It was the news feared in boardrooms everywhere - cyber criminals had compromised the systems of a major European company and stolen sensitive data. The incident happened in the morning, and by the afternoon, the insurance industry knew what was going on. By the evening, the cyber breach had become headline news globally, with significant potential implications for the business's reputation and brand.

In the wake of the attack, the business was criticised for not knowing the extent of the breach (which was not nearly as bad as had initially been feared); for the lack of information issued to its customers; and because it had been compromised previously.

Simon Creasey finds out the real cost of cyber attacks and IT outages, and how companies can minimise the risks.
According to business continuity experts, when managing interruption incidents of this nature the general objective is to ensure they remain just an event and not a headline. So how can companies that are victims of an IT outage or, even worse, a cyber attack, ensure they don’t become headline news? And if they are subject to an attack, what can they do to ensure the income loss to the business is minimised?

Attacks on the rise
Over the past decade the number of cyber attacks on businesses has grown significantly and, despite the best efforts of many business owners, a number of attacks have been successful. Over the same period, demand for cyber risk policies that include business interruption insurance to cover business income losses has risen so that companies can offset any losses.

But according to Paul Handy, head of global technical services for Europe and operational head of cyber risks at Crawford & Company, establishing the financial loss to a business isn’t a straightforward process, particularly as no two claims are the same. He breaks the nature of incidents into two areas: cyber attacks on, or losses stemming from an outage to, IT equipment or systems that are owned by the insured; and interruption or losses caused by the same set of circumstances at a service provider.

The more straightforward loss to establish is when, as a result of a hack or an ‘event’, a business’s systems are impacted or shut down. “There is a direct or tangible link between the attack and the insured’s ability to trade and therefore you can quite easily calculate the resultant business income loss,” says Paul.

Where it becomes slightly more complex is when a cyber event occurs that impacts on the brand or reputation of the business that may affect a company’s income stream because people no longer want, or are less inclined, to do business with that company.

“That’s a more complex calculation to do,” says Paul. “It’s not clear, it’s less tangible and more subjective. What we have to do is look at historical revenue streams and we build into that seasonality, trends and other circumstances that might impact revenue streams. Then we project that forward to determine what the business would have accrued, but for the incident. That enables us to calculate, or estimate, what the losses to the business might be.”

The other main element of business income loss is “dependent income loss”, which occurs when a service provider - for instance, a company that supplies a cloud database or offsite server - has an IT incident that results in lost revenue for its customers.

“You can control what happens and how you manage your own systems, but when it comes to your service providers, it’s one step removed and underwriters perceive this to be a major risk,” says Paul.

“There is a direct or tangible link between the attack and the insured’s ability to trade”
“They’re realising that they have to invest more heavily in intrusion detection and prevention software”

Ready for anything
While companies might not be able to control issues that occur at their service providers, what they can control is how they deal with these issues as and when they arise. How a company responds in the early hours of an incident can have a major impact on the extent of the losses, says Paul.

“These are brand-threatening events so the first 48 hours are critical in order to protect the business,” he explains. “If you sit on the problem these events can be catastrophic and the decisions you make at the early stage of a claim can have a massive impact on potential revenue losses.”

He adds that the earlier businesses such as his are called in to assist, the better the outcome. “We deal with many incidents where we get involved very early on and work with the insured to understand the nature of, and help them to respond to, any potential breach, bringing in our specialists when required,” says Paul. “We help manage the regulatory notification process in line with what are often differing or multi-jurisdictional guidelines and requirements.

“Coupled with the regulatory process, there is a need to carefully manage customer messaging and PR. Without dismissing the gravitas of a breach event and the potential impact on the individuals concerned, the approach adopted by a company in notifying and supporting their customers can have a direct impact on the propensity for litigation and, importantly, reduce the potential for negative publicity and the resultant detrimental impact on the business. Our experience is that, if these events are managed well, they needn’t have an impact on the business and can often fall away long before any claims or negative headlines are made against the organisation.”

Planning ahead
Pre-event planning is another way companies can offset the impacts if the worst-case scenario occurs.

“There is an absolute correlation between those businesses that are event ready and those that are not,” says Paul. “The results and the potential losses are greatly reduced at those companies that are event ready compared with those businesses that, when something happens, start scratching their heads.”

The good news is a growing number of businesses have already started to put in place some of the necessary measures to make themselves event ready, says Paul. It’s a view shared by Tim Stapleton, vice president, cyber insurance product manager, overseas general insurance at Chubb, who says that there has been an evolution in the way companies approach the area of business interruption.

“We’re starting to see a shift from front end defence systems to the back end,” says Tim. “So they’re looking at things like how quickly can we identify and remediate an issue like this? Firewalls, penetration testing, password protection - those are all front-end defence measures that companies use as a baseline, but we’re beyond that stage now. They’re realising that they need to invest more heavily in intrusion detection and prevention software and they need to invest heavily in encryption.”

This is just a taste of some of the wide range of different measures that companies are increasingly considering, according to Tim. “Others include how often do they back up data, can they switch to another server if they need to shut one down that’s been attacked, do they have a robust business continuity plan in place, do they have disaster recovery planning and how quickly could they bounce back from an event? Those are controls that companies are shifting towards,” he explains.

Cyber crime is a growing industry and it’s clear that the threat isn’t going to go away any time soon. Businesses that embrace these safeguards, together with the other measures outlined by Paul, are putting themselves in a strong position to react to an event when it does occur.

“There is a consistent way we deal with these events or claims. By applying a considered or project-managed approach to the event circumstances, it helps to reduce the risk and any corresponding or potential impact on the business,” says Paul. “By reducing the risk, you are immediately helping the business steer and manage itself out of that crisis.”

This ensures an event stays just that - an event and not a headline on the evening news.

Five tips
1. Don’t be complacent: no one is immune from IT outages or cyber attacks - governments, public bodies and private companies have all suffered from cyber-related incidents in recent years.
2. Always remember, the key to minimising the financial impact of these incidents is how you respond to the attacks.
3. Pre-event planning is vital - companies need to work out an instant response strategy for dealing with incidents and these plans need to be tested on a regular basis.
4. When an incident occurs, in addition to triggering the instant response plan, it’s also important that companies notify their insurance provider as soon as possible, because the decisions made at an early stage can have a significant impact on potential revenue loss.
5. Above all, the first 48 hours of any IT event are critical and a good insurance provider can advise companies on how to minimise their losses.