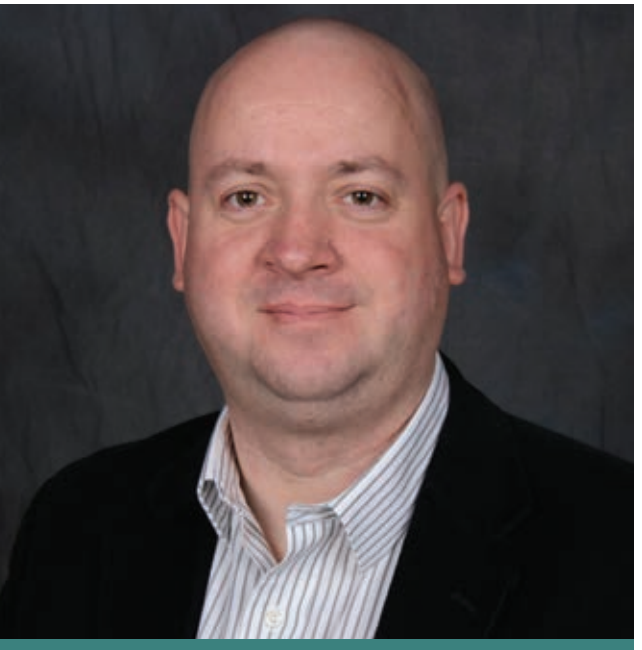
Honoring Our Past. Innovating Our Future



Raef Meeuwisse, CISA, CISM
One of the most popular authors in the field of cybersecurity and social engineering, Meeuwisse's titles include the highly rated global best seller, *Cybersecurity for Beginners*, *Cybersecurity to English Dictionary* and *How to Hack a Human*. His experience includes running eight digital security budgets, consulting on security at more than 50 different organizations, designing a multi-million dollar security software platform, training as a hypnotist and, occasionally, flying helicopters. In addition to making public appearances at countless conferences across Europe, the United Kingdom and the United States, he is also a frequent provider of commentary for multiple technology and mainstream news outlets and has appeared in *Infosec Magazine*, ZDNet, *TechTarget*, TEISS and on Sky broadcast news. Although continuing to provide some boutique cybersecurity consultancy services, he now earns his living primarily from sharing his passion for understanding and communicating security risk scenarios and technology trends, especially in the context of their human factors and impact. Other publications from Meeuwisse include: *Cybersecurity: Home and Small Business*, *How to Keep Your Stuff Safe Online*, *The Encrypted Pocketbook of Passwords*, professional commissions for other organizations including the ISACA® white paper *GEIT for Health Care* and providing updates for global security frameworks.

Q: What is it that drew you to the cybersecurity profession? What keeps you in the profession?

A: I would like to say what interested me in cybersecurity was the money, the travel and an unhealthy interest in disabling cookies and hiding my browser history from an early age. The truth is, I like to work in subject areas where the topic is inherently interesting, continually evolving and presents fresh challenges on a daily basis.

What keeps me in information security is the breakneck speed at which technology and the threat landscape are evolving, coupled with a passion for understanding and helping develop solutions for and with my fellow professionals.

Q: How do you think the profession has changed and evolved? How have those changes impacted the cybersecurity professional and how has the role evolved?

A: ISACA® may be 50 years old, but the same principles that applied to securing information systems back in the early days still remain valid. What has changed is the diversity of how and where we need to apply those principles.

We still have to keep electronic data and information systems secure, but now we also have to do it while navigating very open environments such as over the Internet, public clouds, mobile devices and the Internet of Things.

For the cybersecurity professional, that has meant embracing automation, continuous learning and process engineering to embed security by design throughout the lifespan of the technologies we use. In real terms, security briefly moved to relying on network perimeters as a budget-friendly approach to effective security; but now we have to go back to the core principles of security 1) to understand the value of each set of information we are responsible for, 2) to apply appropriate security at every practical layer, and 3) to continuously monitor, reevaluate and evolve our approaches.

Q: What skills will be most important for cyberprofessionals to develop in the coming years, decade?

A: Cybersecurity has four components; people, processes, technology and information. Many people get stuck trying to understand every single technology that is coming through and, because there is so much of it, that can make the task seem impossible. Delivering effective cybersecurity is really about process engineering, motivating people, identifying and classifying information and using those assets to secure the technologies. My advice in terms of skills development is threefold: 1) Aim to be brilliant on the basic principles that make security work, 2) Embrace models such as the ISACA CMMI Capability Maturity Model to help identify and improve processes, and 3) Work on the soft skills such as being an effective communicator. People who communicate well understand how to apply security principles to any technology (even those that are brand new), and know how to engineer and improve processes will always be in demand.

Q: What cyberthreat keeps you awake at night? How can it be addressed?

A: Internet fragility. The Internet was never designed to do what is does today, and far too many services, especially those providing critical national infrastructure, have gradually moved to a position where they often have no adequate contingency for a wide-scale Internet outage. Yet we know that there are enough botnets out there to cause substantial disruption.

To solve this problem, organizations need to

> “THE INTERNET WAS NEVER DESIGNED TO DO WHAT IS DOES TODAY…A SUSTAINED INTERNET OUTAGE COULD CREATE CATASTROPHIC CONSEQUENCES AND POTENTIAL LOSS OF LIFE.”

have workable business continuity and disaster recovery contingencies in place, especially where a sustained Internet outage could create catastrophic consequences and potential loss of life.

In my opinion, it should be a criminal offense to set up any technology without a suitable failsafe where such a failure can lead to a loss of life. Many would argue that there are some laws out there that achieve this goal, but I do not think those laws are explicit enough at this point.

Q: What do you think are the most effective ways to address the skills gap in the cybersecurity workspace?

A: There is a skills gap, but the extent to which it is a problem varies considerably from organization to organization. Wise organizations have understood that they can fill positions effectively if they seek to make the roles attractive and offer the continuous training and development cyberprofessionals need. They also look to identify people with the right potential and nurture their skills.

When I have been approached by organizations with the biggest skills challenges, they always seem to be offering unattractive terms. For example, looking to recruit a single, internal ethical hacker without being able to offer the ongoing training and experience that person would require to remain effective.

My advice here is simple: If you value your cyberprofessionals, pay them the market rate and provide them with the continuous training opportunities they require, then you probably will not be one of the organizations struggling to fill your cybersecurity roles.

Q: What do you see as the biggest risk factors being addressed effectively by cybersecurity professionals?

A: Cyberprofessionals around the world have really understood the need for security to be embedded into technologies by design. We understand that adding security as an afterthought is impractical and expensive. This is very much what is driving the DevSecOps revolution to ensure that security requirements are considered from the outset of designing and deploying any new technology and that security testing is either continuous or is reapplied on a regular basis.

Q: What was the most significant event or experience to date that has impacted the evolution of your career?

A: My life was once saved by a robot. To be more accurate, it was a DaVinci surgical robot (with a human surgeon at the controls), able to perform maneuvers impossible for the human hand. Although not recommended, having a near-death experience made me realize that a lot of what used to concern me was really not the most important to me. As a result, I became entirely more focused on being true to my principles and relaxed about turning down sensational roles that I knew up front would be likely to be just for the money.

1 What is the biggest security challenge that will be faced in 2019? How should it be addressed?

Consumer and shareholder trust are being eroded by the number of security failures and data breaches. Megabreaches always turn out to have been preventable and I have yet to see a megabreach in an organization in which there was an effective chief information security officer reporting directly to the chief executive officer (CEO). If you want your organization to be ahead of cyberthreats, put an effective CISO in your C-suite or, at least, reporting into the CEO.

2 What are your three goals for 2019?

- Write more cyberbooks.
- Eat less food.
- Work on five new and engaging security presentations.

3 How do you keep your skills and your knowledge current?

I maintain a list of any and all new terms I encounter. I also read around to learn and confirm on evolving topics such as automation, artificial intelligence (AI), and DevSecOps technologies and processes.

4 How do you keep your own information safe? That is, what do you do or not do to protect your own data privacy?

I migrated my company to a zero-trust security model with AI antimalware several years ago. It still has orchestration capabilities that allow me to manage devices and security alerts. I also have hot and cold backups, a kind of honeypot area for would-be attackers, multiple email addresses that have often allowed us to see which organizations have been breached before they seem to know it themselves. I could keep going for a page or more on this topic.

5 What is your number-one piece of advice for other security professionals as they build their careers?

Einstein said, “Try not to be a (person) of success. Rather, become a (person) of value.” Value in the cybermarket means keeping up-to-date on the prevailing threats, knowing how to apply security to reduce the risk and nurturing your business communication skills.

6 What do you do when you are not at work?

I am a serial hobbyist and a compulsive completer-finisher, which has left me with a series of licenses and skills from flying to playing guitar. However, the most enjoyable things I like to do are to hang out with my wife, socialize with friends and I also walk approximately five miles per day, which my dog seems to really appreciate.