
INTERNATIONAL
(RE)INSURANCE
REVIEW 2025/26
Beaumont Capital Markets
www.beaumont-capitalmarkets.co.uk

NORWAY

An overview of the cyber insurance landscape in norway: challenges and opportunities

KVALE

Kristian Lindhartsen
Partner

kli@kvale.no

+47 930 03 313

www.kvale.no

BIO

Kristian Lindhartsen is a seasoned expert in insurance law, with a specialised focus on the intricacies of maritime insurance. His expertise is particularly pronounced in the resolution of marine insurance disputes, where he adeptly handles complex cover disputes and direct-action cases that arise within the maritime sector.

Lindhartsen's proficiency extends to providing strategic advice to insurers, shipowners and charterers, guiding them through the nuances of marine insurance policies as they navigate operational challenges. His counsel is invaluable in matters pertaining to charterparties, contracts of carriage, and commercial agreements, all through the lens of insurance coverage and risk management.

With a strong litigation background, Lindhartsen brings a wealth of experience to the table when representing clients in insurance disputes before ordinary courts and in arbitration settings. His litigation strategy is informed by a deep understanding of insurance law.

KVALE

KVALE

Runar Kristing
Managing Associate

rkg@kvale.no

+47 482 96 123

www.kvale.no

BIO

Runar Kristing is an experienced lawyer specialising in insurance law, tort law and surety law. Runar has broad expertise in insurance law, covering most insurance categories and in particular liability, property and project insurance, as well as surety and cyber insurance.

In Kvale, Runar works interdisciplinary and with his background in risk management and insurance, he offers expertise in business and product development, project management and claims handling.

As a former claims manager, Runar has solid experience in handling large and complex cases, claims settlements and litigation.

In addition to his practical experience, Runar contributes to knowledge development and regularly gives lectures and courses on insurance, guarantees and risk management. Runar is a valuable and trusted partner for Norwegian and international insurance companies, policyholders and third parties. With his combination of analytical approach, practical experience and execution, he delivers results that protect and promote clients' interests.

KVALE

KVALE

Tobias Kilde
Senior Associate

tki@kvale.no

+47 400 13 157

www.kvale.no

BIO

Tobias Kilde is a key member of Kvale's insurance team, bringing experience to the table in advising clients on a broad range of insurance matters. His expertise has been sought after by numerous Norwegian entities for guidance on the intricacies of insurance policies and their application in various scenarios.

Kilde's proficiency is not limited to advisory roles; he has represented both insurers and insured parties in legal disputes, demonstrating his balanced understanding of insurance law in court settings. He possesses specialised knowledge in maritime claims and operational issues.

In addition to his insurance expertise, Kilde is well-versed in anti-corruption and compliance matters within Norway. He offers valuable insights and advice to both national and international clients, ensuring they navigate the complexities of regulatory compliance with confidence.

KVALE

An overview of the cyber insurance landscape in norway: challenges and opportunities

1. Introduction

In recent years, the rising frequency and severity of cyberattacks have brought cyber insurance into the spotlight as an essential element of corporate risk management strategies. Aon's 2023 Global Risk Management Survey list cyber-attacks and data breach as the number one global risk issues on industry leaders' mind[1]. Aon also predicts this to continue to be the number one risk into the next years.

> “
>
> Cyberattacks have proven to be a significant financial threat to businesses across Norway.

Norwegian businesses, both large and small, have increasingly fallen victim to sophisticated cyber threats, incurring substantial financial losses to mitigate the damages. Cyber insurance, also known as cyber liability insurance, is designed to assist organisations in managing the financial risks associated with cyber-related security breaches, data breaches, ransomware attacks, and other incidents.

This article provides an overview of the Norwegian cyber insurance market, highlighting its current challenges and shortcomings, such as pricing uncertainties, coverage limitations, and regulatory ambiguities. It also underscores the vulnerabilities that small to medium-sized businesses (SMBs) face when it comes to cyber threats and the evolving regulatory landscape that affects them.

KVALE

2. Overview of the market: Cyberattacks poses A Growing Financial Burden

Cyberattacks have proven to be a significant financial threat to businesses across Norway. One of the most notable recent incidents occurred on 18 March 2019, when Hydro, a leading international Norwegian aluminium producer, was hit by a large-scale cyberattack[2]. The attack, conducted using the LockerGoga ransomware, was designed to encrypt critical company data and demand a ransom in cryptocurrency. When the attack unfolded, it paralyzed Hydro's IT systems across its global network, with no one fully understanding the scope or potential consequences in the early stages. Senior managers were woken up in the early hours of the morning, and they had to respond quickly to contain the damage. Despite the pressure and uncertainty, Hydro made the decisive choice not to pay the ransom, realising that even if the attackers were paid, they would likely still have access to their systems.

Hydro's immediate response was to shut down all network links and servers, which meant employees couldn't access the company's central IT platform or its supporting infrastructure. With most of their systems down, employees were forced to rely on manual operations. The company faced significant production disruptions as many of its processes relied on the compromised IT platform. However, certain business areas, including Hydro's hydropower facilities, were largely unaffected because they were kept separate from the company's main IT systems, in compliance with Norway's emergency preparedness regulations. In other locations, employees had to quickly adapt to working without access to essential resources, such as customer lists and order books, using whatever means available to keep operations running.

1. The survey can be found here: https://assets.aon.com/-/media/files/aon/reports/2023/aon-global-risk-management-survey-key-findings-2023.pdf
2. For further coverage, see: https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/

The immediate financial toll of the cyberattack was substantial. While Hydro initially estimated the cost of the attack to be around 600 million Norwegian kroner, further assessments revealed that the total financial damage eventually ballooned to approximately 800 million kroner. This figure accounted for the full extent of the production delays, recovery efforts, and business interruptions. However, Hydro's decision to invest in cyber insurance provided some relief, with the policy covering nearly 780 million kroner of the total loss. This incident not only underscores the devastating monetary impact a cyberattack can have on a large-scale organisation, but it also highlights the importance of cyber insurance in mitigating the financial consequences of such a crisis.

Despite the scale of the disruption, Hydro's response to the attack ultimately helped the company learn important lessons about cybersecurity. The experience reinforced the importance of preparedness, from regular drills to robust backup systems, and the need for strong communication strategies. Hydro also recognized that reliance on fully automated systems could be problematic in the event of a cyberattack, as some of its facilities had to revert to manual operations to resume production. This reinforced the value of maintaining a balance between automation and manual control, ensuring that critical systems could still function even during a major technological crisis.

In another incident, Green Mountain, a Norwegian data centre provider with high-profile international clients such as TikTok, DNB, and DNV, was targeted by a phishing attack[3]. The attackers gained unauthorized access to the company's systems, which could have exposed third party data in Green Mountain's possession. This case underscores the growing risk faced by smaller companies, particularly those in the supply chain, which can be targeted by cybercriminals seeking access to larger organisations' networks.

The financial consequences of cyberattacks extend beyond direct costs such as system downtime and data loss. Companies may also face claims from severe reputational damage and third-party claims, including clients and the public sector, adding to the financial burden. Cyber insurance is intended to play a crucial role in helping businesses mitigate these types of losses, offering protection against an increasingly unpredictable and costly risk landscape.

3. Current challenges and shortcomings in the Norwegian Cyber Insurance Market

3.1 Lack of experience

Despite the growing recognition of cyber insurance as a critical risk management tool, the Norwegian market is facing several challenges due to its relative immaturity and limited experience in addressing cyber threats. According to the Cybercrime Survey 2023, [4] a significant concern for insurers and policyholders alike is the lack of sufficient expertise in the field of cybersecurity. This lack of experience has led to uncertainties in various aspects of cyber insurance, including pricing, liability caps, coverage scope, and regulatory compliance.

“

Green Mountain, a Norwegian data centre provider with high-profile international clients such as TikTok, DNB, and DNV, was targeted by a phishing attack.

3. For further coverage from Norwegian news source: https://www.nrk.no/innlandet/dataangrep-mot-green-mountain-1.17091888
4. The survey can be found here: https://bcfc.dk/wp-content/uploads/2023/11/cybercrime-survey-2023.pdf

3.1. Pricing Uncertainties

Another pressing challenges facing the Norwegian cyber insurance market is the uncertainty surrounding pricing. Insurers struggle to accurately assess the potential monetary impact of cyberattacks due to the rapidly evolving nature of cyber threats and the limited data available on the actual losses incurred. This results in risk-averse pricing, which can make cyber insurance prohibitively expensive, especially for small to medium-sized enterprises (SMBs). The lack of comprehensive historical data on cyber incidents further exacerbates the difficulty in setting premiums that accurately reflect the true risk of cyberattacks, transferring this risk to the customer by pricing in the uncertainty.

> “
>
> A recurring issue with cyber insurance products is the lack of clarity in the conditions and policies that govern coverage.

3.2. Coverage Limits and Liability Caps

In the Norwegian cyber insurance market many insurance policies offer limited coverage, particularly in terms of liability caps. In many cases, the liability caps on Norwegian cyber insurance policies are too low to fully cover the costs of large-scale cyberattacks. Additionally, insurers often exclude coverage for significant loss items, such as third-party loss claims or indirect losses, which further limits the effectiveness of the coverage.

As a result, larger Norwegian companies often seek coverage from international insurers who are more willing to assume greater risks and offer higher coverage limits. However, accessing these international markets can be difficult, particularly for smaller businesses that may not have the necessary broker connections or expertise to navigate the complex landscape of global cyber insurance offerings.

3.3. Ambiguities in Coverage Conditions and Policies

A recurring issue with cyber insurance products is the lack of clarity in the conditions and policies that govern coverage. Coverage conditions refer to specific requirements that must be met for an insurance policyholder to be eligible for compensation under a cyber insurance policy. For example, if a policyholder has not implemented the necessary cybersecurity measures such as firewalls, antivirus software, or regular data backups, the insurer may deny coverage for any losses resulting from a cyberattack.

Policy for coverage refers to the rules that allow insurers to adjust or reduce the financial compensation in the event of a claim. For instance, if the policyholder has contributed to exacerbating the damage (for example, by delaying incident response actions). In other cases some insurance companies operate with a panel requirement, meaning that coverage for incident response services is only provided if the policyholder uses providers pre-approved by or in partnership with the insurer. This raises interesting regulatory questions about whether an insurer can deny coverage if the policyholder’s use of a non-panel provider actually limited the loss.

These ambiguities in coverage conditions and policy adjustments can create significant challenges for both insurers and policyholders, especially for small and medium-sized businesses that often lack the technical expertise to understand the intricacies and meet the specifics of cybersecurity requirements.

3.4. The Vulnerability of Small to Medium-Sized Businesses (SMBs)

SMBs represent a particularly vulnerable target group in the face of rising cyber threats. Not only are these businesses directly exposed to cyberattacks, but they are also often used as a gateway for cybercriminals to breach larger organisations' networks. According to the Cybercrime Survey 2023, over 50% of cyberattacks are conducted through third-party channels, making SMBs both direct targets and indirect threats to their larger business partners.

The vulnerability of SMBs underscores the importance of robust cybersecurity measures and comprehensive cyber insurance policies to protect against the growing risk of cyberattacks. Unfortunately, many SMBs in Norway face significant barriers when it comes to accessing affordable and sufficient cyber insurance. This is largely due to the immaturity of the Norwegian cyber insurance market, which has yet to fully cater to the unique needs of smaller businesses.

In the yearly threat report of the Norwegian Police Security Service, the rapid evolvement of how cyberattacks are carried out, is highlighted as one of the main issues related to cyber security. [5] Staying at the forefront of cyber security requires in depth and up to speed knowledge of the cyber security landscape, which often requires resources which can be challenging to muster for SMBs.

Additionally, the rapidly evolving regulatory landscape, driven by initiatives such as the NIS2 Directive, is adding further pressure on SMBs to develop effective cybersecurity practices. The NIS2 Directive is an EU directive imposing stringent cybersecurity obligations on entities classified as "important entities," requiring them to establish risk management processes and report serious cyber incidents. These requirements also apply to SMBs. Non-compliance can result in substantial fines, potentially reaching up 1.4% of global turnover. The directive also holds top management personally accountable for cybersecurity failures, with the possibility of criminal sanctions for gross negligence. The directive came into effect on 18 October 2024, in the EU, and will be incorporated into Norwegian law within the upcoming years.

These developments highlight the growing importance of cyber insurance for SMBs, not only as a financial safety net but also as a key component of comprehensive risk management. However, as previously mentioned, the current challenges in pricing, coverage, and regulatory requirements make it difficult for many SMBs to access the protection they need.

3.5. Conclusion

In conclusion, the cyber insurance market in Norway faces several challenges that limit its effectiveness, particularly for small to medium-sized businesses. The issues of pricing uncertainty, limited coverage options, and regulatory ambiguities must be addressed in order to ensure that businesses, regardless of size, have access to the protection they need to mitigate the risks of cyberattacks.

“

In the yearly threat report of the Norwegian Police Security Service, the rapid evolvement of how cyberattacks are carried out, is highlighted as one of the main issues related to cyber security.

There is a clear and growing need for more accessible, comprehensive, and transparent cyber insurance solutions from Norwegian insurance companies, particularly for SMBs, who are increasingly exposed to cyber threats. Addressing these challenges will require collaboration between insurers, policyholders, and regulatory bodies to create a more mature and effective cyber insurance market in Norway.

5. The report can be found here: https://www.pst.no/globalassets/2024/nasjonal-trusselvurdering-2024/nasjonal-trusselvurdering-2024_uuweb.pdf

4. Kvale's Expertise in Cyber Insurance and Cybersecurity

Kvale stands out as a go-to legal advisor in the Norwegian cyber insurance market due to its deep expertise in both insurance law and cybersecurity. By fronting a multidisciplinary collaboration between legal experts and cutting-edge data technology providers, Kvale offers a holistic and effective approach to cybersecurity, ensuring that its services are not only comprehensive but also seamlessly integrated. This unique synergy allows Kvale to assist clients in navigating the complexities of the ever-evolving cyber insurance landscape with greater precision and foresight. Especially in an environment where challenges such as pricing uncertainties, coverage limitations, and regulatory ambiguities are common, Kvale's integrated strategy positions clients to effectively manage and mitigate cyber risks while remaining compliant with the latest legal standards.

“

Kvale stands out as a go-to legal advisor in the Norwegian cyber insurance market due to its deep expertise in both insurance law and cybersecurity.

Kvale leverages its comprehensive expertise to adeptly assist all market participants through every phase, including the drafting of policies, initiation of insurance relationships, and the effective management and recovery of incidents and claims, ensuring a seamless and informed experience across the entire spectrum of insurance processes.

The firm's commitment to staying ahead of regulatory developments and offering innovative solutions to address gaps in the market further solidifies its reputation as a trusted partner for businesses seeking to navigate the complex cyber insurance terrain in Norway.

KVALE

Kvale is a top legal advisor in Norway's cyber insurance market, blending expertise in insurance law and cybersecurity.

By partnering with data technology providers, Kvale offers a seamless, integrated approach to help clients navigate challenges like pricing, coverage gaps, and regulatory complexities.

Supporting at every stage — from policy drafting to claims management — Kvale ensures clients stay ahead of regulatory changes and effectively manage cyber risks with innovative solutions, making us the trusted partner in a fast-evolving landscape.

Kvale, a leading Norwegian business law firm with over 110 lawyers, assists Norwegian and international clients, whether they are large companies or smaller enterprises. Additionally, we provide assistance to public authorities and organizations.

www.kvale.no/en/