13 Oct 2022
Author: Joseph Lam
Article type: Publication
Page: 18
Australian, The
Readership: 472000
AVE: $11516.85



# Hacked companies' next cost: staff lawsuits

JANE DEMPSTER

**Robert Anderson Jr, in Sydney this week, says companies in the US that have been breached by hackers now find they are heading into a 'death spiral'**

JOSEPH LAM

Company chairs and chief executives may soon find themselves being sued by their own staff.

That's the view of former FBI cyber crime executive assistant director Robert Anderson Jr, who says North American companies that have experienced data breaches now find themselves heading into a "death spiral".

That's because the cost of dealing with class actions, representative claims and ransom amounts from hackers are being added to by employees suing their company and "the individuals that are responsible for protecting data".

"The big thing taking people by surprise is all of a sudden all your employees are suing you because you've lost all their personally identifiable information and their bank accounts are all compromised," he said.

"It really sends a corporation into a death spiral if you have not prepared for this. "The cost of the breach is nothing – it might cost $10m, $20m or $30m – that's nothing compared to what's coming at you after that."

Mr Anderson, now chairman of Dallas-based Cyber Defense Labs, said that, combined, lawsuits in the US were as much as a $1bn. He said the legal repercussions had become the biggest catalyst for change in how data breaches were handled.

"Although the government is trying to get involved and say 'we're not going to tolerate this', the legal landscape is really changing that more than anybody," Mr Anderon, who is in Australia on behalf of ASX-listed TechnologyOne, said in an interview with The Australian.

"In the United States now, when large breaches like this happen, within days if not hours there's class action lawsuits filed against the company.

"And in some cases if the employee data is lost, the employees are suing the company on top of the class action lawsuits."

When Mr Anderson left the FBI in 2015, cyber crime was all anyone talked about. However, its importance and the potential disastrous fallout of cyber attack was only realised a few years earlier.

"It wasn't until the late 2000s that we actually started to build infrastructure and a huge cyber component inside the FBI, and then we linked it to all the other intelligence communities," he said. "In the last seven, eight years since I left the government, I hate to say that I think cyber crime is getting much worse."

Discussing the Optus hack, Mr Anderson said it showed the importance of investment in technology departments and cyber-defensive capability "as opposed to just being just another line item in the budget".

"When you look at large companies, and unfortunately I think it'll probably become more rampant here as it is in the US, it really needs to be something that's on the forefront of the leadership of any of these companies, let alone the one that was just breached," he said.

"The CISO, CIO and CTO, no matter where that person falls in the organisation, should have a direct line to the CEO."

Companies needed to understand that hacking data and selling it back to a company was a business, Mr Anderson said.

"I've been involved in thousands and thousands of breaches in the US and I've probably been involved in different companies paying 600 ransoms over the years," he said. "After companies decide to pay the ransom, I've always seen the bad guys give the code for the data back. I think it goes to show you this has turned into a trillion-dollar industry."

Those commanding the hacks were no longer computer-savvy either, Mr Anderson said.

"People who are launching large-scale ransomware attacks, in most cases, are either subbing the attacks out to hackers or using algorithms that they purchase off the dark web," he said.