Behind the Keys:
Women Who Secure the Future

(In)Securities Special Edition: Day 4 Featuring:

Inssata RICOURT

Celebrating International Women in Tech Day

Inssata RICOURT

Transitional CISO & DPO- Advisor and speaker in Cybersecurity

Inssata RICOURT has over sixteen years of experience in information systems security, specialising in cybersecurity, cloud, and data protection within major national and international organisations. She holds a specialised master's in Management and Protection of Personal Data, which enabled her to become one of the first Black women in France to serve as a Data Protection Officer (DPO).

She began her career in information systems security and data protection before taking on expert roles in data protection, cybersecurity, and cloud security. In these capacities, she developed and implemented cybersecurity strategies, as well as public and private cloud security strategies, ensuring compliance with regulatory obligations and operational constraints in both public and private sector organisations.

As an expert, she has supported organisations through major transformations, including mergers, acquisitions, and restructuring, as well as digital transformations in information systems security and cybersecurity. She has also guided compliance programs to ensure adherence to current regulations.

Feature in (In)Securities- Special Edition- Day 4

Inssata RICOURT

Transitional CISO & DPO- Advisor and speaker in Cybersecurity

Moreover, she founded Black Is Ethical, an initiative dedicated to ethical hacking. This platform brings together ethical hackers, promotes their skills across Africa and internationally, and advocates for their professional recognition by policymakers and regulatory authorities.

Drawing on her experience and expertise, she established INSSATAD CONSULTING, a cybersecurity consulting and training firm that helps organisations transform regulatory and operational constraints into growth opportunities. The firm also delivers training and awareness programs for executives and their teams on cybersecurity, data protection, artificial intelligence, blockchain, and more.

She is also the President of GLOBAL AFRICA EXPERTISE, a network of experts that supports African countries in implementing their projects and programs across various sectors by providing specialised expertise.

Inssata RICOURT

1. What inspired you to pursue a career in technology/cybersecurity, and how did you get started?

My interest in cybersecurity stemmed from my desire to protect customer data in the hospitality industry and my curiosity about information systems. After studying international business, hotel management, engineering, and information systems management, I gradually transitioned into cybersecurity.

Becoming aware of payment system vulnerabilities and the critical need to secure banking data against fraud and identity theft strengthened my commitment to this field.

I obtained certifications and supported various organisations in protecting sensitive data and securing their infrastructures, ensuring compliance with standards such as PCI-DSS and ISO 27001.

Inssata RICOURT
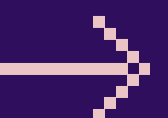
2. Can you describe a defining moment in your cybersecurity career that made you realise this was the right path for you?

As a woman in cybersecurity, I have encountered significant challenges, including underrepresentation, entrenched gender stereotypes, and the ongoing need to prove my expertise in a male-dominated industry.

One of the biggest hurdles has been establishing credibility, particularly in environments where women remain underrepresented in technical and leadership roles. For instance, when I was appointed as a Data Protection Officer (DPO) in a major organisation, I initially faced scepticism. To overcome this, I **committed to continuous learning, earning industry-recognised certifications** such as ISO 27001 and eIDAS, and honing my expertise in data governance and cybersecurity. This relentless pursuit of excellence enabled me to build credibility and demonstrate my value through measurable results, including guiding organisations towards compliance with international security standards.

Another key challenge was the **lack of female role models and dedicated support** networks. To bridge this gap, I actively engaged with organisations such as the Cybersecurity Advisors Network (CyAN), where I serve on the board of directors, and Black Is Ethical, an initiative dedicated to increasing female representation in cybersecurity. Additionally, I founded INSSATAD CONSULTING, a firm specialising in data governance and secure digital transformation. These commitments have provided invaluable opportunities to collaborate with experts, gain strategic insights, and inspire more women to enter and thrive in the field.

Leading cybersecurity certification projects for digitally transforming companies has also required me to juggle multiple responsibilities. Effective prioritisation and organisational skills have been instrumental in overcoming these challenges while maintaining a structured and methodical approach. Today, as a strong advocate for diversity and inclusion within CyAN, I remain committed to empowering young women to pursue careers in cybersecurity. I firmly believe that gender diversity is a powerful catalyst for innovation and enhanced performance in the industry.

*Feature in (In)Securities- Special Edition- Day 4*

Inssata RICOURT

3. Can you share some of the key challenges you faced as a woman in this field, and how you overcame them?

One of the biggest challenges I have faced as a woman in cybersecurity is the underrepresentation of women and the constant need to prove my skills in a predominantly male environment. There were times when I was the only woman in a meeting or project, which sometimes created a sense of isolation or made me question my legitimacy.

I overcame these challenges by relying on three key factors: continuous learning, determination, and networking. Education helped me strengthen my technical expertise and gain recognition for my skills. Determination was essential in persevering through obstacles, asserting my place, and seizing career opportunities.

Lastly, **networking with other women in cybersecurity and participating in diversity-focused initiatives have been crucial in building a supportive ecosystem.**

Today, I am actively committed to promoting women's inclusion in cybersecurity through awareness programs, training, and mentorship, helping future generations thrive in this strategic field.
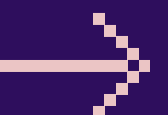
4. Who has been your biggest influence or mentor throughout your career, and what specific lessons or turning points have you experienced because of them?

Over 15 years ago, women in cybersecurity were scarce, typically holding leadership roles in large companies and participating in initiatives like Elles Bougent to promote women's roles in technical fields.

Their presence, though limited, demonstrated that women had a vital role to play in this sector. **My journey has been shaped by family influence and key professional experiences**. Inspired by my father, a telecommunications technician, I developed a passion for technology and digital security, leading me to follow a similar path to protect information systems.

A pivotal moment in my career was recognising vulnerabilities in payment systems and the urgent need to secure banking data against fraud and identity theft. This realisation propelled me to focus on strengthening digital infrastructure security and guiding businesses through this transition.

My professional network and cybersecurity communities have provided essential learning experiences in resilience, innovation, and collaboration, helping me grow in an ever-evolving field.

These influences have reinforced my belief in the importance of diversity and inclusion as key drivers of performance and security, motivating me to actively support and educate the next generation in this rapidly growing field.
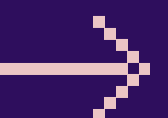
5. What are the biggest challenges women face in the technology/cybersecurity industry today? Can you share specific examples from your own experiences?

The major challenges women face in the tech and cybersecurity industry include underrepresentation, gender stereotypes, and the perception of lacking legitimacy compared to their male counterparts. These barriers make it difficult to access leadership roles and gain recognition for technical expertise. Additionally, balancing professional and personal life, particularly during maternity, remains a significant challenge as many women juggle family responsibilities with the demands of a high-pressure career.

In my experience, family support has played an important role in my career, allowing me to manage both professional and personal commitments effectively. O**vercoming these challenges requires fostering flexible and inclusive work environments** that empower women to succeed while maintaining work-life balance.

6. How has the industry evolved for women since you started your career? Have you noticed any significant shifts, and can you share a personal story that illustrates these changes?

Since the start of my career, the cybersecurity industry has made significant progress in female representation. Fifteen years ago, women made up only 7% of the workforce, with few in technical or leadership roles. By 2019, this number had risen to 24% globally, although in some regions, such as France, it remained lower at 11%.

However, **these figures are improving, as seen in the growing number of women at professional forums, increasing from less than 10% to nearly 30%.** Initiatives like Black Is Ethical, Women 4 Cyber, and CEFSYS have played a crucial role in promoting inclusion and providing opportunities for women in this field. While progress has been made, there is still a long way to go to achieve true gender parity in the sector.

Inssata RICOURT

7. What role do diversity and inclusion play in fostering innovation in tech/ cybersecurity? Can you share a personal example or case study where diversity directly led to innovation within your team or project?

In the field of cybersecurity, diversity and inclusion play a crucial role in fostering innovation and enabling a more comprehensive approach to complex challenges. By bringing together diverse perspectives, organisations can develop more effective and holistic solutions to emerging threats.

As a woman in this sector, I firmly believe that my rigour, methodical approach, and ability to multitask have contributed to the success of numerous projects. This rigour, often observed among women in project management, combined with the ability to juggle multiple priorities, enables us to tackle both technical and organisational challenges effectively.

For instance, in a recent project I led, the diversity within the team allowed us to approach technical aspects from different angles and identify innovative solutions.

The inclusion of diverse perspectives was a key factor in overcoming obstacles that might have seemed insurmountable with a more homogeneous team. Additionally, my ability to manage multiple aspects of the project simultaneously while maintaining a high level of organisation was crucial in meeting deadlines and ensuring the quality of deliverables.

Thus, **female leadership—underpinned by rigour, multitasking skills, and diverse viewpoints—represents a significant asset in cybersecurity.** This approach not only fosters innovation but also strengthens the overall security of information systems against evolving cyber threats.
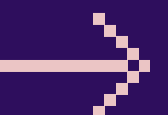
8. What are the most exciting trends or developments in the industry right now that you're passionate about?

Several trends are currently shaping the cybersecurity industry and driving significant advancements. On one hand, artificial intelligence and automation are transforming real-time threat detection and response.

On the other, **securing connected devices (IoT) and cloud infrastructures has become increasingly critical as these technologies continue to proliferate.**

Furthermore, the use of blockchain for authentication and digital identity management is gaining traction, while the concept of Security by Design is encouraging organisations to integrate cybersecurity from the outset of system development.

Additionally, supply chain risk management is becoming a growing priority, as cyberattacks increasingly target suppliers.
These developments are driving innovation and enhancing the resilience of systems against emerging threats, making cybersecurity more proactive and effective.

Inssata RICOURT

9. What advice would you give to young women considering a career in technology or cybersecurity?

To young women considering a career in cybersecurity, my first piece of advice is to believe in themselves and never doubt their legitimacy in this field.

While challenges exist, the industry is expanding rapidly and offers countless opportunities.

It is essential to embrace continuous learning, stay up to date with emerging trends, seek out mentors, and build a strong professional network. Additionally, taking risks and innovating should not be feared, as cybersecurity is a field that rewards initiative and creativity.

Finally, resilience is a key quality—persevering in the face of challenges and viewing obstacles as learning opportunities will be invaluable. **With passion, determination, and an open mind, women have an important role to play in this dynamic and ever-evolving industry.**

Inssata RICOURT
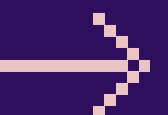
10.Can you share examples of initiatives or programs that have made a real difference in promoting women in our field?

Numerous initiatives have been established to support women in cybersecurity by providing training, mentorship, and networking opportunities.

Programs such as Women 4 Cyber, CEFSYS, AWDC, and the Women in Cybersecurity initiatives by CISA and the SANS Institute have been instrumental in fostering diversity and professional growth in the sector.

Additionally, organisations like Girls Who Code introduce young girls to technical careers early on, equipping them with the skills needed to pursue a future in cybersecurity.

Moreover, CyAN (Cybersecurity Advisors Network), of which I am a member, actively contributes to networking and supporting women in this field. By facilitating knowledge-sharing and best practices, these initiatives enhance diversity and promote the greater inclusion of women in this rapidly evolving industry.

Inssata RICOURT

CyAN
Cybersecurity
Advisors
Network

11.If you could envision the ideal future for women in cybersecurity, what would it look like? What key changes would have been made?

The ideal future for women in cybersecurity would be one where gender equality is fully realised—both in terms of representation and recognition of skills and opportunities.

On one hand, workforce parity would be achieved, with fair representation of women across all levels, including technical and leadership roles.

On the other, the industry would cultivate an inclusive culture, where diversity is recognised as a strength that drives innovation and helps solve complex problems.

Greater access to training, mentorship, and career development opportunities would encourage more women to enter and thrive in cybersecurity. At the same time, flexible work environments would support a better work-life balance, and equal pay would be an unquestioned standard.

Ultimately, this vision would lead to a more inclusive and dynamic cybersecurity industry, where women play a pivotal role in protecting systems and developing innovative solutions against cyber threats.