TOP CYBER NEWS MAGAZINE

SPECIAL EDITION

THOMAS HARRER
IBM DISTINGUISHED ENGINEER
CTO SERVERS & STORAGE EMEA

IBM and IBMers
THE SUCCESS STORY

ARCHITECTING THE FUTURE

EXCLUSIVE ARTICLE BY
MICHEL CAZENAVE
CISO/CSO, PwC France, Monaco, Maghreb
ARE WE APPROPRIATELY SKILLED TO BE TOP CLASS CISOs?

ARCHITECTING THE FUTURE WITH TECHNOLOGY, SECURITY and CYBER-RESILIENCY at IBM TechU 2021

HOW THOMAS HARRER, MEMBER OF THE IBM ACADEMY OF TECHNOLOGY AND TECHNICAL EXPERT COUNCIL DACH, CHIEF TECHNOLOGY OFFICER FOR HARDWARE SALES IN EUROPE, MIDDLE EAST & AFRICA, AND HIS TEAM ARE DELIVERING INNOVATION FOR IBM CLIENTS

Shine
The Light
OF
KNOWLEDGE
TRANSCEND
BORDERS
in
Extraordinary
TIMES

About IBM

International Business Machines Corporation (IBM)

is an American multinational technology corporation headquartered in Armonk, New York, with operations in over 171 countries. The company began in 1911, founded in Endicott, New York by trust businessman Charles Ranlett Flint, as the Computing-Tabulating-Recording Company (CTR) and was renamed "International Business Machines" in 1924. IBM is incorporated in New York.

Nicknamed Big Blue, IBM is one of 30 companies included in the Dow Jones Industrial Average and one of the world's largest employers, with over 345,000 employees as of 2020. At least 70% of IBM employees are based outside the United States, and the country with the largest number of IBM employees is India. IBM employees have been awarded five Nobel Prizes, six Turing Awards, ten National Medals of Technology (USA) and five National Medals of Science (USA).

Sourse: wikipedia.org

"Today's digital transformation is creating millions of jobs that require new skills, especially in STEM fields. I am proud to announce that IBM has committed to skilling 30 million people worldwide by 2030. Learn more about IBM's commitment and how it will impact the global workforce..."

Arvind Krishna, Chairman and Chief Executive Officer of IBM

About **IBM Technical University**

What is **IBM TechU**? IBM® TechU provides deep technical training on IBM IT infrastructure, products and solutions for clients and business partners. TechU events enable attendees to engage directly with IBM's world- class expertise, game-changing technology and each other.

The **IBM TechU 2021 virtual edition** on **25-28 October** - is a premier virtual training event that supports the development of deep technical expertise on IBM Systems products and solutions. It provides you and your teams the opportunity to learn about the technologies required to increase skills, productivity, and innovation.

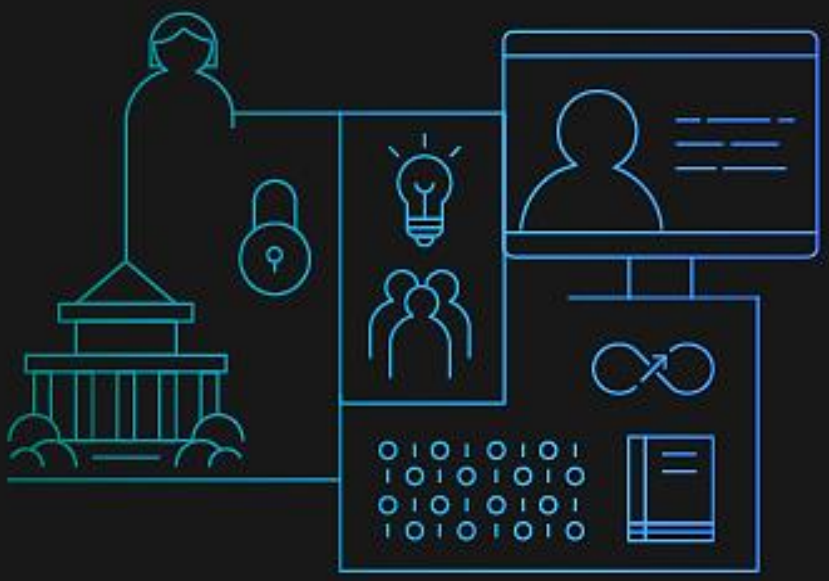
The IBM TechU Experts: Lectures are provided by IBM, IBM clients and IBM Business Partners on advanced technical topics across IBM Power, IBM AIX, IBM i, IBM Storage, IBM Z®, Red Hat Enterprise Linux (RHEL) and IBM LinuxONE.

"Can you believe it? IBM TechU is next week! We look forward to seeing you at IBM TechU this year! Continue to learn. Reinvent yourself."

Mahdad Majd
Global TechU at IBM

IBM TechU

2021 virtual edition
25-28 October



Featuring IBM Power, IBM Storage, IBM LinuxONE and IBM Z

Register now!

IBM TechU

IBM

Architecting the FUTURE

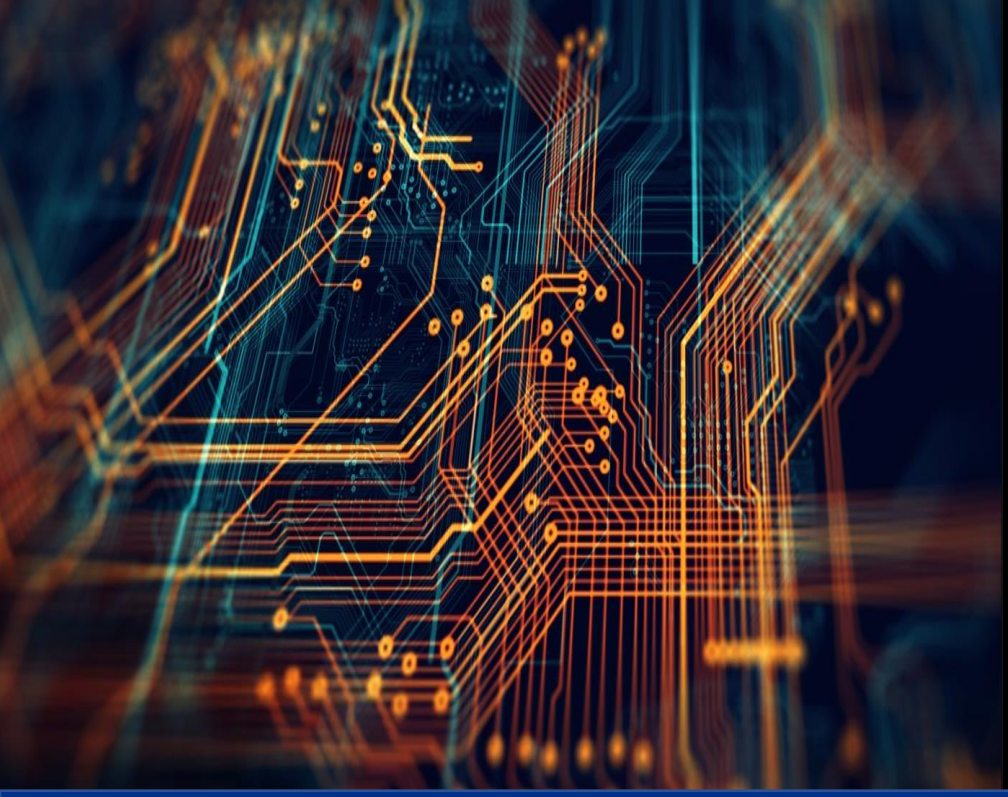
Thomas Harrer

Distinguished Engineer, Chief Technology Officer, Servers & Storage, IBM EMEA

Member of the IBM Academy of Technology

~

Member of the Technical Expert Council Central (TEC)



IBM TechU 2021 virtual edition

27-28 October

Architecting the Future

track

Architecting the Future within the IBM TechU 2021 virtual edition is about innovation based on technology. Targeted for leaders in IT, anyone who is interested in the future of IT and how to drive IT innovation will find value in this series. Participants will get a complete picture of drivers and ingredients for innovating your business with IBM Z, LinuxONE, Power and Storage and beyond from technical leaders. Eight hosted live sessions will inspire you about what's next. 8 Sessions covering the topics:

Architecting the Future - Agenda

Wednesday, 27 October 2021		Thursday, 28 October 2021	
8:30 - 9:20 EDT	**Architecting the Future - Keynote - Innovate with Technology** **Thomas Harrer** - IBM Distinguished Engineer, CTO Server & Storage EMEA **Jamie Thomas -** General Manager, Strategy & Development IBM Enterprise Security Executive **Ken King** - General Manager, Power Systems	**8:30 - 9:20 EDT**	**Architecting the Future with an open Hybrid Cloud platform** **Chris Morgan -** Senior Director, Hybrid Platforms Customer & Field Engagement at Red Hat **Steve Sibley** - Vice President, Power Systems Product Management **Frank van Der Wal** - Technical Lead Data and AI on IBM Z **Thomas Harrer** (Host)
	Break - 10'		Break - 10'
9:30 - 10:20	**Architecting the Future - the Power of Co-Creation** **Elisabeth Stahl** Director and Distinguished Engineer, IBM Garage for Systems **Kris Baritt** VP, IBM Technology Garage Leader **Thomas Harrer** (Host)	**9:30 - 10:20**	**Architecting the Future with Data and AI** **Glenn Brouwer** - CRO Braincreators **Dr. Sebastian Lehrig** - AI Systems Architect **Marvin Gießing** - AI Systems Architect **Sabrina Kopecki** - Master@IBM Technical Sales **Thomas Harrer** (Host)
	Break - 10'		Break - 10'
10:30 - 11:20	**Architecting the Future for Banking** **Niek de Greef** - Rabo Bank - Lead Architect Payments **Donna Dillenberger** - IBM Fellow, CTO Hybrid Cloud Systems Research **Pål Krogdahl -** CTO, Global Core Banking & Payments ISV Practice **Thomas Harrer** (Host)	**10:30 - 11:20**	**Architecting the Future with Security and (Cyber-)Resiliency** **Stéphane Nappo** - Vice President. Global Chief Information Security Officer (CISO) @ Groupe SEB **Martin Borrett** - IBM Distinguished Engineer, CTO IBM Security EMEA **Dr. Axel Koester -** Storage Chief Technologist, ESCC **Thomas Harrer** (Host)
	Break - 10'		Break - 10'
11:30 - 12:20	**Architecting the Future - the Ageless Connection** **Steven Perva -** Ensono, Senior Mainframe Modernization Engineer **Luisa Martinez -** Z Digital Transformation Wizard, Software Engineer **Frank De Gilio** - Distinguished Engineer, CTO of Mainframe Declunkification **Thomas Harrer** (Host)	**11:30 - 12:20**	**Architecting the Future and the Future of Computing** **Dr. Heike Riel -** IBM Fellow, Department Head Science & Technology **Huiming Bu, Ph.D.** - Vice President, Hybrid Cloud Technology Research & Albany Operation **Dr. Robert Haas** - Department Head, Cloud and AI Systems Research, IBM Research Europe **Thomas Harrer** (Host)

About Thomas Harrer

Thomas Harrer holds the title of Distinguished Engineer and the Chief Technology Officer Server & Storage EMEA at IBM. He is a member of the IBM Academy of Technology (AoT), (Board) Member TEC DACH, and a computer scientist with a strong background in mathematics, computer architecture and application architecture.

In the mid-nineties, through his groundbreaking diploma thesis, he combined the world of genomics and Artificial Intelligence by leveraging the power of neural networks for analysing genes in the human genome. He is very open-minded and especially interested in cross-collaboration between different areas of expertise.

Since 1995, Thomas Harrer has been working with IBM as a client engineer and architect focused on infrastructure architecture helping clients to innovate with technology increasing cross-platform efficiency.

Starting 2017, Thomas has taken over the responsibilities of Chief Technology Officer for IBM Servers and Storage for Europe and more recently extended them to EMEA. In this technical leadership role, Thomas Harrer and his team deliver innovation with hybrid clouds and AI, leveraging all types of data and evolving the technology that enables clients to achieve business success.

With a strong foundation in computer/data science and extensive experience in IT infrastructure and technology, Thomas enjoys bringing different elements together to build the architecture of the future. He loves to discuss technology, trends, AI, da blockchains and architectures for mission-critical hybrid cloud solutions.

Architecting the Future

With Technology, Security and Cyber-Resiliency

Author: Thomas HARRER

"In 2021 we see greater enlightenment in all aspects of Cybersecurity, including: Risk, Privacy, Threat, Vulnerability, and Consequences." ~ Scott FOOTE

The total value of Data and Information is constantly growing, and so is the sheer volume of data. Becoming more digital and embracing data-driven automation is enabling organisations to optimise their business models and operations.

"As organisations become increasingly dependent on the data, operational considerations around availability, consistency, and accuracy are mission-critical."

And as data is becoming the new currency, breaking into systems is exfiltrating this data is massively lucrative. A specific incarnation of business risk with growing economic impact is Ransomware.

In the 2021 X-Force Threat Intelligence Index report, based on billions of data points from clients and public sources, a major finding is that Ransomware was the most popular attack method in 2020, making up 23% of all incidents IBM Security X-Force responded to and helped remediate. Ransomware is big business. An estimation was that "Sodinokibi (also known as REvil) ransomware actors alone made at least $123 million in profits in 2020 and stole around 21.6 terabytes of data." **Recent events indicate that the reported figures are the lower limit of the realised gains.** This example alone shows just how lucrative Ransomware has become.

Having an accountable process for vulnerability management is one of the levers helping organisations improve their ability to embed cyber risk management into the fabric of their business. Organisations need the ability to discover, assess, prioritise, remediate, and measure their IT solutions and processes regarding cyber risks. Having resilient IT and data architectures, coupled with insights and services from leading providers, further adds to that equation.

To defend against the threat of Ransomware, a protection that has proven to be effective is having an air gap between the active data and regular copies of the data, particularly when there is technical assurance in place to ensure that the data cannot be modified or deleted even if admin accounts get compromised.

"IBM Servers and Storage provide strong technical assurance capabilities for accessing data in secure enclaves (including in the IBM Cloud-based on Hyper Protect services, running on Mainframe technology) and for immutable copies of the data"

What is clear is that organisations need a modern, open, unified approach to security. IBM Security's mission is to **align the enterprise security strategy to the business strategy,** protect digital users, assets and data, manage enterprise defences against growing threats, and modernise security with an open, multi-cloud platform.

"Improving cyber resiliency requires a multifaceted approach, and there are many products and services available to help organisations. The organisations that are building the highest resiliency are the ones that know how to choose and deploy their technology appropriately to better manage cyber risk by effectively prioritising the threats that matter."

Learning From Adversity

And Building Architecture For A Cyber-Resilient Future

Author: Jay HIRA

"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." ~ Dr. Kirk BORNE

The disruption and forced isolation resulting from this global pandemic has slowed things down for some of us, providing an opportunity to re-evaluate our lives. Through reflections, the one big takeaway for me personally has been realising how resilient we are as a species and how deeply adversity influences change in us, for better or for worse.

"We can choose to learn lessons from our adversity and use this force to transform ourselves into diamonds rather than continuing to go through our lives as ordinary pieces of coal."

In late 2019, when the first case of viral pneumonia got reported, no one would have anticipated that our world was about to turn upside down. Soon after, fearing human-to-human transmission of the virus, most countries invoked the biosecurity screening of arrivals. If we were to draw a parallel, this is similar to how we've traditionally relied on traffic filtering controls as our first line of defence against cyber threats.

Complicated problems such as the pandemic never have a quick fix cure-all solution. In parallel to enforcing supervised quarantine for inbound travellers who may be likely carriers of the virus or the new variants of the virus, we relied on the medical communities to combine their brilliant minds to develop one or more vaccines. When all preventive measures fail, the vaccines are capable of training our immune system to respond and recover when we do get knocked down by the virus. Vaccines are equally capable of protecting us against the evolving mutant strains of the virus. Drawing parallels to our cyber security industry, **businesses in the past may have believed in the fallacies of silver bullet solutions that would assure them of protection against most cyber-attacks but are now planning better for the processes to manage, limit, control and recover back up on the other side of a cyber-attack.**

Cybersecurity, unlike a combat sport, is an unfair fight.

"Cybercrime has evolved significantly from individual cybercriminals to cybercrime groups with similar ideologies and subsequently developing into government-funded nation-state actors. These adversaries that we face today leverage technology to innovate and collaborate at a much faster pace than our cybersecurity teams"

That has pushed us away from the traditional moat and castle methodology to **embracing the cyber resilience mindset. This mindset shift provides a long-term strategy that focuses on withstanding cyber-attacks leveraging risk management principles.**

The very foundation of risk management is the acceptance of the fact that risk can never be zero, and there will always be an inherent risk in doing anything that we may wish. Applying this principle to cybersecurity, businesses have realised that no matter how much they invest in cyber protection controls, they may still not be able to eliminate the imminent risk of cyber-attacks. The only effective way to architect for the future would be to apply risk management principles to bolster the ability to,

"Prepare for, Respond to and Recover from the inevitable cyber-attack"

In the famous words of Rocky Balboa, "It ain't about how hard you hit. It's about how hard you can get hit and keep moving forward".

To sum up, the lessons learnt from the current global pandemic have been to focus efforts on testing and tracing in parallel to isolation and treatment measures to support the world's citizens. Similarly, businesses in the past may have downplayed the potential of being under a cyber-attack. However, they are rapidly adopting a cyber resilience mindset that encourages them to focus on their abilities to respond, recover, learn and evolve from an adverse event.

Executive cybersecurity advisor and internationally recognised cybersecurity strategist, Jay Hira best describes himself as a lifelong learner. He has been fascinated by computers from an early age which prompted him to study the science and engineering behind them at the University. Jay started his career as a pen-tester and has 15+ years of experience across different cybersecurity disciplines such as attack, defence, architecture, and strategy. As a result, he had many different roles, ranging from technical, tactical-delivery-focused, strategic-big picture-focused, and customer-facing. The exposure from travelling continents and rapid adaptation has taught him many things, such as personal resilience, the importance of building strong relationships and picking new things up quickly. It's also given him an incredibly diverse and broad perspective, which helps him get results.

Mr Hira is a team player and has always believed that teams can achieve more together than individuals, which is very important to him as a leader. He is passionate about collaborating with educators, helping students develop skills to transition to the workforce successfully. Continuing on his journey to help businesses strengthen and shape their approach to cybersecurity, Jay is excited by what the future holds, which puts him in a fantastic position to lead teams and customers into a safer, more secure and cyber-resilient future.

How My Non-Traditional Path Led Me to a Career in Cybersecurity

Author: Anne LESLIE

"In the face of a massive industry-wide cyber-skills shortage, my story is evidence that there is cyber-talent out there just waiting to be found; but finding it means defining talent differently, hiring differently, onboarding differently, and managing career progression differently.."

~ Anne Leslie

On paper, nothing predestined me for a career in cybersecurity. I graduated from business school with a dual degree in European business, spent several years working in banking, and the best part of a decade as a stay-at-home mother to my three kids before returning to work in a succession of business development roles in technology companies.

I might have stayed on that track, had it not been for a decision to return to school to do an Executive MBA in 2014. That marked something of a watershed for me because it was the first time that I gave some really deep thought to the kind of work I wanted to do, the kind of people I wanted to work with, and the kind of company I wanted to work for.

I realized that I wanted to be part of something bigger than myself, to work with people who are motivated by more than money. I wanted to work for a company that understands that it has a responsibility to society that goes beyond quarterly results and shareholder returns.

My first step towards my current role as Senior Managing Consultant in IBM Security came about when I was still a software seller in a different company, looking to make a pivot in my career because I had reached a point where simply being told to hit an annual sales target wasn't enough to sustain my motivation and engagement.

"I yearned for purpose, for a higher meaning. I wanted more than a job. I wanted to make a difference"

Pivoting towards purpose

Sometimes life throws us a bone by bringing people into our lives at the very moment we need them the most. A fortuitous encounter with a long-standing cybersecurity practitioner, who runs an initiative called CyberWayFinder that exists to increase diversity in the cybersecurity workforce, flourished into a friendship and mentorship. Soon after, I began looking seriously at the viability of cybersecurity as a future career option.

In 2018, I started working towards my first industry-recognized certification in Cloud Security from (ISC)². I attended a bootcamp where a shame-inducing question from a fellow student — "What on earth are you doing here, you haven't even got a degree in IT?" — made me recoil and forced me to confront my impostor syndrome head-on. I got to grips with a body of knowledge that was largely alien to me and made my peace with the fact that, while I had a lot to learn, I didn't need to know everything.

I studied nights and weekends… and I nailed the assessment. In getting my Cloud Security Professional certification, I proved to myself – and to all the people who doubted me – that I was both serious about moving into security and capable of it.

"In spite of being a divorced mother of three. In spite of having no degree in IT or engineering. In spite of having 'no technical security experience"

Or, actually, maybe because of all of that!

Hiring for potential

Today, I work in cybersecurity at IBM because two exceptional managers hired me based on my leadership potential, my intrinsic capabilities, my transferable skills, and the values that define me. Instead of focusing on everything that I'm not, these two managers identified my attitude, my determination, my adaptability and my ability to learn as key success factors for succeeding in cybersecurity.

They saw what I wanted to be, they believed in what I could be and brought me in to IBM to give me a career and life-changing opportunity for which I will be forever grateful.

Hiring for potential

On paper, I was the consummate 'risky hire': I don't have the 'right' qualifications, I haven't followed the typical career trajectory and when I started out, I had little technical security experience. All of which were factors that had caused other companies to either reject my job applications summarily or make me feel small and ashamed in job interviews for not being the archetype cyber professional they believed they needed.

"For sure, there is still little about me which matches the traditional cyber-professional archetype – and yet, ***I have never been more successful or happier in my career"***

Bringing my whole self to work

I'm finally working in an environment where **I feel an unprecedented level of psychological safety, where I can be authentically me and really do my best work ever.** I'm finally working in an environment where the corporate values aren't just words on the walls and in the annual report: they feel real, I can identify with them, and I'm proud to be associated with them. I'm finally working in an environment which nurtures potential, celebrates learning, protects difference, and upholds integrity.

Ten years ago, I was a stay-at-home mother. Today, I'm a mother AND a senior consultant in cybersecurity. IBM invests in my development as a professional, provides me with the flexibility I need to be the parent I want to be and offers a culture where I can be the kind of person I want to be.

Bringing my whole self to work

In the face of a massive industry-wide cyber-skills shortage, my story is evidence that **there is cyber-talent out there just waiting to be found**; but finding it means defining talent differently, hiring differently, onboarding differently, and managing career progression differently.

This is exactly what IBM is doing and it's the reason I am where I am today.

I consider myself to be immensely fortunate to be in a role in a company that gives me purpose, fortunate to work with colleagues who support me and drive me to be better, and fortunate to have a manager who believes in me and challenges me to reach even higher.

*"I came to IBM by chance, but I will stay by design. I'm proud to work in security and even **prouder to be an IBMer!**"*

Senior Managing Consultant for Threat Management (SIOC) in the EMEA Centre of Competency (CoC) @ at IBM Security, Anne Leslie is a fervent believer in the power of people!

Passionate about responsible technology, Anne's career spanned the intersection of financial services, European regulatory policy, blockchain and IT in leadership roles in both sales and advisory.

Bilingual in French and English, she holds an Executive MBA from HEC Business School in Paris and the CCSP in Cloud Security from (ISC)² in addition to multiple technical platform certifications. Named as One to Watch 2020 by IFSEC, today at IBM,, her focus is on Security Intelligence & Operations Consulting, specializing in Cyber Talent Transformation, on accompanying international enterprises in uplifting their IT/OT/IoT security operations to keep pace with a volatile business and threat landscape.

Anne champions the application of human-centered approaches like Design Thinking to some of the most wicked problems facing Security practitioners. Anne co-hosts two podcasts: Out of Band & Below the Surface – available on You Tube & Spotify – amplifying a broad spectrum of issues related to cybersecurity, emotional intelligence & cognitive diversity, & loves to shine a light on the everyday cybersecurity heroes that do tireless work keeping us all safe.

This article was first published on the **IBM Careers Blog** on 22/09/20:

https://www.ibm.com/blogs/jobs/2020/09/28/how-my-non-traditional-path-took-me-to-a-career-in-cybersecurity/

BRING
CISOs
INTO
THE C-SUITE
CONSIDER
CYBERSECURITY
the
STRATEGIC
PRIORITY

About Michel CAZENAVE

CISO and CSO for PwC France, Monaco & Maghreb, President at CIX-A / Cyber Intelligence X sectors Alliance, **Michel CAZENAVE**, is passionate about cybersecurity. Pragmatic and exploring new avenues, Michel leads his teams to protect people, property and business in line with PwC's goal: building trust in society and solving important problems.

He has been involved for over 25 years in cyber security, security and crisis management in demanding and complex environments such as the Ministry of the Armed Forces and the Ministry of Foreign and European Affairs.

He represented France at the Council of the European Union in the CCIS preparatory body from 2008 to 2017 and has been laureate of 01 Business & Technologies 2012 CISO Special Jury Prize in 2012.

Member of CESIN (www.cesin.fr) since its creation, he is also since December 2019, engaged as President of the CIX-A / Cyber Intelligence X sectors Alliance (www.cix-a.net), ISAC which aims to organize the sharing & the operational, tactical and strategic collaboration between CISOs & their teams to improve the cybersecurity ecosystem and help members and their supply chain to defend themselves collectively.

Are We Appropriately Skilled
To Be Top Class CISOs?

Author: Michel CAZENAVE

"CISO is the 'path-advisor' guiding the best way to successful business decisions at the edge between fears and ambitions"

~ Stephane Nappo

Cybersecurity strategy begins with the CISO himself

While systems become more complex, hybrid, interconnected, nowadays CTI information shows that "cyberattacks have shifted from disrupting to 75% attempts to take control of target" (source Cyber Intelligence x sectorsAlliance) and get a remote access, encrypt and/or steal data, setting backdoors and spying activity associated with criminal 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 preparation of their incident response plans, proactive training and monitoring strategy to be able to react appropriately in case of incident.

"The increasing sophistication of cyber criminals coupled with the rapid shift to digital technologies has emphasized cybersecurity's importance. Those factors will have a knock-on effect on CISO role and impact as well as the C-level view and understanding on cybersecurity"

While C-level consider now cyber security as a strategic priority, the CISO needs to evolve leadership to match this new interest within an organization. It means to switch and ascend to a C-level forward thinking attitude to lead and orient strategy, investment and projects with a clear, didactic prioritized and argumentative discourse on business challenges and threats and potential impacts.

While this internal shift is important, CISO can also focus on creating or joining external circles of trust to collaborate with peers. It creates value by breaking CISO isolation, leveraging knowledge and threat awareness and sharing or benchmarking information, advices, tools, methodologies and procedures in similar context. It is already a trend with ISACs or similar organizations (and even used by cybercriminals). **Collaboration is probably the next additional must-have to leverage CISO's existing weapons and means.**

All other aspects of cybersecurity strategy shall focus on helping IT to deliver business aligned, secured, and resilient services which is quite business as usual for a CISO and combine well known recipes (understand the business, hire experts, use best practices, deploy security tools, use external cybersecurity services and consulting, be certified, analyse risks, define controls, patch, audit… to definitely become a too hard target to hit.

Are we appropriately skilled to be top class CISOs?

What the ancients called a clever fighter is one who not only wins, but excels in winning with ease. ~ The art of war by Zun Tsu

The cyber threat is no longer an illusion nor discussed as a hypothesis but as a certainty. The disaster is imposed on us every day, with shocking publications: "data breach", "spear phishing", "ransomware" and soothing crisis declarations: "we are in control of the situation and are investigating", "we have called in the best experts", "the impact measurement shows that the sinews of the company's war are not affected", "no data has been affected".

The CISO is, within his or her company or organization, THE point of reference for cybersecurity. Charged with defining the right strategies, implementing the right tactics and directing operations to protect the company or entity from cyber threats, the CISO has an enormous responsibility that is extremely difficult to assume in order to effectively defend a perimeter that is by definition porous, shifting and variable in geometry.

Most employ several means to achieve this: recruiting experts (difficult), implementing best practices (demanding), deploying cybersecurity tools (expensive), setting up an SOC or CERT (complex), using service providers or consultants (helpful), obtaining certifications (not sufficient), networking with peers (useful) and share information, successes and failures with trust circles (ISACs). None of these are bad and a CISO who succeeds in getting his entity to run plans that includes a complete and consistent set of these means is probably a fair good CISO.

I might require to be a good performer in many domains including technical, organizational, logistical and administrative. We all have studied, been trained in those domains. If it is not the case, this might be an improvement point for all of us and a starting point for people that wish to become CISO.

The funny is how do one define this "complete and consistent set"?

Successful CISOs adopt whole or part of following or similar steps:

- ***understand how they are a target, what is the threat and how it could turn bad for their company***
- ***align cybersecurity strategy first with non-IT priorities (business, compliance, legal, risk...) and then with IT priorities***
- ***take business users behaviors into account to adapt the plans to business activities and think the best possible cybersecurity user experience***
- ***build a clear problem-solving road map based on people, organization and technic providing supporting argumentation about rationale, expectations, value creation and return***
- ***sell the plan to entity management and stakeholders, including IT, legal, risk management and finance***
- ***run the plan and celebrate each progress or achievement to build collective cyberdefense spirit, including entity management and staff***
- ***make the board aware and train the entity management first, in order they lead all others in the right direction***

You find this simple? It is not! Once you achieve with a great satisfaction the first four items and turn on to the last three of them, problems begin, and it is probably time to understand why. CISO actions and cybersecurity do have an important impact on the organization and thus, the last domain, which is probably the most important and has nothing at all to do with all that cybersecurity stuff, is **how you interact with stakeholders, shareholders, management, experts, staff, providers and suppliers to discuss, convince, coordinate, require, allow, deny (yes, it is possible to say no!) manage and transform.**

If nobody told you so before or if you did not know. I have to tell you that **people relationship is THE main part of the CISO life.** If you don't interact correctly, you will miss your goals, stay painful for each step to achieve your plans and remain a fair good CISO. Let us all move to **become highly skilled CISO**, grow as top-class ones, gain efficiency in the journey to success and train our human relationships.

Editor-In-Chief

TOP CYBER NEWS MAGAZINE

and

RAISE THE CYBERSECURITY CURTAIN!

Ludmila Morozova-Buss

Cybersecurity Woman "Influencer" of the Year 2020

TOP CYBER NEWS MAGAZINE - SPECIAL EDITION - All rights reserved

21

TOP CYBER NEWS MAGAZINE

CYBER FOR GOOD

We communicate
Technology, Innovation, and Cybersecurity

«Cyber-attacks can cause widescale disruption, economic upheaval, and even physical damage. If nothing is done, future attacks could become even more destructive and impact the power, transport, and communications systems we all depend upon to live and work.»

Arvind KRISHNA
Chairman and Chief Executive Officer, IBM

«The increasing sophistication of cyber criminals coupled with the rapid shift to digital technologies has emphasized cybersecurity's importance. Those factors will have a knock-on effect on CISO role and impact as well as the C-level view and understanding on cybersecurity. »

Michel CAZENAVE
CISO and CSO for PwC France, Monaco & Maghreb
President at CIX-A / Cyber Intelligence X sectors Alliance