and organisations must embrace cyber resilience so that a breach is an inconvenience as opposed to a catastrophe.

As we end 2020 and I look into the future, I see artificial intelligence and quantum computing causing a paradigm shift in cyber security.

Quantum computing will allow us to create and exploit new cyber security technology that isn't possible with current silicon-based systems. However, quantum computing will also break all current encryption causing a major headache as well.

Artificial intelligence aided by the increased computing power of quantum computing will allow us to predict and mitigate attacks before they cause an impact. On the flip side, adversaries will use the same technology to create attacks that morph on the go to avoid controls. Even with this paradigm shift, the game of cat and mouse will continue between us as cyber security professionals and our adversaries.

Jurgita LAPIENYTE
Senior Journalist CyberNews

'To make our cyber world safer for our businesses and families alike, we need to take cybersecurity training to a micro-level.'

We already have top-notch technology and know-how. But still, we, as well as our kids, our parents, and even our bosses keep clicking on malicious links, falling for those too-good-to-be-true deals, and underestimating the damage that a single weak 12345-kind-of password could do.

The world of cybersecurity is very complex, but we don't need to dive into technical details to protect ourselves. **Let's share our stories of successes and misfortunes with our loved ones and learn together how to keep the bad guys away from our cyber world.**

As a journalist, I keep talking to the cybersecurity stars who are almost ahead of time with their knowledge and innovations. At the same time, I keep meeting people who still provide the most sensitive data to the fraudsters that way compromising their identity and the company they work for alike.

We need to fill this gap between them and make them see and hear each other so ***'we can build a strong and resilient cyber society.'***

Steve KING
Founding Board Member CyberEd.io

'No matter how advanced our technology becomes, if we continue to fail in the fundamentals, we will never outrun or outgun our adversaries.'

Today, we stand on the brink of an exploding 5G threat landscape and **a rapidly advancing enemy**, yet we don't patch what we should, we are fooled by phishing attacks, our servers are misconfigured, we rush to the cloud without understanding our shared responsibility and we search for the shiniest bright objects we can find.

Nation state adversaries continue to run far ahead in the race for **education and technology leadership**, while the U.S. still has not adopted a national cybersecurity policy. While we spend billions on cybersecurity defense, a coder with a $50 weapon can still take down Capital-One.

Identity theft is rampant and deep fakes are on the horizon. China has perfected Quantum while we are still working on it. We have a skills gap of over a half million jobs. Our world is digital, yet our K-12 teachers don't have the skills to teach Cyber. North Korea has trained 10,000 cyber-hackers who write and speak English perfectly. We just fired our U.S. CISO.

'I'm an optimist, but it's hard to find the silver lining.'

Gergana (KIRYAKOVA) WINZER Unisys

'During and post Covid, CISOs, Security and Risk leaders will have to focus on delivering business outcomes like never before.'

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.

As a consequence the **CISOs, Security and Risk leaders will have to develop even more collaborative approach** with the different teams internally and with their third parties externally.

The **CISOs of the future will have to show up as effective leaders** and outstanding managers possessing soft skills like never before while knowing when to be assertive in order to win for their company and people.

Hence the CISOs/CSOs of the future will have to be a Business and Technology Risk Masters, Empathetic People Leaders and Effective Communication Managers.

Emilio IASIELLO Cyber Intelligence, Author

The global pandemic has required organizations to adjust their work practices, allowing at least some part of their work staffs to conduct business remotely.

While this unexpected turn of events challenged organizations to support remote working (a business practice many were not prepared to undertake), the same understanding cannot be offered to them in 2021.

Hostile actors have already targeted remote workers with the hopes of compromising their devices to gain access to their businesses' networks.

Since remote work is expected to continue well into 2021, this trend will likely escalate. Particularly worrisome is the perseverance of ransomware attacks that have targeted individuals and organizations alike, and **2021 may be the opportunity where the more sophisticated ransomware gangs** (e.g., REvil, DoppelPaymer, Ryuk, Egregor, etc.) adjust their tactics once again. Instead of targeting organizations directly, **remote workers** may very well fall into their crosshairs.

'The end user is frequently the weak link in the information security chain', and therefore an advantageous target to exploit given the potential benefits such a compromise would provide attackers. **Organizations that fail to address remote working in their security strategies risk suffering reputational damage and loss of public trust in addition to any financial damages** incurred by the ransom, remediation efforts, and/or legal penalties.

Scott FOOTE CISO DPO
Cybersecurity Executive

Where 2020 has been a year of great challenges, ***"2021 will see greater enlightenment in all aspects of Cybersecurity, including: Risk, Privacy, Threat, Vulnerability, and Consequences."***

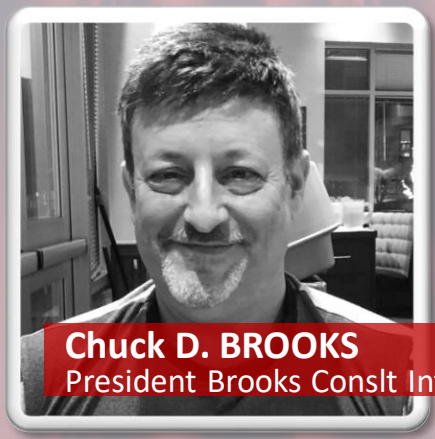
Risk – Experienced leaders will make more informed decisions that balance the risk presented by ever-increasing "digital dependence" with the rewards of seamlessly interconnected business. To better inform those decisions, Business Impact Analyses (BIA) will become far more common practice.

Privacy – Has gone mainstream. Legislation will continue to raise the bar in terms of obligations, but enforcement will be metered as governments everywhere wrestle with acknowledging they are creating greater incentives for threat actors.

Threat – Follows the money. The "easy" money today is in ransomware and extortion. And the threat there will continue to grow geometrically in 2021. Dark web marketplaces and Ransomware-as-a-Service will reap profits that rival legitimate investment markets.

Vulnerabilities – Attack surfaces continue to be porous as "work from anywhere" becomes the norm. Organizations are finally surrendering the mirage of the "perimeter" and will continue to look for more sophisticated controls beyond firewalls and VPNs.

Consequences – Every loss category will continue to grow. But regulatory fines and court settlements will begin to accelerate as a wide range of stakeholders seek to profit from corporate liabilities.



Chuck D. BROOKS
President Brooks Conslt Int.

Two key Cybersecurity Challenges for 2021

by Chuck Brooks

1. *Combating machine-driven hacker threats will be a priority for cyber defenders*

Hackers are already using machine learning algorithms to scan and identify vulnerabilities in networks. They can also combine machine learning (eventually artificial intelligence) to automate their attack capabilities by attaching malware and ransomware to those vulnerabilities. Machine learning can also be used for protection of networks and devices via scanning and recognizing anomalies.

2. *Security at the edge is also trending to 2021*

In the last few years of Internet of Things (IoT) devices (combined with trillions of sensors) have become part of the digital global network. Each device is now a cyber-attack vector soon to be powered by 5G networks on a increasingly large attack surface for exploitation by hackers. To protect IoT, CISOs are looking to reinforce cybersecurity in device endpoints. Aside from changing default passwords, there are a variety of tools and applications such as firewalls, access control, and encryption that can help secure the perimeters.

RAISE THE CYBERSECURITY CURTAIN

Carmen Marsh
CEO Inteligenca

In 2020, the entire world had to adapt to the “common” ways we now interact and communicate with each other. While novel business opportunities emerged in the form of this new “virtual business”, many companies had to effectively ascertain how they could become a “global" company overnight.

This digital transformation also presents new cyber threats that businesses need to contend with. In 2021, companies and their respective cybersecurity leaders will be challenged in some daunting new areas, everything from facing decreased budgets to an increased need for a skilled workforce.

On top of this, the shear number of cyber-attacks will continue to rise at an unprecedented pace. Fast Track programs like **100 Women in 100 Days Cybersecurity Career Accelerator** will be a crucial resolution to the growing cyber threats that all companies must deal with.

Risk Quantification will become more prominent so that decisions about the most suitable cybersecurity strategy and plans can be intelligently made. Furthermore, relentless cyber-criminals in 2021 will continue to target remote workers by conducting phishing, vishing, and crippling ransomware attacks. They will specifically target gaps in companies’ remote security postures and exploit known vulnerabilities.

”Business social media accounts will also be aimed at to carry out cyber-attacks orchestrated by bad actors.”

Tom CUNNINGHAM
Founder & Publisher

Here's an inconvenient truth ...

The good guys have already lost most of the cybersecurity battles. And the threat actors in 2021 are about to win the whole war!

For despite herculean efforts of well-intentioned design and development teams around the world -- truth told -- given time and inclination -- the bad actors can infiltrate any defense, at any time, in any place. Ransomware-wise and otherwise.

“We need a new strategy!”

It's no longer viable to scatter lots of software-centric / SaaS-only solutions across all levels of the IT stack -- application, presentation, transport, network, data link etc. -- and then "pray" they somehow magically align to provide genuine, client security in-cloud and on-prem.

As of now, there must be some sort of physical / storage / appliance defense in place to augment the scattered SaaS options -- while we wait for AI alternatives to hopefully take over 3-5-7 years out.

“We have no choice -- there are only so many battles left to fight. Before the threat actors declare permanent victory. And they would be right! The new year requires new cyber-strategic thinking!”

Alexandre BLANC
IT & CyberSecurity Director

"There is no freedom without privacy!"
Yet many give it all away freely for basic convenience.

Our generation and the next have a RIGHT to their privacy and freedom! We must build upon common sense and understanding through Cybersecurity awareness fundamentals. Privacy protection is our duty which gives us a chance to defend our freedom. We deserve and must defend our freedom of thinking, moving, and speaking.

From these facts I give you:

Connected = Hacked

Cloud = Leak

I decided to create a unique communications strategy to help decision makers ask the right questions. I want to empower security by design instead of it being a bolted-on afterthought. I hope, through my growing audience, that I can help inspire and accelerate privacy and security adoption. Inspire a security culture from conception to delivery. We should not and must not be the product!

People assume that privacy is gone and that there is nothing we can do since we cannot stop the advancement of technology. I wholeheartedly disagree and I know we can correct this path. We can and must advance and innovate technology in an ethical manner. ***"We have a right to choose and I choose freedom!"***

Frank SATTERWHITE
Founder & CEO, 1600 Cyber

As we near 2021, I am reminded of words from Thomas Sowell.

"It is hard to imagine a more stupid, more dangerous way of making decisions than by putting those decisions in the hands of people who pay no price for being wrong…"

The Big Tech that "decides for us" how we use technology in our day to day existence, has created a business model that generates trillions of dollars literally selling the most intimate, private details our lives.

These transactions are made possible by our consent every time we click or accept something on the internet. In 2021, **people will start using technology to protect not accept the exploitation of their privacy and rights.**

Mr. Sowell preceded our generation and the internet, but he understood perfectly necessary conditions for abuse of power.

In 2021, I believe that people will understand the abuses of power and our privacy and what is at stake.

"In 2021, People will demand that connectivity online, and their digital experience with social media be a moral one."

Sarah ARMSTRONG-SMITH CSA Microsoft

In 2021, we can expect to see more companies **adopting the principles of zero trust**.

Whilst it may sound like the latest buzzword, the principles are quite straight forward – **never trust, always verify and assume compromise!**

With the exponential rise of Bring Your Own and IoT devices, coupled with the accessibility of more cloud-based services, and ability to work from multiple locations, it's getting harder for companies to manage and secure their environment.

Zero trust achieves the right balance of security with productivity, by learning user behaviour and attributes to identify anomalies; and applying a risk-based approach to limiting access to core services and data, until they are verified.

"Combining zero-trust with information and threat protection, means that organisations have more visibility and control over their estate by reducing the mean time to detect and respond to external and internal threats."

Stijn VAN IMPE Unisys

Unisys' Cloudbarometer research confirmed ***"93% of organizations are now digitally transforming in the cloud"***, a momentum turbocharged by the pandemic. The global further deployment of 5G in 2021 will continue to fuel this turbocharge, driving that transformation further towards fluid enterprise infrastructures stretched across all perimeters on the pervasive IoT network.

Cyber threats are also evolving as rapidly becoming increasingly specialized and sophisticated. It's a chasing race, evident in many a stream of regrettably public incident reports. What could that mean in 2021?

One response appears in the market appears to outsource security to single security providers. The earlier cited stream of incidents and expected fast pace transformation in 2021 suggest however two important conclusions: firstly, ***any organization must assume breach will happen,*** *and* ***secondly CISOs cannot outsource their accountability for customer trust.*** What is then an alternative?

In cloud transformation, research shows organizations leveraging strong third-party partnerships are 27% more likely to be successful. Similarly, CISOs orchestrating a well-balanced ecosystem of security solutions, will achieve not only an optimized multi-layered defense, but equally empower the differentiated security innovation of their partners. That results in a stronger cybersecurity posture, which will outlower the risk of an outsourced security black box.

Victoria BECKMAN
Privacy & Data Security

In 2021, we will see **the regulatory environment** continue to shift to address the increase in quantity and sophistication of cyberattacks.

Laws need to evolve at the same fast pace as technology, especially in a post-pandemic world that relies on secure communications for all types of professional and social interactions.

The creation of standards and stronger regulation of artificial intelligence, biometric authentication, IoT devices, and smart devices will need to take center stage to combat disinformation, cyber intrusion, and other nefarious attacks to both public and private systems. (California's disclosure of bots law and the DEEPFAKES Act are some examples).

'Well crafted legislation could help shape a code of conduct and minimize disruptions to critical sectors of the economy at unprecedented levels, including healthcare, transportation, manufacturing, banking, and even legal services.'

Edward LIEBIG
CISO Charter Communic.

'For 2021, I see our cybersecurity challenges giving us four very distinct challenge areas: Cybersecurity Hygiene, Threat profiling and tuning, Insider Threat, and Advanced Persistent Threat (APT) activities.'

There will be an uptick and increasingly brazen attack pattern from various APTs around the world. Keeping up on our **Cybersecurity hygiene** will be paramount in our success in thwarting these onslaughts.

Threat Profiling will prioritize the attacks for which we may most likely need to defend. We will require more visibility on **insider activity and risk scoring** to understand where information exposure may be (or becoming) at risk.

And lastly, '***we must know our enemy and understand where they strike, why, and how.'*** As critical infrastructure upgrades the OT environments, it will open these up to more common IT-based attacks that may complicate the security of these (increasingly) connected environments." Greater focus on where and how we obtain our threat data will determine the speed and efficiency with which our defenses are tuned.

Relying on information sharing across industry sectors is a good start, but it doesn't facilitate an efficient mitigation strategy. **Managed feeds that rule your EDR will be more efficient to address Indications of Attack or Compromise (IoA/IoC).**

Agnese MORICI
NATO & CCSIRS

The world has been turned upside down by COVID-19, which has impacted nearly every aspect of our lives this year.

Attackers were quick to seize the opportunity to exploit the keen interest in this topic, including APT threat actors. This means also that nation states will be increasingly active in cyberspace next year. In 2021, there will be a significant increase in cyber espionage campaigns carried out by state-sponsored hackers.

Furthermore, ***"all the aspects of our lives are becoming dependent on technology and connectivity to the internet."***

As a result, we present a much wider attack surface than ever before. It's likely, therefore, that we will see more disruptive attacks in the future. We have seen several changes and refinements in the tactics used by ransomware gangs over the years and almost any ransomware group will adopt a double extortion model.

In addition to this, **the diffusion of IoT devices will attract ransomware gangs** that could develop specific malware variants to target these systems. Moreover a growing number of attacks will benefit from the adoption of Artificial Intelligence to carry out malicious activity.

For these reasons, we have to see cyber security as a multi-disciplinary field and we need the involvement of all the actors (private, governments, civil society) to prevent cyberattacks and to understand that capacity building plays a critical role in fortifying cyber infrastructures.

"If we want to avoid even more dramatic consequences next year, we need to ensure a more inclusive cyber security community!"

Joris DEN BRUINEN
The Hague Security Delta

In contradiction to many people within the field of Cyber security, I am not trying to be alarmist. Rather, **I am offering a path toward building trust** by promoting collaboration between the public and private sectors, and by extension, strengthening the connections of the global cyber security community.

Yes, **there are several risks and challenges in cyber security, but there are also opportunities.**

When it comes to the Internet, there is little difference between security and economy; they are two sides of the same coin.

Cyber security is about the harmonization of technologies, processes, and people. People are the foundation to making this harmony work successfully. As such, we need to educate people to make our world more cyber resilient, and to sustain the development of cyber talent to grow with cyberspace. The cyber security space requires the participation of all individuals, especially women who make up 50 percent of the labor market.

"I commit to give these (female) talents a podium now, in 2021 and towards the future. Because only together we secure this future."

RAISE THE CYBERSECURITY CURTAIN

Cecile MAYE
VP & Co-Founder Swiss AWARE

Our present world is seeing changes on an unprecedented scale. These changes are challenging us in ways that threaten to fracture our common interests and values.

It is **a turbulent world** leading to increasing levels of fear and a frustrated population. **We see ourselves continuously manipulated** by fake news, irreversible climate change, new technologies and machines replacing humans, an anxious young generation, a vulnerable ageing population, disintegrated families devoid of ethics, spirituality and massive changes in our ancestral pattern, as well as a never-ending progression toward new tech and science that invades our privacy for profit.

In the end, our complex relationship with the universe and nature is vanishing. This seems to be a quest at any price. It is a symbol of performance & order over meaning and identity. Would it be the right time now to challenge this situation to give priority to meaning over performance?

On **the forefront of cyber security**, we recently launched Swiss AWARE. A grassroots non-profit designed to reinforce awareness for all, including our youngsters. A foundation with dedicated experts that work collaboratively to build solutions for all humankind. From education and innovation to sound ethics, pleasure and meaning.

"Challenging the status quo & setting a path to a new era!"

Michel CAZENAVE
CISO/CSO PwC France

"Nowadays CTI information shows that cyberattacks have shifted from disrupting to 75% attempts (source Cyber Intelligence x sectors Alliance) ***to take control of target"*** (getting a remote access, encrypting and/or stealing data, setting backdoors and spying activity) associated with revenues either directly claimed from victims or by selling knowledge, data, vulnerabilities and tools on the dark web.

"This evolution should lead every CISO, with the unconditional support of their company boards of directors" who are perfectly aware of the risk even if they still wish to understand how to help, to rush a 360° hardening and best practices review of their processes, assets and systems in order to become a too costly target to pawn, compromise or ransom, associated to an overall proactive training and monitoring strategy to be able to **react appropriately in case of incident.**

Christophe AUBERGER
CTO, CISO Fortinet

As 2021 approaches, there won't be any drastic change when it comes to cyber threats, we can just imagine that they will certainly be more present, more sophisticated and more effective.

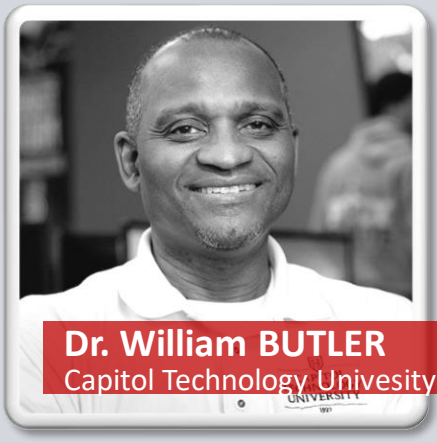
The growth in the number of Ransomware attacks is more than likely, potentially increasingly using the growing capabilities of edge computing, Internet of thing and new communication technologies as 5G.

And at the same time ***"the attack surface of companies will continue to increase with the accelerating digital transformation."***

A strong trend is emerging to improve the proactive approach to cyber risks, which consists of setting up a fusion center. This new business entity will be born from the merger of the SOC, CERT and cyber-Threat Intelligence functions.

Thus, the security operation center, supplemented by the more strategic approach of the computer emergency response team and fed by information from threat intelligence services will further reduce detection times, or even act on the threat before being confronted with it in an operational manner. The emergence of these entities will further increase the more and more frequently challenge facing organizations relating to the ability to sort, store and process a constantly growing mass of data.

"Big data is likely to be an increasingly important ally of cybersecurity."



Dr. William BUTLER
Capitol Technology Univesity

This is truly the 911 moment for the current generation. The pandemic has long term implications both for our economy and our very way of life.

"2021 promises to be another year of challenges for security staffs around the globe." COVID-19 has accelerated digital transformation and telework efforts to support essential business operations just to stay in business.

2021 will certainly be **the year for great advances in collaborative technologies designed to enable and secure vital remote access services.** There will certainly be more emphasis on securing the worker/manager, patient/doctor, and student/teacher virtual engagements for example. These users must get better at recognizing Phishing and Ransomware attempts, thus making effective security awareness training even more critical.

It's all about building TRUST between these parties, while using an untrustworthy global network - The Internet. 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.

Kai Michael HERMSEN
'Charter of Trust' Siemens

Effective Immediately – ***"For any business, cybersecurity must become a strategic source of opportunity."***

It is not just about being open-minded and having a forward-looking perspective on cybersecurity, but it is absolutely an organization's most significant and costliest vulnerability.

The best alternative is to use cybersecurity as a catalyst for organizational and digital transformation. To do this and to be genuinely successful in cybersecurity, it is best to keep the cybersecurity human factor front and center: remember, we need to understand and appreciate at least two groups of people - those we are protecting AND their adversaries.

This will become the organization's best cybersecurity defense - its own people. **Think of them collectively as a "human operating system" that needs to be regularly updated using cybersecurity education.** Where patching and upgrading is the "education" - this is vitally important and a great opportunity - to minimize risk, while helping to fuel overall digital transformation efforts.

And finally, ***"the idea of distributed trust/zero trust must be ubiquitous. You cannot "fix" a decentralized architecture (IoT) with a centralized security model."***

Gary HAYSLIP
CISO SoftBank

As a CISO and mentor in our community, I get asked to predict where I think the field of cybersecurity is going and I believe my predictions over the last several years are now coming to reality due to COVID-19.

I have always envisioned ***"architecting and leading a security program, technology stack, and team designed to be flexible and responsive to change."***

Over the last year due to the pandemic I have witnessed businesses in multiple industries fully embracing **cloud technologies** as their staffs moved to work remotely. These business changes have impacted security programs and through discussions with my peers, I am seeing a shift in how security and its controls are now focused on **cloud infrastructures**, supporting dispersed development teams, and enabling employees to work securely from home.

I believe cybersecurity will continue to evolve as organizations pursue and embrace technologies like SASE, Zero-trust, and 2FA to ***"manage remote operations and protect their sensitive data and employees."***

I also believe CISOs and teams will no longer need to be geographically located enabling them to **recruit talent from anywhere and build security programs leveraging remote work technologies** to meet today's challenges and tomorrow's threats.

Isabel María GOMEZ
Continuity Lead SCA

In crisis times, where your company's strengths will test your resistance, tenacity, and decisions, always remember that you 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.

Let me share with you a few golden lessons learned that will help you to prevent and recover faster your business processes from the major threat that we deal today: ransomware. Review the log of your antivirus, they are your canary bird in the mine.

Check continuous transfers of information that are not 'Business as Usual'.

"***Your backup system is not an expense. It is a priority.***"

Run a prevention audit during an incident to save all records and forensic, meanwhile guaranty a quality check of your recovered systems.

Andrew WILSON
Director Finidhyn® Ltd.

"Cyber security exists to engender trust. Without trust the full potential of the digital economy cannot be realised. In supply-chains the need for traceability and transparency is hugely important." Food and Pharmaceutical fraud are two big areas of risk, and are key areas of risk management.

Blockchain offers a solution to the concerns for security and traceability, however it is still cumbersome and slow as a technology and not as secure as some might think. Increased processing power is required in order to facilitate this technology and the advent of Quantum computing may provide this when it is available.

The question is whether the world can agree a global standard for to end-to-end systems integration for supply chains or whether the current proliferation of systems will continue to dominate.

A global blockchain standard coupled with end-to-end systems integration will be the key to secure future supply chains. If agreement can be reached, then the only remaining security issue will be corrupt data entry at source and data inaccuracy within the process.

Within the Global food and Pharmaceutical supply chains there is ample evidence that actors actively game the systems, so this will remain a security issue for the foreseeable future.

RAISE THE CYBERSECURITY CURTAIN

Lisa VENTURA
CEO & Founder UK CSA

2020 has brought cybersecurity to the forefront like never before, and it has also seen a huge rise in the amount of cyber-attacks that prey on the vulnerability that people find themselves in because of the COVID-19 pandemic.

In the light of the changing world we now find ourselves in, I have ***the following predictions for cybersecurity in 2021:***

Remote working will continue to rise

The COVID-19 pandemic forced us all to change the way we work very quickly. Many organisations decided not to return to the office in 2020 leading to a reduction in real estate, and this is likely to continue in 2021.

Ransomware will continue to be a major threat

Ransomware attacks are more intricate and devastating. Demands can run into millions of pounds, and this is only going to get worse.

Cloud security will become king

Organisations that have migrated to the cloud will need to focus on their cloud security and understand the relationships they have with their providers.

Security validation will be needed to keep defences and budgets in line

With the shift in how we work, organisations will need to rely more on security validation to reduce their spend and optimise their security.

Dr. Robert BORNHOFEN
Strategy & Innovation

'Digital data is the common thread that holds us all together. It defines who we are, how we interact, and what makes economies function.'

And yet, we're being threatened in 2021 by an estimated US$6 trillion in cybercrime.

Business and security leaders are challenged to **change the way they approach cybersecurity risk.** Growing levels of hacking, phishing, stealing, ransomware attacks, etc. are occurring. It's real.

While there a number of countermeasures to consider, attention is drawn to:

Accountability: Cybersecurity success relies on all of us to take ownership, to be active stewards in safeguarding system access and use.

Preparedness: Expect partnerships between companies & schools to sustain and grow a population of talented, highly-skilled technicians.

Cooperation: Organizations will take a more active role than in the past to share and collaborate on cybersecurity threats & countermeasures. Expect international forums like the WTO to put growing pressure on its member states to comply with multilateral cybersecurity agreements.

No doubt, **failure to take cybersecurity threats seriously can be expensive.** CapitalOne's breach in 2019 cost between US$100 million and $150 million. It takes years to build a reputation and only a few minutes for a cyber breach to ruin it.

Diana KELLEY
CTO SecurityCurve

In 2021 **the explosion of passwords** that users need to remember will continue and grow as a challenge. Remember a many strong passwords is hard, but password re-use increases the likelihood of password theft and account take over. This is why I expect 2021 to see consumers adopting **password wallets/managers that generate unique passwords** for each account and then store them safely. Enterprises will continue to move towards "**passwordless**" strategies and ongoing, continuous access verification. Both consumers and enterprises will implement MFA (multi-factor authentication) such as one-time use codes via text and biometrics to improve password-only security.

Another trend to watch in 2021: **attackers are getting better at identifying vulnerable targets**, focusing on **at-risk industries and critical infrastructure**. These are organizations that can suffer severe impacts to human safety and health if access to critical IT systems are interrupted. We saw this happening during the early days of COVID when health systems, non-profits, 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 use to interrupt activity in industries like healthcare, government, and energy.'***

Scott SCHOBER
CEO Berkeley , Cyber Expert

As the world continues to embrace **5G wireless technology** in 2021, consumers will begin to **experience some major advances in speed** and low latency which has always plagued 3G/4G/WiFi/Bluetooth wireless transmissions. Our 5G smart phones will be significantly more powerful as we become even more dependent upon them.

From a **cybersecurity perspective**, cybercriminals will exploit new attack surfaces on our 5G smart phones involving a new wave of IoT (Internet of Things) devices in our homes, cars, and offices which did not have security 'baked-in' when they were designed rather quickly. **Billions of unsecured IoT devices will become the new conduit for cybercriminals** to gain entry into our 5G smart phones containing all of our personal data.

'There are real threats that higher risk industries using 5G technology for mission critical applications need to be concerned with.' This is especially true when looking at the **vulnerable critical infrastructure** as it is wirelessly monitored such as: water, sewer, and electric grid all of which are often relying on legacy older 3G / 4G technologies. It is important to realize that 5G networks will not turn on with a 'flick of a switch' so there needs to be forethought when and where there is no 5G coverage that networks can throttle back and use existing 4G LTE networks that may not have the same level of security.

Dr. Ian McANDREW
Capitol Technology University

Cyber risk is a major risk for all organisations nowadays. This risk will compound more in 2021 to the extent that we are likely not even to control the risk ourselves.

'Almost all Cyber Risks fall within one of the 16 US defined Critical Infrastructures and it is a collective responsibility to do our most.'

These all in turn link to satellite communication and current international treaties are obsolete, ineffective and possibly ignored.

Cybersecurity in space must now be considered as critical as our own systems to maintain robustness in our operations. Space wars are real, the risks and consequences potentially changing all parts of our lives.

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.

Andrey SUVOROV
Kaspersky Lab

"Cyber Immunity is a new way of thinking and designing of digital service in terms of resilience."

Traditional on top security includes anonymizer, device control, anti-DDOS, anti-SPAM, anti-fishing, parental control, update control, sandboxing, and many others... Recognize them?

But, in the era of IIoT, millions or even billions small and smart devices have to execute valuable tasks not security checks, otherwise digital business services will be unreachable.

Welcome, cyber immunity with microkernel, isolation on level of each and every components and security policies engine supervising all interactions.

With current speed of digital changes cyber risk topic should follow (or even precede) morning coffee with stock news...

'Safe future starts today!'

Ken MUIR
vCISO LCM Security Inc.

A vast majority of organizations today are not aware that nation-states and cybercriminals are real organizations with real motives and intent to harm to build their financial empires. These organizations are using the same organizational structure from CEO on down.

They are highly motivated, highly financed, highly disciplined and highly organized in a way we generally are not.

We are in a war to save our businesses and economies. Collateral and economic damage is enormous and is forecast to get worse.

They say, "the truth is out there" Well, the solution is out there also. For many years, the world's best minds have built guide-books on how to increase cybersecurity and reduce risk. It is now time to develop the same discipline needed to protect ourselves.

For 25 years, this is the philosophy I have lived by. It works.

Sun Tsu: "If you **know the enemy and know yourself**, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Follow industry best-practice. It may just save your business.

Dr. Vladimer SVANADZE
Cybersecurity Strategy and Policy

The **accelerated transition to cloud** technologies and related systems will reduce the role of the local-area network over time, being replaced by so-called Secure Access Service Edge (SASE), which implies the remodelling of the security architecture.

The following trend that is currently evolving will be a preferential direction in the field of cybersecurity by 2021; it is the **Zero Trust Network Access Technology** (ZTNA);

Advanced detection and response cybersecurity systems. Systems that monitor and collect activity data to detect potential cyber threats.

Artificial intelligence and machine learning technologies in the digital world will provide even greater impetus in cybersecurity. The widespread use of smartphones in our daily lives will further expand the probability of cyber attacks on mobile applications. The issue of protection of personal data and privacy in cyberspace will have increasing relevance.

Three cybersecurity topics for 2021:

Against the background of digital transformation, it is vital to raise consumer awareness regarding both cyberculture and new technologies continually; Permanent support to ensure business continuity regardless of the workplace or location; Maintaining a resilient critical-infrastructure to compete with global challenges and risks in a constant-changing and unstable world.

RAISE THE CYBERSECURITY CURTAIN

Kris® K.
InfoSec Professional

As we carefully stride towards a post pandemic world and the year 2021, it is important that we acknowledge that we are 'in transition' towards a new normal. 2020 has been a tough year for many of us, Nevertheless, it also offers us a ray of hope towards building a more secure future. The current pace at which we have been embracing technology in our professional & personal life demands **'cognitive agility'** on our part i.e. a reasonably good speed with which we can change and adapt to the new norms. I am hopeful that few pointers below will help position ourselves better:

The manifold **increase in disinformation and deepfake media** across the digital world will test our abilities to separate voice from noise. Our 'common sense approach' to cybersecurity and attempts to stay safe online will be put to test, by lazy and **creative cybercriminals, who will be better armored with automated tools & techniques.**

"Trust will be one of most valuable & difficult instincts to find and part with"; eventually assessing our abilities to conduct 'due diligence' and verify. We are at a juncture in this 'transition' where **awareness/adoption of cybersecurity basics** will help us navigate more swiftly & safely through the dynamic digital world ahead.

"Wishing you all a healthy, prosperous and a safe year 2021."

Thomas HARRER
CTO IBM Systems EMEA

"In the current times, organizations enjoy large opportunities to innovate the business based on Data and AI."

A **hybrid cloud platform architecture** enables agile development combining mission critical data with new and unstructured data. New business services can leverage more information, insights, knowledge and automation to increase the efficiency of digital business processes and solutions.

While the chances are tremendous, there is also **a very dark side of the digitalization** – organizations depend more on their data and securing and protecting systems and data becomes a strategic must. Cybercriminals have evolved their resources and skills to compromise nearly every organization no longer restricted to technical exploits but also by social engineering and by applying specific understanding of the target organizations.

The probability of a data breach is increasing because hackers are becoming smarter and more competent. The average cost of a data breach is about USD 3.86 million in 2020 (Ponemon Study). It is therefore wise to **apply encryption** to the data – mitigating the damage if the data gets stolen.

It is important to protect the data and **establish an air gap to the backup copy** in case the hackers destroy the operational data after having destroyed the backups. **A comprehensive security strategy** helps to mitigate the rising cyber-risks.

Chris KUBECKA
Middle East Institute Cyber

With **the advent of 5G and 6G on earth and in space**, the world of exploitable and vulnerable IOT and IIOT will grow exponentially unless regulations are put in place to protect both privacy and security.

Privacy will become more and more intertwined into cybersecurity, surpassing concerns from consumers and businesses when dealing with technology.

During the COVID-19 pandemic, health related intellectual property became both important in ensuring economic sovereignty and a primary target of nation-state attacks. In the near future, medical and health research data will be paramount, allowing countries with more advanced cyber offensive capabilities an advantage over countries without cyber legislation, planning and adequate cyber defensive capabilities.

"The future in a nutshell is in the hands of technically advanced and capable countries with skilled populations and professionals versus those without said capabilities, preparation and planning."

Cyber peace accords should be seriously discussed and signed, because the future of war is not in the form of tanks and guns but in cyber physical and cyber malicious attacks against critical infrastructure and the technology in our very homes.

Salman QADIR
Founder & CEO SALQ ™ Tech

"Cybersecurity is one of the most important subjects of the Fourth Industrial Revolution", and COVID pandemic showed the importance of Digital Transformation.

Digital Transformation brings new cyber risks that could also impact the initiative of smart cities globally, as cyber threats arise daily to target digital and physical assets.

IoT devices are a key component to enable any businesses or smart city/factory, and the number of IoT devices and their manufacturers also are increasing. When deploying IoT devices, it is important that security steps be taken.

Governments must establish a Regulatory Framework to monitor each stage. As well, **cybersecurity skills are required for government leaders** who otherwise will not be able to implement cybersecurity principles.

A coordinated framework without bureaucratic hurdles will ensure the full alignment of policy initiatives and actions in the digital governance mechanism.

Securing our cyber safety will also lead to **achieving the SDGs 2030 by United Nations**. To achieve these goals, emerging technologies such as Blockchain and Artificial Intelligence can also help. As well, ***"Research and Development in cybersecurity is required to ensure that Digital Transformation initiatives are well prepared."***

Daniella TRAINO
vCISO Pinecone Technology

As Gerd Leonhard explored in his 2016 book Technology v Humanity, anything that can be digitalised, will be.

We're in the throes of that rapid shift. Regardless of the societal challenges of trust and equity, this coupled with automation, virtualisation and algorithms will be the foundations to our future. From a cyber perspective, this poses **a hyper-sized attack surface increasing the pressure on defenders** to manage and respond to threats.

There are many layers of asymmetry inherent to the data-driven economy – between human and machine intelligence, between firms, and between nations across the digital divide.

We could see greater regulation and economic strategy focused on cyber security and privacy from each country -Artificial Intelligence is driving some of this already with Trust Frameworks but it should broaden. In Australia, we're seeing the interconnectedness of economic prosperity and the growing awareness of the cyber threat landscape leading the Federal Government to propose recent amendments to the Critical Infrastructure Protection regulations and Privacy Act.

The critical infrastructure on which we operate is built on and with, many components of hardware and software, which is unassured or for which assurance is increasingly complex to determine. State-based and state-sponsored cyber espionage increasingly targets civil society and corporations, while attribution is not clear (weaponisation of data makes this difficult). This will see cyber security teams increase their focus on threat intelligence, monitoring and supply chain integrity - How do we secure our business and business partners while connected? How do we identify and respond to the emerging threats? With secure coding practices and toolchains not yet matured (developers and data scientists) and support ways of working - we need to see an increased focus on better security training and education in the coming year.

Stewart SKOMRA
CEO Vanderplaats R&D

Single intrusion points increase in Step-Functions with commercial and consumer 'digital' instrumentation. However, these networked nodes push data Acquisition - Transformation - Presentation further and further throughout a Geometrically increasing interconnected constellation. The result is an astounding number of single-points-of-failure of ever-diminishing Value.

"Value declines faster than attack surface grows."

The result is Black Hats will not be able to feed themselves and their families.

State-sponsored Black Hats (the non-Value-Add Breakers) bent on destruction have declining marginal returns.

More and more destruction leaves less to destroy. Systems serve Humans. **The Human-System identity relationship is the point of attack.**

White Hats (the true Maker-Braker-Taker community) have the advantage of Evasion – staying ahead of destroyers through spatiotemporal (Space + Time) elusiveness plus strong encryption. It is key to keep moving.

The Code Maker (i.e. White Hat) will always outrun the Code Breaker (i.e. Black Hat). At risk are only the non-Black Hat, non-Value-Add Breakers thinking they are safe standing still behind their 'barriers'. Peace.

Dr. Merrick WATCHORN
Watchorn Innovation Group

What is Cybersecurity?

Cyber is a team sport with no distinction between the offense and the defense.

Cyber leadership strives to build the best possible balance of potential risk and threat mitigation strategies to offset unknown threat-actors. Thus, all areas of cyber are affected by the decisions made by another area of influence and often are misunderstood at the time of the decision-making process.

Without this underlying understanding and approach cyber leaders are left to play "Whack-A-Mole" for the myriad of cyber-related issues facing any organization.

As the 21st century moves the cyber-domain to the forefront of investment the innovations associated with them become more important.

The various threats, cyber-actors and nation state actors requires that investigation into 5G, Internet of Things, Quantum, Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP) and Semantic Ontologies (SO) can now be blended into a unified service offering of Cognitive Computing, which affords new cybersecurity products such as Quantum-AI services based on learned behavior of a given system and with this potential outcome, the need for cyber leadership to understand these types of innovation becomes paramount.

According to the Federal Bureau of Investigation (FBI, 2018), "***the rise of cybercrime is apparent; however, the diversity of the attack-surface space continues to expand and our funding is limited, we have to prioritize our approach to perceived versus real threats in the 21st century***."

Cyber leadership should consider how conflict, management, providers, users and information technology all affect the outcome of its organizational protection programs for the immediate future and the long-term effects that it may have on its bottom line.

Each organization should strive to define the cyber domain not as conflict but of domain activities, define the importance of education on all areas of topical interest, build a well-trained and defined work force, and most importantly build the next generation of cyber leaders based on fact based analysis that goes beyond the cost and ease of implementation but to the ability to provide true cybersecurity to itself and its clients.

Sailaja VADLAMUDI
SAP Labs India

'Trust is The Ultimate Currency Developed through Security Culture'

Cybersecurity is not only a technical challenge but a human challenge. Criminals don't always exploit technical deficiencies but often rely on people to access sensitive data. Building and sustaining a strong security culture within a company is extremely important at the same time very challenging part of cyber security. To establish a strong security culture, we need to align it with employees' personal values and needs. Create a culture that protects business data, personal data, networks, etc. The only way to not let things fall through the cracks is to make security a habit, make it part of the value system, bring it into the culture! Security is deeply intertwined with trust: with reliability, accountability and responsibility. Trust is the ultimate currency, and that's what must be developed through culture.

CISO's Role is Evolving

The role of CiSO is growing important and it is also evolving at a faster pace than ever. Increasingly they have seats in the executive suite as security is not just about the risk it is about reputation. CiSO is not just limited to Influence budgets at board rooms but they have a huge game to play starting from acquisitions, portfolios, in a nutshell, better aligned with business strategies. As we all witnessed that security is not a technology problem. It is a business problem. And it needs to be decided on from a business perspective. On the other hand, there is a growing dependency between physical and cybersecurity. we can't have cybersecurity evolve without physical security doing the same. Henceforth corporate security and IT security must go hand in hand, coordinate closely with each other as one team to ensure the overall security and safety of our organization and the community.

Career with Purpose & Impact

Cyber Security is no longer only about extrinsic i.e. money, recognition & perks but purely intrinsic purpose & impact. Millennials will make up more than 60 percent of the global work force by 2027. Future workforce is not just motivated by their pay checks. Purpose, new skill, variety, autonomy matters the most to them. One can find purpose and meaning in many ways of protecting organisations and citizens. Above all this is rapidly changing dynamic environment and many a times we have surprises, the challenges it brings keeps your mind sharper.

Security career is much more than hacking. Hacking is tiny piece to do with offensive roles that is breaking into stuff and doing things. The defensive side of it is building i.e. to mitigate and prevent to build and set up systems securely, contributing to protecting business and in turn lives around us. '***Hackers join forces and succeed***'; it is need of the hour professionals work together and contribute on several communities within your organization or other groups and work towards a mission. We all must be a head of the challenges and develop flavour on research and contribute to national policies and frameworks as it is the need of the hour. To sum up the opportunities to share, learn, collaborate and contribute are endless.

Tech for Life

By Jim HAGEMANN SNABE

Chairman at Siemens and A. P. Moller Maersk

"As organizations reassess their purpose, they are turning to technology to drive the changes they need to make. Yet this technology must be managed correctly if it is to deliver the benefits that stakeholders expect. By adhering to the principles of Tech for Life, those who create and use technology can ensure it continues to be a force for good.

Throughout history, technology has helped us meet challenges. It has been an engine for greater prosperity, equality and health. The printing press, the steam engine and the development of electrical power have all transformed our world for the better.

Today, whether augmenting our work with robots, connecting us to our loved ones around the world or using Machine Learning to improve tumor detection rates, technology has the potential to be an even greater force for good.

Indeed, technology is the force that will drive the transformation that organizations must undergo as they develop a wider purpose.

Click for progress

Faced with even the greatest challenges on the planet, technology is providing solutions. We have the technology to make electricity sustainable, cheap and available for all. To deliver this requires both the adoption of existing technologies as well as intelligent electricity distribution and storage solutions.

Tech-utopia or Tech-Dystopia?

As leaders, we must use technology correctly if we are to meet the expectations of our new stakeholders. Yet we have seen how technology is open to abuse, misuse and malicious intent.

And, with the benefit of historical perspective, we have seen how many of the noble uses to which technology has initially been put have given rise to unwelcome and unforeseen consequences."

Dancing With Systems

* “The mindset of the industrial world assumes that there is a key to prediction and control. But self-organizing, nonlinear feedback systems are inherently unpredictable. They are not controllable. They are understandable only in the most general way. The goal of foreseeing the future exactly and preparing for it perfectly is unrealizable. The idea of making a complex system do just what you want it to do can be achieved only temporarily, at best. We can never fully understand our world, not in the way our reductionistic science has led us to expect.…”

“Systems thinking leads to another conclusion, however—waiting, shining, obvious as soon as we stop being blinded by the illusion of control. It says that there is plenty to do, of a different sort of “doing.” The future can’t be predicted, but it can be envisioned and brought lovingly into being. Systems can’t be controlled, but they can be designed and redesigned. We can’t surge forward with certainty into a world of no surprises, but we can expect surprises and learn from them and even profit from them. We cannot impose our will upon a system. Systems cannot listen. We can listen to what the system tells us and discover how its properties and our values can work together to bring forth something much better than could ever be produced by our will alone.”

Cybersecurity is becoming the most important security topic of the future – particularly in the age of digitalization. It’s diversity and complexity require that a fusion of thought leaders, managers and cyber-technical transcend simple ideology and aspire to a higher level of cybersecurity awareness, resilience and criticality (Watchorn, 2020).

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The very nature of the cyber domain has transformed in recent years from a purely technical autocrat discussion group to a globally infused strategy policy agenda for most countries concerned with public health, privacy and digital information protection requirements (Watchorn & Bishop, 2017).

The threat landscape is changing constantly and, probably, by the time you have finished reading this eBook, a new vulnerability was discovered. It is for this reason that the foundation of knowledge and best strategies is so important, because it will assist decision makers in rapidly absorbing new challenges and applying security principles to remediate threats.

People and organizations need to trust that their digital technologies are safe and secure; otherwise they won’t embrace the digital transformation. Digitalization and cybersecurity must evolve hand in hand. The cyber domain depends on cooperation of a diverse group of subject matter experts who are asked to predict current and future threats across a large spectrum of the threat-landscape and this type of leadership is often a challenge to discover and the importance of trust cannot be understated by any measure (Watchorn, 2015).

“Seeing systems whole requires more than being “interdisciplinary,” if that word means, as it usually does, putting together people from different disciplines and letting them talk past each other. Interdisciplinary communication works only if there is a real problem to be solved, and if the representatives from the various disciplines are more committed to solving the problem than to being academically correct. “

After Word

We are living in a complex and messy system which cannot be controlled. Where every solution creates a NEW problem.

Why is cybersecurity so hard?

- It is not just a technical problem
- The rules of cyberspace are different from the physical world's
- Cybersecurity law, policy, and practice are not yet fully developed
- There's not enough manpower in the world to make sure networks are 100% secure 100% of the time, especially with the prevalence of a cloud-based infrastructure
- The definition of cybersecurity is at odds with management
- The training for personnel is often the first budget cut in a fiscal year
- The people making the decisions often do not understand the nature of the problem nor the technical issues at the lowest level.

The technologies of tomorrow are at the heart of our daily life and work. Concurrently, you cannot teach understanding, you construct it. Now is the time for calm, rational, holistic planning and methodical action. Time for diversity and inclusion. Time for emerging technologies to create and add positive values in societies and bring return on capital and human capital invested globally. Time to embrace Augmented and Artificial Intelligence solving the humanity's most burning problems. Time for women to step on the dance floor of emerging technologies and cybersecurity industries. Reskilling is a great issue. Inclusion is as important as innovation. We will have to go into learning mode, be willing to be taught, by each other and by the systems, keeping in mind and making sure that trust, security and ethics in technology is essential in the decades to come.

Let's face it, the universe is messy, it is nonlinear, turbulent, and chaotic. Nevertheless, it is dynamic and fast moving in all directions at once. It spends it time in a transient behavior on its way to somewhere else, not in mathematically neat equilibrium, for example entropy. It self-organizes and evolves without any inputs from external sources. Thus, creating diversity, not uniformity. That is what makes the world interesting, that is what makes it beautiful, beautiful, and that is what makes it work.

References: Donella Meadows. Dancing With Systems. Versions of this piece have been published in Whole Earth, winter 2001 and The Systems Thinker, Vol. 13, No. 2 (March 2002).

Retrieved from https://www.mendeley.com/guides/web-citation-guide

My Research Supervisor: Dr. Ian R. McAndrew (https://works.bepress.com/ian_r_mcandrew/)

Excelsior! *Ludmila M-B*