

# Risk Consulting

01 • 2025

Insights into risk management and loss prevention

4 Space is the  
new black

20 Wood construction  
makes a comeback

28 Vulnerabilities within  
cyber-physical  
ecosystems



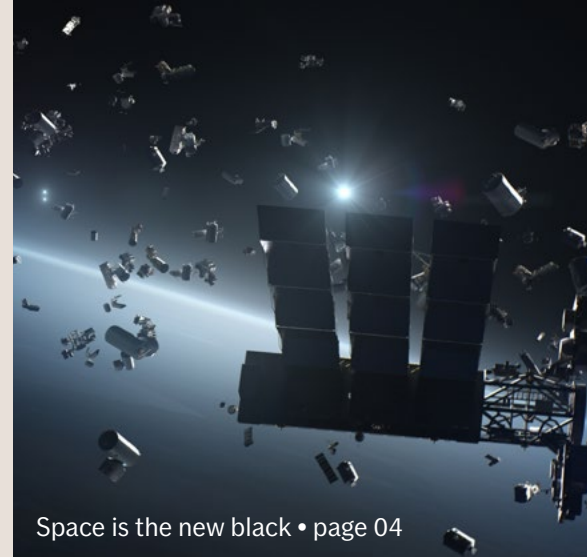
# Contents

- 4 Space is the new black  
Emerging risks from the increasing use of space
- 10 Social inflation inflammation
- 14 Behind the scenes of a mock jury
- 16 The right values protect businesses
- 18 Transformer shortage  
– a threat to business continuity
- 20 Wood construction makes a comeback
- 26 The challenges of cyber-attacks,  
ransomware, and extortion payments
- 28 Vulnerabilities within cyber-physical ecosystems
- 32 Travel insights from claims experts
- 36 Understanding risk perception in  
multicultural workplaces
- 38 If's Nordic Business Travel Report now available
- 39 Short news

**Publisher** If, Keilasatama 2,  
02150 ESPOO, Finland  
+358 10 19 15 15, [www.if-insurance.com](http://www.if-insurance.com)  
**Editor-in-Chief** Kristian Orispää  
**Editor** Carita Hämäläinen-Tallgren  
**Editor** Caroline Bødkerholm Ramsby  
**Art Director** Petri Bergman

**Production** Miltton Oy  
**Printing** Newprint  
**Change of address**  
[industrial.client-service@if.fi](mailto: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.



Space is the new black • page 04



Wood construction makes a comeback • page 20



Vulnerabilities within cyber-physical ecosystems • page 28

## 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



# A year of growth, collaboration, and green innovation

There are many exciting events on the horizon in 2025. The most exciting event of the year, in my opinion, is our integration with Topdanmark. Not only do we get to welcome over 2,000 new, skilled colleagues, but we also gain a stronger market position in Denmark – a milestone we have been looking forward to. This integration will open a wealth of opportunities for growth, collaboration, and innovation.

I am also happy to share that we now have announced the establishment of our Green Energy and Construction Underwriting unit, an evolution from our current CAR/EAR and Energy Competence Centres.

The transition to and development of green energy resources continues at an ever-increasing pace. Industries and societies alike will undoubtedly continue to shift towards cleaner and greener, renewable energy sources, and we believe the focus on sustainable energy projects and solutions will continue to grow.

Putting even more muscle around our project expertise and green energy has been a long-term ambition for If, and we stay committed to support our clients in a safe transition towards green energy.

In this issue of Risk Consulting Magazine, we will dive into cybersecurity, the transformer shortage challenge, and many other topics, including for example US liability. We have also included an article about wood construction and the risks associated with this material.

We are always curious to hear your thoughts and feedback on the articles in Risk Consulting Magazine.

Reach out to your contact person at If to share your comments and suggestions. ●

Poul Steffensen  
Head of Business Area Industrial



**EMERGING RISKS**

# Space is the new black

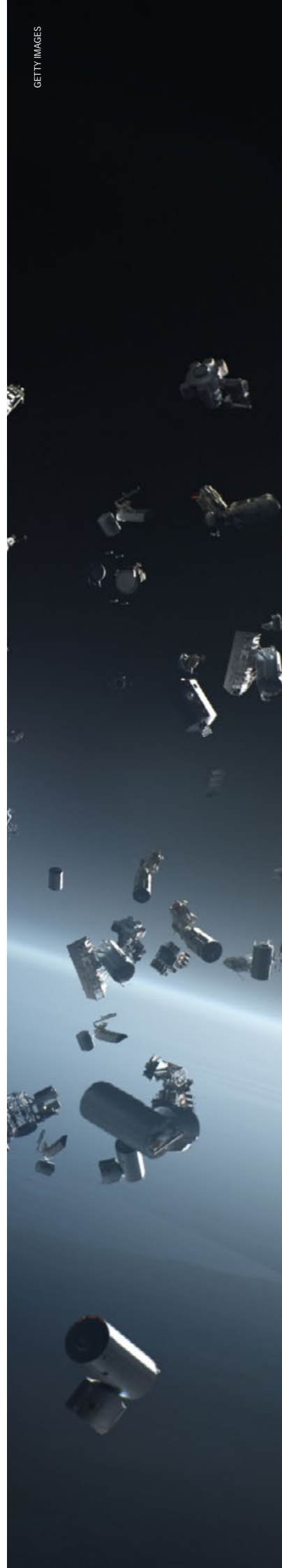
## Emerging risks from the increasing use of space



By **Minna Palmroth**,  
University of Helsinki, Finland  
Finnish Meteorological Institute, Helsinki, Finland

Space is a megatrend. Right now, we are witnessing more satellite launches than ever before. Space is becoming a mundane part of our everyday life, and in fact, many companies may even forget that they are using space-borne technologies in their processes. As society's dependence on space increases, vulnerabilities also become evident. This article highlights the emerging risks that have recently materialised or may soon become a problem with the booming space economy.

**T**he near-Earth space in the close vicinity of our planet is becoming crowded as satellites are launched into orbit. During the Cold War, approximately 150 satellites were launched annually, primarily for defence-related applications. Since around 2015, annual launches have outnumbered those during the Cold War, and from 2020 there has been a rapid increase in the number of launches.



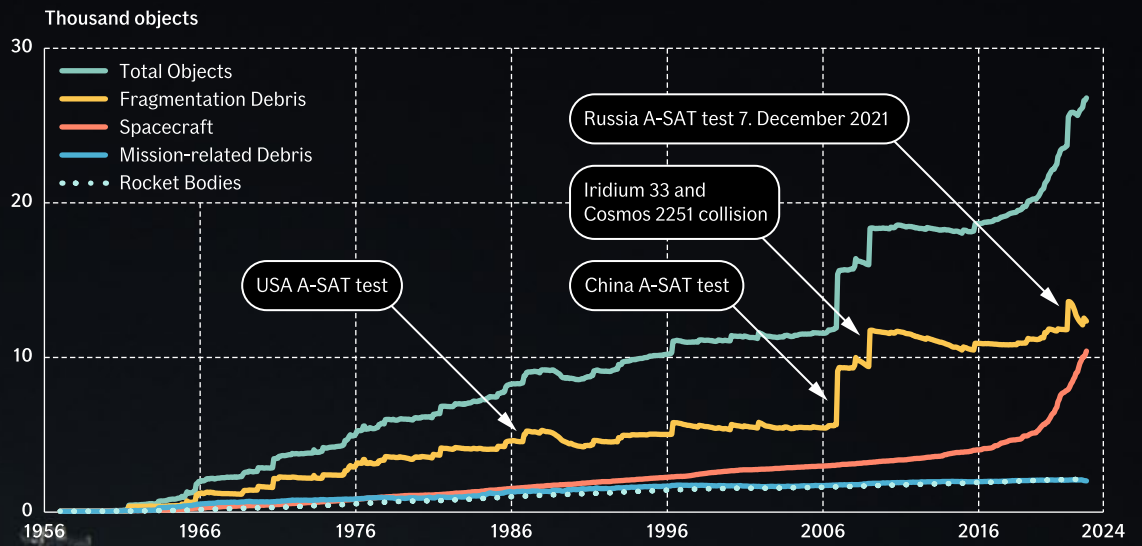


Figure 1: Total number of space debris over time (source: [orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/ODQNV27i1.pdf](https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/ODQNV27i1.pdf)). Some anti-satellite tests, in which a country has destroyed their own satellite with a missile, have been marked alongside accidental satellite collisions. These events have had short- and long-term consequences on the total number of space debris. Only objects that can be monitored from Earth are depicted.



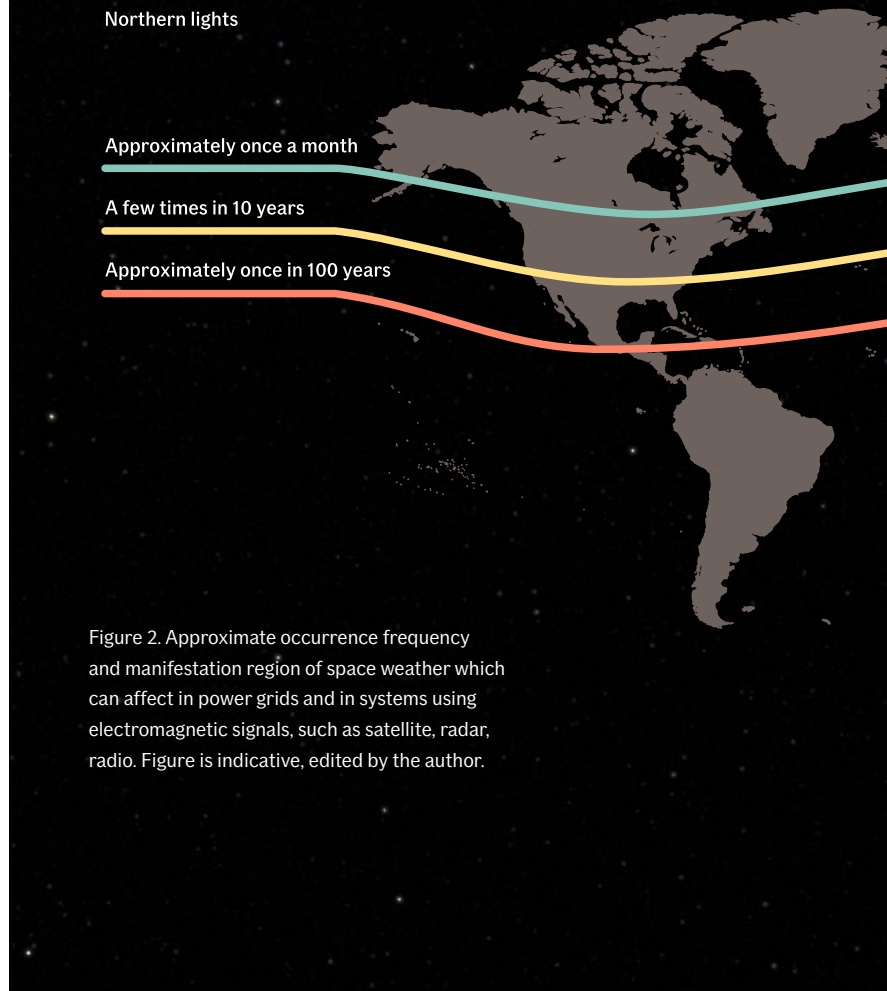


Figure 2. Approximate occurrence frequency and manifestation region of space weather which can affect in power grids and in systems using electromagnetic signals, such as satellite, radar, radio. Figure is indicative, edited by the author.

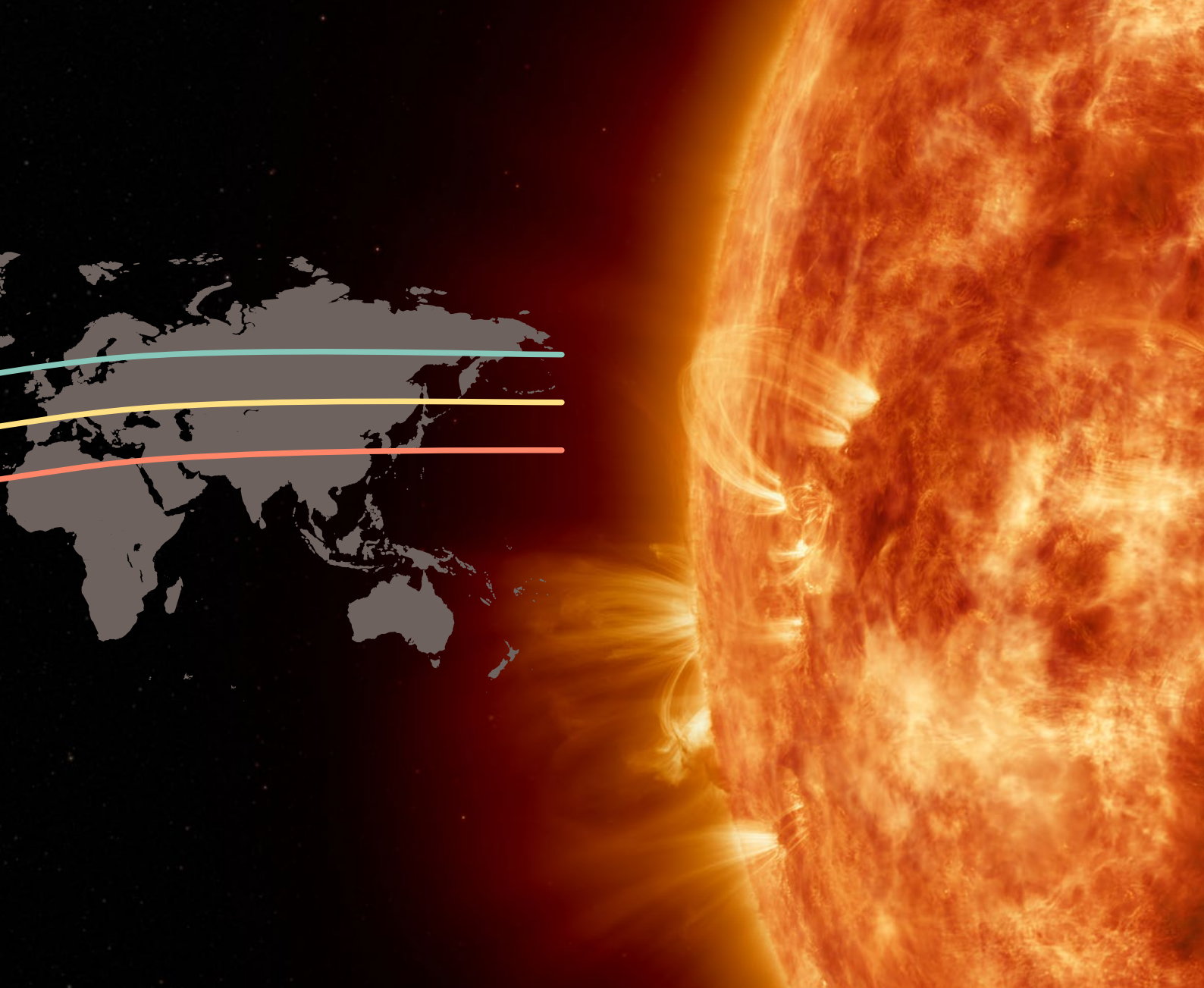
The motivation for sending satellites has shifted to serve commercial purposes, as companies now seek to profit from space. Investment banks have estimated that the total value of the space economy could grow to 1.8 trillion dollars by 2035<sup>1</sup>, as the industry continues to launch new satellites<sup>2</sup>.

The change that has enabled the rapid growth of commercial space economy is the access to space, which was previously controlled by large countries or big organisations like the European Space Agency (ESA). The opening of the launch market changed the situation, and now many launches are arranged by brokers who seek a slot on a rocket for a fee. Another big change is the use of more cost-efficient off-the-shelf technology, which is making space more affordable for small and medium-sized companies<sup>3</sup>. Space offers various business opportunities that are either more affordable compared to the earlier paradigm, or it enables new ways of doing business. Space is a global and scalable platform for customers from various backgrounds. Satellites are used in numerous services, including broadcasting, communications, positioning, navigation, timing, weather and climate monitoring, Earth observation, and defence.

### Space environment from the satellite perspective

Satellites do not fly in a vacuum, as the vicinity of the Earth is filled with the fourth state of matter, *plasma*, which consists of charged particles that are controlled by electromagnetic fields and other collective forces. Another aspect that satellite operators need to consider is space debris and other missions. This chapter concerns the space environment from the satellite's perspective.

**Debris:** Figure 1 on previous page shows the total observed amount of debris in orbit around the Earth. The total mass is over 8,000 tons; however, only objects larger than 10 cm in size can be tracked from the ground, while it is estimated that the total number of objects larger than 1 cm is over one million<sup>4</sup>. Debris exists in those orbits which are most commonly used: Geostationary orbit (GEO, hosting e.g., weather satellites), Medium Earth Orbit (MEO, hosting e.g., navigation satellites), and on Low Earth Orbit (LEO, hosting e.g., Earth observation satellites). The largest number of debris lies on LEO polar orbits, which circulate the Earth via the northern and southern hemispheres (Muelhaupt et al., 2019). One of the most hazardous orbits is between 700–1,000 km altitude on LEO. Due to the high concentration of debris there, many future satellite launches are planned either above or below these altitudes, requiring either more sophisticated instruments, or more fuel, respectively, for commercial



activities, and hence causing more costs for companies.

Both large and small debris objects are equally problematic for satellites. One of the most concerning big objects is the bus sized ESA Envisat<sup>5</sup>, an uncontrollable 'zombie satellite' flying at approximately 750 km LEO orbit. Obviously, if Envisat collides with another satellite, the resulting debris would make the orbit so crowded that it could no longer be used for future satellites. However, small objects are also continuously harmful to satellites: they can, for example, create impact craters on solar cells and jam instruments<sup>6</sup>. The main threat from debris is the so-called Kessler syndrome (Kessler and Cour-Palais, 1978), meaning an incident where debris particles start to collide at a larger frequency, generating more particles while the total mass would stay unchanged. This could lead to an exponential increase in particles, forming a debris cloud around the Earth and making space

unusable for satellites. The scientific community does not agree on the possible infliction point for Kessler syndrome; however, Envisat's collision has been named as one potential trigger.

Often in relation to debris, international agreements or binding legislation are called for to regulate the use of space (e.g., Palmroth et al., 2021a). Internationally, only non-binding agreements exist. To launch a satellite, one must obtain a licence from the country where the satellite is registered, and these licences are granted under binding regulation that stipulates, for example, the risks posed to other satellites. Lately, the European Union, for example, has launched a 'space traffic management' programme<sup>7</sup>. However, agreeing on the approach takes time, meanwhile companies continue to launch satellites. One option that companies are now looking at is the very low Earth orbit (VLEO), where atmospheric density is already high enough that satellite orbits decay naturally if fuel-based orbit maintenance is

## Large and small debris objects are equally problematic for satellites.

stopped. Launching to these orbits would keep the operating environment debris-free naturally. On the other hand, these altitudes are often called the 'ignosphere' (Palmroth et al., 2021b), because it is hard to observe and predict. In the future, we may have tens of thousands of satellites in a region that the scientific community does not fully understand.

**Space weather:** Another environmental aspect that satellite operators must consider is space weather, i.e., the conditions in space which affect technological reliability or human health (e.g., Moldwin, 2022). The Earth's magnetic field interacts with the stream of particles coming from the Sun. Sometimes the Sun ejects large clouds of plasma, causing strong space weather variations on Earth, while the Earth's magnetic field variability also contributes to space weather effects. Broadly speaking, space weather manifests in a region where the aurora can be seen, i.e., in the two zones circling both hemispheres. The size of these auroral zones is directly proportional to the size of the space weather event. There are many small solar eruptions each year, a few medium-size events every decade, and one extreme event per century (see Figure 2). The main impacts of space weather concern the electric power grid, satellites, and all electromagnetic signals.

The worst-case scenario in space weather is an extreme event, such as the Carrington Event that was observed in 1859. During this event, a magnetometer in Mumbai, India, observed ground magnetic variations similar to those that tripped the power network in Malmö, Sweden, in 2003 (Nevanlinna, 2008). Some reconstruction efforts have been made to understand what impacts such event would have on modern technology. While studies are ongoing, there are indications that power grids could be damaged (Ebihara et al., 2021). Satellite impacts could be extensive (Odenwald et al., 2006), including lost spacecraft and/or lost signals. Aviation could face global re-routings or cancellations due to high radiation exposure at flight altitudes (Xue et al., 2023). In summary, the effects of a once-per-century extreme space weather could be very serious, given how dependent modern society is on satellite signals and electricity. The scientific community does not fully understand these extreme events because they have not been observed using modern instruments and because space weather models have been built to reproduce much milder conditions.

The occurrence frequency of extreme events is roughly once per century (Chapman et al., 2020), and there is a scientific consensus that we are already on borrowed time. The event that gathered significant media attention in May 2024 was medium-sized and could have been about 4–5 times smaller than the Carrington Event. Even though the impact scenario might sound like the end of the world, many measures can be taken to prepare for extreme space weather. The first step is to understand whether a specific service or system depend on space weather and whether its effects can be mitigated. For example, mobile networks that are only using satellite-based time synchronisation could face problems during an extreme event, while networks that are also using a ground-based atomic clock are more reliable. The most important point is to trust the preparedness professionals and add redundancy and built-in slack for critical systems (e.g., Roe and Schulman, 2008). The scientific community also welcomes questions and discussions, as this helps them understand new systems that depend on space weather.

### Summary

In summary, the electrification and digitisation of societies are required for sustainability efforts. At the same time, many societal functions are increasingly reliant on launching satellites, which, in turn, are growing exponentially. These two trends make society increasingly vulnerable to space weather and space debris. It is recommended to assess whether individual services are dependent on space weather, and if so, to develop mitigation plans with space weather experts and preparedness professionals. ●





## Sources

1. <https://www.weforum.org/agenda/2024/04/space-economy-technology-invest-rocket-opportunity/>
2. <https://spacenews.com/op-ed-herding-rockets-improved-space-traffic-management-will-accelerate-industry-growth/>
3. [https://www.oecd-ilibrary.org/science-and-technology/the-space-economy-in-figures\\_c5996201-en](https://www.oecd-ilibrary.org/science-and-technology/the-space-economy-in-figures_c5996201-en)
4. [https://www.esa.int/Space\\_Safety/ESA\\_s\\_Space\\_Environment\\_Report\\_2023](https://www.esa.int/Space_Safety/ESA_s_Space_Environment_Report_2023)
5. <https://earth.esa.int/eogateway/missions/envisat>
6. [https://www.esa.int/About\\_Us/ESOC/Space\\_debris\\_assessing\\_the\\_risk](https://www.esa.int/About_Us/ESOC/Space_debris_assessing_the_risk)
7. [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0355\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0355_EN.pdf)

## REFERENCES

- Chapman et al. 2020 <https://doi.org/10.1029/2019GL086524>
- Ebihara et al. 2021 <https://doi.org/10.1186/s40623-021-01493-2>
- Kessler, D. and Cour-Palais, B., 1978 <https://doi.org/10.1029/JA083iA06p02637>
- Muelhaupt et al. 2019 <https://www.sciencedirect.com/science/article/pii/S246889671930045X>
- Moldwin, 2022 <https://www.cambridge.org/highereducation/books/an-introduction-to-space-weather/CC822E727D563A79CF959F49E85214C2#contents>
- Nevanlinna, 2008 <https://doi.org/10.1016/j.asr.2008.01.002>
- Odenwald et al. 2006 <https://doi.org/10.1016/j.asr.2005.10.046>
- Palmroth et al. 2021a <https://www.sciencedirect.com/science/article/pii/S0265964621000205>
- Palmroth et al 2021b <https://doi.org/10.5194/angeo-39-189-2021>
- Roe and Schulman 2008 High Reliability Management: Operating on the Edge. Stanford University Press, Stanford
- Xue et al. 2023 <https://doi.org/10.1029/2022SW003381>

LIABILITY

# Social inflation inflammation



By **Lindsay Dansdill**  
Partner, Mercer Oak, Chicago, IL, USA

In this article, we provide insights into the US legal environment. The rise in social inflation is linked to the public's sentiments regarding the corporate world's responsibilities towards employees, customers, and the general public, increasing jury verdicts against corporations for alleged wrongdoing. These high damage awards are blamed for a growing number of claims, and settlement values, causing unrest amongst insurers.

While social inflation is a term that has been floating around for decades, it has become one of the more highly discussed topics throughout the insurance and legal worlds. Social inflation is rooted in a fundamental philosophy, the “us vs them” struggle, between capital rich corporations and the hard working yet financially insecure, and vulnerable individual. This mentality may provide prospective jurors with a desire to even the score card and punish corporations with nuclear verdicts, typically described as verdicts over \$10M or more, even when the dollar amount exceeds the damage caused to an individual. Often, nuclear verdicts are depicted in the U.S. media as celebratory wins, where “evil corporations” are punished, and justice is served. This sentiment is especially true with younger and more diverse jurors who are consistently wary of corporate intent and perceived greed.

While precise data concerning nuclear verdicts is often varied, studies consistently demonstrate an upward tick in nuclear verdicts, with an increase of over 27% in 2023.<sup>1</sup> Perhaps more startling is the that the number of verdicts over \$100M in 2023 was up nearly 400% from 2013.<sup>2</sup> Not surprisingly, California, Florida, New York and Texas were the states topping the chart with the most nuclear verdicts from 2013–2022, with California and Florida reaching nearly 200 verdicts.<sup>3</sup>

### Third-Party Funding

Third party litigation financiers (TPLFs) remain controversial amongst insurers as they are viewed as enablers of social inflation. TPLFs pay legal costs such as attorney fees and court expenses and the plaintiff only pays back the funder if they win the case, typically in the form of a percentage of the settlement or judgment. Critics believe litigation financing provides attorneys with the valor to file prohibitively expensive, frivolous lawsuit with the goal of reaching large settlements or obtaining nuclear verdicts against deep pocketed corporations.

Alternatively, some studies have determined that TPLFs merely provide access to justice for those who cannot otherwise afford it. These studies indicate that TPLFs do not have an impact on the number of cases filed or the dollar amount awarded to a plaintiff through settlement or a jury verdict.<sup>4</sup> It is therefore arguable that, litigation financing merely provides a vehicle to finance larger, high stakes cases that demonstrate a probability of success of the merits. Proponents of TPLFs assert that litigation financing weeds out frivolous cases that would not be fruitful to pursue and may reduce bullying and delay tactics utilized by disingenuous defense firms.

### Increased Verdicts and Attorney Trial Tactics

Certain trial tactics used by plaintiff's attorneys have been attributed to the increase in large jury verdicts that contribute to social inflation. In particular, the tactic known as "Reptile Theory" has come under significant scrutiny by the insurance industry. The "Reptile Theory" is most often used in cases involving automobile accidents, premise, and construction liability, typically painting the defendant corporation or insurer as an unscrupulous and dangerous bully. Demonizing the corporate defendant triggers a jurors' 'survival instincts,' leading them to consider the corporate defendant as a threat to public health and safety, requiring punishment in the form of large jury verdicts. The tactic is utilized to convince a jury that the power is in its hands to award damages to punish corporate bad actors and further deter future bad behavior.



## International corporate defendants may be an easy target for Reptile Theory tactics.

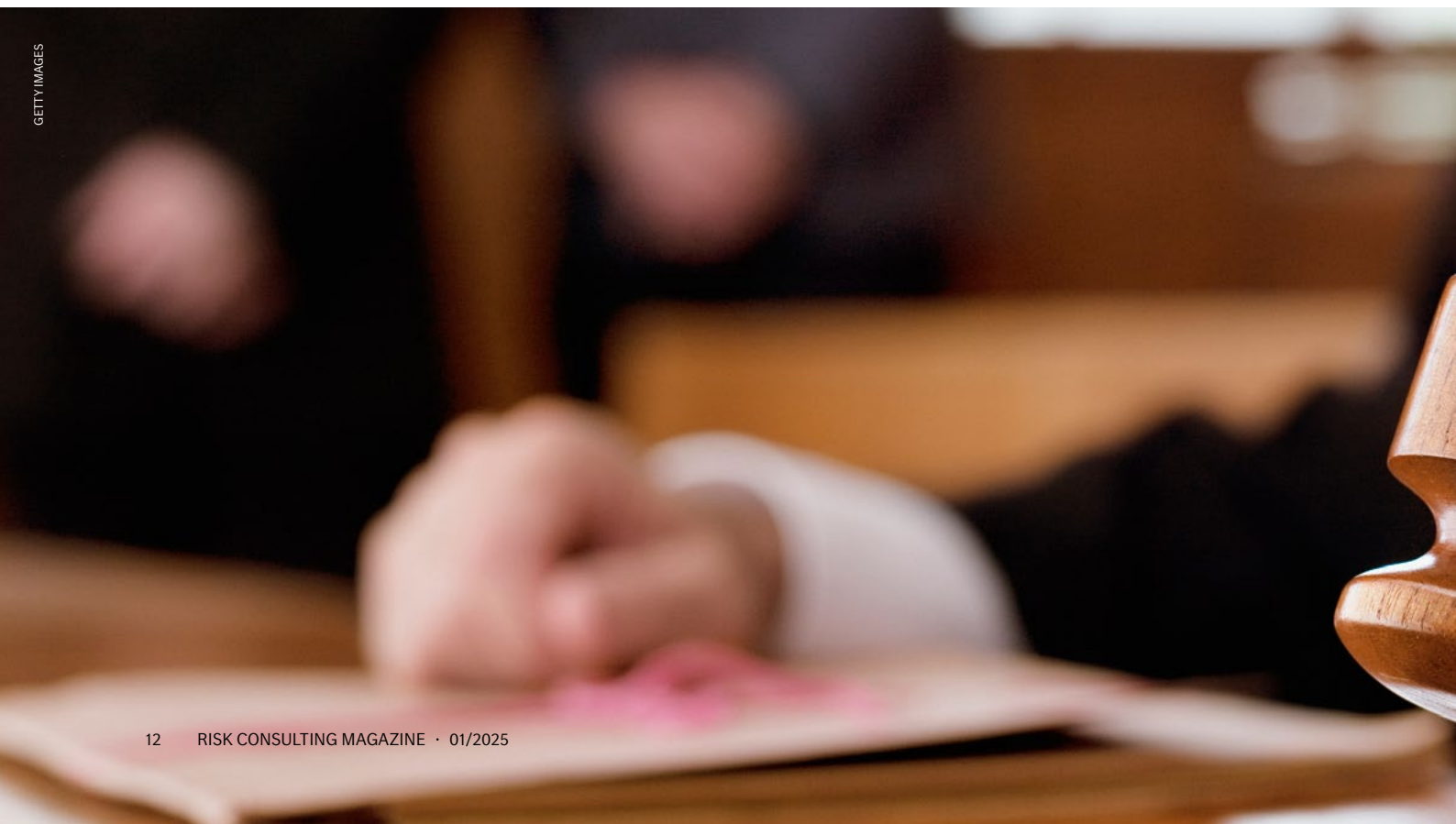
Jury anchoring occurs when the plaintiff's attorney suggests a large and often exaggerated damage award early in the case, relying on jurors to use this number as an 'anchor' or a reference point in determining the actual damages awarded. This tactic can be effective as most jurors have never been placed in a position to award damages to an individual and will rely on the "expertise" of a seasoned attorney to guide them. Even if the number appears egregious to the rather naïve juror, they will usually consider it throughout a trial as the reference point on which to move up or down.

### Defending International Corporations Against Trial Tactics

International corporate defendants may be an easy target for Reptile Theory tactics. It is practically inevitable that a zealous plaintiff's attorney will attempt to villainize the foreign defendant as a greedy corporation who looks to capitalize on the U.S. market while undermining the safety of its residents. This tactic may more significantly impact jurors who have become jaded by the idea of imports due to recent tariff discussions and executive orders issued by the Trump administration.

However, an experienced defense attorney will recognize reptilian tactics during the preliminary pleading stage, providing the opportunity to work with the client to prepare an effective defense. Specifically, pleadings referencing violations of safety rules or allegations that the corporate defendant has endangered the public or community through its actions, should raise a red flag that the corporate defendant will be villainized as a habitual bad actor. Further, allegations of negligent hiring, training or supervision indicate the plaintiff's attorney will attempt to introduce prior incidents or accidents that may not be relevant to the lawsuit. In order to avoid poisoning the jury pool into thinking the defendant consistently places the public in danger by ignoring or violating safety rules, it is important for defense counsel to limit the evidence to only the accident or incident at issue.

The Reptile Theory can also be challenged through testimony by past or current customers' positive experience with the defendant as well as expert testimony stating that the practices and procedures implemented by the defendant provide a safe environment or product for the public. It is therefore important to advise insureds to prepare and regularly update documents

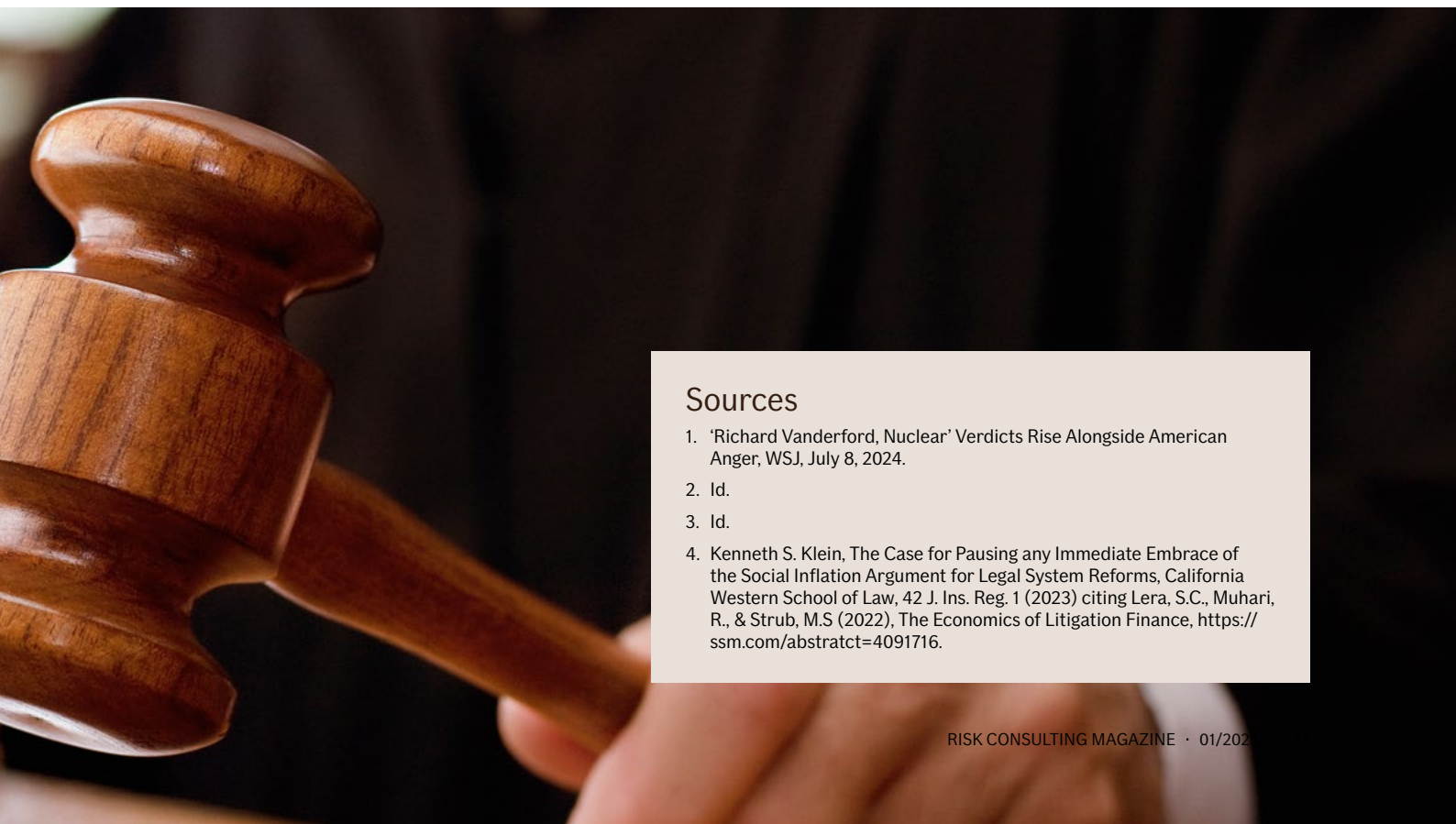


setting forth their practices, safety measures, quality control, and employee guidelines to demonstrate their prioritization of safety and/or quality through diligent implementation and record keeping of proper procedures. However, defense attorneys should ensure the jury does not believe that a company's violation of stringent internal policies and procedures automatically implies that it breached its legal obligations.

Jurors inexperienced in the law and/or insurance claim handling are typically more susceptible to anchoring techniques as they are uninformed about the realistic settlement value of a case. The high verdicts often publicized in the news media also normalize these types of verdicts in the mind of the average juror. In order to combat anchoring tactics, defense counsel should acknowledge plaintiff's egregious demand during opening and closing arguments, informing jurors that plaintiff is utilizing a psychological technique to detract plaintiff from the evidence that will be presented. The defense may also use realistic examples of how anchoring affects sentiment in everyday negotiations such as setting the price of goods or salary discussions.

## 2025 Predictions

While the Trump administration has promised to serve as a zealous business advocate, it remains to be seen whether this will impact social inflation and associated nuclear verdicts. However, it should be noted that most nuclear verdicts arise from state court cases while policies and orders arising out of the Trump administration will have a greater impact at the federal level. It is clear that the plaintiff's bar has worked hard and effectively to incite feelings of anger amongst jurors who ultimately believe a nuclear verdict will deter future corporate bad acts. Unfortunately, it does not appear this tactic will become any less effective during 2025. Therefore, defense attorneys should work closely with insurance carriers and their insureds to implement stringent internal policies and procedures to avoid litigation, or aggressively defend reptilian trial strategies in order to humanize the alleged corporate wrongdoer in the mind of a jury. ●



## Sources

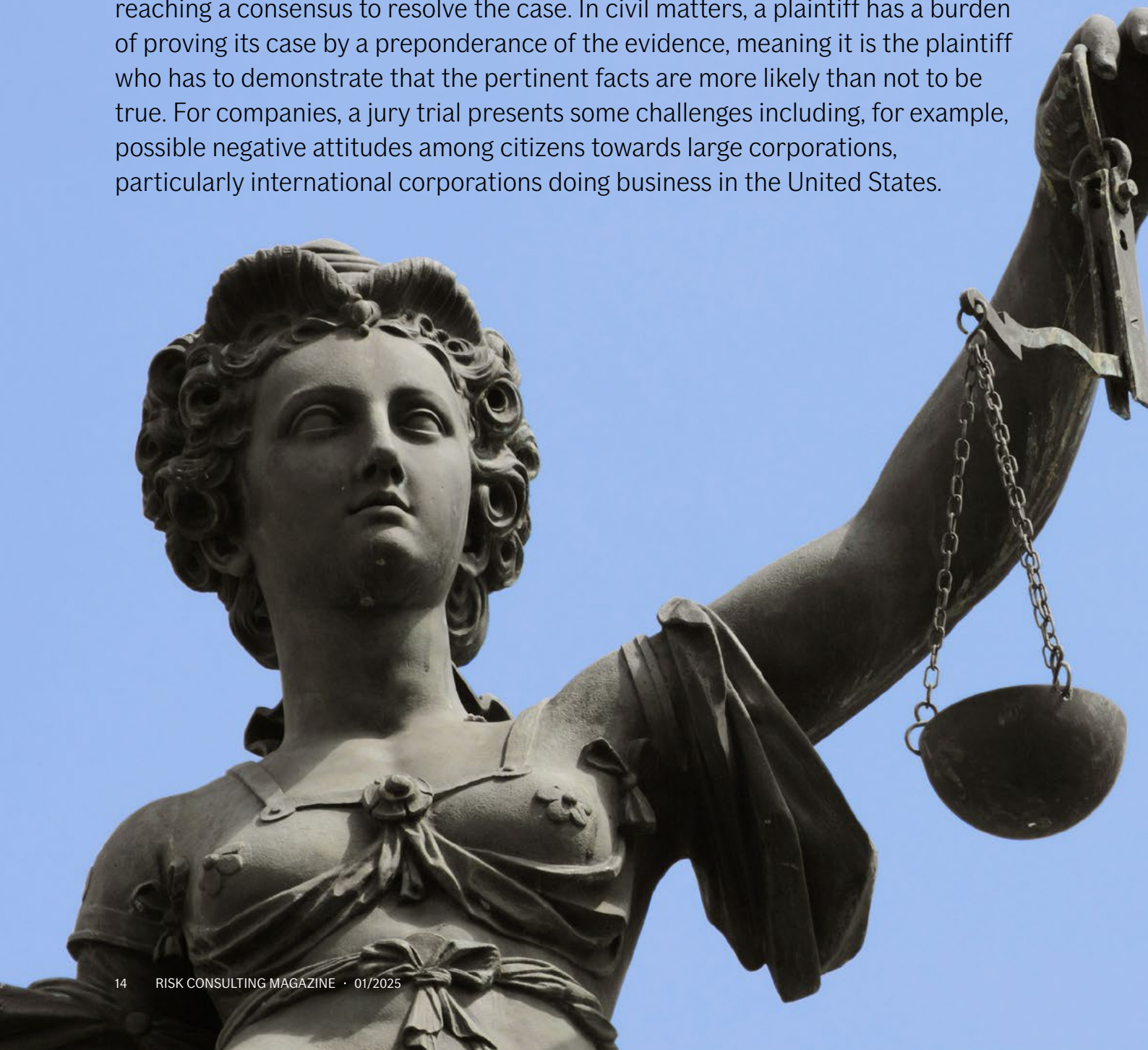
1. 'Richard Vanderford, Nuclear' Verdicts Rise Alongside American Anger, WSJ, July 8, 2024.
2. Id.
3. Id.
4. Kenneth S. Klein, The Case for Pausing any Immediate Embrace of the Social Inflation Argument for Legal System Reforms, California Western School of Law, 42 J. Ins. Reg. 1 (2023) citing Lera, S.C., Muhari, R., & Strub, M.S (2022), The Economics of Litigation Finance, <https://ssrn.com/abstract=4091716>.

## LIABILITY

# Behind the scenes of a mock jury

By Oona Seppä

In the United States, when a company is preparing for jury trial involving a case of significant value, it is common to retain a mock jury to simulate the role of a jury in the courtroom. In a jury trial, lawyers present both sides of the court case to the judge and jury. Jury members weigh the presented facts and are then tasked with reaching a consensus to resolve the case. In civil matters, a plaintiff has a burden of proving its case by a preponderance of the evidence, meaning it is the plaintiff who has to demonstrate that the pertinent facts are more likely than not to be true. For companies, a jury trial presents some challenges including, for example, possible negative attitudes among citizens towards large corporations, particularly international corporations doing business in the United States.



## Mock trials bring multiple benefits

A mock jury is a group of people hired to evaluate the potential situation and reactions to evidence and arguments presented by lawyers. The idea of mock juries is to allow lawyers to identify and predict both challenges and weaknesses that may rise during trial simulation. Generally, a mock jury consists of eight to twelve members that mirror the arrangement of a real jury. Mock jurors have common requirements, similar to a real jury in an actual trial, such as minimum age for participation, US citizenship, English language fluency, a clean criminal record, and mental health requirements.

The main benefits of arranging a mock jury trial are considered to be evidence clarification, witness evaluation, argument testing, strategy refinement, new evidence discovery, cost efficiency for trial preparation, realistic trial simulation, and the possibility to test a diverse juror pool.

The mock jury trial provides the party of a lawsuit with the chance to simulate a real trial situation from opening and closing arguments, presentation of evidence, and overall strategy. Secondly, organising a mock jury trial is beneficial to allow attorneys and the client to gain understanding from juror perceptions, predicting juror reactions and possible verdicts, as well as refining witness testimonies, and uncovering jury selection related issues and details. Mock trials also reduce unexpected developments by familiarising attorneys with a variety of potential juror reactions and questions. This preparation fosters more confident and effective courtroom performances. Overall, mock juries are an invaluable resource for trial preparation, offering attorneys crucial feedback and insights to refine their strategies and enhance their likelihood of success in court.

## Setting up a mock jury

For the selection of a mock jury, four main methods are presented. Attorneys ensure the close resemblances of a real jury by guaranteeing the demographic and characteristic factors of a real jury. Therefore, mock jury selection can be done randomly from choosing participants from a voter or jury duty registration lists, to contacting recruitment

companies, outreach communities, or select a pre-screened focus group.

According to Rauna Irjala, Large and International Claims Manager at If, "It is rather common to use a mock jury in cases where the risks are considered to be high, both in terms of evaluation of our insured's liability and especially related to the monetary amount of the potential verdict against our insured. Often there are multiple defendants in lawsuits and apportionment of liability between these companies is a key legal factor in the case, and also causes uncertainty of the risk of each party. We are all painfully aware that nuclear verdicts of tens or hundreds of millions of dollars are increasingly common in the US. The mock jury or in some cases several juries provide a verdict in the case, offering insight into how a real jury might rule on the distribution of liability for the parties and the amount of the verdict."

## Evaluating the risks

Rauna Irjala highlights that the best practices for setting up a mock jury depend on the case. Usually, the defence counsel can and will recommend how to set up the mock trial. Outside service providers are often used to select the jury and organise the trial where the actual defence counsel then litigates the case. "In our experience, it may be a valuable idea to take part in the mock trial to see the case from the litigation perspective."

Rauna Irjala concludes, that in her experience, the greatest benefit of mock jury trials is their effectiveness in assessing the risks of each individual case, considering the specific venue of the lawsuit. Mock jury trials are a useful tool in the box to evaluate the potential settlement value and strengths and weaknesses of the case. A reasonable settlement benefits the insured, as it saves time and effort while mitigating the risk of an extreme jury verdict which may even exceed the insurance coverage limits. ●



### Meet our expert

**Rauna Irjala**  
Large and International  
Claims Manager Finland

#### REFERENCES USED:

What Is a Mock Jury? (With Common Juror Requirements) | Indeed.com

The Online Trial Experience | eJury.com

7 Benefits of Mock Trials | U.S. Legal Support | uslegalsupport.com

Online Mock Trials vs. In-Person Mock Trials: Pros and Cons | firstcourt.com

age\_rr4| nber.org

How to Use Mock Trials in Case Evaluation and Trial Preparation | Blog | Legal.EmotionTrac.com

Mock Juries in the COVID Era | Attorney at Law Magazine | attorneyatlawmagazine.com

Mock Juries | decisionanalyst.com

Mock jury trials | nlr.com



## PROPERTY

# The right values protect

By Kristian Orispää, If

The importance of accurate values in an insurance policy remains especially relevant as we see risks relating to underinsurance continue to surface, impacting businesses and hindering their recovery when incidents occur.

The British idiom ‘penny-wise and pound-foolish’ rings true in most cases of underinsurance. Underinsurance occurs when the amount listed in an insurance policy does not correspond to the actual value of the conditions covered. If the insured sum is too low, the compensation needed to restore operations after a fire, flood or other extensive damage simply will not be enough. In these cases, without accurate insured values, the gap to rebuild can reach tens or even hundreds of thousands, leaving the company to take the shortfall out of its own balance sheet.

According to Johanna Mola, Nordic Head of Property Underwriting at If, being underinsured is a larger issue than most people realise. “The consequence, in a worst-case scenario, is that a company’s insurance policy might be insufficient to cover the damages incurred. This means that recovering while maintaining operations after a loss will simply be impossible.”

### Dependencies and bottlenecks

Following the COVID-19 pandemic, and rising geopolitical conflicts, scarcity of materials and components have created new dependencies on specific suppliers. “This growing issue challenges many companies—and having multiple suppliers for critical equipment cannot be emphasised enough,” Mola states. “Relying heavily on a single supplier poses a significant risk of long periods of business interruptions, as many companies struggle to secure the goods they need from their usual suppliers.”

There have been cases, where assessing the value seem straightforward at first. In reality, however, it can be difficult to calculate the total values accurately. Securing the materials or components required to keep production going, replacing damaged equipment, and sourcing sufficient construction materials to rebuild must be factored into the





Providing a lower value for your warehouse to save on insurance is a risky decision. In the event of a flood or fire, your insurance will fall short of covering the damages and rebuilding costs.

Underinsurance truly exemplifies the idiom, ‘save a penny, lose a dollar’ or ‘penny-wise, pound foolish.’

Mola emphasises the importance of robust business continuity plans. “Companies need to consider, if something happens, how long will it take for us to be up and running again?” She adds, “At If, our goal is to help clients get the protection they need, whether it is 100% coverage for business interruption or only covering the first 6 months. This must be a conscious decision on the client’s part, with clear understanding of the financial risks the company’s top management is willing to accept.”

### Getting it right

Using an external appraisal company can help clients secure the most accurate valuation of their assets. In the Nordic market, this practice is less common, partly due to industrial companies not being required to review their property and assets regularly—a practise more typical in other European countries.

To keep insured values up to date, external appraisals for different sites and properties should be conducted every 4 to 6 years. Mola explains, “It’s also important on the proper indexation to ensure values remain as accurate as possible over time. Generally, the best valuations often come from full site visits by external appraisers, who can inspect everything on the ground. Having people physically inspect the site increases the chances of getting the values right.”

Mola concludes with a reminder: “By working closely with our clients, we can best secure their business continuity. Managing risks and having accurate values puts us in the best position to support our clients when they need it most. Our goal is for clients not to be disappointed when damages occur—but they will be with inadequate coverage. In the end, insurers can only cover the amount insured.” ●

# businesses

insured value. These variables must be carefully considered before an accident or incident occurs to avoid being significantly underinsured.

### What about goodwill?

As Mola highlights, “We expect to see even fewer leeway clauses going forward. Year after year, we see a growing number of underinsurance cases.” She continues, “Maintaining accurate insured values is the best way to ensure your recovery. Having accurate sums insured provide additional security to a company, protecting their operations and supporting recovery when something happens.”

Understanding the correct values of raw materials, equipment and recovery is vital. The true costs relating to replacing business critical equipment, including for example the rebuilding of damaged electrical installations or systems is increasingly important. As an example, securing a new transformer today has become a daunting task. Over the past year, the shortage of electrical distribution transformers has impacted business operations and construction projects globally.



### Meet our expert

**Johanna Mola**  
Head of Property Underwriting

During 2024, the transformer industry was facing significant challenges due to supply shortages and extended lead times, which threatened business continuity for industrial clients. Lead times for large power transformers surged from the previous 12–24 weeks to 1–3 years, while prices increased by around 70%. The transformer shortage affects all sectors dependent on a reliable electricity supply, especially those reliant on Large Power Transformers, which are critical for many industrial operations.<sup>1</sup>

### What has “transformed” the situation?

Supply and demand—the cornerstone of economic philosophy—dictates that when demand rises, supply should naturally increase to meet it. However, the primary factor driving the transformer shortage is the limited number of manufacturers and their restricted production capacity.

The ongoing shift to renewable energy and electrification has spiked the demand for transformers. Large step-up transformers are increasingly required to integrate renewable energy into the grid. The COVID-19 pandemic exposed many vulnerabilities in global supply chains, especially in critical raw materials essential for transformer construction and function. These include materials such as

electrical steel, zinc, copper, nickel, aluminium, and silicon. Each of these materials is subject to supply chain disruptions, price fluctuations, and environmental regulations. Beyond post-pandemic recovery, ongoing geopolitical tensions have further strained raw material supply chains.

Additionally, the transformer shortage is linked to the aging electrical infrastructure. Much of the existing transformer infrastructure is several decades old and urgently needs replacement. The push for modern, more efficient transformers has also stretched transformer manufacturing capabilities, as transformer production is complex, capital-intensive and requires skilled labour.<sup>2</sup>

### Preparing for transformer losses

Transformer failures, though relatively uncommon, can have significant impacts when they do occur, and can arise for various reasons. For example, internal short circuits or ground faults due to insulation breakdowns or manufacturing defects can generate excessive heat, which ignites the insulating oil in oil-filled transformers. When this flammable oil burns, it generates enough pressure to potentially cause an explosion. Oil-filled transformers are the dominant transformer type worldwide, accounting for over 80% of last year’s annual market revenue, with the remaining transformers being

## ENERGY

# Transformer sh

## – a threat to business continuity

By Tuomas Kaleva, If



dry-type units. In general, dry-type transformers pose less risk of fire or explosion as they do not contain any flammable liquid, thereby eliminating that particular hazard.

This situation presents significant safety and property damage risks. Even if a transformer fire does not spread, it will most likely consume the transformer itself, causing a business interruption.

### What strategies can companies adopt to mitigate the risks associated with transformer losses?

Implementing robust maintenance programmes is a relatively low-effort method to extend the overall lifespan of existing transformers. Predictive maintenance techniques, such as thermal imaging and dissolved gas analysis (DGA) and online measurements for oil-filled transformers, help detect potential issues before they lead to large-scale failures. Also, operator usage and load on transformers will significantly affect the lifespan.

However, all transformers—and some of their components such as tap changers—have a limited lifespan regardless of maintenance and depending on their operating conditions. For this reason, stocking essential components and, ideally, complete spare transformers provide the best buffer against transformer losses. Engaging multiple suppliers and sourcing

from geographically diverse regions can help mitigate the risk of regional supply chain disruptions and replacement/service agreement. Upgrading to more efficient transformer designs and utilising smart grid technologies can also enhance reliability and reduce dependence on older, less efficient models.

Protecting transformers from fires is another critical aspect, especially for oil-filled types, which pose a greater risk of fire spreading rapidly to surrounding equipment and buildings if not contained. If a transformer fire occurs, it can be extinguished using different methods. Water-based systems (e.g., deluge or water mist) are commonly used.

Since critical transformer failures or losses can still occur despite precautions, conducting thorough risk assessments and developing business continuity plans for transformer losses will significantly minimise the expected downtime. This includes pre-planning and emergency procedures for temporary power solutions and regularly assessing rapid replacement options.

### Key takeaways

The transformer shortage poses a significant risk to industrial operations worldwide. By understanding the underlying causes and implementing strategic preparedness measures, companies can reduce the impact of these shortages in their operations. Regular transformer maintenance and operating conditions, fire protection measures, supply chain diversification, and solid business continuity plans are the most important steps to ensure business continuity during the time of transformer shortage. ●

# ortage



### Meet our expert

**Tuomas Kaleva**  
Risk Engineer

### Sources

1. Source: Wood Mackenzie, 2024; Data & analytics solutions, 2024; DOE, 2024
2. Source: PV magazine USA, (2024); DOE, 2024; Data & analytics solutions, 2024; Thunder Said Energy, 2024

### REFERENCES

- Wood Mackenzie. (2024). Supply Shortages and An Inflexible Market Give Rise to High Power transformer lead times. Retrieved from Wood Mackenzie.
- Department of Energy. (2024). DOE and Industry Team Up to Keep the Lights On for America. Retrieved from Energy.gov.
- Thunder Said Energy. (2024). Transformer Shortages: At Their Core? Retrieved from Thunder Said Energy.
- PV Magazine USA. (2024). A Look at the Great Transformer Shortage Affecting U.S. utilities. Retrieved from PV Magazine USA.
- Heritage Foundation. (2024). The U.S. Needs a Resilience Strategy for Its Transformer Shortage. Retrieved from Heritage Foundation.





## CONSTRUCTION

# Wood construction makes a comeback



By Andreas Kräling, If

Following a sharp increase in the construction of wooden buildings, the number of substantial damages has also risen, highlighting the complex risks associated with this material.

In this article, we focus on two types of wooden structures: cross-laminated timber or CLT construction, and modular house construction. When planning a wood-based building project, understanding the risks linked to these types of construction is crucial.

### History of wooden buildings

During the 1800s, the number of wooden house fires increased in the Nordic countries due to urbanisation. For example, there were some 400 major city fires in Sweden during that time period. One of the most devastating events was the Gävle fire in 1869, which destroyed the entire town and left 8,000 residents homeless. These fires led to stricter legislation, limiting wooden structures to only a few stories.

During the 1990s and 2020s, building legislation has changed, and continues to change, in several Nordic countries. Today, it has become possible to build multi-storey buildings with load-bearing wooden frames again. This shift

## Wooden structures are becoming more common due to the growing awareness of their sustainability benefits.

was driven by function-based building codes, which require buildings to meet functional requirements regardless of the material used. In many cases, these legislative changes often lacked sufficient impact assessment regarding wood buildings and fire protection. After the revision, the expectation was that traditional structures with only a few floors would remain the norm, as newer techniques of modular construction and CLT were not yet in use.

### A changing climate impacts construction

The Nordic countries have set ambitious climate goals, with the aim to significantly reduce greenhouse gas emissions by 2050 compared to 1990 levels. Finland, for example, is committed to becoming carbon neutral by 2035 and Denmark by 2050. This presents a major challenge for the

construction industry, which must lower its emissions to meet the Paris Agreement standards.

It is generally known that building with wood can reduce climate impact compared to using traditional, non-combustible materials for larger structures. However, the regulatory framework has not yet adapted to newer construction technologies and there are challenges—especially when it comes to fire protection.

Wooden structures are becoming more common due to the growing awareness of their sustainability benefits. If Insurance is committed to supporting environmentally responsible construction, but it is important to assess each project from a risk perspective. Current building regulations have not fully accounted for CLT and modular construction technologies, making early involvement from If's risk engineers essential for managing risks effectively.



## Standards for CLT structures in 2025

Cross-laminated timber panels are made up of planed timber that has been finger-jointed and glued together to form slats. The slats are then laid crosswise in layers, which gives a solid element, known as CLT. This is a construction that provides a strong and rigid building element with high dimensional stability. The elements are adapted in the factory to the dimensions desired by the customer.

Generally speaking, CLT structures are considered to be more positive than modular structures from a risk point of view, as the spread of fire is highly limited due to solid construction. However, it remains a fact that utilising wood will result in a combustible building, which needs to be taken into account in the risk assessment stages of the building project, and especially during the construction phase, where this can play a greater role.

Additionally, the potential for water damage from firefighting efforts also needs to be considered. Other risks, such as moisture, pests, and mould infestation can increase with this type of material, though there is insufficient data to determine the exact extent. Companies are advised to involve risk engineers early in the process to ensure these issues are properly addressed.

Today, there is no harmonised standard for CLT in Europe. In contrast, the US has established a common standard for the CLT industry. An updated version of Eurocode 5, which will introduce fire resistance calculations for CLT walls and floors, is currently under consultation and is expected to become the approved standard by 2025.

According to Lina Sundgren, Risk Engineer at If, “There are two main fire risks with CLT structures: delamination and reduced bearing capacity during the cooling phase. Essentially, CLT elements can delaminate in the event of a fire due to the release of the adhesive when heated by the flames. This leads to the loss of the protective carbon layer and new fuel is continuously added to the fire, which leads to longer fire processes even if the other fire load in a room has been burned.”

Lina Sundgren continues, “There are a variety of adhesive types on the market that are approved for use in load-bearing structures. Currently, there are no temperature requirements linked to fire performance, rather existing standards only specify a temperature requirement of 70°C, which the glued structural components must be able to withstand over two weeks exposure while carrying a certain load. In the United States, the standard is based on fire tests in which CLT elements are placed in a furnace and exposed to different temperatures, and in this way the impact on delamination is analysed.”

She explains, “One measure to protect the load-bearing wooden structure in a fire is to install fire-retardant cladding, such as fire-rated plaster. The American standard stipulates the maximum amount of exposed CLT and requires the installation of sprinklers in these buildings.”

Reduced load-bearing capacity after a fire is another risk with CLT structures. While fire tests are conducted over a specific time period to check the structure’s load-bearing capacity, the cooling phase also impacts this capacity. Research has shown that even after the fire is extinguished, load-bearing elements like R60 columns can lose their strength 10–15 minutes into the cooling phase, with full failure occurring within 120–240 minutes.

## Understanding modular constructions

Modular houses are manufactured indoors in a factory setting, which offers several advantages such as standardised work methods, better working environment, and cost efficiency. Once ready, prefabricated modules are delivered and assembled on the construction site, often completed within a few weeks.



## If Insurance is committed to sustainability but assesses each case from a risk perspective.

This rapid installation helps ensure compartment boundaries are established early, adding a layer of safety.

Modular constructions, however, come with their own set of risks that need to be properly managed.

- **Cavities Between Composite Modules – Fire Spread**  
Fire stops are placed at the top, and around each module to prevent smoke gases (toxic gases in smoke) from entering the cavities. However, damage has shown that smoke gases can still seep into these cavities, making the fire's path unpredictable.
- **Cavities Between Composite Modules – Water Damage**  
During extinguishing efforts, water can enter the cavities between modules, and drying and repairing these areas has proven to be complex and time-consuming. Moisture trapped in these spaces can lead to mould growth, which is difficult to access and repair.
- **The modules are part of the load-bearing frame.**  
The modules are part of the building's load-bearing structure, and restoring this type of construction after damage is very time-consuming—as only a few modules can be repaired at a time. There are cases of multi-storey buildings, where a fire in a single apartment, caused water, soot, and odour damage in several other apartments due to the firefighting efforts.
- **Rescue service challenges**  
Extinguishing fires in modular construction is more resource-intensive for emergency services, as the spread of fire is often unpredictable and occurs in cavities between the modules. Emergency services may need to battle fires in several areas simultaneously, which is not typical with non-combustible frames. Modular structures also have a greater risk of collapse compared to non-combustible and CLT structures. In situations where the safety of rescue personnel is at risk, firefighting is limited to external efforts.

### Insights and considerations

Modular house constructions are particularly complex, as minor damage can lead to extensive consequences. Stacked modules create gaps where smoke, water and fire can spread between sections. By contrast, in non-combustible material structures, a fire typically remains confined to the individual apartment.

A further complexity is that the restoration of modular buildings is much more difficult as the modules are part of the load-bearing structure, stacked on top of each other. This drives up the costs and time required for restoration. The assessment is that a maximum of two storeys is most suitable for modular house constructions.

On the other hand, while CLT construction presents fewer challenges, there remains a risk of collapse in multi-storey buildings if the glue fails, presenting an unacceptable risk of structural integrity.

Extensive research is being conducted worldwide, especially on CLT structures from a fire safety perspective. Swedish company Södra, a producer of solid wood structures, published Träsäker—fire protection guidance for cross-laminated timber—in December 2023. This guide outlines the measures needed beyond current building legislation requirements.

Guidelines like these provide a useful reference for proposing different solutions that offer effective and reliable fire protection for wooden structures. There are also numerous ongoing research projects, including Fire Protection Wooden Structures during Construction (BIV), Delamination of CLT (BIV), and Fire-Impregnated Wooden Facades (DBI and RISE). ●



### Meet our expert

Lina Sundgren  
Risk Engineer



## Sources

### EXTERNAL REFERENCES

SBUF Fire Protection in BR0 Buildings, Application Support for Fire Engineering Design of High Buildings with Renewable Materials (Wood) SBUF\_13371-Verifiering-av-brandskydd-i-Br0-byggnad-ny-framsida.pdf (briab.se)

Södra Träsäker fire protection guidance for cross-laminated timber Documents (sodra.com)

Fire Safe Use of Wood in Buildings Fire Safe Use of Wood in Buildings | Global Design Guide | Andrew Buch (taylorfrancis.com) brandforsk-Timber-buildings\_Update\_report-3.pdf

### RESEARCH REPORT

Experimental assessment of the burnout resistance of timber and concrete columns Paper Template Sif2018 (jhu.edu)

In-depth accident investigation Fire in apartment building in Luleå Klintvägen Document page - Library - MSB RIB

Accident investigation Fire in building, Malmö Deficiencies in fire protection were discovered after apartment fire Malmö 2022. Document page - Library - MSB RIB

### LECTURES FROM FIRE PROTECTION 2023 CONFERENCE

- Carl Pettersson, RED, *Fire Safety in Wooden Buildings, an updated knowledge overview*
- Nils Johansson, Lund University *Initial results from BIV's Round Robin study of fire engineering design of wooden buildings*
- Henrik Greiff and Magnus Köhlin, Räddningstjänsten Syd. *Experiences from action in the event of a fire in a modular building.*
- Johan Grönkvist, Trygg-Hansa. *How is the insurance industry affected by new technology and new construction methods?*
- Axel Mossberg, Bengt Dahlgren. *Wooden houses and fire loads – easier to make more correct with a new framework.*
- Cecilia Wetterqvist, Bengt Dahlgren. *Fire as a factor in life cycle analysis.*

**CYBER**

# The challenges of cyber-attacks, ransomware, and extortion payments

By Lars Hedensjö, If



**T**here are several reasons why IT environments remain vulnerable. On a micro level, companies producing software, operating systems, and applications lack the ability to eliminate all vulnerabilities. For example, the codebase of a modern operating system has become so extensive that changing components carry significant risk. Every added feature increases the attack surface, making it nearly impossible to guarantee there are no security flaws. Additionally, software companies must continuously modernise the functionality and release new versions to stay competitive, which inevitably introduces new vulnerabilities.

On a macro level, there are additional challenges. Dominant nations in the IT sector often pursue conflicting goals—they seek security vulnerabilities they can leverage for their own national interests while simultaneously working to eliminate weaknesses in their own

IT-environments to prevent others from exploiting them. Over time, these efforts to have exploitable flaws ripple into everyday life, leaving companies exposed to risks that impact both businesses and customers. Currently, these nations tend to prioritise offensive strategies over defensive measures.

## Criminals strive for efficiency

Criminals and organised crime groups operate with a similar mindset to businesses—their aim is efficiency, achieving maximum results with minimal effort and reduced risk. In the cyber arena, ransomware attacks have increased in recent years. Indicators now suggest that attacks on large Nordic companies have plateaued, although they remain at high levels, while attacks on midsize companies continue to rise. One possible explanation is that larger companies have refined their cybersecurity defences, making midsize companies more attractive targets

due to their comparatively weaker security. Cybercriminals often operate in countries with weak law enforcement, further reducing the risk of getting caught. This operational environment allows them to execute attacks more effectively, with fewer consequences.

## Cyber-attacks and the insurance industry

Insurance companies offer various services to help businesses recover from cyber incidents. These include incident response and restoration, coverage for business interruption (including incidents at service providers), cyber-crime protection, third-party claims, confidentiality, and privacy liability, network security liability, and media liability. However, there is one area that differentiates If Insurance from its competitors. Unlike most insurers, If will not reimburse ransom payments, challenging the prevailing market practice. This decision reflects a strategic stance that prioritises all parties' long-term benefits over some parties' short-term convenience.

## Ransom extortion payments exclusion, insurance, and well-informed decisions

The fundamental reasons for not offering insurance coverage for ransom payments are:

- reducing the incentive for organised crime to engage in extortion
- clarifying ethical responsibility against organised crime
- mitigating legal risks—as ransomware payments risk breaching legislation regarding terrorist financing or sanction lists

## Addressing common arguments against this approach

There are often perfunctory arguments against If's stance on excluding insurance for extortion payments. These arguments have several weaknesses, as highlighted in the following counterarguments:

*“When you experience a cyber-attack, you must pay ransom to recover”*

- There are several ways to resolve a cyber incident involving ransomware without paying the ransom. For example, one security company handling hundreds of cases has successfully avoided ransom payments in all instances.

*“All organisations want ransom payment coverage”*

- What companies often seek during a cyber-attack is priority access to external professional specialists, including, technical incident responders, forensics experts, hostage negotiators, and legal advisors.

- In several cases, organisations that experienced a cyber intrusion lost their cyber insurance policy to the perpetrators, making explicit ransomware coverage more of a liability.

*“The easiest solution for the organisation is to pay the ransom”*

- Paying assumes the blackmailers will fulfil their promises. It has been reported, based on one security company's data, only 67.6% of extortionists deliver on their promises, while 20.6% fail to do so.<sup>1</sup>
- Organisations who pay the attackers are sending the message that extortion schemes work on them, a message which malicious actors could use to justify subsequent attacks and extortion attempts. One security company found that 80% of organisations who paid a ransom demand ended up incurring another attack. Close to half (46%) said it was the same attackers that hit them again, while more than a third (34%) might have been another threat actor that's responsible for the follow-up infection.<sup>2</sup>
- Even if the ransom is paid, the problem still remains as the attackers retain knowledge of the system's vulnerabilities and access to the organisation's IT environment with any information therein. They can sell this data or sell entry to third parties, perpetuating the risk.

*“No one will know the organisation paid the ransom”*

- Depending on the payment method, information about the transaction could become traceable and public, exposing the organisation.

## Potential risks of ransomware coverage

Some customers or brokers might seek maximum coverage, without considering the negative implication of certain provisions, such as ransomware payment coverage. This could lead to a false sense of safety, reducing proactive cybersecurity measures and unintentionally contributing to organised crime. ●

1. 2024-unit42-incident-response-report.pdf [https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf)
2. [www.Cybereason.com/Three-Reasons-Why-You-Should-Never-Pay-Ransomware-Attackers](http://www.Cybereason.com/Three-Reasons-Why-You-Should-Never-Pay-Ransomware-Attackers).



# Vulnerabilities within cyber-physical ecosystems

By Caroline Bødkerholm Ramsby, If

According to ENISA (the European Union Agency for Cybersecurity), the top emerging cybersecurity threats for 2030 are supply chain compromises of software dependencies, advanced disinformation campaigns, and the rise of digital surveillance authoritarianism. Additionally, human error and exploited legacy systems within cyber-physical ecosystems are highlighted, as are targeted attacks enhanced by data from smart devices.

**T**he evolving threat landscape poses risks to affirmative products and conventional ones, such as property and liability insurance. In this article, we will explore human error and legacy system exploitation to address some of the core issues in Cyber-Physical Systems (CPS) security.

## The Cyber-Physical Systems of today

CPS can be defined as networked systems where the computational (cyber) part is tightly integrated with physical components. A similar term, OT (operational technology), is also used to describe these systems.

The CPS market is expected to grow at a considerable rate, fuelled by the rapid advancement of intelligent features that enhance the capabilities of physical systems in several areas.

Examples of these systems include network monitoring, medical devices, & robotic systems. Key industries developing in this area include healthcare, cybersecurity, and utilities. From smart grids to Building Management Systems, cyber-physical systems are increasing efficiency across companies and society as a whole. The defence industry, transportation, as well as warehousing and storage, also utilise CPS.

Modern CPS include features such as real-time data acquisition, process automation, and monitoring by integrating sensors, the Internet of Things (IoT), and artificial intelligence (AI) to deliver increased automation, realise efficiencies and secure services, to name a few examples.

## Unfortunately, in the insurance industry, we often encounter companies still using legacy systems.

### Plenty of vulnerabilities exist

Although there are clear benefits to CPS, serious vulnerabilities have emerged, many of which create opportunities for cyber criminals and carry serious consequences.

When physical devices and systems are connected to one another—whether through cloud services or other internet connections—the data it generates, the functionality, and the solutions provided become vulnerable to potential cyberattacks and malicious activities.

Examples of these vulnerabilities include the 'isolation assumption' which is based on the false belief that a hidden system is also secure. This is a common practice in modern companies and dangerous approach to cyber security.

Furthermore, with increased connectivity and uniform or similar CPS, both factors can be considered as vulnerabilities. Increased connections broaden the opportunity for cyberattacks. Meanwhile, similar systems share related vulnerabilities, meaning that hacking one CPS could compromise multiple devices. For example, if CPS are connected through a centralised management system, hacking the main system grants access to all connected CPS. Alternatively, if CPS are of the same type but lack centralised management, a common vulnerability exploited in one device could make others equally easy to hack.

Failure to update legacy systems poses serious risks; unfortunately, these weaknesses are compromised regularly around the world. Maintaining legacy systems is, in fact, a major concern for many companies.

For example, in 2017, the WannaCry ransomware attack affected numerous organisations worldwide, including the UK's National Health Service (NHS). The attack targeted a security gap in the Windows operating system and spread rapidly through unpatched systems. The NHS was particularly vulnerable due to its reliance on legacy systems and a lack of adequate cybersecurity measures.

### Understanding human error in cybersecurity

Human errors, such as clicking on malicious links, using weak passwords, falling victim to phishing attack, or accidentally disclosing confidential information, create substantial security risks that cybercriminals can exploit to access critical systems and data.

When it comes to cyber-physical systems, human error typically occurs in incidents involving a programmer or network engineer. These human issues include, poor coding, faulty updates, misconfiguration, inconsistent or misaligned network security, and reliance on legacy systems or outdated solutions for critical operations.

### An insurer's perspective on threats today

Lars Hedensjö, Cyber Underwriter at If explains, "In the Nordic region, the number of ransomware attacks has increased marginally in 2023 when compared to 2022. Extortionists prefer to target large companies as they have

more resources. Still, in 2023 the proportion of ransomware attacks against large companies (over 5,000 employees) has decreased in relation to medium-sized companies (501–5,000 employees). Currently, the percentage of ransomware attacks, as distributed by company size, is:

- 17% of incidents occur in large companies
- 34% in medium-sized companies
- 25% in smaller companies (51–500 employees), and
- 24% in small companies (1–50 employees)

Presumably, large companies' investments in improved security have had an impact, which then influences the extortionists to continue with more vulnerable medium-sized companies."

He continues, "In 2023, the most common type of attack in the Nordic region was extortion, accounting for 32% of cases. The second most common was contained attacks at 20%, where the attacker gained an initial foothold but was detected and stopped before further damage could occur. Business Email Compromise (BEC), accounts for 16% of cases. These attacks often begin with a phishing email that allows the attacker to obtain the victim's email login credentials. The attacker then monitors the email correspondence waiting for opportunities, such as intercepting account details. BEC attacks have seen a large percentage increase from 2022 to 2023."

The primary attack vectors used were vulnerabilities, which accounted for 38% of cases. These weaknesses were found in services that were directly accessible from the internet. When extortionists engage in mass exploitation, they often install backdoors to maintain access if the organisation updates its systems to remove the vulnerability, allowing them to return later for an extortion attempt. Additional attack vectors include valid accounts (26%), phishing (23%), trusted services and supply chain attacks (10%), and other methods (3%). Trusted services have shown the most growth in usage, although they are primarily used by the most advanced ransomware groups.<sup>3</sup>

According to Ghita Meyer, Head of Liability and Cyber Underwriting, the evolving cyber threat landscape continues to influence on the insurance industry.

"Cyber threats influence the insurance industry in the broadest sense. They appear across different coverages, from property and liability to personal lines. Historically, the cyber insurance product was developed to address cyber risk, which has allowed our B2B business to identify and cover the risk in a more transparent way. Still, the distinction between cyber insurance and traditional property and liability insurance will need practical application over the coming decade."

Lars Hedensjö provides insights from recent studies to add perspective. "According to one source, there has been a 75% increase in attacks on the healthcare sector since last year. This is likely due to the fact that medical and health industry providers hold customers' protected health information (PHI), financial information (such as card and



account number), and personable identifiable information (PII), all of which are valuable targets for attackers.” He adds, “Attacks on consulting and professional services have increased by 141% since last year. This sector also has access to sensitive information, either directly or through close interaction with clients.”<sup>4</sup>

He also explains that there are statistics available on how companies fare after paying extortionists. In cases where a company has paid its attacker, the blackmailers’ promises were fulfilled in 67.7% of the cases, unfulfilled in 20.6%, and partially fulfilled in 3.9%. In 7.8% of cases, the outcome was unclear.<sup>5</sup>

### Endless possibilities

In its simplest form, consider a customer producing a product in a factory. The systems at risk are those that control the production machines, or for instance, the power to the building itself. In other cases, the risks can be more elusive. Cyber threats may target numerous smaller devices scattered around the world, where attackers look to track people or items that register and send information.

Lars explains, “The consequence of a cyber-attack can involve more obvious losses such as interruption of service or unauthorised access to information in the service. There are also more evasive aspects, depending on the system’s function and the attacker’s form of attack.”

He highlights the example of Stuxnet, a malicious worm, noting “Stuxnet clarifies the range of what is possible. It targeted supervisory control and data acquisition (SCADA) systems, specifically programmable logic controllers (PLCs), which allow the automation of electromechanical processes, such as gas centrifuges for separating nuclear material. Exploiting four zero-day flaws, Stuxnet targets machines using the Microsoft Windows operating system and networks, then seeks out Siemens Step7 software.”

Reportedly, Stuxnet compromised Iranian PLCs causing fast-spinning centrifuges to tear themselves apart, by manipulating rotor speed, first increasing the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. Stuxnet allegedly ruined almost one-fifth of Iran’s nuclear centrifuges.<sup>6</sup>

### Digitalisation and cyberattacks

When asked if these cyber threats impact affirmative products and conventional ones, such as property and liability insurance, Ghita Meyer comments, “Manufacturing products and production techniques are changing and becoming increasingly digital. This brings new challenges for both product liability and property insurance.”

“As cyber risks evolve, legislation seeks to follow—which is natural,” she notes. “The most recent legislation from the European Union includes the new Product Liability Directive and Cyber Resilience Act. Both increase the producer’s responsibility when selling digital, online-connected products that pose a risk for potential data loss.” ●



#### Meet our experts

**Lars Hedensjö**  
Cyber Underwriter



**Ghita Meyer**  
Head of Liability and  
Cyber Underwriting

### Sources

1. Threat Intelligence Report 2024, page 4, 8, Truesec
2. Threat Intelligence Report 2024, page 5–6, Truesec
3. Threat Intelligence Report 2024, page 7, Truesec
4. 2024 Threat hunting report, page 10, CrowdStrike
5. Incident response report 2024, page 22, Palo Alto
6. Stuxnet - Wikipedia  
<https://en.wikipedia.org/wiki/Stuxnet>



## BUSINESS TRAVEL

# Travel insights from claims experts

By Kristian Orispää, If

We at If take a proactive approach to understanding clients' evolving expectations for travel insurance plans, while also anticipating and addressing their specific needs.

**B**y working closely with clients, we are able to ask the right questions to continually refine our services and identify the most effective ways to meet those needs. This approach is reinforced by a preventative strategy that includes online travel-risk mapping services, helping companies better prepare for trips and proactively avoid or mitigate common risks.

During the Covid-19 pandemic, it was seen that several guidelines were inadequate in preventing the spread of the disease. Many companies were aware of hygiene challenges when traveling internationally, especially the difficulty in maintaining sufficient standards—yet some employees still opted to go abroad during





this time. For example, travel to Asia increased employee vulnerability due to the region's initial severe impact from the virus and the strain on healthcare systems in several countries.

One way to reduce health risks when sending employees abroad that is recommended for companies is to consider the possibility of optional health check-ups for business travellers. These health check-ups can help prevent hospitalisation, emergency transportation home, or even death. Naturally, the Nordic countries apply different legislation, so it is advisable for a company to find out in advance any restrictions and obligations imposed by legislation.

### **Collaborating with healthcare partners**

Reliable and modern health services are common in many Nordic countries. However, companies cannot rely on foreign health systems to operate with the same efficiency in other destinations, especially when employees have complex health needs.

Increased collaboration with healthcare partners can offer significant benefits, such as:

- a dedicated claims team specialising in international travel claims to ensure swift and effective handling

- effective coordination between claims teams, local healthcare providers, and assistance partners to reduce response times in addressing medical needs
- continuous improvement in claims handling processes and alignment with partners to promote transparency and expedite claim management
- accurate reporting and data analytics to identify patterns and help prevent future claims

Illness abroad can lead to significant business disruptions. For instance, if a key employee with specialised expertise becomes ill, it could delay or disrupt the completion of an entire project. As mentioned previously, conducting an optional preventative health check-up before travel is one way to mitigate these risks.

Depending on the situation, it may be more efficient to transport the ill or injured employee to a neighbouring country for medical care. With extensive experience in this area, we can optimise the treatment paths and costs without compromising quality. Clients can also stay ahead of travel risks through their own travel portal.

For instance, at If, we initiate claims by assessing the risk landscape and asking the right questions to establish an overall understanding of what needs to be done and to identify the appropriate partners to contact. Companies adopting a similar service model have experienced fewer claims, gained insights into managing their employees' health during travel, and are now able to make informed decisions when these employees are unwell.

The evidence is clear: companies investing in travel safety solutions can achieve long-term financial benefits and stability.

### Supporting employees

According to Tiina Isoniemi, Claims Manager at If, clear travel policy guidelines are essential for employees who travel. "Careful and clear guidelines must be provided to employees and confirmed by the company's customer or contact in the destination country, so that it's clear what needs to be done in case of an emergency or if the employee requires medical help abroad. Furthermore, all employees must carry relevant documents and have, for example, their travel insurance numbers and important contact information (such as travel assistance contacts) with them on their business trip."

Regular health check-ups are also recommended for frequent business travellers to identify any potential health risks and take any preventive measures as needed.

Tiina Isoniemi reminds travellers to keep up-to-date records in their company HR and travel portal. "Your next of kin or emergency contact numbers need to be in the employer's HR portal. These will be needed if a serious situation arises, and the employer must contact your family or emergency contacts."

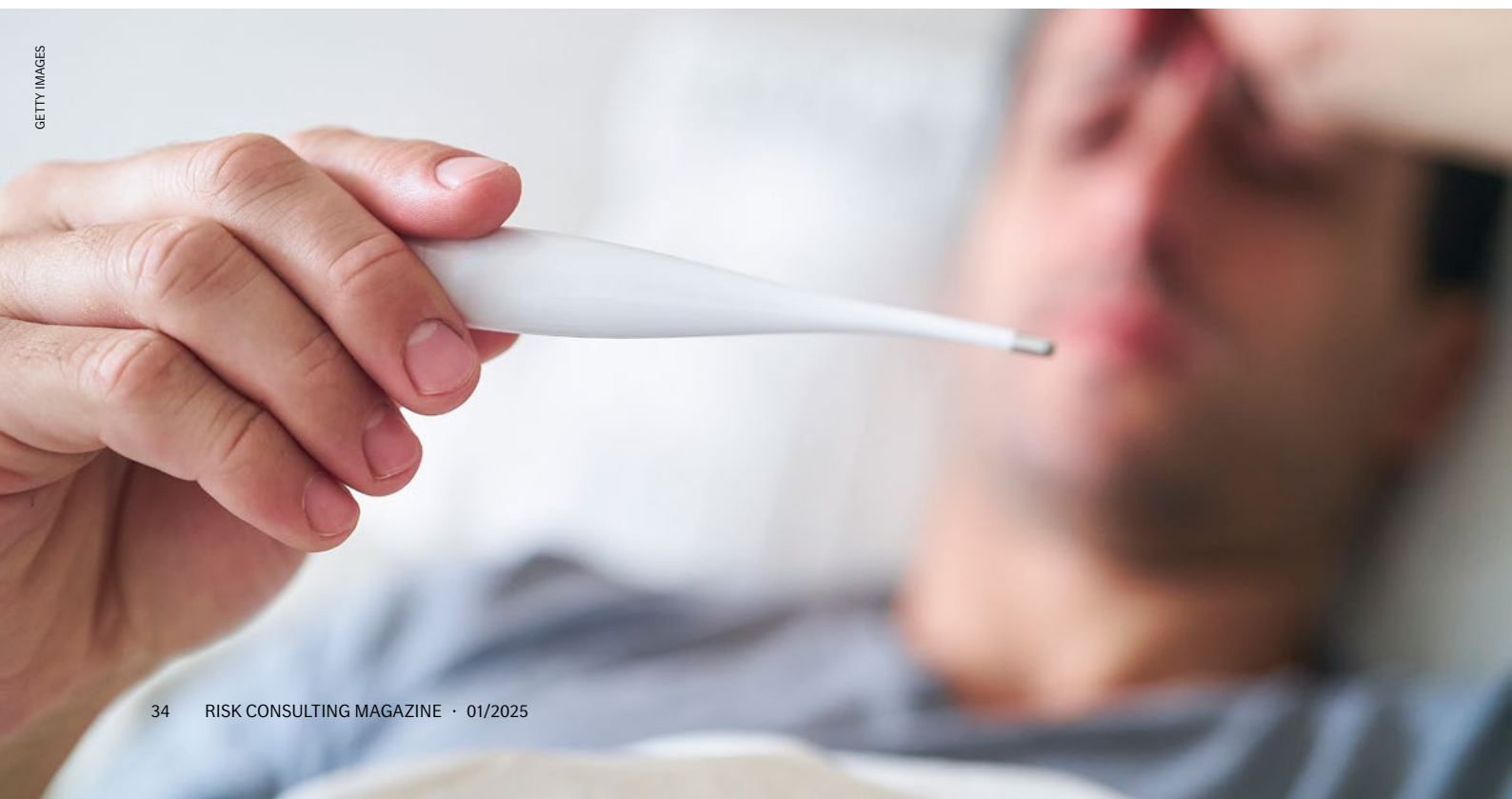
"Always complete travel bookings (flights/hotels) through the employer portal and remember to cancel any reservations on time so that reimbursements can be collected from the travel agency."

"Theft continues to be a leading cause for claims. Employees are encouraged to take care of their luggage, including employer property, to avoid theft or damage."

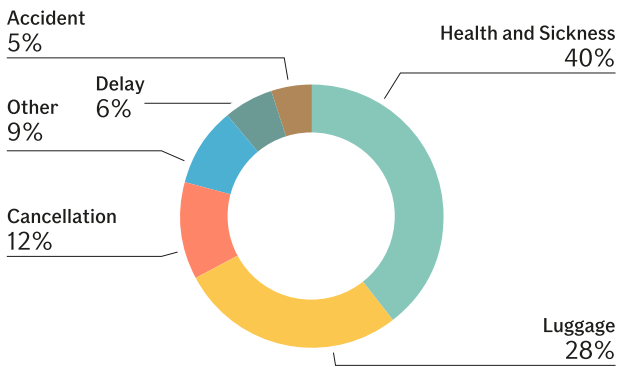
### Looking at the numbers with If Claims

In total, there were over 48,000 travel claims in 2023, with sickness claims accounting for over 19,000 cases and having the highest share of paid claims. The second-largest category relates to luggage, with over 13,000 cases recorded in the same year. Additionally, there were over 2,000 accident-related claims, having the highest average cost per claim. The majority of cases, excluding Expat claims, occurred in Spain, Greece, and Turkey. When Expat claims are added, the United States ranks first, with around 1,500 cases in 2023.

Tiina Isoniemi concludes, "Expectation management is just as important. Travellers need to understand what their insurance covers and



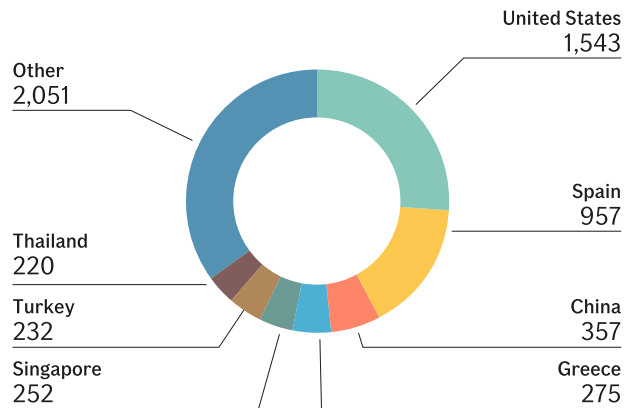
**TOP CLAIMS CATEGORIES, 2023<sup>1</sup>**



<sup>1</sup> Source: If Claims, 2024 (based on number of claims)

<sup>2</sup> Source: If Claims, 2024

**CLAIMS BY MOST COMMON LOCATION, 2023<sup>2</sup>**




what it does not. This is based on the insurance agreement between the company and their insurer, and it is helpful to grasp these details before travelling.”

“One further reminder, which most people understand but may forget, is that some countries do not offer the same level of care and clinical facilities as their home country. Therefore, when an accident or health concern arises, the reality of medical care may not meet the expectations they have of hospitals and clinics.”

“We always recommend that, as part of travel preparations, business travellers familiarise themselves with the conditions in their

destination, especially when heading to new or less familiar locations, or when planning for a longer stay.” ●



**Meet our expert**

**Tiina Isoniemi**  
Claims Manager



## RESEARCH

# Understanding risk perception in multicultural workplaces

By Moona Kiistala

Article is based on Moona Kiistala's thesis for If 2024



In today's diverse and globalised work environment, understanding risk perception is crucial for maintaining safety, especially in multicultural and multilingual organisations (Porru & Baldo, 2022). Nowadays, employees have and will have diverse cultural backgrounds and may not necessarily share a common language (Mattila et al., 2024). In Europe, the workforce is culturally more diverse than ever before (European Commission, 2021). Foreign-born workers face greater exposure to occupational risks compared to native workers, and these risks are often more serious (Flynn, 2014; Giraudo et al., 2019; Porru & Baldo, 2022; Salminen, 2012). Communication challenges are estimated to be the primary root cause (Guldenmund et al., 2013; Lindhout et al., 2012) but cultural differences, language barriers, and management approaches are also significant contributing factors (Flynn, 2014; Giraudo et al., 2019).

Several cultural factors that affect workers' varying perceptions of safety, include conceptions of safety, safety responsibility among managers and subordinates, appropriate interaction between superiors, subordinates, and equals, discrepancies between communicated and actual ways of working, employees' perceptions of work-related dangers compared to other daily risks, and adaptation to workplace risks (Flynn et al., 2018).

To address these observations, I conducted a comprehensive study involving interviews with 11 companies across various industries, two labour unions, and a Finnish Authority. These extensive interviews with companies and

experts provided a good picture of the current situation. The study aimed to answer three key questions: what factors cause challenges in multicultural and multilingual organisations, what specific challenges do employees and employers face, and what best practices and solutions are being used or should be adopted by companies to communicate clearly and efficiently.

## The impact of varying safety standards

Different cultures and previous work experiences shape employees' understanding of safety. Varying safety standards can stem from different cultures but also from working in other companies, particularly contractors, often encounter varied safety cultures and standards. This can lead to differing tolerances for risk and diverse interpretations of what constitutes safe practices. For instance, a safety procedure considered routine in one company might be seen as excessive or insufficient in another, causing confusion and inconsistency. In addition, foreign employees might be more willing to accept lower standards of safety due to fear of discrimination, or a desire to fit in.

## Hierarchical perceptions and communication gaps

Perceptions of hierarchy within a workplace significantly affect safety communication. Employees' views on their relationships with coworkers and managers influence how they communicate concerns and report incidents. In some cultures, hierarchical structures might discourage open dialogue, while in others, a more egalitarian approach

could facilitate better communication. Effective safety communication hinges on bridging these hierarchical gaps to ensure that every employee feels comfortable voicing safety concerns.

### Cultural and linguistic diversity

Companies often struggle with effectively addressing cultural and linguistic diversity in their safety communication practices. This challenge arises from the absence of clear guidelines on how to appropriately navigate cultural and linguistic differences without resorting to stereotypes or incorrect assumptions. Companies might find it difficult to balance tailored communication with avoiding the appearance of discrimination or inequality. Additionally, many companies lack awareness of these challenges, leading to an oversight of the critical role that effective communication plays in maintaining workplace safety.

### Proactive vs. reactive approaches to safety

Balancing proactive and reactive safety measures is a challenge for many multicultural organisations. Proactive measures involve anticipating potential risks and implementing strategies to mitigate them before incidents occur. In contrast, reactive measures address issues after they arise. Both approaches are essential, but without recognising and addressing cultural and linguistic factors, companies may find it difficult to implement these strategies effectively.

### Practical solutions and cultural awareness

Addressing these challenges requires both practical and cultural solutions. Practical solutions involve implementing concrete best practices, such as increasing visibility in forms of pictures and videos, utilising plain language, and translating material to multiple languages. For instance, safety manuals and training sessions could be available in multiple languages and designed to accommodate different cultural norms. Furthermore, management should undergo education on utilising plain language and understanding the nuances of diversity, multiculturalism, and multilingualism, ensuring these factors are duly considered in workplace practices.

Organisational culture solutions focus on fostering an inclusive environment that values diversity. This includes recognising the unique challenges faced by a diverse workforce, acknowledging cultural differences, and providing tailored safety training that considers cultural and linguistic differences. Companies should actively involve their multicultural employees in the planning of safety materials and orientation sessions to ensure that the messages are tailored to their intended audience.

### Enhancing safety through cultural sensitivity

Recognising and addressing cultural differences and language barriers is essential for effective workplace safety. Employees from different cultural backgrounds

may not be familiar with certain behavioural norms, safety standards or hierarchical structures that are obvious to the dominant population. By acknowledging these differences, companies can better understand their impact on safety and communication, ensuring that all employees are adequately supported.

### Some considerations

Creating a safe work environment in multicultural and multilingual organisations requires more than just implementing standard safety protocols. It involves understanding the diverse perceptions of risk and addressing cultural and linguistic barriers that can hinder effective communication. By fostering an inclusive culture and providing tailored resources, companies can enhance safety and ensure that every employee, regardless of their background, can work efficiently and safely. ●

## References

- European Commission. (2021). Industry 5.0 : human-centric, sustainable and resilient. *Publications Office*.
- Flynn, M. (2014). *Safety and health for immigrant workers*. Centers for Disease Control and Prevention.
- Flynn, M., Castellanos, E., & Flores-Andrade, A. (2018). Safety Across Cultures: Understanding the Challenges. *Professional Safety*, 63(01).
- Girardo, M., Bena, A., Mosca, M., Farina, E., Leombruni, R., & Costa, G. (2019). Differences in work injury risk between immigrants and natives: Changes since the economic recession in Italy. *BMC Public Health*, 19(1). <https://doi.org/10.1186/s12889-019-7178-2>
- Guldenmund, F., Cleal, B., & Mearns, K. (2013). An exploratory study of migrant workers and safety in three European countries. *Safety Science*, 52. <https://doi.org/10.1016/j.ssci.2012.05.004>
- Lindhout, P., Swuste, P., Teunissen, T., & Ale, B. (2012). Safety in multilingual work settings: Reviewing a neglected subject in European Union policymaking. *European Journal of Language Policy*, 4(2). <https://doi.org/10.3828/ejlp.2012.10>
- Mattila, S., Lindholm, M., & Kivistö-Rahnasto, J. (2024). *Työturvallisuuden megatrendit*. [www.tvk.fi](http://www.tvk.fi)
- Porru, S., & Baldo, M. (2022). Occupational Health and Safety and Migrant Workers: Has Something Changed in the Last Few Years? In *International Journal of Environmental Research and Public Health* (Vol. 19, Issue 15). <https://doi.org/10.3390/ijerph19159535>
- Salminen, S. (2012). Are Immigrants at Increased Risk of Occupational Injury? A Literature Review. *The Ergonomics Open Journal*, 4(1), 125–130. <https://doi.org/10.2174/1875934301104010125>

## NEWS

# If's Nordic Business Travel Report now available

Business travel is on the rise, and companies face the challenges of increasing travel costs, ensuring employee well-being, and meeting sustainability goals. By utilising technology, prioritising health, and effectively managing risks, businesses can better prepare for potential losses, accidents, or incidents.

The business travel landscape is evolving rapidly, influenced by global events, regulatory changes, sustainability initiatives, and technological advancements. These diverse transformations require organisations to reassess their travel risk management frameworks, ensuring that employee safety measures are robust, adaptive, and aligned with regulatory and risk management standards.

When managing travellers and their safety, employers have a legal and ethical duty to identify and assess the risks and hazards employees may face during their journeys. Companies are required to establish various measures and strategies, as well as practical

guidelines, to mitigate potential risks and their impacts. Planning and implementing necessary services are essential for managing any incidents, accidents, or illnesses that may arise during business travel. This principle extends to travel safety management, where action and recovery plans are formulated for emergencies. It is crucial for companies to foster a proactive safety culture, which includes business travel. Adherence to the safety protocols should remain consistent and adapt accordingly, whether employees are traveling or working onsite.

The COVID-19 pandemic, ongoing conflicts such as the war in Ukraine, and environmental crises have profoundly changed global mobility,

compelling organisations to prioritise safety, adaptability, and sustainability. Moreover, the rise in remote work has shifted traditional travel patterns, promoting more flexible working arrangements and locations.

In response to these dynamic conditions, the demand for robust and adaptable travel-related services for globally mobile employees is at an all-time high. The increase in extreme weather events, such as hurricanes and wildfires, driven by climate change, also necessitates effective crisis management and adaptable travel policies.

This report seeks to provide insights into the significant shifts in both Nordic and global travel dynamics, including tightened travel



regulations, expanded sustainability policies, and a broader commitment to Duty of Care—encompassing mental health support and digital security for travelling employees. Geopolitical tensions, along with increased sensitivity to social and cultural issues, are driving critical updates to existing travel policies. Business travel continues to be a regular part of working life, with employees commonly travelling as a necessity in their day-to-day roles. For this reason, employers must carefully evaluate the potential risks associated with business travel, including health, safety, and security concerns, to ensure comprehensive risk mitigation strategies are in place.

Our report assesses the current state of business travel within the Nordics and globally, addressing evolving responsibilities and the need to maintain and update travel risk management strategies and insurance models. By consolidating analyses of real-world claims data, expert insights from insurance and risk management professionals, clients, and a global network of partners, we provide actionable recommendations to meet the diverse needs of employers and their travelling employees. ●



To access the report, simply scan the QR code.



## Short news

### NEW UNDERWRITING UNIT FOCUSING ON GREEN ENERGY AND CONSTRUCTION

If is putting more muscle behind our ambitions, with greater focus on this growing market area, as well as on our Green Energy ambitions. Industries and societies alike will continue to shift towards renewable energy sources and focus on sustainable solutions. Simultaneously, construction projects, and projects in general, are increasingly more sustainable, from wooden constructions to increased demand for the utilisation of renewable sources of power.



“As the market leader in the Nordics, we are in a unique position to support our clients with a strong international network, alongside experienced underwriters as well as in-depth green energy Risk Management competencies,”

Kristine Birk Wagner, If Group Senior Vice President & Head of Underwriting, BA Industrial explains.



IN THE NEXT ISSUE

How will hackers exploit artificial intelligence?

---

Securing cargo as geopolitical risks continue to increase

---

B2B insights from the Nordic Health Report 2025

---



Subscribe to Risk Consulting magazine and the monthly If Insights newsletter at [www.if-insurance.com](http://www.if-insurance.com)

Risk Consulting is If's professional magazine on risk management and loss prevention, and is one of the first client magazines in the Nordic countries

