

# Technology risk news

25 January 2010  
Issue No: 383



## Privacy: Tough new penalties for data breaches

Big Four firm Deloitte has warned about new data protection rules which increase the penalty to £500 000. Justice Secretary Jack Straw **has given the final tick for tough new penalties for personal data security breaches**. Simon McDougall, head of privacy and data protection at Deloitte, is quoted in an **Accountancy Age** report as saying that the new penalties, which come into force in April, will come as no great surprise to security or privacy professionals. 'What this means in practice is that, from April this year, the Information Commissioner's Office now has a bigger stick to wield,' he said.

[Full Accountancy Age report](#)

## Security: Yahoo targeted in Chinese attack

Yahoo! Inc, owner of the second most used search engine in the US, was targeted by an attack in China that was similar to the one that affected Google, according to a **WA Today** report. Google had earlier said **at least 20 other companies were targeted in a series of 'highly sophisticated' attacks last month**. Yahoo, which said it 'stands aligned' with Google in condemning the attacks on users, was also affected.

[Full WA Today report](#)



## Security: US financial services firm warns on data breach

A Concord, New Hampshire, financial services company is sending data breach notification letters to customers after discovering that shared passwords, set up to simplify administrative functions nearly 10 years ago, **could have exposed the private data of 1.2m customers**, notes a **PC World** report. 'This username and password had been shared among certain employees ... and employees of affiliated companies,' Lincoln National's letter states.

[Full PC World report](#)



## Security: Passwords, etc no longer enough protection

Security measures such as the use of one-time passwords and phone-based user authentication – considered among the most robust forms of IT defences – are no longer enough to protect online banking systems against fraud. **PC World** notes that according to a Gartner Inc report, cybercriminals **are using increasingly sophisticated tactics to outmanoeuvre security systems** so they can steal customers' log-in credentials and pillage their bank accounts. Gartner analyst Avivah Litan says Trojan horse programs lurking inside a customer's Web browser can steal one-time passwords and immediately transfer funds, or intercept a transaction between a bank and a customer and make changes unbeknownst to the user or the bank.

[Full PC World report](#)

## Privacy: Data breach at New York state bank

The login details of 8 378 Suffolk County National Bank customers have been stolen after a hacker gained access to the computer server hosting its online banking system, reports **Finextra**. The New York state community bank says **the intrusion occurred over six days between 18 and 23 November**, affecting around 10% of its customers. It was discovered during an internal security review on 24 December, prompting the bank to rebuild the compromised server and take 'other measures to ensure the security of data'.

[Full Finextra 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

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

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.