

## User errors will lead to data leakage – worldwide survey on IT security

Date: 10-22-2009 11:14 AM CET

Category: [IT, New Media & Software](#)

Press release from: [Dimension Data](#)



57% of the organisations interviewed are planning investment in data loss prevention

Dubai, United Arab Emirates – 21 October 2009 - A worldwide survey of over 400 organisations with over 500 employees shows that, although organisations believe that they will suffer data leakage in some form at some stage, it will be accidental rather than malicious.

The survey which was commissioned by Dimension Data and carried out by research house IDC during 2009 focused on IT security and interviewed IT security decision makers and influencers in 18 countries in Western Europe, the Americas, the Middle East and Africa, and Asia and Pacific.

“The fact that 57% of the organisations that IDC polled are planning investment in data loss (or leakage) prevention (DLP) indicates broad acceptance of the need to complement the traditional network-centric security approach with data-centric security,” says Neil Campbell, Dimension Data’s global general manager security solutions.

“Organisations (45%) also believe that data leakage is more likely to occur through human error on the part of their own employees, rather than through intentional theft from outside (15%).

“In addition, with the increase in layoffs taking place in the current economic climate, the probability of a vengeful employee deliberately destroying or stealing sensitive data from the organisation has increased.”

According to Eric Damage, IDC EMEA program manager, European security products and strategies, the survey reveals that organisations believe the most significant impact of a security breach would come from the lack of control of its intellectual property (IP). “The next most severe impact would come from customer sensitivity to security and privacy - followed by the availability of IT systems in order to offer products and services.”

Campbell adds, “The challenge when protecting an organisation from internal attack is that traditional defences are designed to face outward, at the perimeter of a network, whereas the inside of the network remains relatively free of security controls. Compounding the problem, security awareness training initiatives for employees often go unfunded. That’s because organisations find it difficult to demonstrate a return on investment for such training.

“Besides, at the employee level, protection of data goes beyond technology in that it involves the human resources department and in turn, raises a range of new legal issues around areas such as monitoring and fair use”, explains Campbell, and points out that organisations tend to believe that it will add a layer of managerial and process complexity that they don’t

want to confront.

“To tackle these challenges, organisations are moving towards DLP as it involves a holistic approach to the protection of information, rather than simply the protection of networks and systems. It creates automated, technical barriers to both human error and malicious intent.”

“Organisations in the Middle East too are losing critical data due to employee errors and are working towards tightening security controls internally. Companies in this region are seriously looking at investing in DLP, which allows them to define and enforce an effective security policy for information flow in order to keep control of critical information such as blue prints, financials metrics, and source code, prevent accidental breaches of compliance regimes and confidentiality policies, and support the user's ubiquity while using laptops or smaller devices,” explains Nader Atout, Sales Director – Gulf Region at Dimension Data.

DLP is applied to data in motion (in between networks, users, and machines), data in use (when being accessed), and data at rest (when stored, archived), regardless of whether the data is inside an organisation's network or not.

“But,” warns Campbell, “DLP is not an off-the-shelf product, silver bullet, or a quick fix. It's a portfolio of data-centric solutions. DLP is IT security matured. And because it focuses on data rather than the network or systems, it is a business rather than a technical issue. It's a technology-centric approach to managing the issue of protecting sensitive data, it's an important strategic step forward.

“After its people, data is an organisation's most crucial asset, and those active in security realise that if they protect data, they automatically protect their organisation.”

#### About the Security research commissioned by Dimension Data

This research on the status of IT security across multiple geographies globally was commissioned by Dimension Data. The research was carried out by IDC, and represents the accumulated results from interviews conducted with representatives from 407 companies (employing more than 500 employees) across 18 countries worldwide covering the Americas, Western Europe, the Middle East and Africa, and Asia and Pacific. [www.dimensiondata.com/securityresearch](http://www.dimensiondata.com/securityresearch)

#### About Dimension Data

Dimension Data plc (LSE:DDT), a specialist IT services and solution provider, helps clients plan, build, support and manage their IT infrastructures. Dimension Data applies its expertise in networking, converged communications, security, data centre and storage, Microsoft and contact centre technologies, and its unique skills in consulting, integration and managed services to create customised client solutions.

Mechelle Buys du Plessis

Dimension Data, UAE

Sheikh Zayed road, Dubai, UAE

Tel: +971 44 33 1749

Fax: +971 44 35 5612

Mobile: +971 50 881 4832

[You can find this press release here](#)