Personal data has become the most important currency for hackers

Cyber attacks are ultimately about money, but the path to that goal increasingly involves the theft of personal data.

By Martin Wex

DKK 25 million. That is the average cost of a data breach. This is according to Willis' Cyber Claims Intelligence Report 2025, which is based on more than 4,600 cyber incidents in 90 countries between 2013 and 2025. Data breaches are the most frequently reported and also the most expensive type of cyber incident.

»Like so many other things, hacking has become a business, which is why most cyber attacks are about money. To that purpose, personal data is the hackers' currency, as it can be resold or used to extort money from the company,« says Senior Cyber Specialist Brian Fabricius from Willis, a WTW business.

According to Microsoft's Threat Intelligence Report 2025, more than half of all cyber attacks are about money – and in 80 percent of cases, hackers specifically target personal data.

> “
>
> Every year, we help hundreds of companies that have been exposed to cyber attacks, and it turns out time and time again that the weakest link by far is poor IT maintenance
>
> **Morten von Seelen**
> Vice President, Trusec

»Traditionally, it has been the larger companies with large quantities of personal data that have been targeted by hackers, but in recent years, smaller companies have been increasingly exposed to attacks, so that according to *Orange Cyberdefense*, cyber attacks are now evenly aimed at small, medium, and large companies,« says Brian Fabricius.

Focus on IT systems

The increased risk of being exposed to a cyberattack places growing demands on IT security, and according to Morten von Seelen, Vice President at Truesec, Willis' partner and expert in cybersecurity, it is particularly important to focus on the company's IT systems.

»Every year, we help hundreds of companies that have been exposed to cyber attacks, and it turns out time and time again that the weakest link by far is poor IT maintenance. Therefore, it is our clear recommendation that companies focus first and foremost on keeping their IT systems up to date so that the risk of a successful attack is minimized, and that they monitor the use of their systems so that any illegal intrusion is detected quickly,« says Morten von Seelen.

Brian Fabricius from Willis agrees but also believes that backups are the foundation of a company.

»It is crucial for a company's ability to resume operations after a cyberattack that all data is backed up and that this is done on an ongoing basis. My principle is that backups should be made according to the 3-2-1-0 model. This means three backups at two different locations, at least one of which is offline so that it cannot be hacked, and it is important that there are zero errors when the backup is used to restore data,« says Brian Fabricius.

However, it is not enough to keep track of your own IT security. According to Willis' Cyber Claims Intelligence Report 2025, half of all data breaches occur via third parties such as suppliers who operate systems and store information for the company.

»We are seeing a significant increase in so-called ‘supply chain attacks’, where instead of going directly after the individual company, attempts are made to target suppliers. It is therefore important not only to maintain a high level of IT security, but also to monitor the IT security of suppliers,« says Brian Fabricius.

Insurance makes a difference

Many companies now have cyber insurance, which covers their costs for restoring operations and paying any ransom, and they can also receive coverage for their operating losses while production is at a standstill. This is valuable coverage, but cyber insurance offers much more than just compensation.

> “
>
> Cyber insurance has become a ‘license to operate’ for many companies because their clients and partners see cyber insurance as a requirement for working together
>
> **Brian Fabricius**
> Senior Cyber Specialist, Willis

»If you are exposed to a cyber attack, cyber insurance gives you access to emergency assistance from a highly qualified team of cyber experts who have the necessary knowledge and experience to extinguish the digital fire and limit the damage as much as possible. There are also lawyers ready to help ensure that the company complies with all the rules that apply in the event of a data breach,« says Brian Fabricius.

However, he still believes that far too many companies do not have cyber insurance – and this could prove to be a problem, as cyber insurance has in many cases become a necessity.

»Cyber insurance has become a ‘license to operate’ for many companies because their clients and partners see cyber insurance as a requirement for working together. Cyber insurance provides the assurance that even if disaster strikes, the company will likely survive despite it,« says Brian Fabricius.

The good news is that more and more insurance companies have started offering cyber insurance, and according to Brian Fabricius, the increased competition has led to both lower prices and better terms for clients.

Another piece of good news is that figures from Willis' Cyber Claims database show that companies that have taken out cyber insurance through Willis and subsequently reported a claim to the insurance company have received coverage for 92 percent of the reported cyber claims.