Cyber-attacks are at the forefront of news, now seen as one of the largest and most crippling threats to business, constantly increasing in volume, success rate and sophistication.

Last month one of the UK's largest phone and broadband providers, TalkTalk, suffered a cyber-attack which resulted in attackers accessing personal and banking details of potentially up to four million customers.

This was not the first time TalkTalk had been the victims of cyber-attacks, however it was by far the most significant and sustained with an estimated one-off cost to the company of between £30m and £35m.

Looking at media reports on the BBC website, this event can be broken down to demonstrate how a cyber-attack occurs, the direct implications it has to the business and the need for cyber resilience.

Type of attack on TalkTalk

- DDoS attack overwhelms website servers
- Hackers steal confidential customer data
- Confirmed 157,000 of its customers' personal details accessed
- More than 15,600 bank account numbers and sort codes stolen
- CEO received email demanding ransom

Timing to communicate with customers and regulator

- CEO said the company was "rushing to communicate with customers" but that it would take 36 to 48 hours to email all of them.
- The Information Commissioner Christopher Graham told Radio 4's The World at One programme that TalkTalk should have alerted his office sooner
- CEO said "Potentially it could affect all of our customers, which is why we are contacting them all by email and we will also write to them as well."

Estimated Loss

CEO estimates one-off costs are between £30m and £35m - that's covering:

- response to the incident
- incremental calls into TalkTalk's call centres
- additional IT and technology costs
- online sales declined with lost revenue as a result
- in recognition of the uncertainty that this had caused customers, they would be offered an upgrade

Contractual issues and goodwill

- Customers who were financially affected directly will be free to leave TalkTalk without financial penalty
- Those who can't prove a financial loss will need to continue with their contracts
- Now going to have to reassure its customers that its security practices are robust enough to regain their trust

"Today's announcement reinforces **how significant the cost impact of this sort of event can be**. There can be **a very long cost tail** to these scenarios, **which may run for years** as new systems and processes have to be adopted and claims handled," she said.

This recent example is just one of hundreds of cases worldwide which demonstrates the need for businesses, large and small, to put strategies in place to protect themselves from cyber-attacks.

Insurance Response

The insurance market now provides dedicated policy wordings that can provide the following responses:

- Forensic investigations
- Legal and PR advice
- Communication and advertising (emails, letters, websites, media)
- Call centres costs
- Credit and reputation repair
- Loss of profit, normal operational costs (payroll) and extra expense
- Claims preparation costs (forensic accountants)
- Goodwill (vouchers/incentives)
- Ransom
- Third party liability claims (legal defence and settlement)
- Regulator investigations and fines

Preventing Cyber-attacks cost money - not preventing them costs more

Next steps

If you would like to discuss any of the issues raised in this article, or enquire about Cyber Insurance, please contact Lesley Kerr at Aon in the first instance.

Lesley Kerr
Executive Director
Phone: 09 362 9000
Mobile: 021 587 661
Lesley.kerr@aon.com