Capgemini RESEARCH INSTITUTE

Harnessing AI for cyber resilience

A conversation with
Corence Klop
CISO
Rabobank

Con
ver
sa
tions
FOR TOMORROW

CORENCE KLOP

CISO

Rabobank

HARNESSING AI FOR CYBER RESILIENCE

Corence Klop holds almost 20 years of experience within Rabobank with leading roles in the areas of digital transformation, innovation and data & analytics. In her current role, as Chief Information Security Officer, Corence is responsible for setting the information security vision, strategy and priorities, develop and maintain the information security standards and frameworks, and representing Rabobank in matters of resilience within The Netherlands.

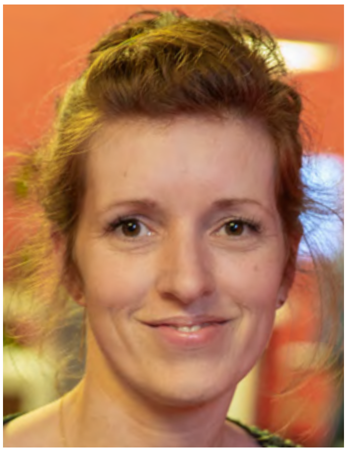
She also works as a non-executive board member of the Rabobank Pension fund and member of the supervisory board of a library.

Can you walk us through your journey at Rabobank and your current responsibilities as CISO?

Corence Klop: I stepped into the role of CISO at Rabobank in September 2023. In this position, I hold global and group-level responsibility for the security of the bank. This includes our central operations, as well as regional branches and subsidiaries. It's a role that comes with immense accountability. If something goes wrong, the buck stops with me. But it also gives me the freedom to shape the bank's strategic agenda for change.

Prior to this, I spent three years in the bank's data and analytics division. I led, for example, a community of 600–700 professionals focused on data and analytics – a key area of expertise within the organization. My interest lies in analytics and uncovering ways to extract value through actionable insights.

I have a background in innovation management, which fuels my passion for emerging technologies. I'm constantly on the lookout for new tools and techniques that can help us stay ahead, particularly in security and operational resilience.



Corence Klop
CISO
Rabobank

> “Security isn't just about preventing risk – it's also about creating the greatest value for your organization and our customers"

Do you find there is friction between creating value with data and protecting it?

Corence Klop: There is friction, but I think it partly comes from my personality. I'm opportunistic, always thinking about what can be done with data or certain technologies. At the same time, working in security means a strong focus on protecting privacy and assets and ringfencing sensitive data. Both aspects are important. Security isn't just about preventing risk – it's also about creating the greatest value for your organization and our customers.

THE SURGE IN CYBERATTACKS

Since assuming leadership, have you noticed a rise in the number and nature of cyberattacks?

Corence Klop: The increase has been exponential. In the first half of 2025 there has been a major increase in distributed denial of service (DDoS) attacks. March 2025 saw more denial requests than entire 2024. Financial Services is the most frequently attacked industry (34% of all global attacks). In Q1 2025, we have seen more than 250k phishing attacks against Rabobank. That's a staggering number and testament to how aggressive the threat landscape has become.

> "In Q1 2025, we have seen more than 250k phishing attacks against Rabobank"

The attack maturity is also increasing, which has massive operational implications. We are talking about phishing, QR code scams, man-in-the-middle attacks and, increasingly, deepfake-based threats. What's more concerning is that this trend is not plateauing. Rather, it's escalating.

That's why technologies such as AI are not just a strategic advantage, they're a necessity. With threats increasing both in volume and sophistication, we need smarter, more scalable solutions to prevent and respond and to stay resilient.

TECHNOLOGIES SUCH AS AI ARE NOT JUST A STRATEGIC ADVANTAGE, THEY'RE A NECESSITY

What do you see as the primary drivers of this surge in cyber threats?

Corence Klop: A major factor is the volatile geopolitical environment. These dynamics have real consequences on the cyber landscape.

Nation-state actors and politically motivated threat groups are becoming more active. And even beyond state-driven actions, the general level of criminal sophistication has risen. Bad actors are evolving fast. They're using AI themselves now. It's no longer just lone hackers or small-time phishing scammers; there's a whole ecosystem behind this.

Could you expand on the evolution of phishing and how attackers are adapting their methods?

Corence Klop: Phishing remains one of the most persistent and effective forms of attack, but it's evolving. It's no longer just about fake emails with suspicious links. Phishing kits have added AI integration to simplify the process to build multi-language tailored phishing pages delivering much more sophisticated results.

> Deepfakes are entering the equation. Imagine receiving a video call or voicemail from someone who looks and sounds exactly like your boss, asking you to approve a financial transaction urgently"

Perhaps more alarmingly, deepfakes are entering the equation. Imagine receiving a video call or voicemail from someone who looks and sounds exactly like your boss, asking you to approve a financial transaction urgently. Deepfake continues to be on the rise. Threat actors increasingly offer deepfake services claiming to be able to circumvent Know-Your-Customer protocols.

This evolution of threats makes it clear that conventional security measures are no longer sufficient. Attackers are using emerging technologies, and we need to keep up.

KEEPING UP WITH THE THREAT ENVIRONMENT

With such advanced threats, how is Rabobank preparing for the future?

Corence Klop: Security is a core capability. We have an information security strategy with a solid foundation to defend against most future threats.

The sheer volume of attacks means we need systems that can prioritize, detect, and respond, often autonomously. This is where AI and automation come in. For example, automating the triage of security alerts can save thousands of hours of analyst time and ensure critical incidents are caught early.

> "Automating the triage of security alerts can save thousands of hours of analyst time and ensure critical incidents are caught early"

Beyond that, the people and process part of our strategy are very important. All employees have a role to play and should have a minimum level of security maturity so they know how to behave in a secure way. Security is not the job of one department. It's embedded in our IT, operations, and customer-facing units. Everyone has a role to play.

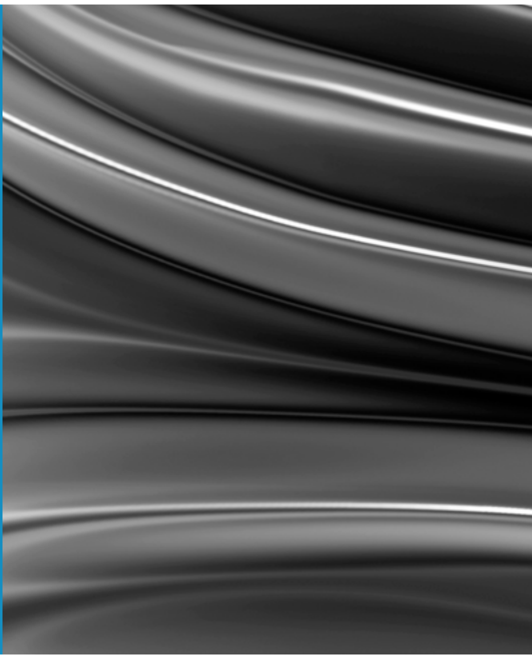
We are not alone in this. We actively join forces with other major organizations in the Netherlands by sharing our experiences and knowledge, to stay prepared for future challenges.

How do you align that long-term security view with agile ways of working?

Corence Klop: As mentioned in our security strategy, we've defined a Foundation, which includes all essential security measures. But beyond that, we also prepare for emerging technologies such as AI and quantum computing.

Our strategy is translated into yearly priorities. Of course, we cover the basics that every organization needs, but we also explore how to prepare for developments that may arise in two or three years. I try to strike a balance in ensuring we have the technology we need today, while building for the future.

"Post-quantum cryptography — it might not be an imminent risk, but we know it's coming"



A good example is post-quantum cryptography. It might not be an imminent risk, but we know it's coming. I push for topics like that to be included in our priorities. That means starting with an inventory of what we currently have, building internal expertise, and embedding these topics in the organization's agenda.

AI AND CYBERSECURITY

In your view, where does AI – and specifically generative AI (Gen AI) – hold the most immediate potential in cybersecurity operations?

Corence Klop: In the short term, I believe the greatest potential for AI and Gen AI, lies within the security operations center (SOC). The SOC deals with a massive volume of alerts daily, and that's precisely where Gen AI can be a game-changer.

One key use case is assisting analysts during the alert investigation process. Gen AI can streamline their workflows by quickly searching across multiple databases and offering recommendations for action. It essentially acts as an advisor, advising whether to escalate an alert, ignore it, or take specific action.

What approach are you taking to improve detection and response?

Corence Klop: Since we didn't find a reliable off-the-shelf solution, we've started building our own ML model specifically trained on our own data.

The advantage here is twofold. First, we control the dataset, which means we can fine-tune the model to our environment and threat landscape. Second, it allows us to embed domain knowledge directly into the model, which generic solutions struggle to do.

It's still early days, but the results are promising. We can work better with high volume data sources and can better detect.

What are some of the challenges you've faced in building AI models for in-house cybersecurity?

Corence Klop: One of the first challenges we encountered was the expertise gap. In cybersecurity, we traditionally don't have data scientists embedded in our teams. Conversely, the data science teams at our bank, while very skilled – especially in areas such as fraud detection – aren't familiar with the specifics of security data. This divide made collaboration difficult and our security team had to start learning the principles of AI.

Another major issue was tooling. Many of the standard tools we use in security, like Microsoft Defender, aren't designed to handle large datasets or ML. You can't just run Python or complex queries on these platforms. So, we needed an updated infrastructure to run and train models efficiently, which could handle the scale of data we were working with.

As you're building AI models internally, how do you handle ethical concerns like explainability, transparency, and bias?

Corence Klop: Our analytics teams follow a structured AI Way of Working (WoW) that guides them through every step of model development. The AI WoW ensures AI risk minimization and AI value maximization including ethical considerations. It emphasizes explainability, transparency, and documenting decisions. You can find out why a particular modeling choice was made, even years later.

At Rabobank, we make a Responsible AI building block available for teams. This is designed to be compliant and in control by translating AI related standards, guidelines and frameworks into technical components to embed in all use cases.

What advice would you give an organization just starting its AI cybersecurity journey?

Corence Klop: My first piece of advice is to get your data in order. Before you build or even adopt an AI model, you need a clean, consolidated source. Our early modeling efforts were hampered by inconsistent and incomplete datasets.

Secondly, I recommend starting with what's already available. Don't try to build everything from scratch. Run experiments with available tools, understand their capabilities and limitations, and build internal expertise along the way.

How do you balance AI tools with skill development in your team?

Corence Klop: First of all, there is a strong focus on building AI skills, not only in the security organization but in the whole organization. DataWise is a global learning program for all employees. Rapid innovations in data and AI impact our work. Data and AI help us provide excellent customer service, improve efficiency and performance, and make the right decisions. This requires continuous skill development. DataWise supports employees in this development.

Also I've experienced that security analysts are fast in learning how to design, build and deploy detection rules and models in a short timeframe.

Finally, it's about focus. AI tools will not replace a security analyst. It will augment their work. This also means you should be careful how to build up AI. The model should be validated since it should do what it's supposed to do.

> "AI tools will not replace a security analyst. It will augment their work"

A big part of cybersecurity success depends on end-user behavior. How do you manage awareness without creating fatigue?

Corence Klop: I focus on integrating attention-worthy topics into the daily routines of my users – or, in my case, colleagues – without making it feel like a burden. It's about using small, everyday moments to raise awareness.

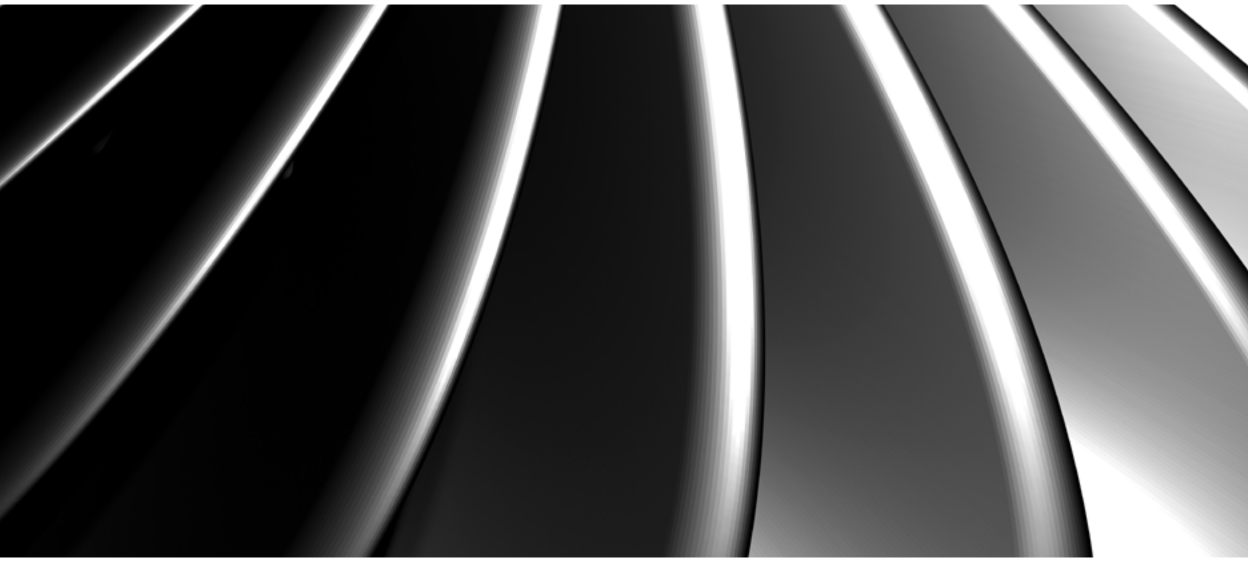
Phishing is a great example. We regularly send simulated phishing emails and monitor responses. Instead of following up with long training sessions, we provide micro learnings of one to two minutes to highlight what they could have checked, what they might have done differently, and offer additional resources to those who are interested. It's all about keeping it simple and accessible, and finding creative approaches to keep them engaged.

Which trends do you see shaping the future of AI in cybersecurity?

Corence Klop: One major factor will be talent. Finding people with the right blend of AI and cybersecurity expertise is only going to get tougher. These technologies will need to help teams do more with less.

Education is the foundation. You can have the best tools, but if your people fall for a deep-fake video or phishing attempt, those tools might never come into play. We stress critical thinking, skepticism, and adherence to process. My team works hard to keep everyone aware, not just of existing threats, but also of how they're evolving.

From a technical perspective I see a few developments: 1) Identity fraud – onboarding fake customers, 2) Attacks will be harder to detect, faster and more convincing, and 3) More and better personalization in scams.



Corence Klop
CISO
Rabobank

"Finding people with the right blend of AI and cybersecurity expertise is only going to get tougher"

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion

Get the future you want | www.capgemini.com

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the UK, and the US. We are proud to have been ranked #1 in the world for the quality of our research by independent analysts for six consecutive times - an industry first.

Visit us at www.capgemini.com/researchinstitute/

#GetTheFutureYouWant

www.capgemini.com