

The risk manager is too slow for AI

Column van CFA Society Netherlands

The conventional method of cyber risk management is under pressure. Time pressure, mind you. After all, how do you arm yourself against the latest generation of AI models, which can find and exploit vulnerabilities ever faster?

Globally, financial authorities are warning with striking unanimity this year about the cyber risks of the latest generation of AI models.

And not without reason.

These cutting-edge AI models now have the capabilities to autonomously find and exploit vulnerabilities in widely used ICT systems and shared infrastructures in no time. This poses a threat to the stability of the financial sector, according to the European Systemic Risk Committee.

In contrast to this technological acceleration stands the traditional risk management of financial entities. This is specifically designed for careful assessment: vulnerabilities are assessed individually for severity, likelihood of exploitation, and potential impact. Based on the level of risk, security updates are subsequently tested and rolled out in a controlled manner.

That takes time and capacity, and often requires the involvement of external suppliers.

The current way of working comes under pressure if attackers, armed with advanced AI, expose significantly more vulnerabilities. This quickly creates capacity problems on the defense side, meaning high-risk vulnerabilities may be addressed (too) late and lower risks might be left on the shelf altogether. The current system threatens to no longer be able to keep up the pace.

So what do you do as a risk manager? The classic choices are not becoming any more attractive. Updating faster increases the risk of incidents, continuing to test extensively leaves systems vulnerable longer, and sharp prioritization means that other weak spots are overlooked. But what then?

Part of the answer lies earlier in the chain. The DORA Regulation requires financial entities to embed security during the development of ICT systems and to thoroughly test them before commissioning. In other words, 'secure by design'. According to the European Commission, AI can be widely deployed within that development cycle, for example by automatically analyzing code for security weaknesses.

The European Union Agency for Cybersecurity (ENISA) also calls for scaling up defenses to 'machine speed'. This means extensive automation and the deployment of AI in security processes, for example in the analysis and prioritization of vulnerabilities and the (almost) immediate detection of anomalous activities. The goal is for security teams to be able to respond virtually instantly.

That is easier said than done. Scaling up to that level is a major challenge for many (particularly smaller) parties. Therefore, mutual cooperation and collaboration with government organizations remain of crucial importance. Regulators also play an important role by emphatically continuing to monitor compliance with the DORA Regulation and the European Cybersecurity Regulation. Without 'machine-speed defence', the risk manager might be too slow for AI, but at least he is not alone.

for. ■



Door **Can Yilmaz**,
Regulatory & Compliance
Consultant and member of the
Advocacy Committee van
CFA Society Netherlands