

Nordic Cyber Insurance Claims Overview 2018

Over the past couple of years, the number of cyber incidents has increased, and the data protection regulations have gotten tougher, especially in Europe with the introduction of the GDPR in 2018. In 2018, we experienced a strong growth in the demand for cyber insurance and expect growth to continue in 2019 as the awareness, attention and interest around cyber will continue to increase.

Key Cyber Insurance Claims Statistics in 2018

In 2018, our seasoned team of cyber claims handlers in the Nordics handled over 30 claims notifications which is approximately a 50 % increase compared to 2017. The most frequent types of claims are different types of security failures, such as data breaches, phishing attacks, malwares, extortions and DDOS attacks, representing almost 90 % of all of the claims notified to AIG Nordics during 2018. This is in line with the general perception that cyberattacks have increased in frequency and severity during the last couple of years with several high profile breaches. Our insureds are most frequently facing data breaches, which may affect personally identifiable information. Phishing attacks along with hacked email accounts represent a significant portion of attacks as well. The most common industries where we experienced claims in 2018 were manufacturing followed by business services and hospitality. Financial institutions and professional services are also represented with several claims.

AIG's offering

As a leading provider of cyber insurance in the Nordics with around 500 policyholders we have the experience of handling different types of cyber claims in a variety of industries and geographies. AIG was one of the first carriers to provide cyber insurance in the Nordics and have built a strong team of dedicated cyber underwriters and developed our cyber product to fit the needs of our clients in an evolving market. Our First Response providers, involving top-tier law firms, IT- and forensic consultants and public relations firms, are always ready to help our clients to manage incidents. Several claims have been solved under the First Response time, which shows the importance of this module under AIG's cyber insurance. The First Response module usually triggers without retention, making it an attractive coverage for insureds since they get immediate access to a range of consultants. However, there are also several incidents that continue beyond the initial First Response time, where our consultants continue assisting our clients and where some clients even experience a loss of profit.

AIG's loss prevention services have been appreciated by our clients and the most frequently used services have been the BitSight Security Ratings, the Employee E-Learning and the Infrastructure Vulnerability Scan. We encourage our insureds to contact us if they are interested in our loss prevention services or if they would like to know more. As result of an increasing interest around cyber insurance and the increasing number of insureds, we have hired a cyber risk specialist in the Nordics who will help identifying key risk factors and support our clients to manage their cyber exposures.

