



## Biting the hand that feeds IT

### Research and Whitepapers - Free Download

#### [Making the Connection](#)

Business connectivity and the online individual

#### [Getting The Package Right](#)

A guide to choosing and using mobile services

#### [Live Migration with AMD-V™ Extended Migration Technology](#)

Live migration functionality works seamlessly across a broad range ...

#### [Alternate Client Architectures](#)

An overview of alternative architectures to deliver applications ...

[The Register](#) » [Public Sector](#) » [Law](#) »

Original URL: [http://www.theregister.co.uk/2008/06/13/it\\_manager\\_rampage\\_sentence/](http://www.theregister.co.uk/2008/06/13/it_manager_rampage_sentence/)

---

## Disgruntled admin gets 63 months for massive data deletion

---

By [Dan Goodin in San Francisco](#)

Published Friday 13th June 2008 21:35 GMT

An IT manager who sought revenge for an unfavorable job evaluation was sentenced to more than five years in federal prison after being convicted of intentionally triggering a massive data collapse on his former employer's computer network.

Jon Paul Oson, 38, of Chula Vista, California, was sentenced to 63 months behind bars and ordered to pay more than \$409,000 in restitution, according to federal prosecutors in San Diego. He was immediately taken into custody after the sentence was handed down on Monday. It is one of the stiffest penalties ever for a computer hacking offense.

### Whitepapers - Free to Download

[Getting The Package Right](#)

[Why Green Security Makes Good Business Sense](#)

[Wireless Email Solutions](#)

[Alternate Client Architectures](#)

[Redefining FOTA deployment in EMEA](#)

Oson was hired in May 2004 as a network engineer at the Council of Community Clinics in San Diego, a nonprofit that provides various services to 17 regional health clinics in Southern California. He performed well in that role and five months later was promoted to technical services manager. He ended up bitterly resigning a year later after a performance evaluation cited interpersonal difficulties, according to court documents.

On December 23, Oson logged onto servers belonging to his former employer and

disabled the program that automatically backed up medical records for thousands of low-income patients. Six days later, he logged on again, and in the span of 43 minutes, methodically deleted the files containing patients' appointment data, medical charts and other information.

The dollar cost of Oson's rampage was pegged at \$409,337.83 and accounted for expenses for technical investigations and moving to a paper-based system in the weeks following the attack. But the real toll came when doctors at North County Health Services no longer had medical records for thousands of low-income patients who sought medical care. North County Health Services contracted with Oson's employer to store the records.

### Health threat

By destroying the records, Oson threatened the health of patients who visited the clinic immediately after the attack, prosecutors argued. They cited two examples, including a nine-year-old who had been diagnosed with an ear infection several days before Oson's rampage. When he returned a few weeks later, doctors had no record of the previous diagnosis, and they also had no idea he was due for a routine physical exam.

"Patients who visited the clinic in the weeks following the network disruption were kept waiting hours and sometimes futilely while their charts were located and delivered to the appropriate clinic and doctor," prosecutors said in court documents. "With the shutdown of its Practice Management system, NCHS had to shift to a paper-based system."

After ransacking his former employer's network, Oson took pains to cover his tracks. When FBI agents raided his home in May 2006, they found all but one of his PCs had been wiped clean, irretrievably destroying data that might have shown he was behind the attacks.

But Oson slipped up and left other clues. One was an HP 2100 LaserJet printer he kept at his home and another was an HP LaserJet 4M printer physically located near the workstation Oson used at his new job.

It just so happened that in the weeks leading up to the data meltdown, an intruder had cased the network by logging in from at least three different machines. One was a computer named "TEMP3" that was equipped to work with an HP 2100 LaserJet printer. A second PC happened to contain drivers for the HP 2100 and a LaserJet 4M.

Even more incriminating, the nickname of this second PC was "kuku" and one of the printers it was configured to work with was named "mike2003 HP Laserjet 4M". That just happened to match the name of Oson's son and the network name of the printer sitting by his workstation.

"At the sentencing hearing, the court talked about the impact of Oson's actions and his arrogance," Assistant US Attorney Mitchell Dembin, who prosecuted the case, wrote in an email to *The Reg*. "The court said that Oson seemed to think that he was the smartest guy around but, as often happens, he ran into someone smarter (the FBI)." ®

### Related stories

[Rubbermaid bot master sentenced to 41 months](http://www.theregister.co.uk/2008/06/11/rubbermaid_botmaster_sentenced/) (11 June 2008)

[http://www.theregister.co.uk/2008/06/11/rubbermaid\\_botmaster\\_sentenced/](http://www.theregister.co.uk/2008/06/11/rubbermaid_botmaster_sentenced/)

[Security breach at Belgacom exposed](http://www.theregister.co.uk/2008/06/11/security_breach_at_belgacom_exposed/) (11 June 2008)

[http://www.theregister.co.uk/2008/06/11/security\\_breach\\_at\\_belgacom/](http://www.theregister.co.uk/2008/06/11/security_breach_at_belgacom/)

[Hacker cops to \\$70k botnet rampage](http://www.theregister.co.uk/2008/06/11/botherder_admits_to_ddos_assault/) (11 June 2008)

[http://www.theregister.co.uk/2008/06/11/botherder\\_admits\\_to\\_ddos\\_assault/](http://www.theregister.co.uk/2008/06/11/botherder_admits_to_ddos_assault/)

[I Was A Teenage Bot Master](http://www.theregister.co.uk/2008/05/08/downfall_of_botnet_master_sobe_owns/) (8 May 2008)

[http://www.theregister.co.uk/2008/05/08/downfall\\_of\\_botnet\\_master\\_sobe\\_owns/](http://www.theregister.co.uk/2008/05/08/downfall_of_botnet_master_sobe_owns/)

[NZ teen botnet mastermind cops a plea](http://www.theregister.co.uk/2008/04/01/nz_teen_botmaster_guilty_plea/) (1 April 2008)

[http://www.theregister.co.uk/2008/04/01/nz\\_teen\\_botmaster\\_guilty\\_plea/](http://www.theregister.co.uk/2008/04/01/nz_teen_botmaster_guilty_plea/)

[LSDigital drops federal botnet confession](http://www.theregister.co.uk/2008/03/14/bot_herder_cops_plea/) (14 March 2008)

[http://www.theregister.co.uk/2008/03/14/bot\\_herder\\_cops\\_plea/](http://www.theregister.co.uk/2008/03/14/bot_herder_cops_plea/)

[Thievin' teen bot herder admits to infecting military computers](http://www.theregister.co.uk/2008/02/12/bot_herder_cops_plea/) (12 February 2008)

[http://www.theregister.co.uk/2008/02/12/bot\\_herder\\_cops\\_plea/](http://www.theregister.co.uk/2008/02/12/bot_herder_cops_plea/)

[FBI crackdown on botnets gets results, but damage continues](http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/) (29 November 2007)

[http://www.theregister.co.uk/2007/11/29/fbi\\_botnet\\_progress\\_report/](http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/)

[Botmaster owns up to 250,000 zombie PCs](http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/) (9 November 2007)

[http://www.theregister.co.uk/2007/11/09/botmaster\\_to\\_plea\\_guilty/](http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/)

[Portrait of an \(alleged\) cyber bully as a young man](http://www.theregister.co.uk/2007/10/04/bot_herder_profile/) (4 October 2007)

[http://www.theregister.co.uk/2007/10/04/bot\\_herder\\_profile/](http://www.theregister.co.uk/2007/10/04/bot_herder_profile/)

[FBI logs its millionth zombie address](http://www.theregister.co.uk/2007/06/13/millionth_botnet_address/) (13 June 2007)

[http://www.theregister.co.uk/2007/06/13/millionth\\_botnet\\_address/](http://www.theregister.co.uk/2007/06/13/millionth_botnet_address/)

© Copyright 2008