WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
GREECE

W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

INTERVIEW WITH ELENI!

Name: Eleni Psychia
Job Position: Group Head of Cybersecurity | Governance, Risk & Compliance
Current Employer: Motor Oil Hellas
Cybersecurity areas of interest: Governance, Risk & Compliance, Information Security Strategy, Regulatory Compliance, Risk Management
Previous career(s): 9 years of experience in IT and cybersecurity across the healthcare and oil & gas industries
Educational background: BSc in Information and Communications Engineering, MBA in Technology Management, MSc in Law and Information and Communication Technologies
Other interests/hobbies: Reading, traveling, exploring technology trends, painting
Favourite quote: “Let curiosity lead you and determination carry you forward.”
Network with me: https://www.linkedin.com/in/eleni-psichia/
Are you hiring? : At the moment, I can’t comment on specific openings, but opportunities do come up regularly - I’d recommend keeping an eye on our Motor Oil careers page and LinkedIn for upcoming roles

Intro & Inspirational

1. Which values are guiding your life and work?
Integrity and courage are my compass. Integrity because trust is fragile, in cybersecurity and in life, and once it's lost, it is very hard to rebuild. Courage because often we must take decisions without guarantees, defend ideas that are not popular, and open doors for others even if no one has done it before us. These two values, combined with empathy, allow me to lead with both strength and humanity.

2. What's the most important life lesson you've learned?
That growth often hides in discomfort. Every time I've been outside my comfort zone, whether it was taking a project I didn't feel fully "ready" for, or taking on unexpected challenges, I discovered resilience and skills I didn't know I had. The lesson is: don't run from discomfort. Lean into it, because it is usually where the most powerful transformation happens.

3. Success mean different things to different people. How do you define success?
I define success as living in alignment with my values, while contributing to something larger than myself. Titles and achievements come and go, but the real measure is whether you've created impact and stayed true to who you are. My best advice: don't confuse speed with progress. Sometimes success means slowing down, reflecting, and choosing deliberately, rather than rushing to check boxes.

4. ***Do you think your job makes a difference? How?***
Yes. Cybersecurity is about enabling trust. Every secure system, every protected piece of data, every awareness campaign, is a way of telling people: you are safe, your voice matters, your identity is protected. I don't see it as just protecting assets; I see it as protecting dignity and freedom in the digital age.

5. ***What is the best and the worst piece of advice you received? (+How did you unlearn the latter or use it to your favour?)***
Best: "Learn to say no without guilt." It changed my career and personal life. Saying no is not rejection, it is prioritization.

Worst: "You need to act tougher if you want to be taken seriously in cybersecurity." I tried this mask for a while, but it was exhausting. Over time, I learned that true authority comes from expertise and consistency, not from suppressing who you are.

6. Can you name a book that has influenced your journey?
"Daring Greatly" by Brené Brown. It taught me that vulnerability is not weakness, but courage in its purest form. In cybersecurity, a field that often thrives on certainty, embracing vulnerability means admitting what you don't know, asking questions, and building stronger, more human teams.

7. How can someone stand out in a competitive cybersecurity job market?
The best way to stand out is by building a personal narrative. Cybersecurity is a broad field so, instead of trying to be “good at everything,” focus on a theme: privacy advocate, incident response strategist, risk translator. When people can clearly associate your name with an area of impact, you stop being “another candidate” and start being the person for that role

8. *What trends in the technology & cybersecurityindustry are you keeping an eye on for the future?*
Beyond AI and quantum, I’m closely watching two interconnected shifts: the rise of regulatory-driven cybersecurity and the evolution of digital identity and trust ecosystems. New frameworks like NIS2, DORA, and global privacy regulations are redefining security from a purely technical function into a strategic business differentiator. At the same time, as more of our personal and professional lives move online, the question of who we are in the digital world, how we prove it, protect it, and preserve our rights, will become central. These forces together will shape not only how organizations secure themselves, but also how societies define trust, freedom, and responsibility in the digital era.

9. What is the most common mistake someone could make when applying for a role in the cybersecurity industry? What do you believe makes a successful candidate/application?
The biggest mistake is trying to look “perfect” instead of authentic. A CV listing every certification with no narrative doesn’t stand out. A strong application connects the dots: why this role, why now, what you bring that others may not. Hiring managers don’t look only for skills, they look for clarity of purpose.

10. From your point of view, do you believe that there are misconceptions people have about working in the cybersecurity industry?
Absolutely. The biggest one is that cybersecurity is only about technology. In reality, it’s also about law, psychology, risk, governance, even storytelling. Another misconception is that you need to “know everything” before you join. Nobody knows everything in this field, the real skill is knowing how to learn quickly and how to work with others.

11. Which concrete recommendations would you give to women who want to change career and join cybersecurity?
1.*Don’t try to “fit the mold.” Cybersecurity needs your unique perspective.*

2.*Translate your existing skills — from law, business, psychology, teaching — into security value.*

3.Surround yourself with supportive communities of women and allies; this industry can feel intimidating, but it doesn’t have to be lonely

12. And any tips for those who are still very young and might be considering it?
Absolutely. The best preparation is to stay curious and build strong foundations. Learn how systems and networks really work, not just from textbooks but by experimenting, try out labs, Capture-the-Flag games, or even simple coding projects. At the same time, follow cybersecurity news to understand how threats evolve in real life, and explore broader topics like privacy and digital ethics. But here’s the key: cybersecurity is not a sprint; it’s a lifelong marathon of learning. You won’t master everything at once, and you don’t need to. What matters most is developing problem-solving skills, clear communication, and an ethical mindset. If you can learn to enjoy the process of discovery and growth, you’ll not only be prepared for a career in cybersecurity, you’ll also be resilient enough to thrive in it.

13. What skills do you think are not “most important “, as this very limiting, but skills that are key for a career in cybersecurity no matter the specific profile?

1. *Analytical thinking (to see patterns and connections)*
2. *Communication (to translate security into language others can act on)*
3. *Adaptability (because the threats never stay the same)*
4. *Integrity (because trust is your currency)*

14. 1. Do you (or did you) have a mentor or someone who guided you? What is your opinion on mentoring as well as on getting a start via an internship/traineeship? Are you planning to mentor or coach others in the future, or have you been mentoring already?

Mentoring is transformational. A good mentor doesn't give you answers, they give you the courage to find your own. Internships are equally important because they make theory tangible. I mentor young professionals and plan to continue, because opening doors for others is the most meaningful way to measure success.

You & Your job

15. What was your childhood dream job (and why you liked it)?

As a child, I dreamed of becoming a detective. I was fascinated by solving mysteries, piecing together clues, and uncovering hidden truths. In a way, cybersecurity is the modern version of that dream, every investigation, every incident response, every risk assessment feels like solving a puzzle. The thrill of protecting people by finding what others might miss is what keeps me passionate about this field.

16.Did peer pressure, trends or other factors play a role in your choosing cybersecurity and particularly your specific field of work in it?

No, it was more about timing. I saw technology growing rapidly, law and governance evolving, and realized cybersecurity sits at the intersection of both. It was less about pressure, more about purpose.

17. Did you face any challenges related to your gender, race, visual appearance, or background, or any stereotypical biases? How have you overcome these?

Yes. Early on, I was underestimated. Sometimes spoken over, sometimes tested harder. I overcame it by mastering my craft and letting my work speak louder than stereotypes. Over time, respect follows results, but the key is: never let others define your worth.

18. Do (did) you ever experience imposter syndrome and self-doubt about your career and skills?

Absolutely. I think most people do at some point. For me, the turning point was realizing that imposter syndrome often shows up when you're operating outside your comfort zone. Instead of seeing it as a weakness, I've learned to see it as proof of growth. It means I'm pushing into new territory, tackling challenges I haven't mastered yet. So rather than resisting it, I take it as a signal that I'm levelling up, and that mindset shift has made all the difference.

19.What has been your most exciting role to date?

The most exciting roles for me have been those that challenged me the most, where cybersecurity was elevated from a purely technical function to a strategic driver of trust. Leading projects that improved governance, built risk frameworks, and aligned with regulations allowed me to grow as a leader while making a tangible impact on how the business operated. These experiences taught me that cybersecurity isn't just about protecting systems, but also about inspiring people and shaping a culture of resilience. That combination of strategic influence and personal growth is what makes the role truly fulfilling.

20.What is the best and worst experience you have had in your career?

Best: *Seeing a team, I trained step into new challenges with confidence and independence. That moment when they didn't need me anymore, that was true success.*

Worst: *Witnessing burnout in talented colleagues who felt unsupported. It reinforced my commitment to build healthier environments for the next generation.*

21.Do you enjoy your work, and why? What's your favourite and least favourite part of your job?
Yes. My favorite part is solving complex puzzles with brilliant people, and seeing ideas become real protections. My least favorite is bureaucracy that slows down innovation — but even that teaches patience and strategy.

22.What role has networking played in your skill development?
Networking has been less about collecting contacts, more about building trust-based relationships. Some of my most important opportunities came not from applications, but from conversations where people saw my genuine interest.

23.What's the next big milestone you're working towards (if you can and want to share)?
I'm working towards building frameworks that not only ensure compliance but shape culture. The future is not just about meeting regulations, but about creating a digital culture of trust and ethics.

24.Do you have any passion or side-projects you´re focusing on?
Yes, I'm deeply invested in cybersecurity education. I design awareness materials and training modules for people outside the field. Spreading security knowledge beyond experts is a passion of mine.

Other

25.How do you handle criticism?
By separating tone from content. Even harsh words can hide a valuable lesson. I extract the lesson, discard the noise, and move forward.

26.How do you manage stress?
I anchor myself with routines: exercise, writing, and spending time with family. Stress is inevitable, but it doesn't have to control the narrative of your life.

27.Cybersecurity is considered a very demanding and "intrusive" career in someone's life (takes a lot of hours, lots of learning constantly, you are "seeing" cybersecurity triggers everywhere even outside of work). How do you balance work and personal life?
By being intentional. When I work, I give my full focus. When I'm with family, I protect that time fiercely. Balance is not about perfect division, it's about presence in whichever role you are at that moment.

28.What do you do to prevent burnout in such a demanding line of work?
By remembering that I am not my job. Cybersecurity is important, but so is health, joy, and human connection. I prevent burnout by creating a full life outside work, friendships, hobbies, family.

29.How do you set boundaries in the workplace?
Clear communication and consistency. I say "no" with respect but without apology. Boundaries are not walls — they are bridges that allow sustainable collaboration.