"As we have abandoned him I fully expect that he will consider himself free to speak with whomever approaches him. I did not want this." Ray Adams on Lee Gibling

Days after Adams sent the email to the NDS lawyer, Adams' boss at Operational Security, Reuven Hasak, a former spymaster who had been the deputy head of the Israeli secret police Shin Bet, approved £8000 in payments to Gibling.

changing

health insurance and superannuation by the company. Photo: PANORAMA

site used by 14 top Australian hackers), had hacked into the thoic server using a "back-door" and gained administrator rights that gave him access to all of Gibling's records and files.

Miller was unaware that thoic was an NDS operation and was puzzled by the volume of email traffic to a European site that he didn't recognise.

Gutman reported: "If George can do this — ANYONE can, including our competitors and other hackers."

"A lot of money has already been invested in Lee's operation, so even if we think that it is only a matter of time before he could be 'burned', there is still a lot that we can get from his network before that happens."

Gutman flew to Britain on February 3 to work out a crash program to hide all links between NDS and thoic.

NDS would install a new firewal l on the US server before moving to a new server in Sweden, and would set up a stand-alone computer that Gibling could transfer thoic files to, with new software that would automatically send the files to NDS.

Most important was to protect Gibling, whose wife was about to have a baby. By protection, Gutman did not mean from the thoic users whom Gibling was betraying but protection from NDS competitors.

"To avoid approach by competitors and their agents, the source and his family will relocate and be given untraceable phone numbers," Gutman wrote after her visit.

By this stage Hasak was alarmed and instructed Gibling that "until further notice he should not deal with the 'mails' nor remail or notify us of their contents".

Hasak was still worried and emailed Adams: "Bearing in mind our basic rule according to which we SHOULD prevent any embarrassment to NDS, I suggest we [cancel] our special relations with Lee, and stay with him as a regular informer.

"We should prefer this way on sleepless nights re NDS reputation. I am sure we came to a point where we are facing UNCALCULATED risk."

Hasak told Gutman: "We have too many external factors which might cause uncontrolled exposure = embarrassment to NDS." He wanted to scale down plans for Gibling. "Make sure all the 'history'/backup was deleted." Meanwhile they should start planning a new "in-house" pirate site.

The discussion went back and forth about keeping access to the "delicate material" on thoic.

"I would not like to discuss it with Abe [Peled] — this is one of the subjects that I do not want him (as the big boss) to be part of — I want to keep him away [from] it in case we might get into some potential trouble," Hasak wrote to Adams.

Adams told Gutman, "If we cannot ensure deniability for ourselves we won't be able to use THOIC."

Gutman was more sanguine. "Reuven [Hasak] was especially concerned about the 'special info' we used to get, because of the legal issues if ever exposed," she wrote on March 31. "Once we can show that all measures are in place and that (a) Lee is not in danger of exposure and (b) we have deniability regarding the information, I believe we will be able to resume operations with him."

This is what transpired. With the new system in place, NDS resumed monitoring thoic emails and using Gibling's passwords to trawl through the sites at will.

Meanwhile Gibling's marriage was breaking down. In May 2001, in the middle of a messy divorce, a group of hackers obtained a copy of the hard drive of his stand-alone computer, showing his emails to NDS. The site closed immediately and Gibling fled. Operational Security immediately went to the thoic site in Cornwall and removed and destroyed all records.

NDS says this was at Gibling's request, for his personal safety.

NDS continued to make payments to Gibling in Turkey for the next eight years.

Hacking masterminds are hard to prosecute

Cybercrime

Hannah Low

Hacker Vittorio Lalli-Cafini escaped jail. He was one of the lucky ones.

When the former Australian army communications expert started work at a small business in Perth called the Mod Shop back in 2003, his boss told him to figure out a way to hack into Foxtel.

Lalli-Cafini did as he was told, and less than a month later, he had found a way in.

The owners of the Mod Shop then set up a program to allow card-sharing for legitimate Foxtel card-holders.

Four years on, the company was ordered to pay up more than $1 million. Foxtel took the family business and their shonky practices to the Federal Court and demanded they hand over any money made.

Federal Court judge Antony Siopis said the defunct company allowed almost 6500 people to watch Foxtel without paying.

But Lalli-Cafini did not face time behind bars. The authorities did not prosecute. The "serial hacker", as he was later called, was never charged. In fact, his bosses took the brunt.

This is not always the case.

More often, in corporate hacking and cybercrime, it is the foot-soldier who is targeted. Low-level players are the only ones held to account. The weakest link in the corporate chain, the hacker, is charged, prosecuted, ordered to spend time in prison and left without a job.

The alternative is often too difficult to prove — especially in criminal cases — so the masterminds behind the hacking, and usually those who stand to benefit financially, escape scott free.

According to one expert in the field, management cannot be prosecuted unless a whistle-blower, or someone from within the organisation, is prepared to give evidence against them.

The issue has been thrust into the spotlight following a four-year investigation by *The Australian Financial Review*, which uncovered a secret unit within Rupert Murdoch's News Corporation that promoted piracy and hacking in Australia that damaged rivals Austar, Optus, and Foxtel.

Hacking and piracy violates a number of Australian laws, both criminal and civil. Most criminal prosecutions to date have been brought under the commonwealth Criminal Code; and a perpetrator must be shown to have knowingly and intentionally broken the law.

Although this can be imputed and direct evidence is not needed, typically the lack of direct involvement by management in the pirating makes any case against them fraught with difficulty.

Many cases settle before trial after the accused enters a guilty plea, but in one case in Queensland, Vitek Boden was sentenced to two years behind bars after being convicted of 26 counts of using a restricted computer without the consent of its controller, thereby intending to cause detriment or damage.

Experts say another investigation under the same law is under way in Victoria.

Cybercrime is a niche area of the law, making key players hesitant to comment on the current debacle.

All experts contacted for this article requested that they not be identified by name.

The Australian Federal Police coordinate investigations and prosecutions in the cybercrime area, working with international counterparts and state police departments to track down hackers.

Perpetrators face up to five years behind bars for each hacking offence under the criminal code, although lawyers say it is likely the judge would consider some sentences could be served concurrently.

If the damage caused is more than $5000, a court can order 10 years behind bars.

The code prohibits unauthorised access to a computer, rather than a set-top box, but experts say the word would be given a wide definition to include pay TV hacking.

Hackers could also face two years behind bars for violations of the telephone interception act or the telecommunications act or be fined $6600 per offence under another criminal act called the Technological Protection Measures Act. This act has only been in place since 2006, and would not apply to any emails sent before this time.

Although easier to prove than some other white-collar crime offences, the number of prosecutions for hacking is not huge, although is tipped to grow. High-tech hackers are good at hiding their tracks.

For the pay TV competitors left out of pocket following piracy, there are other options.

Companies can bring a number of civil suits, including breach of copyright, breach of contract and confidential information.

Depending on the claim, they can ask for damages, equitable compensation or even an account of profits, which is all of the profit the hacker company gained from pirating smartcards.

This is what happened in the Mod Shop case. And while the hacker himself may not have had to pay up, Foxtel ended up with more than $1 million in the bank.

Foxtel successfully prosecuted a small family company that allowed viewers to watch without paying. Photo: ROB HOMER

Legal demand about emails

Lawyers

Angus Grigg

Lawyers for News Corp subsidiary NDS have demanded *The Australian Financial Review* remove thousands of emails from its website.

Law firm Allen & Overy wrote to the *Financial Review* on yesterday saying the emails contained confidential information about NDS's employees. The *Financial Review* used the emails as the basis for an investigation that found NDS had promoted a wave of high-tech pay TV piracy in Australia and overseas.

The emails also support claims by the BBC *Panorama* program, aired in the UK on March 26, that News sought to derail OnDigital, a UK pay TV rival to News's BSkyB, that collapsed with losses of more than £1 billion in 2002 after it was hit by massive piracy, which added to its other commercial woes.

News Corp has categorically denied any involvement in promoting piracy and points to a string of court actions by competitors making similar claims, from which it has emerged victorious.

On Monday, NDS issued a comprehensive statement denying any role in promoting piracy or providing competitors' codes for use in piracy. A full version of the statement can be found online at broadbandtvnews.com.