Many companies are not protected against cyber attacks

The risk of being exposed to a cyber attack is sky-high, but many companies have neither the necessary IT security nor cyber insurance, even though insurance prices are at rock bottom.

By Martin Wex

The consequences of a cyberattack can be so serious that, in the worst case, it can threaten the very existence of the company. Nevertheless, the analysis 'Digital security in Danish SMEs, 2024' by the Danish Agency for Public Security shows that 40 percent of small and medium-sized enterprises have a digital security level that is too low in relation to their risk profile, and that 44 percent of companies have experienced at least one IT security incident in the last 12 months.

> “
>
> The cyber threat to Danish companies is very high, and digital developments in areas such as artificial intelligence have given fraudsters new opportunities to carry out cyber attacks
>
> **Brian Fabricius** | Senior Cyber Specialist, WTW

»The cyber threat to Danish companies is very high, and developments within artificial intelligence have given fraudsters new opportunities to carry out cyber attacks with even modest means. It is therefore worrying that so many small and medium-sized enterprises are not adequately protected against cyber attacks,« says Senior Cyber Specialist Brian Fabricius from Willis, a WTW company.

The analysis from the Danish Agency for Public Security also shows that 15 percent of small and medium-sized enterprises do not implement basic measures such as updating software and backing up data. This is despite the fact that, according to the analysis, 60 percent of companies would be unable or only minimally able to perform their core tasks if they were to lose connection to their central internal IT systems.

»If, for example, a service company is subjected to a cyberattack that puts the company's booking and payment systems out of commission, the company risks both its revenue base and its existence,« says Brian Fabricius.

New threats

The rapid technological advancement of artificial intelligence (AI) and so-called deepfake technology has given criminals entirely new opportunities to imitate company executives in both voice and appearance, increasing the risk of employees being tricked into transferring money or handing over data to fraudsters.

© WTW Oktober 2025

»We are seeing more and more examples of employees participating in a Teams meeting where they think they are talking to their boss, but in reality, it is a fraudster using AI to imitate the boss. This can be very convincing because the fraudsters can use videos and voice recordings taken from the company's official social media accounts, for example. AI technology can therefore be used as a tool to create credible forgeries with uncanny precision,« says Brian Fabricius.

He also sees a significant increase in the number of so-called supply chain attacks, where instead of going directly after the company, fraudsters try to target the company's suppliers and partners, where the attacks can affect more companies and thus hit harder.

Lower prices for cyber insurance

Despite the increased risk, according to Brian Fabricius, less than a third of small Danish companies currently have cyber insurance, even though cyber attacks today affect a wide range of industries and companies of all sizes. However, he is seeing increasing demand for cyber insurance in line with the stricter documentation requirements for cybersecurity imposed on European companies, not least by the EU's NIS2 directive.

> “
>
> Companies that can demonstrate robust systems and solid insurance coverage are in a stronger position with customers and investors
>
> **Brian Fabricius** | Senior Cyber Specialist

»More companies are seeking our help because they are facing increasing demands from the authorities and their own customers, but also because cybersecurity has become a key competitive factor. Companies that can demonstrate robust systems and solid insurance coverage are in a stronger position with customers and investors. Therefore, the question is no longer whether companies can afford to buy cyber insurance, but whether they can afford not to,« says Brian Fabricius.

The good news is that it is not only demand that has increased but also supply. Several insurance companies now offer cyber insurance, and the increased competition is pushing prices down.

»The cyber insurance market has matured to such an extent that many insurance companies are now willing to insure almost all new customers, even if they do not yet have complete control over their cyber security,« says Brian Fabricius.

He expects cyber insurance prices to fall by around 10 percent overall during 2025. And companies that can demonstrate a high level of digital security have a good chance of obtaining better prices.

A customized insurance product

Cyber insurance has also proven to be a good investment for companies that have taken out insurance through Willis and subsequently experienced a cyber attack. Figures from Willis' Cyber Claims database show that in the first half of 2025, 92 percent of reported cyber claims were covered. According to Brian Fabricius, this is significantly higher than the average for other insurance products.

Willis has also created an insurance facility that combines cyber insurance and crime insurance, giving even smaller companies access to attractive prices and broad coverage that suits their needs.

The price depends on turnover and coverage needs:

- Price for turnover below DKK 50 million: from DKK 3,400 per year
- Price for turnover above DKK 50 million: from DKK 7,600 per year

Contact your usual advisor at Willis to find out more about how we can contribute to your cyber security.

© WTW Oktober 2025