LLOYD'S

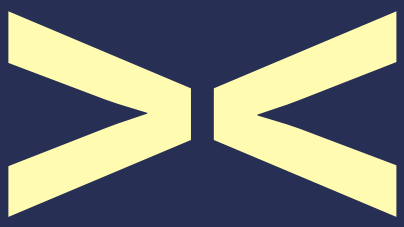
Closing the gap

Insuring your business against evolving cyber threats

June 2017

Executive summary

In association with KPMG and DAC Beachcroft



KPMG

DAC beachcroft

Executive summary

1.1 Overview

Over the past few decades the internet has enabled extraordinary innovation to take place, creating new business models, giving rise to world-changing companies and generating millions of jobs.

But this progress has come at a cost. By their nature, digital systems are susceptible to cyber-attacks by malicious individuals or groups with increasingly serious repercussions for businesses around the world. The nature of the threat is evolving so fast that it is becoming more and more difficult for organisations to counter it.

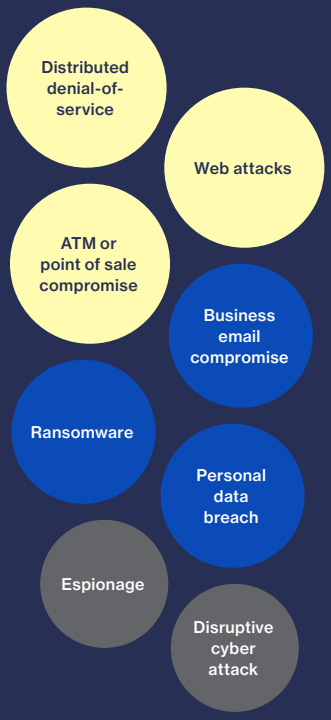
But while the threat is becoming more complex, many business leaders lack awareness about the cyber threat. A recent Lloyd's survey of more than 350 senior decision-makers across European business revealed that although 92% of businesses had experienced some form of cyber breach in the past five years, only 42% were worried that another incident could happen again in the future.

This Lloyd's report, produced in association with KPMG in the UK, international law firm DAC Beachcroft and Lloyd's insurers, helps companies understand the cyber threat better.

The first part of the report offers a unique assessment of the various cyber threats facing companies today, broken down by sector (an example for financial services is displayed here), and looks at ways to mitigate them. It also details the full financial impacts of data breaches and analyses some of the costs associated with recent high-profile cyber-attacks.

The second part looks at four reasons why companies need to raise their game when it comes to tackling cyber risk and offers expert insight from Lloyd's cyber insurers on some of the ways they can do this.

Financial services sector risks



- Primarily targeted
- Frequently targeted
- Occasionally targeted
- Rarely targeted

(The order of the circles in the same category does not indicate relative frequency.)

To view in full the report's unique sector-by-sector analysis of the cyber threats facing businesses today visit lloyds.com/cyberriskinsight

Sectors covered include:
- Education
- Financial services
- Healthcare
- Hospitality
- Information technology
- Manufacturing
- Media and entertainment
- Oil and gas
- Professional services
- Public Sector
- Retail
- Telecommunications
- Transportation
- Utilities

For more information on these threats, read Lloyd's full 'Closing the gap' report at lloyds.com/closingthegap

1.2 Key findings

The types of cyber-attacks against businesses vary from sector to sector and are constantly evolving. For example:

- There has been a major growth in targeting companies through CEO fraud, which is resulting in significant financial losses.
- The financial services sector finds itself at the sharp end of targeted attacks by organised cyber-crime but retail is increasingly being targeted.
- Professional services firms such as lawyers and accountants are increasingly targeted as a gateway to attacks on their clients, which are often large corporates.
- Ransomware and distributed denial-of-service attacks are increasingly used against businesses with healthcare, and media and entertainment particularly targeted.
- The public sector and telecommunications sectors are highly susceptible to espionage-focused cyber-attacks.

Businesses need to be aware of the full costs of a cyber-attack, in particular, the "slow-burn" costs (i.e. those associated with the long-term impacts of a cyber-attack, such as the loss of competitive advantage and customer churn). When added to immediate costs (i.e. legal and forensic investigation fees, and extortion pay outs), slow burn costs can dramatically increase the final bill.

There are four factors that aggravate the damage caused by cyber-attacks, making it all the more important that businesses mitigate their cyber risks and improve their cyber security:

- Higher penalties for companies that breach cyber-security rules as set out in forthcoming European legislation.
- Cyber-breach victims' greater willingness to sue companies that have lost their data.
- Increased responsibility for cyber security in the supply chain.
- Greater vulnerability through the increasing use of connected devices (the internet of things).

1.3 Next steps

Lloyd's is home to more than 70 insurers who offer cyber insurance cover. Based on unique and expert insight from the Lloyd's market, the report highlights four key ways in which businesses could prepare for and mitigate the cyber threat:

1. Understand the specific threats to your company, including both the immediate and slow-burn costs – everything from reputation as perceived by customers and the value of the data held, to supply chain vulnerabilities and business-leader profiles.

2. Evaluate both current and future threats: underwriters will evaluate both so they can offer you the insurance cover that best suits your needs.

3. Ensure all employees, including management, have a comprehensive understanding of the cyber threats your company faces and promote a cyber-risk management culture.

4. Seek expert help when it comes to arranging cyber insurance to ensure that your risks are adequately covered.

6 Conclusion

The cyber threat is evolving on a daily basis so companies must be better prepared for the consequences of a cyber breach. Not only are the costs – both immediate and slow-burn – likely to increase with the introduction of new European legislation but the number of ways companies can be targeted is increasing.

While it is not possible to be 100% secure from a cyber-attack, there are a number of measures companies can take to reduce the risk of it happening – and to help ensure they minimise the consequences and recover more quickly should a breach occur.

Insurance is part of this solution. Every day, Lloyd's specialist cyber underwriters work with thousands of companies, from multinationals to SMEs, across the world to understand their risks better and to provide them with the expert advice and insurance cover they need.

To read Lloyd's full 'Closing the gap' report visit **lloyds.com/closingthegap**

To find out how Lloyd's insurers can help you, visit **lloyds.com/cybercover**

Sector Attack Chart: Source Data