CITYNET
LLOYD'S BROKER

DATA BREACH CYBER CLAIM

The company is a prominent e-commerce platform that sells a wide range of travel packages online. They store sensitive customer information, such as names, addresses, payment details, and login credentials, on their servers.

DESCRIPTION OF BREACH

Hackers exploited a vulnerability in company's website's security and have diverted the company's website to a false site where payments were made directly to attackers. This way the thieves gained access to sensitive information such names, street addresses, email addresses, credit card numbers, expiration dates and card security codes, enough to allow them to steal from accounts. The breach was detected by company's cybersecurity team during a routine security check in September 2018.

EXTENT OF DATA COMPROMISED

- Names and contact information (address, emails)
- Payment card data (credit/debit card numbers, expiration dates, and CVV codes)
- Encrypted passwords of 4 million customer accounts.

IMMEDIATE ACTIONS TAKEN

- The company immediately took their website offline to prevent further data exposure.
- They notified affected customers via email about the breach and advised them to change their passwords.
- The company hired a leading cybersecurity firm to investigate the breach and determine the scope of the data breach.
- The company informed regulatory authorities and relevant data protection authorities as per legal requirements.
- They cooperated with law enforcement agencies to identify and apprehend the perpetrators

COSTS AND DAMAGES

- Legal Expenses: The company hired a team of lawyers to handle the regulatory and legal aspects of the data breach, which was costly.
- Forensic Investigation: The cybersecurity firm conducting the forensic investigation also charged a sum for their services.
- Data Recovery: The implementing data recovery measures and improving security protocols cost the company also came at a cost.
- Customer Support: The company established a dedicated call centre to address customer concerns and enquiries, incurring a further cost.
- Customer Damages: The company apologised and reached an out of-court settlement with the victims of the data breach and will be paying thousands of customers and undisclosed sum.
- Regulatory Fines: The data protection authority imposed a fine of £20 million on the company for not having adequate security measures in place.

CONCLUSION

It is not known if the company had a cyber policy in place but even if it did, it might have not been enough to cover all the damages incurred. Please note that this example is based on the British Airways cyberattack occurred in September 2018.