Risk Consulting

2 • 2026

Insights into risk management and loss prevention

4 Why supply chains must prepare for more extreme weather

16 Expanding into U.S. markets

26 Truck gate procedures in Europe



Contents

4 Why supply chains must prepare for more extreme weather

8 Electricity enables the green transition, economic growth, and security of supply

13 Climate change challenges infrastructure durability

16 Expanding into U.S. markets

19 Controlling hot work risks

22 Preventing conveyor belt fires

26 Truck gate procedures in Europe

30 Understanding recourse in insurance claims







Publisher If, Keilasatama 2,
02150 ESPOO, Finland
+358 10 19 15 15, www.if-insurance.com
Editor-in-Chief Kristian Orispää
Editor Carita Hämäläinen-Tallgren
Art Director Petri Bergman
Production Miltton Oy

Printing Newprint
Change of address
industrial.client-service@if.fi
ISSN 1459-3920
Cover Photo Gettyimages

Disclaimer This publication is and is intended to be a presentation of the subject matter addressed. Although the authors have undertaken all measures to ensure the correctness of the material, If P&C Insurance does not give any guarantee thereof. It shall not be applied to any specific circumstance, nor is it intended to be relied on as providing professional advice to any specific issue or situation.

If P&C Insurance contact information

Finland: +358 1019 15 15
Sweden: +46 771 43 00 00
Norway: +47 98 00 24 00
Denmark: +45 7012 24 24
France and Luxembourg: +33 142 86 00 64
Germany: +49 6102 710 70
The Netherlands and Belgium: +31 10 201 00 50
Great Britain: +44 20 7984 7600
Estonia: +372 6 671 100
Latvia: +371 7 094 777
Lithuania: +370 5 210 89 25

EDITORIAL

Winds of change

The Nordic climate is changing faster than many business strategies and continuity plans account for. The question is no longer if changes are coming, but where will vulnerabilities surface first. How can preparedness support stronger assets, more dependable value chains, and better decision-making as the environment in which we are operating becomes less predictable?

Why this matters now

Europe has been experiencing the effects of climate change first-hand for years. According to the Copernicus Climate Change Service (C3S) and the World Meteorological Organization (WMO), it is the world's fastest-warming continent, with temperatures rising at roughly twice the global average since the 1980s. Sicily's verified European temperature record of 48.8 °C from August 2021 is an example of the extreme temperatures that will test the resilience of the continent in the future.

Across the Nordics, the climate is becoming warmer and wetter, with milder, increasingly wet winters, heavier precipitation, and changing flood risks. The shifting weather is also revealing hazards in places where they may not previously have existed, urging continuous business continuity planning for companies.

A changing climate can simultaneously strain facilities, energy systems, logistics, employees, suppliers and customer behaviour. Adaptation to these changes is ultimately an investment in continuity.

Investing in what comes next

Nordic companies already benefit from strong engineering, mature risk management and close cooperation between business and society. Insurers can support clients before and after losses by bringing data, engineering insight and practical experience into decision-making. Perhaps a cliché but nonetheless, resilience and preparedness are investments in future growth.

At If, we are adapting to these changing conditions together with our clients, partners, and brokers. Having a reliable source of energy and robust infrastructure are central to this. Climate change can place pressure on electricity networks, while electrification, renewable energy and digital services make dependable power even more important.

In this issue of Risk Consulting magazine, we dive into the risks involved with meeting electricity demand on the grid level, look at how extreme weather is impacting supply chains, as well as present variety of insights from our risk management and loss prevention experts; from controlling hot work risks to preventing conveyor belt fires. ●

Poul Steffensen
Head of Business Area Industrial



CARGO

Why supply chains must prepare for more extreme weather

By **Laura Hyytiäinen**, If

Recent heatwaves across Europe underline a growing reality for global supply chains: cargo risk is no longer limited to storms, floods or long-distance shipping routes. Rising temperatures, more frequent extreme weather events and increasingly volatile weather patterns are creating new vulnerabilities for goods in transit and temporary storage. For large enterprises, climate-related cargo losses can increase logistics costs, disrupt operations and threaten business continuity.

Climate change is increasing both the frequency and severity of weather-related disruptions, placing growing pressure on global supply chains. As a result, climate-related cargo risks are no longer limited to isolated damage events. They can also lead to delays, cargo accumulation, production interruptions and a higher total cost of risk.

Higher baseline temperatures are increasing the intensity and duration of heatwaves, while more volatile weather patterns can create consecutive disruptions, such as drought followed by flooding. The result is a growing likelihood of severe, compounding supply chain disruption. For companies, the direction is clear: exposure to climate-related cargo risks is increasing, making resilience and proactive risk management essential.

"With several parts of Europe facing unprecedented heatwaves, companies would benefit from reassessing how exposed their goods are during road transport, terminal waiting times and temporary storage. For cargo owners, extreme heat creates risks throughout the supply chain. Even short periods in high temperatures can damage sensitive goods or reduce shelf life, affect packaging performance and place additional strain on refrigeration units," explains **Eva Nyholm**, Underwriter specialised in cargo insurance at If.

Extreme weather is becoming a cargo risk multiplier

Heat can also affect the infrastructure that supply chains depend on. Roads, rail networks and logistics facilities may face operational challenges





GETTY IMAGES

GETTY IMAGES

during prolonged hot weather. Drought can lower river levels and limit inland waterway transport, while water shortages can reduce transit capacity through key trade routes such as the Panama Canal.

These disruptions often lead to rerouting, longer transit times and port congestion, extending cargo exposure to heat, humidity and theft risks.

Flooding and storms add further complexity

Heat is only one part of the climate risk picture; increasingly frequent heavy rainfall and flash flooding are also affecting cargo. These events can disrupt port operations, increase flood exposure for warehouses and put inland transport routes under pressure worldwide. Water damage to cargo during transit and temporary storage has become increasingly common, particularly in regions where logistics infrastructure is not designed to withstand severe weather.

"According to our experience, water damage to goods in transit and during temporary storage is increasing. In Asia, many storage sites close to ports are not prepared to withstand heavy rain or flooding. Containers may be placed directly on the ground, allowing water to flow inside, or goods may be loaded and unloaded in heavy rain. These conditions are contributing to rising warehouse accumulation losses, especially in Asia-Pacific and LATAM countries," Nyholm says.

Humidity is another growing concern. Increased moisture levels can cause corrosion, mould, and condensation damage, particularly for machinery, electronics, textiles and other sensitive products.

"Storm patterns are also becoming less predictable. More severe storms and changing weather tracks increase the likelihood of vessels and cargo encountering unexpected conditions, raising operational and loss-related risks," she continues.

El Niño and global supply chain disruption

The World Meteorological Organization has warned of a high probability of El Niño conditions developing during the latter part of 2026. Historically, El Niño events have been associated with increased frequency and severity of weather-related disruptions across multiple regions.

Combined with longer-term climate change trends, these weather events can create systemic impacts that extend far beyond individual cargo losses.

"Climate impacts are no longer only a source of physical damage. They also drive disruption losses, port congestion and spikes in cargo accumulation during transit. Rerouting may introduce unfamiliar corridors with higher theft or handling risks, while greater reliance on multi-modal transport, from sea to rail to road, adds further complexity," Nyholm shares.

Building climate-resilient cargo operations

The greatest challenge for many large enterprises is not a single cargo incident but the accumulation of risks throughout the supply chain.

"When cargo is delayed at ports, exposed to heat during road transport or temporarily stored in facilities not designed for today's weather extremes, financial exposure can increase rapidly. Accumulation of high-value goods in warehouses, terminals or transit hubs can significantly amplify loss severity," says Cargo Underwriter **Marianne Zambrano** from If.

The consequences often extend beyond physical damage to include:

- Production interruptions
- Missed delivery commitments
- Customer claims
- Increased storage costs
- Contractual penalties
- Higher insurance costs

Simple measures that help reduce exposure to cargo risks

- More durable packaging and protection: Use temperature-resistant packaging, moisture barriers, thermal liners and climate-resilient materials to protect goods against heat and humidity.
- Improve routing and logistics planning: Avoid high-risk routes and regions during peak heat periods. Use dynamic routing based on weather forecasts and consider timing measures such as night transport to reduce heat exposure. Assess port risks, including flood exposure and the likelihood of congestion.
- Increase monitoring and visibility: Deploy real-time sensors (temperature, humidity, shock) and online tracking for early warning and intervention. Set automated alerts for threshold breaches.
- Review storage conditions: Use climate-controlled, shaded or covered storage where possible, and minimise unnecessary waiting time at ports and terminals. Reassess storage limits during transit and monitor accumulation risks and peak cargo values at ports and warehouses.
- Enhance contingency planning: Build buffer times and identify alternative routes. Move from static accumulation limits towards event-sensitive accumulation frameworks. Pre-arrange backup warehousing and carriers and establish clear incident response protocols.
- Use data to drive decisions: Analyse historical weather and loss data to identify risk hotspots. While weather patterns are changing, historical data can still reveal valuable insights into recurring exposures. Where newer data is limited or harder to access, companies should strengthen their analysis with predictive analytics in logistics planning and supplier or carrier risk scoring.

As a result, cargo risk management should be integrated into broader supply chain resilience and business continuity planning.

A strategic partner in cargo risk management

Companies should regularly review their insurance policies to ensure the coverage reflects climate-related exposures, increasing cargo values, longer transit times and, where relevant, temperature-controlled transportation. However, managing climate-related cargo risks requires more than insurance alone. A comprehensive approach combines prevention, risk analysis and claims expertise.

"At If, we help businesses identify vulnerabilities in transport routes, storage arrangements and logistics operations. We act as a strategic sparring partner, helping companies navigate evolving risks and build resilience through prevention, advisory support and claims data insights," Marianne Zambrano adds.

A key priority is preventing losses before they occur. This involves assessing transport routes and storage arrangements to identify vulnerabilities throughout the supply chain.

As climate change continues to reshape global supply chains, organisations that proactively address cargo exposures will be better positioned to protect assets, maintain continuity and control their total cost of risk and strengthen long-term resilience. ●



Meet our experts

Eva Nyholm
Cargo Underwriter, Denmark



Marianne Zambrano
Cargo Underwriter, Denmark

If helps businesses manage climate-related cargo risks through loss insights, expert advice and tailored insurance solutions. Our specialists identify trends and vulnerabilities, helping companies strengthen risk management, while efficient claims handling and recovery support help minimise disruption when losses occur.

REFERENCES

- WEF warns El Nino poses systemic risk as shipping flags food and coal risk | S&P Global
- IPCC AR6 (2021), NOAA Climate.gov ENSO Resources, NOAA Climate Prediction Center og WMO El Niño/La Niña Updates
- Chapter 11: Weather and Climate Extreme Events in a Changing – IPCC





IF

ENERGY

Electricity enables the green transition, economic growth, and security of supply

By **Vilma Torkko**, If and **Kosti Rautiainen**, Caruna

How will the increasing demand for energy be met? Kosti Rautiainen, Head of Customer Relations at Caruna, a Finnish electricity distribution system operator, provides insights into the challenges modern power grids are facing, specifically diving into the Finnish energy landscape.

Electricity has become one of Finland's most critical drivers of growth, resilience, and the green transition. While the electrification of industry, transport, and heating provides a competitive advantage, grid capacity could become a significant bottleneck.

Kosti Rautiainen from Caruna notes: "Renewable and affordable energy is a competitive advantage. Nordic economies and companies can be winners in the transition also on a global scale if we together are brave and determined to make the decisions needed to accelerate system-level investment and act fast enough."

Reliable but under pressure

A key issue is not only how much electricity is used over a year, but how much is needed at the same time. The grid is dimensioned for peak demand. This means even moderate growth in total consumption can still strain the system if demand concentrates into the same hours. In practice, "energy" and "power" are very different challenges.

Finland has made strong progress in electricity network reliability. Investments over the past decade have significantly improved the grid's ability to withstand storms and disruptions, which was clearly demonstrated during the Hannes storm in 2025, when the system remained far more stable than in the past. As a result, Finland now has one of the most reliable electricity networks in Europe.

However, the nature of the challenge is changing. The key question is no longer only whether the grid provides a steady power supply, but whether it can deliver sufficient capacity, fast enough, to support rapid electrification.

At the same time, electricity networks are no longer just technical infrastructure, rather they have become critical to national security and emergency preparedness. As societies become more dependent on electricity, power grids are increasingly exposed not only to storms and equipment failures, but also to cyberattacks, sabotage, and other deliberate disruptions.

Increasing grid capacity

The pressure to increase grid capacity is already visible. Distribution networks have recorded new peak demand levels, with multiple municipalities reaching record highs in early 2026. Several trends are converging: heating is being electrified, industry and data centres are expanding, large heat pump plants are being deployed, cities are growing, and electric vehicles are spreading rapidly.

Bottlenecks in Finland's energy landscape

- Heating electrification is one of the strongest drivers of peak demand growth. Electric boilers are a clear example, as they can add large amounts of demand very quickly. Finland could reach around 3000 MW of electric boiler capacity by 2027, representing a significant system shift. While this supports decarbonisation, it also increases peak demand and the need for network capacity.
- Electric transport is another major driver. Home charging is becoming the norm, and even a single EV charger can significantly increase a household's peak load. More importantly, charging often concentrates in the same time windows, overnight or during low-price periods, and automation reinforces this behaviour.
- A more technical but important issue is phase imbalance in residential networks. As high-power devices become more common, uneven loading can cause voltage fluctuations and stress equipment, from wiring and fuses to sensitive electronics. At larger scale, this becomes both a reliability and safety concern.
- Energy storage adds another layer of complexity. Batteries can support the system, but they can also increase peaks depending on how they are operated. If many systems respond to the same price signals, they may charge simultaneously, creating new demand spikes. Home battery connections are expected to grow significantly by 2030. The key issue is not the technology itself, but how it behaves collectively. This highlights the importance of well-designed incentives and market signals, ensuring flexibility reduces system stress rather than amplifying it.



> If electrification outpaces grid expansion, capacity can effectively hinder economic growth and risk energy security.

In a more uncertain operating environment, grid capacity can no longer be scaled only for normal conditions. The system must also be able to withstand sudden interruptions, power outages, damage, and exceptional situations without compromising the functioning of society. In practice, resilience means not only protection, but also spare capacity, backup connections, and the ability to restore electricity quickly after disruptions.

At the same time, price-driven automation is synchronising electricity use. When prices fall, systems often activate simultaneously, charging batteries, heating water, and charging vehicles, which creates sharper peaks. Managing this increasingly complex system depends on better data, forecasting, and digital tools, including real-time visibility and more advanced control systems. Looking ahead, AI-driven optimisation and improved forecasting are likely to play an increasingly important role in balancing the system.

Electricity production is also evolving. More renewable power generation is being connected to local networks, while traditional combined heat and power is declining in many growth areas. This shift increases weather dependency and variability in supply. As a result, the need for adaptability and flexibility is growing, along with the importance of coordinating the system as a whole, rather than optimising its individual parts in isolation. This requires closer integration between production, transmission, distribution, as well as end users, supported by data sharing and secure system operation.



Kosti Rautiainen
Head of Customer Relations at Caruna

Capacity limits are slowing growth

Constraints are not limited to local networks. Bottlenecks can also emerge upstream in the transmission grid. Even if a distribution network has capacity, new connections may be delayed if the higher-level network is constrained. This is particularly important for large industrial projects, data centres, and electrified heating solutions, all of which require significant new capacity. Constraints already identified in parts of Finland's transmission network indicate that this is not a distant risk. Impacts are often regional, with high-growth areas facing the tightest limitations.

Experiences from elsewhere in Europe illustrate how quickly this can become a real constraint. In the Netherlands, grid congestion has significantly delayed new industrial projects and connections. Denmark has also faced situations where parts of the grid are effectively full.

Finland is not in the same position, but the lesson is clear: if electrification outpaces grid expansion, capacity can effectively hinder economic growth and risk energy security. In practice, permitting and planning processes are often among the slowest parts of grid development, and delays risk becoming a structural chokepoint.

Flexibility cannot replace grid investment

So, what needs to happen? No single solution is enough. In practice, three elements must work together: investing in grid capacity, reducing peaks through tariffs that reflect system stress, and enabling smarter electricity use through flexibility solutions such as demand response and storage. A resilient power system depends on both physical infrastructure and operational preparedness, from spare parts to training staff and employees for various scenarios.

Even so, flexibility cannot solve a situation of structurally rising peak demand. It depends on functioning markets and incentives, as well as aggregators to combine smaller loads, pricing that reflects local constraints, and mechanisms that reward consumers and businesses for shifting demand. Without sufficient investment, the system risks shifting from enabling growth to managing scarcity.

Time is one of the most critical constraints. Grid projects often take significantly longer than industrial investments, largely due to



GETTY IMAGES

permitting and planning processes. This creates a structural mismatch, where demand can grow quickly while supply infrastructure takes years to develop. Closing this gap requires stronger long-term planning across the entire value chain. While targets such as Finland's carbon neutrality goal for 2035 are important, grid planning must extend further, towards 2040, to align industrial development, generation, network expansion, and flexibility solutions. Faster and more predictable permitting processes will be critical.

- Ventilation: Helps reduce gas concentration but does not eliminate explosion risks. Different levels of ventilation – basic, preventive, casualty – are recommended.
- Deflagration panels: These are designed to lessen the impact of explosions, with effectiveness dependent on covering sufficient surface area.
- Fire suppression systems: Water-based systems provide long-term cooling and can reduce explosion pressure. Gaseous systems can help if gas concentration is maintained at a sufficiently high level. ●

Increasing capacity is vital

Grid capacity is no longer only an energy issue. It is increasingly a question of economic growth, competitiveness, and regional development. In practice, the availability of network capacity can determine whether major industrial investments move forward, where they are located, and how quickly new business opportunities can be realised.

In Finland, Storm Hannes demonstrated what long-term investment can achieve for reliability. The next step is to apply the same level of ambition to capacity and speed of grid expansion.

Ultimately, the electricity system will shape how successfully Finland can grow, decarbonise, and compete with other nations. With forward-looking planning, faster permitting, and coordinated action across the value chain, electrification can remain a driver of growth, supporting investment and jobs while lowering emissions. Failing to act will only hinder economic opportunities, constrain supply chains, and impede the green transition.

GETTY IMAGES



PROPERTY

Climate change infrastructure



challenges durability

By **Vilma Torkko** and **Markus Sjunnesson**, If

Climate change is increasingly influencing the long-term durability and service life of infrastructure assets. Changes in temperature, precipitation patterns, atmospheric carbon dioxide concentrations, sea levels, and extreme weather exposure can accelerate material degradation and affect structural performance over time. As a result, infrastructure owners may face higher maintenance costs, shorter asset lifetimes, and increasing challenges in preserving the reliability of critical structures.

Why climate change matters for infrastructure

Infrastructure is generally designed around environmental conditions expected over several decades. Many deterioration mechanisms are strongly influenced by external conditions, meaning that changes in climate can alter the rate at which materials degrade.

Where degradation accelerates, structures may reach critical maintenance thresholds earlier than anticipated. Even modest increases in deterioration rates can have significant consequences over the lifespan of bridges, industrial facilities, ports, buildings, utility networks, and other long-lived assets.

Climate impacts on reinforced concrete

Reinforced concrete is susceptible to deterioration through carbonation and chloride ingress, both of which can initiate corrosion of embedded reinforcement.

Carbonation occurs when atmospheric carbon dioxide penetrates concrete and reduces its alkalinity. Once the protective environment surrounding reinforcing steel is lost, corrosion can

> Climate change should be viewed not only as a source of extreme weather events, but also as a long-term driver of material deterioration.

begin. Rising carbon dioxide concentrations and higher temperatures can accelerate this process, increasing the risk of cracking and deterioration.

Chloride ingress presents an additional threat, particularly in structures exposed to marine environments. Chlorides can penetrate concrete and attack reinforcing steel, causing corrosion, cracking, concrete spalling, and reductions in structural capacity. Rising sea levels may increase the exposure of coastal infrastructure to aggressive chloride-rich environments.

As corrosion progresses, the cross-sectional area of reinforcing steel is reduced, weakening structural resistance and shortening service life.

Corrosion risks for steel structures

Corrosion is one of the most significant threats to the long-term performance of steel infrastructure. Material loss reduces both strength and stiffness, affecting a structure's ability to withstand operational and environmental loads.

Corrosion rates are influenced by several environmental factors, including temperature, precipitation, chloride deposition, atmospheric pollutants, and the amount of time steel surfaces remain wet. Changes in these conditions can alter corrosion rates and accelerate deterioration in exposed structures.

Coastal and marine infrastructure are particularly vulnerable because chloride deposition can significantly increase corrosion rates. Rising sea levels may also alter exposure conditions and shift corrosion-prone zones in waterfront and harbour structures.

The performance of corrosion protection systems is equally important. Protective coatings gradually deteriorate with environmental exposure, increasing the likelihood of corrosion once the protection begins to fail.

Climate impacts on timber structures

Timber structures are sensitive to humidity and temperature conditions that influence biological deterioration.

When timber is exposed to conditions that support fungal activity, decay can gradually reduce structural capacity and long-term performance. As decay progresses, timber elements become more susceptible to damage and may require more frequent inspection, maintenance, or replacement.

The rate and severity of decay depend on environmental exposure, timber species, preservative treatments, and local climatic conditions, making long-term durability highly dependent on the surrounding environment.

When material degradation meets extreme weather

One of the most important durability challenges is the interaction between material degradation and environmental loading. Climate change can simultaneously accelerate material degradation and increase exposure to extreme weather, creating combined risks for infrastructure.

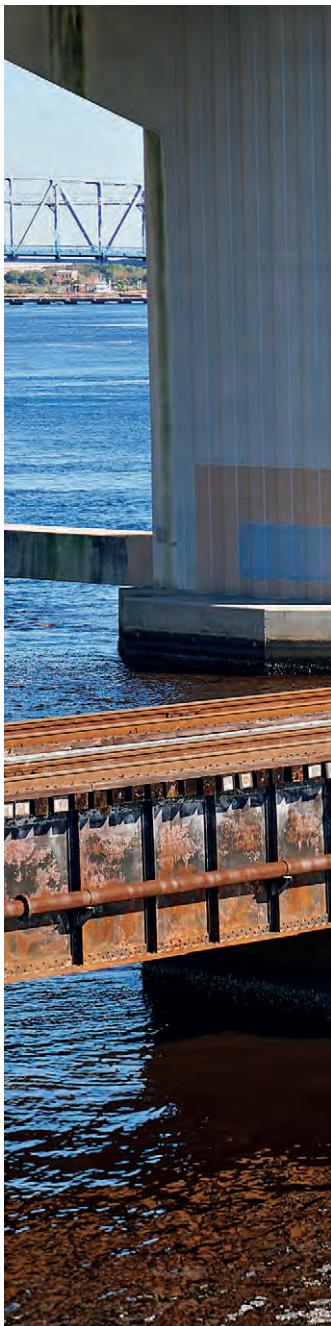
Structures that have already experienced degradation may therefore be less capable of resisting future loads. Assessing material deterioration and climate-related hazards separately can underestimate long-term vulnerability. Considering their combined effects provides a more realistic picture of future risk.

Building resilience into infrastructure management

Climate change should be viewed not only as a source of extreme weather events, but also as a long-term driver of material deterioration. Through its influence on corrosion, carbonation, chloride ingress, biological decay, and other degradation mechanisms, it has the potential to reduce service life, increase maintenance demands, and affect the long-term reliability of infrastructure assets.

Maintaining durable infrastructure therefore requires an understanding of how changing environmental conditions influence material degradation throughout an asset's life. Improving resilience will require changes in both design practice and asset management, with greater emphasis on condition assessment, monitoring, maintenance planning, and life-cycle management. Recommended approaches include:

- Incorporating climate projections into structural design.
- Using corrosion-resistant materials and protective coatings.



- Applying structural health monitoring systems to detect early deterioration.
- Performing risk-based maintenance and inspections, supported by life-cycle cost analysis.
- Developing adaptation strategies based on projected future climate conditions.

Together, these measures can help infrastructure owners extend service life and improve the reliability and resilience of critical assets.



Meet our expert

Markus Sjunnesson
Risk Engineer, Sweden

REFERENCE

- HAL open science
https://hal.science/hal-03906687v1



GETTY IMAGES

GETTY IMAGES



LIABILITY

Expanding into U.S. markets

What Nordic companies need to know about the liability risks

By **Laura Hyytiäinen**, If

Despite increasing geopolitical tension and regulatory uncertainty, Nordic companies continue to expand into the U.S. market. For many, growth in North America continues to be strong, driven by market size, access to capital, innovation ecosystems, and customer demand.

The U.S. remains the world's largest unified commercial market, offering scale that other nations cannot easily replicate. For growth-oriented companies, especially in technology and digital services, the incentives are clear: vast revenue potential, faster market access, and closer ties to investors.

From a liability and risk management perspective, however, the U.S. market operates on entirely different principles as it is not merely "another jurisdiction". Rather, it is a complex and unique liability landscape with legal standards, incentives, and exposure levels that differ significantly from the Nordics and broader Europe.

Understanding this difference is critical before scaling operations, integrating U.S. technology platforms, or bringing products and services on the American market.

Why liability risk looks different in the U.S.

Nordic companies are accustomed to predictable regulatory enforcement, proportional damages, and strong administrative oversight. In the United States, liability risk is shaped by different logic and demands an alternate approach to risk management.

Key distinctions include:

- Jury based civil litigation, where outcomes are more difficult to predict;
- high damage awards, including so called nuclear verdicts exceeding USD 10 or even 100 million;
- plaintiff driven litigation models, often supported by third party litigation funding;
- a fragmented legal structure, with both federal and state level exposure.

"In practice, a single claim can jeopardise the survival of a company. Liability exposure should therefore be assessed not only by likelihood, but by taking a specific US severity potential into account," explains **William McKechnie**, Head of Casualty Underwriting at If.

The incentive mismatch: when large damages become "Business as usual"

One challenge for European companies operating in the U.S. is a clear imbalance in incentives. For global technology providers and large U.S. corporations, large settlements or fines may be absorbed as part of doing business. When revenues are measured in the tens of billions, even nine figure claims may not fundamentally alter behaviour.

"From a liability standpoint, this matters because Nordic companies often act as suppliers or business partners to large U.S. corporations. Contracts can transfer significant liability risk to them, even though they may not have the same U.S. revenue base against which to absorb that exposure. As a result, Nordic companies may find themselves responsible for regulatory compliance, compensation claims, or customer losses that can amount to disproportionate liability exposures," McKechnie explains.

This asymmetry is particularly evident in areas such as data protection, digital services, software-as-a-service, and complex technology supply chains. It is therefore crucial for Nordic companies to consult U.S.-based counsel before entering into agreements with American partners, distributors, platform operators, or enterprise customers.

The opportunity – and the exposure: SaaS as a product

For companies delivering SaaS, AI tools, data platforms, or other digital solutions, one shift in particular demands immediate attention: in the United States, software and digital tools are increasingly being evaluated not only as services, but also through a product-liability lens.

Across much of Europe, software delivered as a service has traditionally been treated under service-law concepts, where liability is typically tied to professional negligence, contractual fault, and proportional damages. The provider is assessed on whether it performed its obligations competently.

"In the United States, this shift is already visible in how courts, regulators, and plaintiffs scrutinise SaaS platforms, AI systems, and digital tools. The focus is on how the technology is designed, how users rely on it, what safeguards are in place, and whether harm could have been prevented through clearer warnings, defaults, controls, or design choices," **Lindsay Dansdill**, Partner at Chicago-based law firm Mercer Oak points out.

Under product-liability theories, a claimant may argue that the software was defective in its design, deployment, warnings, or safeguards, and that harm resulted. The focus may shift away from whether the provider acted negligently and toward whether the product experience itself was unreasonably dangerous or inadequately controlled.

Recent litigation illustrates this shift. In *Raine v. OpenAI*[1)], plaintiffs alleged that ChatGPT's design fostered emotional dependency, failed to provide adequate safeguards, and should have responded differently to crisis-related signals. The claim was framed around AI architecture, guardrails, monitoring signals, and product behaviour rather than isolated chatbot outputs.

"For insurers and Nordic companies, the significance is clear: contractual labels describing software as a 'service' may offer limited protection if the technology functions like a product in the real world," reminds Dansdill.

The EU response: expanding product and digital liability

Europe is also expanding its liability framework for digital technologies. The updated EU Product Liability Directive formally classifies software, AI systems, and digital services as "products", lowers the burden of proof for claimants, and recognises new categories of compensable harm, including data destruction.

For Nordic companies operating transatlantically, this creates a dual layer of exposure: U.S.-style litigation risk on one side of the Atlantic, and increasingly stringent EU liability on the other. The revised framework adopts concepts familiar from product-liability systems and may increase exposure for companies operating across both jurisdictions.

From a U.S. perspective, these developments may also influence litigation strategy.

"Plaintiffs may cite European developments as evidence that software, AI, and digital services should be treated as products, or that certain risks were foreseeable and should have been addressed through design controls, warnings, or safeguards," Dansdill describes.

The contract as a first line of defense

Contracts with U.S.-based distributors, resellers, platform operators, and enterprise customers frequently contain provisions that shift product liability exposure onto the software vendor, impose open-ended indemnification obligations, or include warranty representations that inadvertently support a product liability theory.



Lindsay Dansdill
Partner at
Mercer Oak

> The U.S. market is a complex and unique liability landscape with legal standards, incentives, and exposure levels that differ significantly from the Nordics and broader Europe.

"It is important for Nordic companies to engage U.S.-based counsel before entering into agreements with American partners or customers," Dansdill stresses. "What reads as a standard commercial contract to a European lawyer can contain enormous liability transfer provisions that would be immediately flagged by a U.S. practitioner," she concludes.

Dansdill notes that, at a minimum, an agreement covering between a software service provider and a U.S. based vendor should contain a liability cap covering all theories of recovery — including product liability — tied to fees paid in the preceding 12 months, and an express warranty disclaimer using Uniform Commercial Code (UCC)-compliant language that excludes implied warranties of merchantability and fitness for a particular purpose. Many states impose these warranties automatically unless they are conspicuously and specifically disclaimed; a general limitation clause may not be sufficient.

A consequential damages waiver should also be included, excluding lost profits, business interruption, and data loss and other indirect damages to the fullest extent permitted by the governing jurisdiction.

Beyond these baseline protections, vendors should negotiate narrowly scoped indemnification obligations limited to defined claim categories such as intellectual property infringement rather than open-ended language covering "any claims arising from use of the software". Where appropriate, a product-liability carve-out or characterisation of the agreement as a services contract may preserve an additional line of defense, even if it is not dispositive in all jurisdictions.

Governing law, venue and arbitration provisions

According to Dansdill, governing law and venue should be negotiated toward predictable commercial jurisdictions such as Delaware or New York, with language that prevents plaintiffs from electing their home court. Contracts should also clearly assign compliance responsibilities and acceptable use obligations to the customer and should restrict the customer's ability to bring claims on behalf of end users or downstream parties whose conduct the vendor cannot control.

"Where the commercial relationship is business-to-business, mandatory arbitration clauses are worth serious consideration. Properly drafted, arbitration provisions can reduce litigation costs, preserve confidentiality, and keep disputes away from juries," Dansdill mentions.

When contracts are not enough

Even a well-drafted contract is not an impenetrable shield. Courts may override limitation clauses, governing law provisions can be challenged, and product liability claims may be brought by end users or third parties, outside the original agreement.

For Nordic software companies entering the U.S. market, a comprehensive insurance assessment is essential. Key considerations include, for example:

- Whether the policy covers claims arising from software embedded in or bundled with a customer's product offering;
- Contractual liability coverage, including whether indemnification obligations are covered when they exceed what the base policy would otherwise cover;
- Accumulation risk across multiple customers, users, deployment environments, or products using common code or shared infrastructure;
- Access to defense counsel with experience in American litigation and settlement dynamics; and
- Policy sublimits, exclusions, and aggregation clauses that could limit coverage in a multi-claimant or multi-jurisdiction scenario.

The central lesson is that U.S. exposure should be addressed before market entry, not after a dispute arises. For insurers, this requires underwriting that looks beyond traditional service-error scenarios and accounts for design-defect theories, downstream use, accumulation risk, and the potential severity of U.S. claims.

Liability insurance is not merely a financial safety net; it is a strategic enabler of growth. Properly structured, it helps companies to absorb severe but low frequency losses and to navigate complex litigation environments. It also supports long term expansion without disproportionate risk concentration. ●



Meet our expert

William McKechnie
Head of Casualty Underwriting

Source

1) *Raine v. OpenAI* Docket No. CGC25628528 (Cal. Super. Ct. Aug 26, 2025)

REFERENCES

- Expanding to the USA from the Nordics: Complete Business Guide
- Unlocking US Growth: EU Software Firms Eyeing Expansion Stateside
- Scaling Beyond Borders: Strategies for Nordic Founders Entering the US Market



GETTY IMAGES

RISK MANAGEMENT

Controlling hot work risks

By **Kristian Orispää**, If

Hot work remains a persistent ignition source. Effective control starts with avoiding hot work altogether where possible and using safer methods instead. When hot work is unavoidable, a robust permit system, adherence to agreed rules and guidelines, and consistent enforcement by everyone involved are vital.

Comparable Europe-wide data on hot work fires is not yet available as reporting is not fully harmonised. England provides an indicative example: official incident data shows 199 hot work-related fires in 2023 to 2024 and 182 in 2024-2025, with 85% linked to welding or cutting. These figures underline why permit discipline, competent supervision and post-work inspections remain essential when hot work is carried out.

Expert insights & observations

Jyrki Eskola, Insurance Investigator in the Investigation unit at If in Finland, has gathered observations across industries on common causes of fire incidents. He notes that accidents often occur near the end of a task, before lunch or late in the workday, when concentration typically starts to slip.

Actual fire investigations show how small oversights can turn a routine welding job into a serious fire.

- Granting a hot work permit as a routine without assessing the risks at the actual location
- The location-specific risk assessment is not communicated to the hot worker
- Penetrations, gaps and openings are not properly covered, despite this being specified in the permit and required as a basic precaution
- Surfaces exposed to upward-travelling sparks are not protected or wetted down
- Structures are not opened before work begins, and hidden combustible materials are not identified in spaces where oxygen and draught can create a flue effect
- Sawdust and sawing waste are not thoroughly removed; sweeping the area alone is insufficient
- Safer alternative methods are not considered
- The effect of weather, especially wind, is not sufficiently addressed or reviewed
- There is insufficient understanding of fire behaviour, the effects of ventilation and the fire properties of different materials
- Extinguishing equipment is not placed close enough to the work area for rapid access in an emergency
- Urgency takes precedence over sound judgement and due consideration

Jonatan Loman, Fire Investigator at If Insurance in Sweden, notes: “Details matter. In one case, the preparations were correct, but the extinguisher and hose were too far from the work area. When a fire started, the workers lost the chance to stop it before it spread.”

Jyrki Eskola notes: “Alternative methods should be considered during the kick-off meeting. The permit issuer and the hot worker must then assess the risks together before work begins.”

Thorough planning before work begins remains the best approach to hot work safety, as every task presents different challenges—from the materials used to the careful assessment of the work area and its surroundings.

“A hot work permit must be more than a signed form,” Jyrki Eskola adds. “It should confirm that the workers can respond to an early-stage fire and that the work area, equipment and possible routes for sparks or heat have been properly checked.”

Drawing on 20 years of experience as a fire investigator, Jyrki Eskola says: “Many roof fires could be prevented by avoiding open flames near walls. Contractors should always consider safer, non-flame options, such as adhesive bonding, as alternative ways to complete the job.”

AI generated hot work accident scenario

Consider a common fictional hot work scenario that demonstrates how poorly controlled work can escalate into a major factory fire. The case presented in the following



Fires are less common in new-build projects. Most roof fires, for example, occur in older buildings, often because the existing structure or materials have not been adequately assessed and important details that could influence fire development have been overlooked.

GETTY IMAGES

> Thorough planning before work begins remains the best approach to hot work safety, as every task presents different challenges.

paragraphs was generated with support from AI and is not based on an actual investigation; any similarities with actual incidents are coincidental.

What began as a routine late-afternoon maintenance job quickly developed into a serious fire. A contractor carrying out cutting and welding inadvertently continued working outside the designated hot work area. The task itself was minor, but it had been assigned to an inexperienced person, and the permit controls and supervision were inadequate.

According to the company's initial account, the area had not been properly assessed, protected or monitored. Sparks entered a concealed space and ignited combustible material, allowing the fire to develop unnoticed until smoke appeared. The facility was evacuated, several workers were treated for minor smoke inhalation, and extensive fire and smoke damage disrupted production for months. Missed deliveries, costly production recovery, facility reconstruction and customers switching to alternative suppliers ultimately turned a minor hot work task into a major business loss extending far beyond the physical damage.

Proper permit discipline

The fictional case highlights familiar hot work failings: the repair was performed outside a permanent hot work area, combustible materials were not fully removed or shielded, hidden spaces were not adequately checked, and supervision was weak. Those gaps allowed sparks and heat to move beyond the immediate task and develop into a fire out of sight.

Beyond the inexperienced contractor, the example draws attention to the person who authorised the hot work permit. A permit should only be issued when the worker understands the risks, is properly trained, and the site has been prepared, protected and monitored. When these conditions are not met, a routine maintenance task can become a major loss event.

Jyrki Eskola notes, "When approving and issuing a hot work permit, the permit issuer must be properly trained to understand the risks associated with the planned task. They are responsible for ensuring that the person carrying out the work is fully aware of the risks, understands the alternative methods available, works only when a fire guard is present, and has the knowledge and skills needed to manage the risks and extinguish an incipient fire."

Swift and decisive action

Andreas Kräling, Head of Property Risk Management in Sweden, stresses: "Staff should be properly trained, being able to respond promptly when a fire incident occurs. Also, before hot work begins the people and equipment that have been specified in the hot work plan to be present must be in place. If they are not, the agreed controls have failed, and work should not be done."

"When a small fire starts, the outcome often depends on immediate human response. Sprinklers also play a vital role; however, they are not always available above a hot work area. A common mistake is, for example, when both the welder and the fire watch leave together for a lunch break, leaving no one to monitor the worksite while they are away. Again, this is a failure in supervision and adhering to guidelines that most companies have in place, but do not enforce."

In practice, at least one person should remain on site to watch for smouldering materials or hot tools that could come into contact with combustibles.

Andreas concludes, "Without continuous monitoring, a hidden fire can develop, not only during a break, but even an hour after the work has been completed. By the time smoke appears and an alarm is raised, the fire may already be spreading rapidly. The rule is simple: maintain a continuous fire watch, check the area also after the work has been completed, to ensure early detection and prevent escalation."

Pre-work inspections, supervision, and thorough risk assessment keep hot work under control. If's Risk Engineers are ready to support your organisation's fire safety planning and management, helping to prevent losses and manage risks with expertise and confidence. ●



Meet our expert

Andreas Kräling
Head of Property Risk Management, Sweden

REFERENCES

- General fire safety and risk engineering guidance on hot work permits, fire watch, combustible control, and post-work monitoring.
- European Fire Safety Alliance (EuroFSA) and related European fire statistics initiatives on the current limitations of harmonised fire data across Europe.
- Office for National Statistics (ONS), UK. Fire and Rescue Incident Statistics for England, including underlying incident data referenced for hot work-related fires.
- CE Safety; https://cesafety.co.uk/news/latest-figures-regions-with-the-most-hot-work-fires-2023-2025/
- Fire Safety Matters; https://www.fsmatters.com/Hot-work-fires-still-posing-major-risk



GETTY IMAGES

RISK MANAGEMENT

Preventing conveyor belt fires

By **Kristian Orispää**, If

Conveyor belts are essential to keeping forest industry operations moving, but they can also create serious fire exposure when combustible material, mechanical faults and limited access come together. Effective prevention depends on early risk identification, proper maintenance, appropriate sprinkler protection and clear emergency planning.



In the forest industry, conveyors transport single items and bulk materials such as wood chips, sawdust and bark across mill sites, over distances ranging from a few metres to even a kilometre or more. Common conveyor types include belt, scraper or chain, pneumatic, tubular and vibrating conveyors. In a belt conveyor, the belt runs around a motor- and gearbox-driven head pulley, with a tail pulley at the receiving end, and is supported and guided by idlers or rollers. The belt is usually layered, with a smooth or patterned surface made from a rubber mix selected for the operating environment to improve grip, traction and transport performance.

Managing exposure and risks

Belt conveyor systems generally have scrapers or brushes to keep the belt clean. However, a typical challenge of a belt conveyor is that material sticks onto the belt's surface and drops off only on the return end of the belt, generating piles of material under the conveyor. The costliest fires in

> Effective prevention depends on early risk identification, proper maintenance, appropriate sprinkler protection and clear emergency planning.

conveyor systems start from electric or bearing failures, or friction caused by the moving belt or transported material. Another source of fire is glowing or burning material loaded onto the conveyor, frictional heat from a bearing failure, or belts jamming or slipping.

Sprinkler protection is an essential control when a conveyor layout could allow fire to spread quickly or make manual firefighting difficult. This is especially relevant where conveyors are fully enclosed or elevated with restricted access, where galleries are built wholly or partly from combustible materials such as wood, where combustible materials are transported, or where a conveyor outage could create significant business interruption exposure.

To minimise fire risks, avoid placing conveyors above stacks, buildings, or essential machinery. Maintain a clear space of ten metres on each side of the belt conveyor, including ground vegetation, goods storage, and vehicle parking. Additional risk mitigation measures include using non-combustible materials in conveyor galleries, considering grated steel walkways and open mesh nets below the conveyor where applicable, selecting fire-retardant belt materials, using only IP-classified devices and device enclosures for all electrical installations with respect to water and dust, and placing warning or clearance signs on elevated galleries where traffic can be expected below.

Sprinkler systems prevent losses

Belt conveyors in the forest industry should by default be protected by automatic sprinkler systems. The exact design of the systems depends on a multitude of factors. If a conveyor is partially or fully enclosed, making it hard to reach from the outside, sprinkler protection covering the entire enclosure is required. Also, tubular belt

Swift action earns safety award

The August Ramsay Foundation awarded Mantsinen Group employee **Niilo Siivonen** a financial stipend for his swift response to a fire incident near a log conveyor.

Presenting the award, **Sirja Pajari**, Head of Property Risk Management, Finland, stressed that people who recognise danger and act decisively play a crucial role in emergency situations.

In April, Siivonen spotted a fire near a log conveyor at a laminated veneer lumber mill and extinguished it with wet wood before it spread. Left unchecked, the fire could have reached nearby facilities and a large construction area potentially causing serious damages and risking lives.

In her speech, Pajari highlighted that safety culture is about people, highlighting that how people respond in a serious situation really makes a difference.

The August Ramsay Foundation

Established in 1929 in honour of Finnish industrial fire insurance pioneer **August Ramsay**, the Foundation promotes loss prevention among If-insured companies and supports risk management research and development.

It awards scholarships, grants and recognition for contributions to safety, loss prevention and insurance, including actions that prevent major property damage or business interruption. ●



conveyors can be equipped with sprinklers for fire protection. Consult your Risk Engineer at If for guidance and support.

At least one row of sprinklers should be installed above the delivery belt. If the conveyor belt is wider than 800 mm, sprinklers under the return belt are also needed. If there are 2–4 conveyors in the same gallery, additional sprinkler rows might be needed also on the lower level and under the return belt.

Maintenance and testing is vital, conduct release tests for challenging conveyor deluge sprinklers during the annual maintenance shutdown period. Always, follow the manufacturer's testing procedures for each fire detection system including the release of a fire extinguishing system.

Emergency planning and response

Develop a firefighting plan for the conveyor system in collaboration with the local fire brigade, including detailed guidance on appropriate tactics. Invite brigade personnel to the site regularly so they remain familiar with the layout, emergency equipment and its use.

Provide the local emergency response team with appropriate training for conveyor incidents. Ensure team members can operate the conveyor safely in an emergency, access all areas of the system and apply suitable firefighting tactics, such as cutting the belt to prevent a fire from spreading and to limit damages.

For new conveyors or when making modifications to old conveyor belts, consult your Risk Engineer at If during the planning phase. ●

Scan the QR code to download our Conveyor belt hazard information sheet for more information.



Meet our expert

Sirja Pajari
Head of Property Risk Management, Finland

Fire and occupational safety are closely linked to keeping the conveyor area clean and free of debris: a well-fitted system that reduces cleaning needs will improve user safety and reduce risks.

GETTY IMAGES

Truck gate procedures in Europe

By **Mike Barry**, If



GETTY IMAGES

As truck and terminal thefts are on the rise across Europe, robust gate controls are becoming increasingly important. This article outlines the essential checks that ports and inland terminals should apply to verify drivers, vehicles and cargo, as well as strengthen security and maintain a clear chain of custody.

Truck gates at European ports and inland terminals serve as critical control points ensuring security, compliance, and cargo integrity from pre-arrival through final exit. These procedures integrate vehicle and driver verification, cargo authority checks, customs compliance, and safe terminal movement to mitigate theft and operational risks.

Across Europe, the truck gate is a critical interface between public roads and the controlled environment of a port or inland terminal. It combines security, safety, customs compliance, cargo integrity, and traffic management. Although local arrangements vary, the common sequence is to pre-advise the movement, verify the driver and vehicle, confirm authority for the cargo, control activity inside the site, and validate the truck again before departure.

For seaports serving international shipping, the International Ship and Port Facility Security (ISPS) Code provides the international security framework. Within the European Union Regulation (EC) No 725/2004 implements the relevant ship and port facility security requirements, while Directive 2005/65/EC complements that framework by addressing security across the wider port area. Practical gate measures are determined on the basis of the applicable port or port-facility security assessment and security plan, together with national legislation and local terminal rules.

An important distinction is that full ISPS requirements normally relate to designated maritime port facilities. Inland terminals may not be ISPS facilities, but commonly apply comparable access, customs, safety and cargo-control measures.

A truck gate is the terminal's physical and digital control point between public roads and secure operations, protecting cargo flow and maintaining a clear chain of custody.



GETTY IMAGES

Before the truck arrives

Gate control normally begins with electronic pre-arrival information. The hauler submits a booking or time slot together with vehicle registration, driver details, cargo or container reference, collection or delivery authority and customs status. Dangerous goods information must be declared where relevant. The terminal can then identify incomplete releases, mismatched references or security holds before the vehicle reaches the barrier.

Pre-advice reduces manual processing and queues while creating an auditable link between the driver, vehicle, transport order, and cargo unit. Where information is missing or inconsistent, the truck is normally held outside the operational area or directed to a service desk until the discrepancy is resolved.

Driver, vehicle and access verification

At the gate, the terminal confirms that the person and vehicle presenting themselves are authorised for the movement. Drivers may need a passport or national identity card, driving license, company credential or port access card. Details are compared with the booking, often with support from automatic number-plate recognition, CCTV, and electronic barriers.

Access is generally limited to the time, purpose, and operational area required. Visitors and contractors may need additional registration, induction, or escort. A valid booking does not provide unrestricted access to quays, cargo areas or other restricted zones, which remain governed by the security plan and current security level.

Vehicle, cargo and customs checks

Vehicle checks are risk-based. Routine controls may include a visual condition check, confirmation of trailer or container identity, seal verification and observation for signs of tampering, concealment or unauthorised passengers. Random or targeted inspections can extend to the cab, load space, undercarriage, or security devices. For dangerous goods, the declaration, placards, and required vehicle equipment may also be checked under the applicable ADR (Agreement concerning the International Carriage of Dangerous Goods by Road) framework.

Cargo authority is normally verified electronically against the booking, unit number, shipping-line release, customs status and any operational hold. Entry may be refused when customs formalities are incomplete; the cargo has not been released, unit or seal details do not match, or the vehicle is unsuitable. These controls reduce misdelivery, theft and unauthorised removal.

Safe movement inside the terminal

After admission, the truck enters a high-risk workplace shared with cranes, reach stackers, forklifts, rail movements and pedestrians. Terminals therefore enforce local routes, parking areas, and speed limits. High-visibility clothing and safety footwear are common requirements, with helmets, eye protection or other PPE (Personal Protective Equipment) added according to the site and task.

The driver receives a lane, stack, bay, or loading position. During handling, the driver may have to remain in the cab, use a designated safe zone, or follow instructions from terminal personnel. Before moving away, the correct cargo should be confirmed and doors, twist locks, securing devices or seals properly applied as relevant.

Exit control and inland terminals

The outbound gate must confirm that the correct unit is leaving on the authorised vehicle, and that customs or terminal holds are cleared. Seal information, documentation, and vehicle identity may be checked again. Random outbound inspection provides protection against substitution, theft, stowaways and documentation errors.

Inland rail terminals, dry ports and container depots often follow the same sequence even when outside an ISPS-designated maritime facility. Their controls focus on booking, identity and vehicle verification, customs status, safe movement, cargo interchange records, and final exit validation. Controls should be proportionate to cargo value, threat profile, and operational complexity.

Focusing the perspective on risks

Stronger facilities combine secure perimeters and controlled gates with reliable driver authentication, electronic pre-advice, integrated customs checks, CCTV, seal procedures and disciplined traffic management. Weaknesses commonly arise when manual exceptions are poorly controlled, identities are not matched to transport orders, seal discrepancies are not escalated, CCTV leaves gaps or trucks can move without clear routing.

Looking ahead, the strongest truck gates will combine smarter digital verification with disciplined human oversight. Technology can identify discrepancies faster, but security ultimately depends on acting upon any possible issue that may emerge, before a vehicle or cargo unit is allowed to proceed. ●



Meet our expert

Mike Barry
Cargo Risk Specialist, Sweden



CLAIMS

Understanding recourse in insurance claims

By **Kristian Orispää**, If

When an insurance claim is filed, the financial outcome often remains uncertain until the possibility of recovering compensation from a responsible third party has been fully evaluated. This action, known as the recourse process, is essential for both insurer and customer, as it can significantly influence the total cost of the claim. An insurer plays a crucial role here, ensuring that the customer receives not only compensation but also strategic support in maximising recovery.

While the concept of recourse exists in many legal domains, this article focuses exclusively on recourse in the context of insurance.

Having the right insurance, with the correct values, is always the fastest and most secure route to compensation after an incident. However, accidents can involve the need to pursue a responsible third party directly, provided that a liable party can be clearly identified. This pursuit requires legal expertise, incurs costs, and carries the risk of the claimant losing both damages and legal expenses if unsuccessful.

In general, the insurer's obligations are defined by the insurance agreement and its limits, deductibles, and exclusions. In situations of underinsurance or uncovered costs, a strong insurer-customer partnership becomes critical. An insurer works proactively to help customers pursue recovery beyond the policy payout, ensuring that the party responsible contributes to the financial remediation.

> Successful recovery ensures compensation for uncovered losses and repayment to insurers. This can positively impact the customer's claims history and future premiums.

Engage your insurer early

After a claim is filed, the insurer assigns a claims adjuster to assess recourse opportunities. For high-value or complex claims, a team may be formed to evaluate the case collectively.

An insurer further strengthens this process by, for example involving senior adjusters and legal experts early to secure the customer's position. Insurer's may also be better positioned to launch investigations.

Early and comprehensive preparation significantly increases the chances of a successful recourse. The ideal scenario is one where the insured identifies the responsible party and provides clear documentation in the incident report. Larger companies often have dedicated teams for insurer contact, but even then, the depth and quality of insurer support can be decisive.

According to **Kari Ketven**, Head of Recourse Claims at If, "Timeliness and evidence collection are key. When the insurer is involved early on, we can help ensure that customers receive strategic guidance and consistent communication at every stage, which helps customers avoid potential pitfalls."

Similarly, accurate and timely evidence collection is essential. This includes photographs, damage reports, witness statements, technical data, and more. To avoid cases where unnecessary delays complicate securing evidence, the swift deployment of adjusters and If's technical experts can provide clear benefits, for example, regarding guidance on what evidence to secure immediately.

Why collaboration matters

Typically, the insurer claims the amount it has compensated, while the customer claims uncovered costs. Both parties may jointly pursue the responsible party. The insurer manages legal reasoning; the customer justifies their own uncovered losses.

Kari Ketven highlights, "Success is based on simple but vital details, for example, proactive communication and transparency on responsibilities, processes, and expectations. Early collaboration ensures a shared understanding of scope, timelines, and information needs."

What can go wrong

Disputes are common and often require skilled legal support. An insurer can provide guidance and support to their clients via their in-house legal teams who have deep legal experience across various industrial losses.

If the responsible party ignores or rejects the claim, litigation or arbitration may be required. Customers must weigh risks and costs with their legal counsel.

Complex legal environments, contract structures that waive damage claims, and shifting insurance responsibilities, pose challenges. It is important to identify hidden risks and clarify implications before problems arise.

Rauna Irjala, Manager, Large & International Claims at If notes, "The landscape is changing. Today's world is very different, and we see the impacts of geopolitical tensions, increased protectionism, and large-scale global supply chain disruption. In the past, we at If Insurance, have always recommended that our clients can rely on established industry agreements when forming business relationships. We continue to highlight the importance of customers to meet all contractual insurance obligations and ensure they address every significant risk."

Rauna continues, "There is no simple answer to the volatility facing markets today, change is now a constant possibility, and we must adapt to the current conditions. Having a strong partner is now more important than ever before."

In turbulent times, clients benefit from partnering with insurers who maintain high standards of transparency, ensuring customers understand the long-term financial value of recourse success. Collaborating with customers, insurers can help ensure consistent and fair recourse handling, both internally and externally. It is also important to promote sector-based accountability, which encourages prevention and reduces long-term insurance costs for all. ●



Meet our experts

Kari Ketven
Head of Recourse Claims, Finland



Rauna Irjala
Manager, Large & International Claims, Finland



GETTY IMAGES

IN THE NEXT ISSUE

Fatigue poses real business risks

What to do when a major claim occurs?

Hidden steam turbine risks

Subscribe to Risk Consulting magazine and the monthly If Insights newsletter at www.if-insurance.com

Risk Consulting is If's specialist magazine focusing on risk management and loss prevention, and is among the first client publications of its kind in the Nordic countries.