

# Technology risk news

20 February 2010  
Issue No: 388



## Security: Charities warned to handle information securely

The Information Commissioner's Office is reminding charities that personal information must be handled securely after finding the Alzheimer's Society in breach of the Data Protection Act, notes a **Workplace Law** report. Several unencrypted laptops were stolen during a burglary at the society's office in Cardiff last August. **The laptops were neither physically secured by cable locks nor locked away securely.** One of the laptops contained personal details including names, addresses, national insurance numbers and salary details for about 1 000 staff across England, Wales and Northern Ireland.

[Full Workplace Law report](#)

## Security: Shell must explain data breach

A full-scale investigation was under way last night into a security breach at Royal Dutch Shell as the oil company faced explaining to staff **how the personal details of 170 000 employees and contractors had made their way on to the Internet.** *The Times* reports that seven non-governmental organisations who were e-mailed a database of all Shell staff this month have been dragged into the row. The list includes names, telephone numbers and other details of employees and contractors working for Shell worldwide.

[Full report in The Times](#)



## Security: Researchers find flaw in Chip and PIN technology

Security researchers have demonstrated a gaping security hole in Chip and PIN credit card authorisations which undermines trust in the technology as a means to verify retail purchases. *The Register* reports that Cambridge University security researchers have demonstrated how it **might be possible to trick the card into thinking it's doing a chip-and-signature transaction** while the terminal thinks it's authorised by chip-and-PIN.

[Full report in The Register](#)



## Security: Microsoft alert on malware conflict in update

Microsoft is warning users to scan their machines for malware following a recent string of system crashes, notes a **v3** report. The company said that one of the patches included in its February security update **is potentially causing a conflict with certain malware infections on Windows XP systems.** The MS 10-015 patch addresses a vulnerability in the Windows kernel, but the infected systems experienced the infamous 'blue screen of death' system crash.

[Full v3 report](#)

This Newsletter has been compiled in association with EBrief News: delivering a world of information in a 10-minute read.

## Security: Vendors warn of renewed Trojan attacks

Security vendor Websense is warning of a renewed spate of global attacks aimed at stealing information from staff in government and military departments via the notorious Zbot, or Zeus, Trojan. A **v3** report notes that **the malware was originally designed to steal banking data,** but was used in a campaign targeting government workers in the US and the UK at the beginning of the month. 'The spoofed e-mails capitalise on the last Zeus attack, and claim that installing the "Windows update" via the links provided will aid protection against Zeus attacks,' said Websense.

[Full v3 report](#)

While APR Insurance & CFC Underwriting Limited has taken all reasonable steps to ensure the accuracy of this Newsletter, the information contained herein is provided "as is" and APR Insurance & CFC Underwriting Limited makes no express or implied representations or warranties with regard thereto. Without limiting the generality of the foregoing:

APR Insurance & CFC Underwriting Limited does not warrant that this Newsletter or information contained herein will be errorfree or will meet any particular criteria of performance or quality. APR Insurance & CFC Underwriting Limited expressly disclaims all implied warranties, including, without limitation, warranties of compatibility, security and accuracy; and

Whilst APR Insurance & CFC Underwriting Limited has taken reasonable measures to ensure the integrity of this Newsletter and its contents, no warranty, whether express or implied is given that any files, downloads or applications available via this Newsletter are free of viruses, Trojans, bombs, timelocks or any other data or code which has the ability to corrupt, damage or affect the operation of the user's system.