Forensic Services

www.pwc.cz

Protection against data leakage and its investigation

Is it possible that your company might experience a costly data breach? You should be concerned if:

- Employees are leaving the company
- Outside vendors or consultants have access to your data
- Personal e-mails are used for business data
- It's not clear where sensitive data resides
- Your competition is always one step ahead

pwc

Manage incidents to minimise cost and disruption to your business

The risks faced by a typical organisation have never been more significant, or more complex, and as threats have proliferated. Safeguarding people, processes and technology has got much harder. At the same time the whole concept of 'security' has expanded way beyond this traditional remit into areas like brand and intellectual property protection, loss prevention, anti-counterfeiting, cybercrime, parallel trading, online and traditional fraud.

In recent years, an increasing number of high-profile data security breaches have made headlines. No matter how hard an organisation might try to prevent it, corporate crime is an equal-opportunity threat that can strike entities large or small, domestic or international, public or private. Regulatory investigations, large fines, and reputational damage can follow, adversely affecting the overall stability and competitive position.

Insurance company UNIQA confirmed the data leakage from its system. Information about clients who took out travel insurance during years 2005-2007 appeared on the internet - it totalled several thousand people.

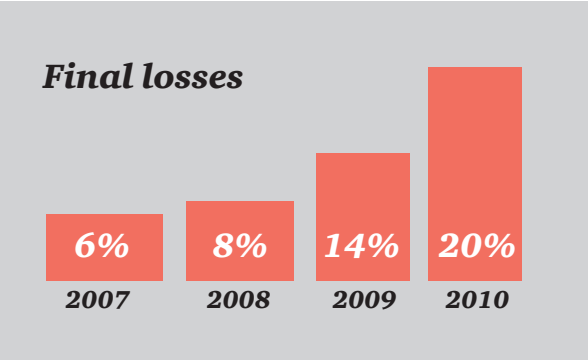
Source: SecurityWorld | 04/09/2009

Increased information security – but has it got the right focus?

PricewaterhouseCoopers' 2011 Global State of Information Security Survey® showed that "the increased risk environment has elevated the role and importance of information security" and that Business Leaders see data protection as one of their most important priorities. However, financial losses due to data

As organisations continue to gain new visibility into security incidents, they are learning more about the real costs of breaches

For years, the percentages of respondents who reported not knowing about key security event-related facts have been painfully high. Today the number of respondents being unaware of what type of events occurred in the past 12 months has decreased significantly.



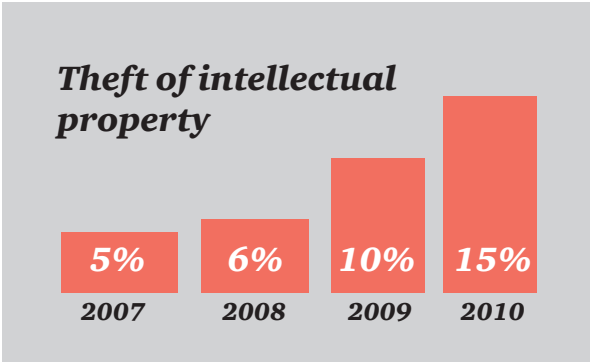
The impact of security events on business has risen to significant levels — particularly with respect to financial losses, theft of intellectual property and compromises to brands or reputations.

Social networking represents one of the fastest emerging new areas of risk

As if protecting data across applications, networks and mobile devices wasn't complex enough, social networking by employees is presenting organisations worldwide with a new and growing frontier of risk. The risks include the loss or leaking of information; statements or information that could damage the company's reputation; activity such as downloading pirated material with legal and liability implications; identity theft that directly and indirectly compromises the company's network and information.

One of the leading priorities for many companies is mitigating the consequences of a breach — through better incident response

58% of respondents report that they have a plan for security incidents, but only 63% report it is effective, which means that most organisations have no plan or the plan they have doesn't work.



Company Panasonic risks a fine of several million crowns. One of the company's employees acquired a database of all employees with their personal identification numbers, addresses, positions as well as monthly salaries.

Source: www.denik.cz | 30/10/2007

How we can help?

Using our Forensic Technology Solutions centres and dedicated labs throughout the world, we offer the latest technology to best serve our clients' needs. Our services include:

- investigations of data leaks
- assistance with data breach response and cybercrime
- information risk management

Representatives of the German telecommunication company Deutsche Telekom confirmed that contact information for more than 17 million customers was stolen. Their personal data was stolen from the internal databases of this telecommunication concern. This major security breach was reported publicly by the magazine Der Spiegel.

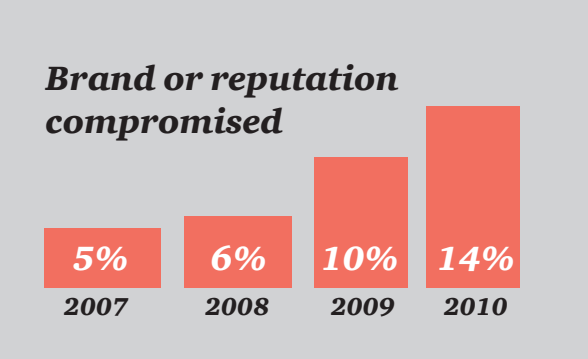
Source: www.itbiz.cz | 06/10/2008

1) Data leak investigation

Our Forensic Services practice helps clients identify the areas where sensitive data was transferred out of the organisation. We assist with data leakage risk assessments in order to identify areas of focus. We will point to data that provides evidence of leakage. We will collect this data and analyse it to find out who leaked the information, what information was leaked, when it leaked and how. Typically, this data can include e-mails, e-mail backups, user files on PCs and notebooks, various log files as well as data on mobile devices.

2) Assistance with data breach response and cybercrime

The ability to forensically investigate cybercrimes is critical to protecting data, the infrastructures that store and transmit data, and the organisations responsible for those infrastructures and data. Our technical teams rapidly respond to data breaches throughout the world by helping our clients identify the source, location and nature of the breach; quantify and mitigate the associated losses; and remediate known vulnerabilities to minimise future occurrences.



Sony admitted that the personal details of 77m Playstation users may have been stolen by hackers. Since the breach was revealed, shares in Sony have fallen by 4%.

Source: www.bbc.co.uk | 03/05/2011

3) Information risk management

We help clients develop strategies to handle the entire life cycle of information — from creation to destruction — and integrate the people, processes and technologies necessary to give companies centralised control over that information. We assist clients to increase awareness of the importance of information security to ensure that employees are the first line of defence.

Common vulnerabilities and practices that can compromise sensitive data:

- third-party vendor handling and transfers
- improper access or broad access controls
- paper handling and dumpster diving
- phishing, web/e-mail vulnerabilities
- mobile and home-based workforce
- call centres and social engineering
- use of personal information in authentication processes (online, phone)
- backup tapes
- peer-to-peer networks (hand-held devices, for example)
- collecting/using personal info

Who we are?

The PwC CEE Forensic Technology Solutions team is a group of dedicated professionals with experience from many local and international assignments in a wide range of industries.

Our state of the art technology and tools are always at your disposal.

We understand the needs of data security and legal limitations concerning the protection of personal data. We can therefore help you design the most convenient solution while respecting your legal environment.

Our goal is to serve as your investigative, forensic accounting and compliance resource anytime you have an incident or a concern.

For more information please contact

Sirshar Qureshi
Partner

Tel.: +420 251 151 235
Mob.: +420 602 348 926
sirshar.qureshi@cz.pwc.com

Pavel Jankech
Senior Manager

Tel.: +420 251 151 336
Mob.: +420 739 342 277
pavel.jankech@cz.pwc.com

Filip Volavka
Senior Manager

Tel.: +420 251 151 269
Mob.: +420 733 169 155
filip.volavka@cz.pwc.com

pwc