LLOYD'S

Facing the cyber risk challenge
Key highlights for Germany

To read Lloyd's full report of Facing the cyber risk challenge, visit lloyds.com/cyber

Today, almost every business, regardless of size or location, relies on digital technology. While it helps companies become more efficient, reduces their costs and opens up new markets, it also makes them more vulnerable to cyber risks.

Companies can lose business, face litigation, see share prices tumble and have their reputations destroyed if they fall foul of a cyber incident.

Regulations are also getting tighter. In 2018, the European Union will introduce the General Data Protection Regulation (GDPR), which will set rigorous requirements for any businesses that deal with European consumers' data and impose severe financial penalties on those companies that break the rules.

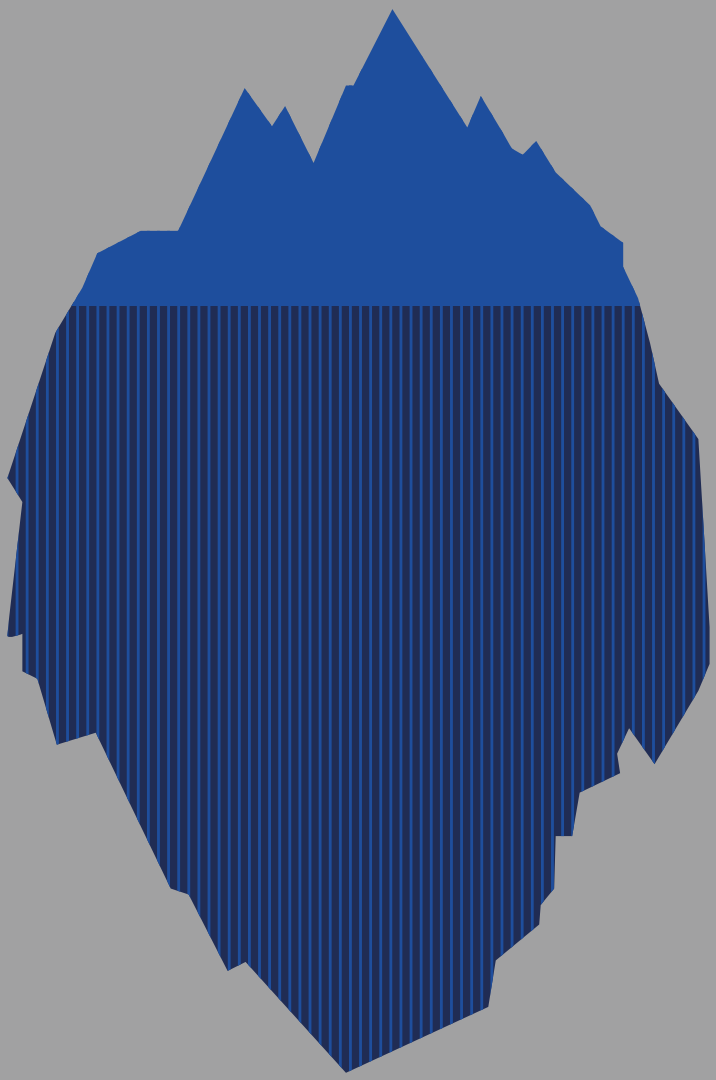
Lloyd's, as the global centre for cyber insurance with a range of insurance products that help protect against the consequences of cyber threats, has unique insight into this fast-changing risk landscape.

We commissioned a survey of nearly 350 decision-makers in European companies with revenues of €250m or more to find out how they are preparing for the GDPR and their level of awareness of its consequences, what they are doing to tackle cyber security and their knowledge of how cyber insurance can help protect their business.*

False sense of cyber security

24%
Businesses are concerned about a future data breach

86%
Businesses experienced a data breach in the past five years



Implications for businesses

Impacts German businesses are most concerned about:

52%	Financial penalty
48%	Impact on profit
43%	Investigation by a regulator
10%	Yet a low number believe they could lose their customers as a result of a data breach

Biggest threats German businesses believe could result in a data breach

Hacking for financial gain	53%
Human error	50%
Ransomware	47%

A new era of cyber regulation

97%
Businesses have heard about the new EU regulation - GDPR

68%
Businesses know little or nothing about the new EU regulation - GDPR

Boardroom taking responsibility

47%
CEOs that drive decisions for protection and planning for a data security breach

88%
Businesses with C-suite involvement in decisions for protection and planning for a data security breach

* The survey of nearly 350 senior business decision makers from across Europe included 34 from Germany

Turning to the experts
How insurance at Lloyd's can help

Cyber is the most complex, current and critical risk businesses face today: it is a matter of "when" not "if" a business becomes a victim of a cyber incident.

At Lloyd's, customers have the greatest choice and variety in one market for their cyber insurance needs. 65 Lloyd's insurers offer insurance solutions that can be tailored to meet the needs of each client.

The Lloyd's market offers a variety of cyber policies, covering everything from financial pay-outs after a cyber-attack and on-the-ground support during the period of crisis, to business interruption, pre- and post-breach risk management, and helping businesses to deal with operational, financial and reputational impacts.

To find out more and contact a Lloyd's cyber broker visit, lloyds.com/cyber

Lloyd's syndicates offering tailored cyber insurance products

65

€ million capacity for cyber insurance

356*

Typical cyber products at Lloyd's

Notification

Coverage includes the costs of notifying third parties (normally customers) that are potentially affected by a data breach. This includes all associated PR, customer service and legal costs. It also covers the cost of IT forensic investigation to assess the cause of the breach and to ascertain who to notify in the first place.

Liability

Includes liability to customers, clients, and employees for breaches of their private information. It also includes costs for lawsuits and class actions, all legal defined costs.

Regulatory

Covers all the costs that result from defending against regulation breaches.

Loss of income caused by network and business interruption

Covers the costs of business lost due to an interruption of a business' computer systems- as well as any additional expenses incurred. This includes the cost of restoring a company's websites if it has been taken down.

Extortion

Covers the costs of "ransom" if a third party demands payment to refrain from publicly disclosing or causing damage to a company's confidential data. Extortion usually comes from DNS attacks.

Reputational harm

Covers the financial losses incurred by customers terminating contracts with a business, as a result of a cyber breach. It does not include any predicted future financial repercussions such as losing new business to the competition.

* Conversion as of 12 Sept 2016