Watch out for these security risks in 2026

Cybersecurity has never evolved as rapidly as it has in the last years.

AI-driven attacks, increasingly targeted threat actors, and rising concerns around data sovereignty are reshaping the way Swiss companies need to think about digital risk and cybersecurity. Which developments should IT teams prepare for in 2026? How has AI changed the game for both defenders and criminals? And what does this mean for organizations that rely on Cloud infrastructure?

To explore these questions, we spoke with Nadir Jabiyev, Head of IT Operations and Security at Xelon. With more than two decades of hands-on IT experience and a career that spans system engineering, FinTech compliance, and modern cyber-security leadership, Nadir offers a grounded and forward-looking perspective on what Swiss IT leaders should know and what they should be doing right now.

xelon

> "The last two years have produced a threat environment that is faster, more precise, and more strategically damaging than ever before."
>
> — **Nadir Jabiyev**

Nadir, please tell us a bit about your background. How did your career in IT begin?
I started my IT career more than 20 years ago; this was back when "cybersecurity" wasn't yet a defined specialty. At that time, you didn't have roles like "security engineer" or "cloud security analyst." You were simply the IT person, and you did everything. I spent those early years learning every part of the stack: helpdesk, system administration, networking, Linux engineering. I did anything that needed to be done. That broad, hands-on foundation shaped the way I look at technology even today.

As my career progressed, I moved into a management role in a highly regulated FinTech environment. That was my first serious exposure to security from a compliance and governance point of view. Achieving PCI DSS certification, for example, forced me to think differently about risk, controls, and accountability.

What ultimately motivated you to move from general IT into cybersecurity?
About a decade ago, I witnessed the industry begin to formally separate security from traditional IT operations. I chose to stay on the IT side, partly because it was familiar, and partly because the scope of security roles wasn't entirely clear at the time. But the landscape kept evolving. Cybersecurity grew into a massive, multifaceted discipline with its own methodologies, processes, technologies, and challenges. It became obvious that security was no longer just a compliance checkbox or a side responsibility, it had become a critical domain requiring dedicated expertise. At some point, I realized that security was where the biggest impact would be. That's when I decided to fully commit to cybersecurity and make it my primary focus.

What are the top signs that an organization is not taking security seriously enough?
A key warning sign is the absence of a structured and ongoing security awareness program. If employees don't understand the risks associated with their day-to-day actions – whether that's mishandling credentials, misconfiguring systems, or falling for social engineering – the organization is effectively leaving its first line of defense blind. When people don't know the potential impact of their mistakes, even well-designed technical controls won't be enough.

Another strong indicator is when security becomes a reactive function rather than a proactive one. In many organizations, meaningful security initiatives only start after an incident has already caused damage. When investments, policies, and processes are only triggered by breaches, it means that security isn't embedded into the business strategy. That is simply a firefight after the fact.

How has the threat landscape evolved? Which new cyber threats have emerged over the last two years?
The last two years have produced a threat environment that is faster, more precise, and more strategically damaging than ever before. This was largely driven by the rapid adoption of AI and the increasing sophistication of attackers. One major change is the sheer speed at which new threats are created. Malware, phishing campaigns, and exploitation tools can now be generated, tested, and refined in a fraction of the time it used to take. This means defenders are facing a constantly growing volume of threats that evolve much faster than traditional security cycles.

Another trend is the rise of far more targeted attacks. Threat actors are moving away from broad, opportunistic campaigns and focus instead on specific companies, systems, or even individual employees. These targeted intrusions increasingly involve data exfiltration, long-term persistence, and multi-stage attacks designed to cause maximum operational and reputational damage. There's also a surge in highly automated reconnaissance,

xelon

meaning attackers using AI to scan environments, identify weak points, and customize exploits.

Is it true that employees are often the weakest chain of security strategies?
I wouldn't say they're **the** weakest link, but employees definitely need proper awareness training. And this works by making security part of everyday work, not a once-a-year checkbox exercise. When people understand why certain rules exist and how attackers actually operate, they stop seeing security as an annoyance.

Awareness training works best when it's practical, relatable, and even a bit fun. Nobody learns much from a 50-page PDF they're forced to skim. But short, regular sessions, simple examples, and real stories about what can go wrong will stick. Throw in a few phishing simulations or interactive workshops, and suddenly everyone becomes much more alert.

With the right approach, employees transform from "the weakest link" into one of the strongest defenders. After all, even the most advanced technology can't stop someone from clicking on a suspicious link, but awareness training absolutely can.

What role does AI now play in both cyber defense and cybercrime?
AI is now deeply embedded on both sides of the cybersecurity battlefield. As stated before, AI has become a powerful enabler. AI allows cyber criminals to write malware, generate phishing content, automate vulnerability discovery, and craft highly convincing social-engineering messages – all with minimal technical knowledge. As a result, cyber threats have become easier and cheaper to create, lowering the barrier to entry for less skilled threat actors. At the same time, advanced groups use AI to analyze targets, prioritize high-value assets, and design attacks tailored to a specific organization's environment.

On the defensive side, AI is equally transformative. Modern security tools use machine learning to analyze behavior patterns, detect anomalies in real time, and correlate huge volumes of events across endpoints, networks, and cloud platforms. This allows security teams to identify suspicious activity earlier and respond faster. AI also helps automate routine tasks, like triaging alerts, classifying incidents, and recommending remediation steps. This frees up human analysts to focus on more complex threats.
In short, AI has escalated the capabilities of both defenders and attackers. Organizations that leverage AI intelligently gain a significant defensive advantage, while those that don't risk falling behind an increasingly automated and adaptive threat landscape.

Can a Cloud infrastructure be as secure as an on-premise IT infrastructure?
If planned and implemented correctly, a Cloud environment can actually be more secure than traditional on-premise infrastructure.

One reason for this is the security maturity and scale as good cloud providers invest massively in security; this usually goes far beyond what most organizations can match internally. They maintain dedicated security teams, continuous vulnerability research, built-in hardening, global threat intelligence, and 24/7 monitoring. This creates a baseline of protection that is often superior to what an average on-prem environment can deliver.

Second, Cloud architectures enforce clear, standardized security patterns. When properly configured, these guardrails eliminate many of the human errors and inconsistencies typically found in on-premise IT environments where teams build and maintain everything manually.

Finally, Cloud platforms support a level of automation that is difficult to achieve on-premise: infrastructure-as-code, auto-remediation, immutable deployments, automated backups, and scalable monitoring. This results in faster patching, more consistent configurations, and significantly reduced attack surface. Additionally, Cloud-native services often provide built-in redundancy and disaster recovery options that dramatically improve resilience.

We see growing skepticism toward global hyperscalers. Why are some Swiss companies becoming more cautious about fully trusting providers like Microsoft Azure? What security and data-protection concerns are driving this development?

A significant factor in this skepticism is the CLOUD Act (Clarifying Lawful Overseas Use of Data Act), enacted in the U.S. in 2018. The CLOUD Act requires U.S. companies to provide data to U.S. authorities even if the data is stored outside the United States. Even if an American Cloud provider operates data centers in Europe, like Microsoft Azure, they can still be compelled to release this data.

Additionally, the policies of U.S. President Donald Trump have been heavily focused on U.S. interests, leaving little room for trustworthy international cooperation. This has led companies in Switzerland and across Europe to question whether a Cloud provider from a country with an unpredictable foreign and economic policy is reliable in the long term.

In what ways can Swiss-based Cloud providers, such as Xelon, address the security, compliance, and data-sovereignty challenges that make some companies hesitant to use global hyperscalers?

Across Europe, and especially in Switzerland, there has been a steadily increasing focus on digital sovereignty. Organizations want greater assurance about where their data resides, which legal frameworks apply, and how much control foreign jurisdictions can exert over their infrastructure. Geopolitical developments have only amplified these concerns by highlighting the risks of relying too heavily on global providers governed by external regulatory environments.

Swiss-based cloud providers such as Xelon address these security and sovereignty challenges in several concrete ways. All customer data is stored exclusively in ISO-certified data centers within Switzerland. As a result, the data is fully governed by Swiss data protection and privacy laws, which are known for their clarity, stability, and strong emphasis on confidentiality.

Because the IT infrastructure is operated entirely under Swiss jurisdiction, organizations also avoid exposure to foreign extraterritorial regulations such as the U.S. CLOUD Act. This provides businesses, especially those in regulated industries, with a higher degree of assurance that sensitive workloads remain protected from cross-border access requests.

Companies maintain full visibility into where their workloads are running, how data is handled, and which entities have jurisdictional authority over it. This is especially important for sectors with strict regulatory requirements. Local providers are often better positioned than hyperscalers to meet region-specific regulatory expectations, industry certifications, and audit requirements, which can reduces the compliance burden for customers.

Who owns and controls the data in a Swiss Cloud by Xelon?

The data always belongs 100% to the customer. It is up to the customer to decide what goes into the Cloud, how it's used, who has access, and when it's deleted. Nothing happens to the data in a Xelon Cloud unless customers say so.

Xelon's role is simply to provide the secure infrastructure and platform that your systems run on. We take care of the hardware, the network, the availability, and the protections around it; but the data itself remains entirely the customers'.

What are the biggest misconceptions people still have about security?

One of the most persistent misconceptions is the idea that security is a one-time project, something you set up once and then forget about. Many organizations still believe that buying a firewall, configuring multi-factor authentication, or passing an audit means they are "done" with security. In reality, security is an ongoing practice that needs continuous monitoring, updating, testing, and adaptation. Threats evolve, infrastructure changes, new employees join, and attackers find new ways to exploit old weaknesses. Treating security as a static box to check almost guarantees blind spots and vulnerabilities over time.

Another major misconception is that security budgets only need to rise after an incident. This reactive mindset is extremely common: investments are approved once something goes wrong, not before. Unfortunately, responding to a breach is always far more expensive – financially, operationally, and reputationally – than preventing one. Mature organizations understand that proactive investment in security tools, training, and processes is not a "nice to have" but a core part of risk management.

Together, these misconceptions create a dangerous cycle: security is underestimated until a breach occurs, and only then does it become a priority. Breaking that cycle requires recognizing security as a continuous, evolving discipline. Security deserves sustained attention long before an attacker forces the issue.

xelon

Thank you for downloading this interview on cybersecurity!

We hope it gave you thought-provoking insights and practical ideas for shaping your IT strategy for 2026. As our Head of Security, Nadir Jabiyev, pointed out: security and IT can no longer be treated as separate worlds.

Are you curious how secure your data and systems are in a Swiss Cloud? Have you won dered how to relief the burden of following strict compliance rules and regulations? Would you like to learn more about how to prevent security issues instead of mitigating them? Set up a free consultation with our Security Experts and Cloud Experts.

Extra tip: In the Xelon blog, you can dive further into cybersecurity and the latest developments in the Cloud and tech space.

xelon