DIGITAL NEWS ASIA

# Preventing data loss, and the health of your business

A. Asohan Apr 09, 2014

- ***DLP market growing at about 20% per year; so is the number of data leaks***
- ***Even a single data leak can cost a company millions, plus loss of reputation***

THE whistleblowing activities of former US National Security Agency (NSA) contractor Edward Snowden, whether you believe it was irresponsible and damaging or a valiant effort to expose governmental misdeeds, has certainly thrown the issue of data protection into the limelight.


But awareness of Data Loss Prevention (DLP) has been growing anyway, according to Andrey Sokurenko ***(pic)***, business development director at Russia-based InfoWatch, which specialises in DLP, intellectual property protection, risk management and compliance solutions, amongst others.

It's this awareness that is causing the "DLP market to grow by about 20% every year," he told Digital News Asia (DNA) in Kuala Lumpur recently.

According to Gartner, the DLP market will grow 28.6% in 2014, and will transition "from compliance demand to intellectual property protection," while technology research and advisory company TechNavio predicts the global

***FULL TEXT***

# Preventing data loss, and the health of your business

*A. Asohan Apr 09, 2014.*

- ***DLP market growing at about 20% per year; so is the number of data leaks***
- ***Even a single data leak can cost a company millions, plus loss of reputation***

THE whistleblowing activities of former US National Security Agency (NSA) contractor Edward Snowden, whether you believe it was irresponsible and damaging or a valiant effort to expose governmental misdeeds, has certainly thrown the issue of data protection into the limelight.

But awareness of Data Loss Prevention (DLP) has been growing anyway, according to Andrey Sokurenko ***(pic)***, business development director at Russia-based InfoWatch, which specialises in DLP, intellectual property protection, risk management and compliance solutions, amongst others.


It's this awareness that is causing the "DLP market to grow by about 20% every year," he told Digital News Asia (DNA) in Kuala Lumpur recently.

According to Gartner, the DLP market will grow 28.6% in 2014, and will transition "from compliance demand to intellectual property protection," while technology research and advisory company TechNavio predicts the global DLP market will grow at a compound annual growth rate (CAGR) of 17.5% from 2011–2015.

Part of the reason for this increased awareness is the increasing number of data leakage incidents. According to InfoWatch's *Global Data Leakage Report 2013*, last year, 1,143 leaks of confidential information were recorded and reported in the media and registered by the company's Analytical Centre.

This figure is 22% higher than the number of leaks (934) registered in the previous year ***(see chart below)***.

"We see the number of leakages as growing too fast, with the major source of such leakages being employees," said Sokurenko.

"And even if there is a small number of leakages, it can still cost you millions," he said, adding as an example how damaging data leakage could be in the case of an oil and gas company bidding for a multimillion-dollar tender.

Other highlights from InfoWatch's report on the year 2013:

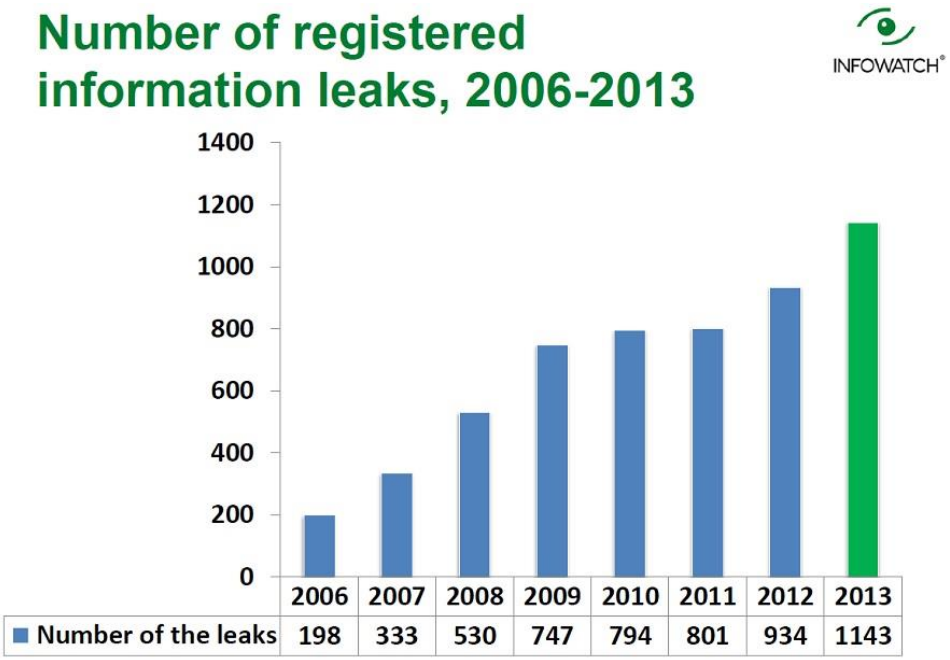
- More than 561 million records were compromised, including financial and personal data.
- The United States was No 1 in terms of the number of data leaks (679, or 59.41% of the total) which occurred in 2013, with Russia in second place (134 leaks) and the United Kingdom in third (80 leaks).

- The proportion of leaks occurring in state and municipal organisations worldwide remained stable at a high 31%. State organisations, together with medical institutions, are the main source of personal data leaks.

- The majority of information leaks – 85% – involve personal data.

- According to media reports, the damages (the cost of elimination of the

consequences from the data leakage, legal investigations, and compensation payments) suffered by companies as a result of data leaks during 2013 amounted to US$7.79 billion.




The report is based on InfoWatch's own database, which its experts have been updating since 2004. The company said its database of leaks includes incidents (information leaks) which have occurred in organisations as a result of the inadvertent or intentional actions of their employees, and which have been reported in the media or other publicly available sources (including blogs and web forums).

Part of the reason why most data leakages seem to be happening in the developed world is, oddly enough, their long-time awareness of info-security.

“If you look at companies in Western Europe and the United States, they’re very aware of the importance of security and data protection – they know the topic, as it were,” said Sokurenko.

“But that’s a problem in itself – they’ve spent a lot of money and security, and have become very complacent.

“In markets like the Middle East and Asia Pacific, and Latin America, I’m proud to say that the people who take care of IT security in their organisations are very interested in this kind of technology – they’re really hungry for knowledge [in this area], and they really ask a lot of questions … a lot of very smart questions.

“In fact, it’s questions like these that is invaluable feedback as we further develop and improve our products,” he added.

**SME push**

InfoWatch was formerly a subsidiary of Russian info-security and antivirus company

Kaspersky Lab, set up in 2003 with Kaspersky Lab cofounder Natalya Kaspersky – the ex-wife of company founder Eugene Kaspersky – as chief executive officer. In 2012, InfoWatch became completely independent.

"InfoWatch in reality is a holding company for a group of companies – Kribrum (social media monitoring and analysis for online reputation management), EgoSecure (end-point security and Appercut (business application source code analysis) – each of which cares for a different technology," said Sokurenko.

"Each company focuses on its particular technology, and only that, so that it can concentrate on making it amazing technology," he added.

InfoWatch Ltd itself specialises in DLP, with its flagship product being InfoWatch Traffic Monitor Enterprise, which according to Sokurenko, is typically used in large enterprises, especially in the financial services, the oil and gas, and government sectors, its top three markets.

"Traffic Monitor has become more than just a DLP solution," he claimed. "It has to do with the health of the company – not just protecting it from any data leakages, but also from the risk and damage such data leakages may cause."

Traffic Monitor protects against the leakage of data from not just an internal source (employees) but also external (partners, suppliers, etc.), and not just intentional bus also accidental data loss from carelessness or mistakes.

While InfoWatch's biggest market is with large enterprises, its solutions are also in use with small and medium enterprises (SMEs) too – indeed, about 20-30% of its customers come from this segment, according to Sokurenko.

"Everyone wants to find a unique value proposition, so everyone needs to protect their data," he said.

"We understand that SMEs may not have specialised IT staff, so we ensure that our technology is not only effective, but also easy to deploy – easy to install and easy for the data to be analysed," he claimed.

Sokurenko expects the SME portion of InfoWatch's customer base to take off even further with its new Personal Data Protector solution, adding that the company has seen "a huge number of pre-orders" for the new product.

The introduction of the Personal Data Protection Act (PDPA) late last year in Malaysia also convinced the company to begin aggressively marketing its product in the domestic market, according to Renganathan ***(pic)***, Asia Pacific regional head at InfoWatch's Malaysian office.

"With the PDPA, a large number of SMEs now need to be compliant – even your

typical pizza company will now have to comply with the Act to protect customers credit card information, for example, so we expect a huge uptake of this product in the Malaysian market," he said.

In tandem with the aggressive marketing for the Personal Data Protector solution, InfoWatch also did the same for its Traffic Monitor solution.

"We've had discussions with about 40 customers, and did about 15-16 proof of concepts (POCs), and expect our first implementation in about a month," said Renganathan.

"And when we say POC, it means actually using our solution," said Sokurenko. "When you install it, you will immediately see what is going on in the company – we can show real data, not only in the past, but in real time.

"And the amazing thing about Traffic Monitor is that it takes only about a week to deploy – and it doesn't matter if you have 50 to 100 users, or tens of thousands," he added.

Indeed, according to Renganathan, in one POC InfoWatch did with a Malaysian organisation, the solution immediately showed that an employee who had tendered his resignation two weeks earlier was sending out the most amount of email and data.

"We extracted the email and data for the company, and they had to have an emergency management meeting on that," he added.

Sokurenko pointed out that while Traffic Monitor allows the customer to extract information and analyse it, InfoWatch itself has no access to such information. "We're about protecting our customers' confidential information, after all."

Source