



Sony's business. The Federal Trade Commission in the United States could impose a requirement that Sony have an external security test across their business every year for the next 30 years. This would lead to considerable cost – some estimate in the region of US\$30 million plus. Clearly the investigation will not be an overnight exercise and the total clean-up cost is likely to be enormous.

While considerable, these losses are to a degree quantifiable. The unknown costs are more worrying.

### Law suits

Legal troubles may be looming. The Australian Privacy Commissioner opened an own-motion investigation into both the PSN and SOE data breaches. He has expressed concerns in particular about information being stored on an out-of-date database, which has only served to reinforce his view that organisations need to consider further limiting the amount of information they collect and store about people. It is currently a requirement of the Privacy Act that information be destroyed when it is no longer needed and there are a number of significant reforms to the Act currently being considered by the government.

Overseas, a Toronto law firm has announced a CD\$1 billion class-action suit against Sony for breach of privacy, naming a PlayStation user from Ontario as the lead plaintiff.

A lawsuit was quickly filed in the United States against Sony by a PSN user when the original breach was revealed. And a US senator is calling on the US Attorney General to probe whether or not Sony should be held criminally or civilly liable for losing its customers' personal information and, potentially, financial records.

These breaches have affected millions of people around the globe, so there is the potential for further lawsuits in Europe and Asia as well. The legal defence costs will be enormous, even if Sony proves to be successful and the class action(s) cannot prove damages in fact.

The company has estimated **the data breach will result in a**  
**US\$170 million**  
**hit to its operating profit.**

And the potential for contractual liability cannot be ruled out. If credit card data is affected then Sony could be liable under its merchant agreements for any fraud on the cards.

### The role of insurance

So will Sony be able to recover its losses from insurers?

Technology has revolutionised the way in which organisations do business, yet traditional insurance policies have not kept up with this evolving landscape. Firms could be mistaken if they assume that standard general liability or business interruption policies will respond.

A traditional property policy requires physical damage in order to be triggered, yet in the case of a hack attack the servers themselves are untouched – only the intangible property, the data, is affected. Business interruption policies share the same trigger, meaning that cover for Sony's direct loss of revenue is unlikely to be covered.

Nor is it likely that standard policies would meet the costs of employing crisis communication and PR experts to help shore up and repair the business' reputation. And while Sony has in fact been the victim of a crime, rather than gaining the sympathy of the public at large as you would expect, the accusing finger

is firmly being pointed in Sony's direction. The PR effort to win back the trust of its customers is going to be significant.

Privacy breach notification costs are not covered by traditional policies – and in the Sony case that cost will be considerable. Depending on the legal requirements of the individual states, territories and countries where customers have been impacted, Sony may well have not only had to write to every customer but undertaken advertising to ensure that customers are aware of the issue. While it is not required under current legislation, the Australian Law Reform Commission has recommended that consideration be given to the introduction of mandatory data breach notification laws – a call that has been echoed by the Queensland University of Technology's Information Security Institute.

It is likely, however, that Sony will attempt to recover third-party liability costs under one of its core liability policies. With large limits potentially available under Directors & Officers, Professional Liability and General Liability policies, it is likely that these insurers will be in the frontline. Previous case history does not bode well, however when it comes to making a claim for a privacy breach, as this type of event was never envisaged when these policies were first constructed, nor was it the intention to ever cover them.

A new breed of cyber insurance policies addresses the new type of risks faced by companies with a heavy reliance on technology. The vast majority of the losses described above, including business interruption, system restoration, privacy breach notification and privacy liability, are now insurable – and market capacity has never been greater. ✓