# Eight cyber risk scenarios

**1 – Social networking slip**
An employee who is responsible for the corporate Twitter or Facebook account accidentally writes an embarrassing or offensive update. The story blows up online before the company even realises there's a problem, leaving the company looking a little red-faced.

**2 – Social media gossip**
One or more persons or forums online start malicious rumours regarding a company's products or services. These rumours go viral, spreading worldwide and into the mainstream media, threatening a company's reputation.

**3 – Social media account hijacked**
Malicious hackers hijack a company's social media accounts (Twitter or Facebook) by guessing the account passwords. For a few hours of the day (while the account is in their hands), they write embarrassing and offensive messages.

**4 – Corporate website hacked**
A group of hackers attack a company's website because they are aggrieved by the company's recent actions or behaviour. Using distributed denial of service (DDoS) attacks, they manage to shut down the website for more than a day, causing serious disruption.

**5 – Cyber espionage**
A business competitor based in the Far East uses online channels to access and steal private company information pertaining to a new corporate strategy, investment or product. The incident threatens the victim's competitive edge and could even enable the attacker to leapfrog ahead in competitiveness.

**6 – Data loss**
A company mistakenly loses, through procedural error, the credit card information or personal details of a significant number (maybe millions) of its customers. The media gets hold of the story, because the company is required to fess up, and the incident severely tarnishes its corporate reputation.

**7 – Cyber theft**
A criminal organisation, based in eastern Europe, manages to break through a company's online defences and steals customer credit card information or personal data from its private database and posts them for sale online. Customers rapidly lose faith in the company's security systems and take their business elsewhere as a result.

**8 – Cyber war breaks out**
Two or more nations engage in all-out cyber war. A country in the Middle East attempts to disable its neighbour's computer networks and the neighbour threatens to respond with conventional warfare. As well as potentially disrupting the region's internet connections, effectively shutting down e-commerce, the conflict threatens to spill over into full-blown war.