



W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

INTERVIEW WITH IRO!

Name: Chatzopoulou Argyro (Iro)

Job Position: Senior Policy Advisor / Lead Auditor

Current Employer: APIROPLUS Solutions Ltd.

Cybersecurity areas of expertise: Conformity Assessment, Organizational security and resilience

Educational background: 2 Master's Degrees, currently undergoing PhD

Favourite quote: Security is a team sport

Network with me: <https://www.linkedin.com/in/argyro-iro-chatzopoulou-1151057/>

Intro & Inspirational

1. Which values are guiding your life and work?

My key values are ethics and curiosity. Curiosity drives me to keep learning and improving, while ethics guide how I act—both professionally and personally. For me, it's important not just to grow, but to grow in the right way.

2. What's the most important life lesson you've learned?

That you can only control a limited number of things—mostly those directly connected to you. Failure is inevitable, but what really matters is how you respond to it and what you learn from it.

3. How do you define success? And what's the best advice that you can give about success?

I think my generation set a very high bar for success, especially for women in their professional lives. For me, success is about being the best version of myself—being useful, fulfilled, and happy. My advice would be to define success on your own terms, not based on external expectations.

4. Do you think your job makes a difference? How?

That's a tough question. I do believe my work makes a difference in its own way. I provide assistance, knowledge, and support to people who need it. I may not be doing something life-altering like curing a disease, but I do believe that even small contributions can lead to meaningful improvements.

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?)

The worst advice I received was: "Hurt them like they hurt you."

In competitive environments, I was often told to toughen up and treat people poorly if they did the same to me. But that goes against my principles. I strongly believe you shouldn't compromise your values or character just to fit into a workplace or advance your career.

The best advice I received was: "Let them be."

You can't change other people, but you can control how you react to them. Accepting people as they are—and not letting their behavior affect you—was something that took me time to fully understand, but it made a big difference.

6. Can you name a book that has influenced your journey?

That's a difficult one because I love reading.

But if I had to choose, I'd say "Guards! Guards!" by Terry Pratchett. It's part of the Discworld series, which introduced me to fantasy. A quote from the book—"Who watches the watchmen?"—has always resonated with me, especially in the context of auditing and accountability.

Cybersecurity General

7. How can someone stand out in a competitive cybersecurity job market?

There's no magical formula. What has worked for me is consistently putting in the effort and staying committed to learning. Curiosity, persistence, and a willingness to grow go a long way.

8. What trends in the technology & cybersecurity industry are you keeping an eye on for the future?

There are a few key areas I find particularly interesting right now:

- a. Developments in conformity assessment, especially with the EU Cyber Resilience Act and emerging certification schemes.
- b. AI and quantum computing, which have the potential to significantly reshape cybersecurity in the coming years.
- c. Cybersecurity skills development. I'm a strong advocate for frameworks like ENISA's ECSF and for closing the skills gap through structured training and education.

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?

Overconfidence and an unwillingness to learn are major pitfalls. Cybersecurity is constantly evolving, so thinking "I know it all" is a fast track to failure. A strong candidate shows curiosity, adaptability, and a genuine commitment to continuous learning.

10. Do you believe that there are misconceptions people make about working in the cybersecurity industry?

Yes—one of the biggest is seeing it as purely technical. Cybersecurity is much broader. It includes human, organizational, physical, and even cultural aspects. Ignoring that bigger picture can lead to incomplete or ineffective approaches.

11. Which concrete recommendations would you give to women who want to change career and join cybersecurity?

Get the right skills—and go for it. It sounds simple, but it requires commitment. Set a clear goal. For example, if you want to become a CISO, look at the role's requirements (such as those outlined in the ECSF), identify the gaps in your knowledge, and work toward them step by step. Start small, gain knowledge and experience and continue onwards.

12. And any tips for those who are still very young and might be considering it? Can they start "preparing" somehow from early on?

Age isn't really a factor. The approach is the same: decide where you want to go and start preparing early. Build knowledge, stay curious, and explore the field.

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

Due to the vastness of the domain, it is not easy to say a specific skill. But, if we use the ECSF navigator provided by ENISA ([ECSF - European Cybersecurity Skills Framework](#)) all roles require the ability to “Communicate, present and report to relevant stakeholders”, so maybe that could give us a clue also.

14. 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?

I’ve been very fortunate to have strong support early in my career. My former General Manager, Mr. Kaparos, believed in me, trusted my abilities, and gave me the space to grow. He wasn’t from a cybersecurity background, but he created the right environment for me to develop.

Along the way, many others also shared their knowledge and guidance. That’s why I strongly believe in mentoring and “paying it forward.” I’ve already mentored others and plan to continue doing so as long as I can offer something meaningful.

You & Your job

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

I started working in information security quite early—back in 2005. At the time, the field was seen as purely technical and very limited in scope.

So I was young, female, working in what was considered a technical domain, and in a position of authority as an auditor. That combination did create some friction. I encountered skepticism, occasional rudeness, and people testing whether I really knew my subject.

What helped me overcome it was confidence in myself and a strong investment in my knowledge and experience. Over time, I proved my capabilities, and those challenges gradually faded. My academic background and professional certifications also helped reinforce that.

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

On the positive side, every new environment, company, project, or challenge is a great experience for me. It’s always an opportunity to contribute, learn, and grow.

On the negative side, I went through a period of workplace bullying. It was a very difficult time, and I won’t try to sugar coat it. But looking back, it also gave me the chance to reflect, reassess, and learn important lessons about myself and my boundaries.

17. Do you enjoy your work, and why? What’s your favourite and least favourite part of your job?

I truly enjoy what I do. I get to work with different companies, experience new environments, and share my knowledge—that’s something I find very rewarding. If I had to pick a favorite part, it’s definitely the variety and continuous learning. As for the least favorite, like in most jobs, it would probably be the occasional challenges that come with difficult environments—but even those can be learning opportunities.