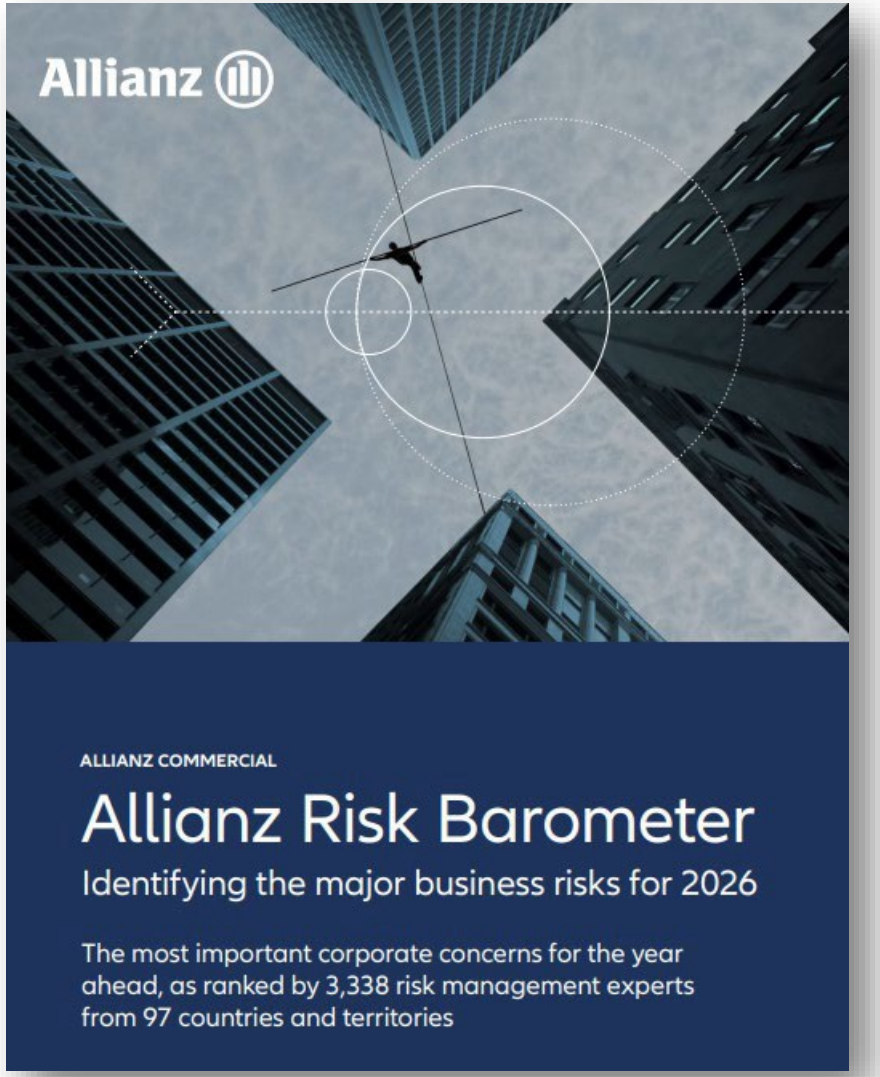
German-American IT Security Forum

San Francisco, 23.03.2026

Industrial Cyber Resilience in the Age of Hybrid Warfare

Sudhir Ethiraj, TÜV Süd

Cybersecurity Risk tops the global business risk index



- Global insurance giant Allianz's Risk Barometer rates **Cybersecurity Risk to be the top risk or businesses for the 5th consecutive year**
- **Small and Medium Size Enterprises are highly vulnerable** and form critical parts of global supply chains
- **Deep reliance on digital technologies, with increased attack surface**, combined with **geopolitical risk (hybrid warfare)** landscape makes cyber risk top the list
- Outages, espionage, reputation risk, production halts and product recalls all trigger the need to take this up seriously with **critical actions and mitigation measures**

Trends & Challenges in ensuring Industrial Cyber Resilience

Building Resilient ecosystems

Evolving **cyber threats, sophistication of cybercrime** (Cybercrime-as-a Service), **hybrid warfare** demand for highest levels of security principles

Targeting Harmonized policy

Emerging **local and global cybersecurity regulations**, demand for harmonization in the creation of cybersecurity policy & ensuring global market access

Accelerating with Emerging technologies

Accelerating with **emerging technologies such as agentic AI and Quantum** and addressing their impact on cyber risks and trust associated

Cross-Disciplinary Education & Upskilling

Fostering cross-disciplined and cross-functional education to combine domain-specific know how to understanding digital technologies at scale

What drives Cybersecurity investment across sectors?

Industry Segments


Automotive


Medical devices & diagnostics


Transportation (rail, airport)


Energy (Generation/Distribution)


Manufacturing


Buildings & Elevators


Consumer Products & retail


Processing


Pharma

Drivers

Regulations

Mandatory and harmonized regulations for Cybersecurity in that sector (e.g., Medical, Lifts, Automotive UNECE, Energy Sector, BFSI, etc.)

Cyberattacks

Increased cyberattacks in that particular industry (Automotive Supply Chains, Smart Grids etc.)

Awareness & need from their customers

Awareness of cybersecurity risks, demand from their customers and to stay ahead of the competition (e.g., TISAX, CSA STAR, etc.)

Tackling Cyber Risks: Principle of Security by Design & Security by Default for enhanced resilience

The principles of security by default & security by design

The principle is based on the fundamental concept that cybersecurity and data protection considerations are included right from the start of a design of a product (secure by design), process and organisational model

Ways these principles enable industrial resilience

- *Ensuring the **development and delivery of secure products***
- *Ensuring that **secure processes** (including secure software development, secure supply chain, resilient production environments) are involved*
- *Ensuring that **security is at the highest priority level** at the design phase ensures trustworthy services, secure products and resilient infrastructures*

Cybersecurity by default and third-party assessment are must-haves across the entire value chain

Illustration

Design	Development & Procurement	Production	Delivery & Logistics	Sales, Marketing, Office IT, HR
Security by design & Security by Default	**Security in the supply chains**	**Security in both the production environment**	**Security and availability of logistics**	Security of **webshops and Point of Sales Terminals** (Retail)
Security embedded at an early stage during the design phase of products, component and processes	Security both at supplier & “supply” level **Supplier training** at organizational level	Manufacturing processes and at the product/component level **Employee Training** at production level	**Availability of secure information** on the logistics	**Secure Backoffice** (Convergence of OT & IT Security) **Secure Onboarding & Offboarding** of employees Encryption & Availability of Information **(Cloud & On-Prem)**

Cybersecurity by default and third-party assessment are must-haves across the entire value chain

Secure by default products

- Ensuring security requirements are considered right at the outset with product design phase
- Requirements such as regular software updates, regular patch mechanisms, product manual for consumers, high level of authentication methods etc., are crucial
- ***Secure by design products and components ensure trustworthy products are placed in the market***

Secure by default processes

- Ensuring secure development lifecycle processes are maintained to ensure security is not just at the "product level" but beyond and in the processes behind the development of products
- Requirements such as risk management procedures, secure supply chain, regular audits are extremely crucial
- ***Secure organisational processes are baseline in ensuring resilient ecosystems that can identify, detect, respond to and recover from cyber attacks***

Secure by default organisations

- Security by default as part of the core DNA of organisational models behind products and services
- Crucial requirements such as security drills, training, risk assessment & mitigation procedures are all part of a secure organisational DNA
- ***Services and products from secure organisations ensure competitive advantage and resilient business models***

Risk Assessment as a crucial key to ensure resilience in industrial and critical infrastructure environments

A Large Food Manufacturing Company Example

- Recently, a multinational food and beverage company, **suffered a cyber attack (NotPetya malware)** that damaged the entire production network and infrastructure
- The attack wiped out more than **20,000 laptops and servers** within their network.
- The company has ever since taken cybersecurity (focus OT) very seriously and **has commissioned an independent organisation to do third-party cyber risk assessment** for their OT infrastructure in 4 locations in 2 countries

Value Addition

- A **10-stage OT/ICS Cybersecurity risk assessment (4-day onsite & 7-day offsite)** based on the following standards:
  - NIST Framework and Standards
  - IEC 62443-2-1 & IEC 62443-3-2
  - Company's own risk assessment questionnaire
- The **neutral risk assessment report** based on a combination of standards gives **a clear picture for the customer on their OT Cybersecurity Posture**
- The report is also aimed to support the company's management to **invest in the right areas and mitigate cyber risks** in the future

Trustworthiness as a core element of new technologies and ensuring “Digital Trust”

01

Ensuring key aspects such as trustworthiness, ethics, transparency and accountability

02

Ensuring AI/Data Quality

03

Compliance to regulations such as, the EU AI Act, EU Data Act etc.,

Regulations

Regulations are currently being developed for ensuring trustworthiness in development of new technologies such as AI (EU AI Act, US Directives etc.,)

Standardization

Organisations such as ISO and VDE have developed and are developing new standards such as the ISO 42001 (AI Management Systems), ISO 5259 (Data Quality etc.,)

Cybersecurity will be “key”

Aspects of **cybersecurity and data protection will be key** to ensure success of any AI enabled digitization initiative

What can organisations do to keep up and ensure resilient industrial infrastructure?

Prepare an A-Team of Cybersecurity players within your company – across business units, regions and with **reporting anchored to the top** of the organisation

Identify the top risks with help of the team (and third-party as necessary), **plan for extensive mitigation measures** and make this **a continuous exercise**

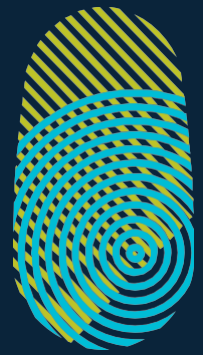
Involve your entire organisation beyond the cybersecurity team in the cybersecurity drills and **get involved in cross-company initiatives** to gain latest insights on cyber threats. Educate your consumers too!

Cybersecurity in the age of hybrid warfare requires cross-industry, global collaboration

Growing cyberthreats, both in volume and severity and including supply chain security risks, advanced with new technologies (e.g. AI) the Charter of Trust (CoT), founded in 2018, is a global ecosystem of leading companies and organizations working together to build a safer world.

Partners

Allianz · Atos · Bosch · Danfoss · elastic · IBM · Infineon · Microsoft · Mitsubishi Heavy Industries · msc · Siemens · TÜV SÜD · zscaler



Charter of Trust

Associated Partner Forum

Bundesamt für Sicherheit in der Informationstechnik · Canadian Centre for Cyber Security · CEBRI · CCN Centro Criptológico Nacional · certin · CSA · CR2 · CSIR · CyberPeace Institute · Cyber Readiness Institute · Global Cyber Alliance · Hasso Plattner Institut · METI · 総務省 MIC · Shared Assessments · Tecnológico de Monterrey · TU Graz

1 **Protect the data** of individuals and businesses.

2 **Prevent damage** to people, business, and infrastructure.

3 Create a reliable foundation on which **confidence in a networked, digital world** can take root and grow.

Thank you!

Contact

Sudhir Ethiraj

TÜV SÜD Global Head of Cybersecurity Office (CSO) & CEO Business Unit Cybersecurity Services

Sudhir.Ethiraj@tuvsud.com