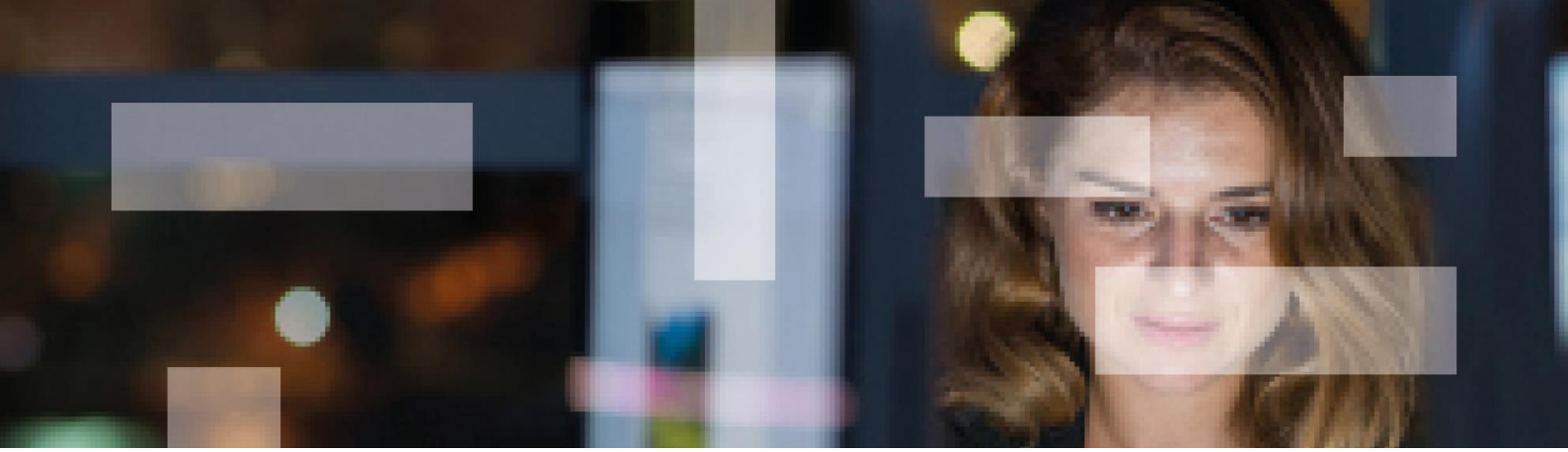

Data breaches often occur due to human error

Technical investigations and external consultants are the main expenses covered by the cyber insurance, according to a Willis Towers Watson study of cyber claims from around the world.

By Kristine Seest

From 2013 to 2019, Willis Towers Watson reported 1,200 cyber claims from across the globe on clients' cyber insurance policies. Data breaches – where the company intentionally or unintentionally destroys, loses, alters or transmits personal data – are the most common causes for damage claims.

»Data breaches are mainly due to human error – typically when an employee by mistake gives unauthorized people, from inside or outside the company, access to personal information. These mistakes can easily happen and are associated with large costs for the company. Companies need to perform critical reviews of their risks, procedures and internal communication on cyber threats,« says Cyber Risk Expert Tine Simonsen from Willis Towers Watson.

> Companies need to perform critical reviews of their risks, procedures and internal communication on cyber threats

When damage occurs, technical investigations are necessary and external IT consultants often need to be recruited. These services are the largest items of expenditure and having the right cyber insurance to cover the cost is therefore of great importance. This is one of the conclusions in Willis Towers Watson's Cyber Claims Analysis Report on cyber damages reported from 2013 to 2019.

Damages and insurance coverage

The report shows that 71 percent of the average loss associated with data breaches is covered by the cyber insurance. And cyber insurance covers 75 percent of the operating loss and the cost of re-establishing data and software.

»When companies have experienced problems with coverage on their cyber insurance, there have typically been two scenarios: The company has either made use of IT suppliers that the insurance company was not informed of when the insurance policy was taken out or the company has acted on the damage and thus incurred expenses without the insurance company's consent,« says Tine Simonsen.

Preparing for cyber insurance

It is Willis Towers Watson's experience that larger companies have a professional approach to cyber risk management, while smaller and medium-sized companies have less focus on the company's cyber security and risk management.

Companies that are looking to take out their first cyber insurance may be surprised by the demands made by the insurance companies. Therefore, it is helpful if the company, in preparation for tendering its cyber insurance, can answer the following questions:

- Do you have a Business Continuity Plan and an Incident Response Plan in place?
- What sensitive / confidential data do you store or process?
- Can you present an overview of your IT network – including the environment and segregation of IT?
- What procedures for awareness training or campaigns have you targeted at your employees?
- What IT policies apply to your employees?
- Which IT strategy applies?
- What backup solution do you have? And how often is backup taken?
- Is End Point Detection implemented on all servers?
- Do you have an automated Patching?
- Do you monitor your network through a Security Operations Centre (SOC)
- Have you implemented Multi Factor Authentication (MFA) on all external accesses to the company's systems?
- How can Willis Towers Watson help?

Willis Towers Watson helps companies assess their cyber risk and security level as well as to deal with cyber damages by offering services that include:

- Scenarios of the company's cyber risks and estimate of the potential financial losses in case of a cyber incident
- Action plans for cyber incidents
- Review, advice and design of IT organization setup, Cyber Risk Management and Business Continuity Planning