FOX IT
part of ncc group

Are Benelux insurers moving too fast with AI, or not fast enough on resilience?

By Alex Douven,
Insurance Lead @ Fox-IT

AI adoption is accelerating across the insurance sector. That creates a real dilemma. Move too slowly and you risk falling behind on efficiency, claims handling, customer experience and future competitiveness. Move too quickly without strengthening resilience and you increase exposure to identity abuse, data theft, supply chain risks and operational disruption."

- Alex Douven, Insurance Lead @ Fox-IT

Insurers differ from other companies that make up the financial services sector. Just like banks or FinTechs they process high volumes of financial and transactional data. But insurers manage additional information linked to some of the most personal and sensitive events in people's lives like: illness, death, disability, income, health, life expectancy, fraud investigations, criminal records, property, genetic defects, family circumstances or long-term financial security.

That makes insurance data highly attractive to criminals. A claims file, medical context, income profile or fraud investigation can be used for identity fraud, social engineering, extortion, targeted scams or manipulation of customers, brokers and support teams. For insurers, cyber security is therefore not only about protecting systems and data. It's about protecting the trust that insurance companies and their customers depend on.

Meanwhile, insurers are under growing pressure to modernize, as their traditionally stable business models are becoming increasingly unpredictable and subject to rapid change. AI adoption will increasingly be necessary to remain relevant, competitive and efficient in areas such as claims handling, underwriting, fraud detection, customer service and internal operations driving both operational efficiency and higher levels of personalization. But AI also increases dependency on data quality, access control, supplier resilience and identity governance. AI systems only create value when they can access data and support or trigger workflows.

That also means the consequences of poor access control, excessive permissions, weak validation or unclear accountability become much larger. For Benelux insurers, the challenge is to keep innovating while ensuring that cyber resilience develops at the same pace.

Vulnerability management, ransomware resilience, fraud prevention, supplier governance, identity, detection, response and AI assurance are all part of that same challenge.

Looking back at 2025, the pressure is clear. Our recent annual cyber threat intelligence report[1] found 7,874 ransomware attacks globally, up 50% year on year, with Europe accounting for 22% of claimed incidents. At the same time, European insurers are already moving quickly on AI.

For insurers, the boardroom question is no longer only: "How do we adopt AI safely?" It is also: "Can we protect sensitive customer data, detect misuse quickly, keep critical services running, and coordinate with suppliers when something goes wrong?"

2/3 Insurers use Gen AI

EIOPA reports that nearly two-thirds of insurers are actively using GenAI, while earlier EIOPA research found that nearly 80% of insurers rely on US Big Tech providers for cloud storage services.

References:

[1] https://www.nccgroup.com/annual-cyber-threat-intelligence-report-2025/

Risk is scaling faster than control

Claude Mythos: a glimpse into the future of vulnerability management

Claude Mythos is an advanced AI model that can be leveraged for cyber security tasks such as vulnerability discovery, exploit reasoning, and attack simulation. Mythos should not be framed as a sudden revolution, but as a warning signal for a trend that was already underway: attackers are getting faster at finding, understanding and exploiting vulnerabilities.

It also gives a glimpse into the future. These models, and even more powerful models that will follow, show how vulnerability discovery, exploit development and attack preparation can become faster, more scalable and more accessible.

For insurers, the implication is clear. Vulnerability management can no longer rely on periodic review cycles, slow internal governance or supplier SLAs that assume weeks of response time. Internet-facing systems, identity platforms, VPNs, CRM-connected environments, broker portals and third-party interfaces need faster triage, faster patching, more automation and more continuous validation.

For cyber insurers, this also directly impacts portfolio risk: when hundreds or thousands of insured organizations operate at this speed, delayed remediation or weak vulnerability management at scale can quickly translate into systemic exposure, higher claims frequency and accumulation risk across the portfolio.

This also makes continuous threat and exposure management more important. Insurers need to continuously discover exposures, prioritize them based on business context, mobilize the right owners and validate whether remediation and controls will work.

Continuous penetration testing and managed external attack surface management help organizations understand where they are exposed and whether controls still work. But this is only one side of the story.

As attackers become faster, the risk increases that attackers will get through prevention more often. That makes layered defense more important. Insurers need to optimize not only how they find, prioritize and patch vulnerabilities, but also how they detect, respond and recover when something does happen. This means reviewing the managed detection strategy across EDR, NDR, SIEM, identity, cloud and SaaS environments.

It also means improving incident response processes from both a technical and organizational perspective: who detects what, who decides, who communicates, which suppliers need to act, and how quickly containment can happen.

> The real challenge is no longer only finding vulnerabilities faster. It's understanding which vulnerabilities matter most in the context of your business: which insurer service they affect, whether existing controls reduce the risk, which supplier or system owner needs to act, which detection logic should be in place, which remediation decision must be made first, and how to respond effectively when a threat does get through.

In light of Claude Mythos and similar models, the practical leadership question is clear: when a critical vulnerability is disclosed, can you quickly identify exposure, understand the potential impact to your organization, prioritize the most business-critical services, decide what needs to happen first, validate whether controls are working, patch or mitigate quickly, and ensure the same urgency across your suppliers?

Ransomware, fraud & suppliers

Ransomware is an operational resilience test

For insurers, the core question is not only whether data is encrypted or stolen. It's whether policy servicing, first notice of loss, claims triage, broker communication, customer support and internal decision-making can continue during disruption. That is why insurers should define their minimum viable operating company before an incident forces the decision.

In practical terms, insurers must determine which manual workarounds are acceptable? Which suppliers must be contactable? Which decisions need board-level involvement? Which communication channels still work when core systems are unavailable? A long outage is a no-go for insurers. It quickly becomes a customer, commercial, regulatory and reputational problem. DORA[2] reinforces this by focusing on the ability of financial entities to withstand, respond to and recover from ICT disruption.

Ransomware resilience is therefore not only a technical recovery topic. It's a business continuity challenge that requires clear decision-making, tested recovery priorities, supplier coordination and communication under pressure.

Cyber incidents lead to fraud incidents, so teams need to work together

Recent public incidents show why cyber security, fraud, claims, customer operations, communications, legal, privacy and business continuity teams need to work together more closely. Cyber incidents often don't stop at data theft. Stolen customer data can be reused in the next stage for phishing, impersonation, fraudulent applications, account takeover or payment manipulation. That is where cyber security and fraud move closer together.

For insurers, this matters because leaked policy, claims, identity or customer data can become fuel for highly convincing fraud. The response cannot sit only with security. Fraud, claims, customer operations, communications, legal, privacy and business continuity teams need to rehearse these scenarios together. That rehearsal should include concrete fraud triggers: bank account changes, unusual payout requests, account recovery attempts, broker impersonation and outbound scams that use stolen customer data.

This is also where AI-enabled deception matters. Deepfake voice, vishing and realistic phishing do not replace basic controls. They make weak verification processes fail faster.

The answer is not just awareness training; it is stronger validation: call-backs, dual approval for sensitive changes and clear escalation routes when something feels wrong.

Third-party risk is operational risk

Insurance is structurally exposed to supplier risk. More vulnerabilities aren't only an internal IT risk; they also increase pressure on SaaS platforms, cloud services, CRM environments, broker portals, claims systems and outsourced support. DORA[3] makes this explicit by treating ICT third-party risk as part of operational resilience. Supplier exposure can therefore be treated as procurement paperwork.

Logging, access paths, incident obligations, fallback arrangements and patch SLAs need to be designed around disruption. Your resilience is no longer limited to the systems you own.

This becomes more important as AI adoption increases. Many AI use cases depend on cloud platforms, data integrations, external models, SaaS environments and third-party tooling.

Insurers need to understand not only whether a supplier is compliant on paper, but also how that supplier behaves during disruption, data exposure or urgent remediation.

References:

[2, 3] https://www.nccgroup.com/campaign/preparing-for-the-digital-operational-resilience-act-dora/

[4] https://www.nccgroup.com/solutions/digital-identity/

Identity, DORA & Governance

Identity and data is critical for AI adoption and security

For insurers, identity is no longer just an IT hygiene topic. It's becoming critical for both AI adoption and security. AI systems need access to data and workflows to create value. Recent attacks on, for example, CRM environments and customer support chains show the pattern clearly: attackers are using voice phishing, stolen credentials, connected apps, token theft and helpdesk manipulation to gain valid access and move quickly to data theft or extortion.

That's why identity and access management (IAM)[4] matters more than ever. If an attacker can compromise a broker portal, claims workflow, customer-service environment, support account or privileged admin path, they may not need advanced malware. They can create fraud, interrupt service or persist quietly through legitimate access. For insurers, identity should be treated as the first resilience layer, not a subtopic within architecture.

It's also mandatory for safe AI adoption. As insurers introduce AI into claims, customer service, underwriting, fraud detection and internal operations, they need to know who or what can access which data, trigger which workflows and support which decisions.

This becomes even more important with AI agents and non-human identities. Agents need permissions to be useful. But if those permissions are too broad, poorly monitored or not linked to clear business accountability, they can remove important control steps from processes that used to depend on human review, especially as many insurers are now moving from pilot environments to scalable, production-grade AI use cases.

Is DORA enough for AI?

DORA[5] and NIS2[6] are important resilience frameworks. They help raise the baseline around ICT risk, incident response, supplier governance and operational resilience. But insurers should not assume that compliance automatically covers the full risk profile of AI and agentic systems.

AI changes how data is accessed, interpreted and acted upon. It introduces new questions: Which data is used? Is it accurate? Who approved the use case? Which model or supplier is involved?

Can the output affect a customer, claim, underwriting decision or fraud investigation? What happens if an AI system is manipulated, over-permissioned or unavailable?

For insurers, this means AI governance should be connected to cyber security, data protection, identity, fraud, legal, compliance and operational resilience. It should not sit in isolation as an innovation topic.

References:

[5] https://www.nccgroup.com/campaign/preparing-for-the-digital-operational-resilience-act-dora/

[6] https://www.nccgroup.com/campaign/nis2-prepare-your-organisation-for-compliance/

What insurers should do now

7 priorities for resilient AI adoption

1. How fast you patch now matters as much as what you patch

Attackers move within days or hours of disclosure. Organizations and their suppliers need fast decision-making, business-context prioritization, clear ownership and remediation processes that move just as fast.

2. Invest in detection and response, not only prevention

You cannot always patch, block or prevent quickly enough. Stronger detection across endpoint, identity, network, cloud and SaaS environments helps reduce the impact when something gets through. Response should be prepared from both a technical and organizational perspective: containment, decision-making, communication, supplier coordination and recovery priorities all need to be clear before an incident occurs. This also needs to be exercised in practice, because the real response during an incident often differs from the process described on paper.

3. Treat key suppliers as part of your incident response

Know in advance how quickly they act (review SLA's), what visibility you get, and how you operate together when something breaks.

4. Harden identity where attacks actually succeed

Focus on phishing-resistant multi-factor authentication for critical access, stricter helpdesk checks, fewer always-on privileges, and tighter controls for brokers, third parties, administrators and non-human identities.

5. Ransomware resilience

Identify what must keep running, define manual workarounds, recovery order and backup priorities, and rehearse executive decision paths before an outage forces real-time improvisation.

6. Trust, but verify, especially under pressure

Add independent verification for sensitive actions and test those controls with realistic vishing and deepfake exercises across support desks, IT service desks, finance teams and board-level decision-making. Not just assumptions on paper.

7. Validate AI before and after deployment

AI use cases that touch sensitive data, customer processes or decision-support should be tested. This includes secure coding, model and application testing, LLM pentesting, access control reviews and scenario-based assurance.

Closing thought

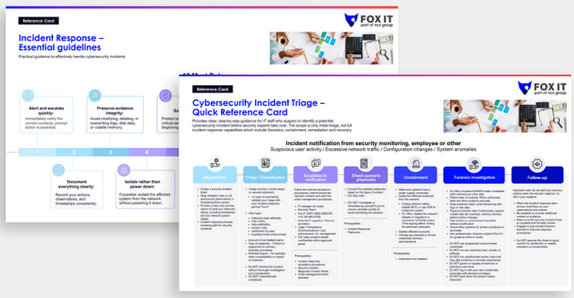
The most resilient insurers will be those that connect technical innovation, security, fraud, operations and supplier governance from the start.

They'll budget for resilience as part of transformation, not after it. They'll know which services must keep running, which vulnerabilities must be fixed first, which suppliers must act quickly, and how to validate what is real during an incident.

In this environment, resilience is not about slowing the business down. It's what allows organizations to adopt new technologies faster and with control, and to keep delivering when the next incident, vulnerability or technology shift puts that control to the test.

The boardroom question is not whether every risk can be prevented. It's whether the organization can quickly determine what matters, who must act, and how essential services continue when technology, suppliers, identity controls or AI systems fail.

Scan to download our step-by-step Incident Response triage card



Do's and Don'ts for every stage of a cyber incident, including an offline contact's sheet.

If you would like to discuss what all this could mean for your insurance organization, contact me at **alex.douven@fox-it.com** or call **+31 630 900 188** to schedule a **30-minute executive session** with one of our experts.

FOX IT
part of ncc group

Cyber attack?

Call our 24/7 Hack Hotline now.

Fox-IT - Benelux
0800 369 23 78 (NL)
+32 2304 22 16 (BE)
+31 (0) 88 369 23 78 (Int)

UK & Europe
+44 331 630 0690

U.S. & Canada
(855) 684-1212

Australia
1800 975 310

Singapore
+61 2 8379 7870

We are here for you

Contact us today to learn more about global cyber security regulations.

Fox-IT - Benelux
+31 (0)85 799 0680 (NL)
+32 2304 22 19 (BE)

UK & Europe
+44 (0) 161 209 5200

U.S. & Canada
+1 (800) 813 3523

Australia
+61 (0) 2 9552 4451

Singapore
+65 6800 0950

Philippines
+63 2 8540 9450