Q&A

CHRIS BETZ

Chief Information Security Officer -
Amazon Web Services (AWS)

Cyber-resilience in the age of artificial intelligence

How is AWS helping its financial services customers innovate and optimize their operations? What are the future prospects?

Today, the pace of technological change is unprecedented and the financial services sector is not immune to this. In a rapidly shifting landscape, financial firms are investing in technology to modernize IT infrastructure and using cloud technology to reimagine how they operate, elevate customer experience, and stay secure and resilient. There are stark differences between those who invest in technology and those that don't. This is reflected in their ability to provide essential financial services that transparently and easily meet the needs of citizens across the EU and around the world as well as to operate with both efficiency and environmental care. At AWS, we work closely with financial services organizations to help them harness the power of cloud computing, artificial intelligence (AI), and automation to scale operations, optimize costs, and focus on what truly matters – innovation and business acceleration – rather than getting bogged down in IT maintenance.

Financial services are about trust. Being worthy of trust and being trusted. Innovation in finance is as much about resilience, trustworthiness, and efficiency as it is about modern customer products. The financial sector faces an ever-growing cyber-threat landscape, with attackers becoming more sophisticated amid regulatory pressures increasing. But true cyber resilience extends beyond mitigating attacks – it is about ensuring that when incidents do occur, businesses can recover swiftly and continue operating without disruption. That is why AWS continues to invest in cutting-edge security tools, AI-powered threat detection, and resilient cloud architectures that empower financial institutions to stay one step ahead of adversaries.

The next big frontier? AI, including generative AI and AI agents. These technologies are unlocking entirely new ways to improve fraud detection, risk management, and customer experience. But they also warrant close consideration of risks, especially in terms of security and compliance. Our focus at AWS is to help financial institutions integrate AI responsibly while also helping to ensure the strength of their security postures.

If we look beyond the EU, from a global perspective, what do you think are the most effective public interventions when it comes to achieving the objective of enhancing the cyber resilience of the financial sector? Are European authorities equipped with the right tools? Have we overcomplicated things without really focusing on the outcome?

Cyber resilience is not something any one country or region can tackle alone – it is a global challenge, requiring a coordinated and collaborative approach between regulators, financial institutions, and technology providers. The financial industry is deeply interconnected so global approaches that focus on fostering supervisory collaboration, public-private partnerships, and real-time intelligence sharing are the most effective.

The EU has already taken significant steps with the Digital Operational Resilience Act (DORA), setting a strong regulatory foundation. However, we need to make sure that we leave space for improvement, learning from our experience and global best practices. Public-private partnerships play an important role in this space, for example by fostering best practices in relation to threat intelligence sharing and incident reporting. On the latter, as discussions continue around centralizing incident reporting in the EU, looking at global best practices like these can help strike the right balance between compliance and efficiency.

In order for DORA to be a success, we also need to make sure that the European Supervisory Authorities (ESAs) and national regulators have the right resources to match their expanded mandates. Ensuring regulatory agencies have the right resources and are able to architect their programs to achieve consistent and more effective risk management as it applies to supervised firms but also, importantly, themselves will be critical. Further, in a rapidly changing world, living risk processes take on an even more important role relative to traditional control approaches. The ability of a financial institution to rapidly identify risk, prioritize and take appropriate action to mitigate becomes even more important.

Similarly, the ability of regulators to assess institutions' capability to identify and respond appropriately across the breadth of existing and new risks is critical today and will be even more so in the future. Point-in-time checks will have diminishing value, especially as threat actors are willing to employ a broad variety of tools designed to bypass well-understood controls. Technology can play a critical role here. We are seeing a real opportunity for Supervisory Technology to help regulators manage this growing complexity. Instead of relying on periodic reports and manual assessments, supervisors can leverage AI-driven analytics and machine learning for ongoing monitoring and compliance.

For financial firms, this shift could be a game-changer. More efficient supervision means fewer surprises – clearer expectations, faster feedback, and more consistent regulatory assessments. Ultimately, better enforcement does not just benefit regulators – it helps firms focus on resilience as an ongoing practice rather than a reactive exercise. And that is a win for the entire financial ecosystem.

How is AI and Generative AI impacting cybersecurity? Are we less safe as a result of the emergence of Generative AI? How do we make sure we stay ahead of attackers given the constant evolution of technology? Do you have any specific concerns and recommendations related to the financial services sector?

We know generative AI is being used to aid threat actors' efforts, for example, improving phishing campaigns, and making it easier to gather information for social engineering to name just a few. However, generative AI can and is also being used to improve technologies to help make systems more secure.

That means embedding security by design – ensuring strong governance, transparency of our AI models, and customer control over their data. For example, with services like Amazon Bedrock, organizations can build generative AI applications with confidence, knowing their data remains private, encrypted, and never shared outside their environment.

It is important to emphasize that cyber resilience is built on multiple layers of defense. AI is an incredibly powerful tool, but it should complement, not replace, established security measures. Strong fundamentals – like encryption and multifactor authentication – are still critical. The firms that combine these foundational principles with AI-driven insights will be best positioned to stay ahead of emerging threats.

What are the first lessons from the implementation of DORA at AWS and its financial sector customers? Are DORA requirements achieving their objectives? Can more be done by market participants or supervisors to leverage the use of technology and AI in particular to fight cyber-risk e.g., in terms of cooperation, exchange of best practices?

The early months of DORA's implementation have been a learning curve for the financial sector. DORA provides a unified framework for operational resilience, which is something financial firms have been asking for to replace the patchwork of national regulations. That is a win. But with any regulatory shift, there is always an adjustment period. Many financial institutions are still working out how to integrate DORA into their existing risk management strategies without adding unnecessary complexity. As such, we are already observing some friction – especially when it comes to concerns about overlapping with other frameworks, such as the NIS2 Directive and the GDPR.

The biggest lesson so far? Compliance alone is not enough. Regulatory frameworks like DORA provide the basis, but resilience is not about ticking boxes – it is about embedding security into the fabric of an organization so that it becomes second nature.

Another major takeaway is that technology has to play a bigger role in cyber resilience. Financial firms and regulators alike are still scratching the surface when it comes to using AI and automation to strengthen security. AI-driven threat detection, predictive risk management, and automated compliance monitoring have the potential to transform how firms stay ahead of cyber threats. In this context, there is a huge opportunity for closer public-private collaborations – involving financial institutions, regulators, and cloud providers – to develop best practices and security frameworks that remain future-proof.

Ultimately, DORA is a step in the right direction, but the real test is whether financial firms see it as an ongoing process of learning and adaptation to ensure they are prepared for new cybersecurity threats which will emerge in the future.