Atos Cybersecurity:

Safeguarding the Digital Supply Chain in Insurance.

Welcome to the forefront of supply chain security! In our increasingly interconnected digital world, safeguarding your supply chain is absolutely vital, particularly for organisations in the insurance sector. As you engage with a range of stakeholders, including reinsurers, third-party administrators, data providers and technology vendors, it is important to recognise that vulnerabilities can arise from various sources. These potential risks can pose significant challenges to your operations and reputation. Find out how you can strengthen your supply chain security and confidently navigate these complexities.

Navigating the Complexities of the Insurance Supply Chain

According to IOA (Insurance Office America) "supply chain risks associated with software and partner dependencies are key points of consideration for insurers that are asked to provide cyber insurance, and insurance companies expect organizations to know their vulnerabilities and address those through internal controls and contractual risk transfer with partners and vendors. Even organizations that have high-quality internal cybersecurity measures are at risk of business interruption—sometimes severe—due to supplier, vendor, and downstream distributor disruptions resulting from cyberattacks or failures. Cyber due diligence and Third Party / Supplier Cyber risk mitigation are two practices all organizations should follow when contracting with a company for services or material inputs." (Focus Report - 2025 Cyber Market Outlook | Insights | IOA)

Understanding the critical nature of these challenges, we are eager to partner with you. Our tailored cybersecurity solutions are designed to empower your organization, enabling you to navigate complexities with confidence and resilience. These solutions address key areas such as:

- Reinsurers: Facilitating effective risk transfer mechanisms.
- Third-Party Administrators (TPAs): Streamlining claims processing and enhancing customer interactions.
- Data Providers: Delivering essential information, including actuarial data, weather forecasts, and health records.
- Technology Vendors (ICT Third Party Service Providers): Supporting platforms for underwriting, claims management, and customer relationship management.
- Regulatory Bodies: Ensuring compliance with industry standards and regulations, including the EU Digital Operational Resilience Act (DORA), while emphasizing the importance of effective risk management by ICT Third Party Service Providers.

Digital and cyber supply chain risks have their own specifics in Insurance sector but also in other sectors like shown below table for Banking, Manufacturing. Differences between them indicate both on scope, priorities and types of technologies (limited OT aspects in Financial Sector).

Sector	Supplier Categories	Exemplary Digital or Cyber Supply Chain Risks
Insurance	- Reinsurers (risk transfer) - Brokers/Agents (insurance distribution) - Third Party Administrators (claims processing) - ICT Suppliers (core ICT systems: underwriting, CRM, claim management, actuarial systems, insurance premium calculations, etc.) - Data Providers (actuarial, weather, health data)	- Data breaches (personal/health or property claims data) - System downtime in claims platforms - Inaccurate risk data feeds - AI/algorithmic bias in underwriting - Dependency on few reinsurers
Banking	- Fintech Partners (payments, APIs) - Credit Bureaus (credit data) - Cloud Providers (core banking infrastructure) - Card Networks (Visa, Mastercard) - Outsourced KYC/AML services	- API security issues - Third-party fraud exposure - Compliance failures from outsourced providers - Cyberattacks via weak fintech links- Data residency/ regulatory gaps
Manufacturing	- Raw Material Suppliers - Component Manufacturers - OEM Partners - Logistics Providers- Maintenance/IoT System Vendors	- Supply chain cyberattacks (e.g., ransomware on logistics) - IoT security flaws - Intellectual Property theft via digital CAD/CAM tools - Disruption via ERP system outage - Supplier compliance data manipulation

Third-party breaches pose additional risks, often **serving as entry points for ransomware attacks**, which can affect multiple targets across the supply chain.

Optimizing Cybersecurity for Your Supply Chain

We are excited to offer our expertise in cybersecurity, empowering your organization to enhance its resilience and trustworthiness. By implementing robust security measures, you can:

- Foster customer trust by demonstrating a commitment to protecting client data.
- Ensure operational resilience, minimizing downtime during incidents.
- Achieve regulatory compliance, streamlining processes to meet required standards while avoiding penalties.

We can help you start with value-oriented advice, documented through risk-based assessments that go beyond mere compliance. Our actionable recommendations are informed by real-time cyber threat landscapes, drawing from the expertise of our 17 Security Operations Centers worldwide. **We align our practices with established frameworks** like ISO/IEC, ISA, and NIST, ensuring you receive the best possible support based on our multi-year operational experience in diverse ecosystems, including securing major events like the Olympics in Paris 2024.

Atos's Distinct Advantage: Security Advisor and Managed Services Provider

What sets Atos apart is our ability to seamlessly integrate advisory services with managed security solutions. As your security advisor, we provide in-depth risk assessments that evaluate your supply chain vulnerabilities. Our experts utilize advanced cybersecurity rating platforms, offering you actionable insights that inform your strategic decisions.

As a managed services provider, we take this a step further by implementing and continuously monitoring security measures across your supply chain. This comprehensive approach ensures that your organization not only identifies risks but also actively mitigates them. Our 17 global Security Operations Centers enable us to deliver real-time threat intelligence and advanced response capabilities tailored to the insurance sector. Together, we can enhance your cybersecurity posture and build a resilient supply chain that fosters trust and innovation.

Conduct Suppliers' Cyber Due Diligence
• **Initial Assessments:** Evaluate vendor's security posture and compliance. • **Security Ratings:** Use cybersecurity rating platforms for insights.
Implement a Robust Third-Party Risk Management (TPRM) Program
• **Define Criteria:** Set clear selection criteria based on cybersecurity capabilities. • **Ongoing Monitoring:** Continuously track vendor security performance.
Assess Fourth-Party Risks
• **Vendor's Vendors:** Recognize and mitigate risks from a vendor's suppliers. • **Supply Chain Audits / Independent Tests:** Conduct audits to identify vulnerabilities.
Establish Clear Security Requirements
• **Contractual Obligations:** Include cybersecurity requirements in contracts. • **Incident Response Plans:** Ensure vendors have effective incident response plans.
Conduct Regular Security Assessments
• **Periodic Reviews:** Schedule regular assessments of vendors. • **Penetration Testing:** Test critical vendors for vulnerabilities.
Foster Communication and Collaboration
• **Open Dialogue:** Maintain communication regarding security concerns. • **Collaboration on Security Initiatives:** Work together on security efforts.
Educate and Train Internal and Suppliers' Teams
• **Awareness Programs:** Train employees on third-party risks. • **Best Practices Sharing:** Share effective management practices.
Utilize Technology Solutions
• **C-SCRM / TPRM Software:** Implement tools for streamlined assessment and monitoring. • **Threat Intelligence Platforms:** Leverage platforms for ongoing vulnerability awareness.

Benefits of Partnering with Atos

- **Enhanced Security Posture:** Proactive identification and mitigation of risks across the supply chain.
- **Regulatory Compliance:** Streamlined processes to meet regulatory requirements (EU DORA, etc.) industry standards and avoid penalties.
- **Operational Resilience:** Minimized downtime and maintained service continuity during incidents.
- **Customer Trust:** Demonstrated commitment to protecting client data fosters confidence and loyalty.

Join Us in Strengthening Cybersecurity

By collaborating with Atos, you can enhance your digital supply chain's security posture and protect your valuable assets. Our comprehensive services are designed to meet your unique needs and ensure that you are well-equipped to tackle the challenges of today's cyber landscape.

Customer Success Stories

Case Study: Improvement of Cyber Supply Chain Assurance Framework

The Client

Global public-private partnership focuses on raising and distributing funds to combat major health issues in low- and middle-income countries. It funds country-led programs based on proposals from the countries themselves, ensuring broad participation from governments, civil society, and the private sector. This organization is a major player in global health, providing significant portions of international funding for these efforts.

The Challenge

Elaboration of Cybersecurity Assurance Framework in the Procurement Process which will be compliant to EU Regulations like DORA, NIS2, Cyber Resilience Act and other regulatory requirements indicated by the client. Assessment of "as-is" status and postulation "to be" blueprint.

Solution

Elaboration of Cybersecurity Assurance Suppliers' Framework (CASF) which is linked to Information Security Policy and Procurement Processes based on best practices like NIST Cybersecurity Framework, ISO best practices for Security Assurance, UK Government Supplier Assurance Framework, etc.

Deliverables included:

1. Management Presentation summarising current and target operational model.
2. Mapping all NIS2, DORA, Cyber Resilience Act requirements with Customer ISO management systems ISMS (ISO 27001), BCMS (ISO 22301), IT SMS (ISO 20000) and NIST CSF 1.1 and 2.0.
3. Delivery of control framework to fit various criticality of suppliers.
4. "Delivery-ready to implement" recommendations to improve cybersecurity posture of client's suppliers.
5. Proposing high-level cost scenarios for Suppliers Assurance Programme for auditing suppliers based on elaborated CASF.
6. Postulation of Programme-based approach on recognized organisation "Charter-of-Trust" to increase mutual trust and information security awareness training.

Take the Next Step

Secure your insurance supply chain with Atos' cybersecurity expertise. We invite you to explore our services and discover how we can work together to build a secure digital environment for your organization.

- **Explore Our Services:** Atos Cybersecurity Services (https://atos.net/en/services/cybersecurity)
- **Contact Us:** https://atos.net/en/contact-us

About Atos

Atos Group is a global leader in digital transformation with c. 72,000 employees and annual revenue of c. € 10 billion, operating in 68 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

106532-SB-OP