CXOtoday.com
IT Perspective for Decision Makers

Businesses Ignoring DLP Are At Risk

by Sohini Bagchi   Feb 15, 2015

Today every business sector is using huge volumes of data and is highly susceptible to data leakages.As for the consequences of data leaks, companies across the world incur significant financial and reputational losses as a result of data leaks. A Ponemon Institute research noted that the average total cost of a data breach for the companies increased 15 percent to $3.5 million in 2013 and the number is escalating year after year. In such a scenario, many companies are opting for data leakage prevention (DLP), a strategy that ensures end users do not send sensitive or critical information outside the corporate network. In an exclusive interaction with CXOtoday,**Vsevolod Ivanov, Deputy CEO, InfoWatch** speaks about the importance of DLP practices in an evolving threat landscape and the company's recent and upcoming DLP initiatives for the India market**.**

Of the various security solutions deployed in an enterprise, how do Indian CIOs rank the importance of DLP solutions?The importance of DLP is still underestimated globally, and India is no exception. Antivirus solutions, firewalls and other types of infrastructural protection are more common among enterprises than DLP. Nevertheless, taking into account the constantly growing number of data leaks including incidents with huge financial losses we see the growing demand for data protection solutions among Indian CIOs. From our clients and partners experience we can say the companies understand the severity of data leakage problem and the necessity for reliable protection and so are ready to invest. The key customer considerations for DLP are the constantly growing amount of data leak incidents worldwide which bring significant financial losses to companies, reputational losses, and compliance inducing DLP adoption.

With the government's initiative of 'Make in India' expected to give a major boost to the manufacturing sector, what are the key challenges faced by CIOs of manufacturing companies as they try to secure their data and how can DLP help?

Manufacturing companies possess highly confidential information such as manufacturing secrets, know-hows, technology designs and graphics. This highly sensitive data is a titbit for competitors and its leakage can be fatal for the whole business of the company. Therefore, confidential information owned by companies of manufacturing industry must be reliably protected. DLP solution, along with a set of organisational measures can minimize the amount of occasional data leaks (employee mistakes and negligence) and deliberate data theft (early detection of employee's suspicious behaviour).

Which other sectors in India are highly susceptible to data breaches and how can they be prevented?

Companies with most valuable information are most at risk. They are banks and insurance companies, healthcare and pharmaceutical, governmental structures which operate highly sensitive data. As well as companies which have big volumes of personal data (mobile operators, big online retailers, logistics, authorities working with citizens, etc.) Then there are companies which possess different trade secrets (manufacturing, oil and gas, media etc.). We can add to the list any other company which considers its information valuable.

Data leakage prevention is a complex task. Companies should implement both specialized data protection solutions and a set of specific data security policies and measures to create secure environment for confidential data usage, storage and flow in corporate perimeter. InfoWatch at their end provides a number of reliable data protection solutions customized for different industries and together with partners deep consultancy in implementing data protection policies.

What are the key highlights of InfoWatch's recent Global Data Leak Report? How does India compare to other emerging markets in data leakage incidents?

In 2014, the InfoWatch Analytical Center uncovered globally (in the media and other sources) and recorded 1395 cases of confidential information leakage, which is 22% higher than the number of leaks recorded in 2013. Most often, information leaks were related to personal data - in 92% of cases, this was the type of information leaked. Over 767 million personal data records were compromised.Financial institutions along with internet-services, retailers, and healthcare institutions are the main sources of personal data leaks. In 54% of cases, company employees were responsible for the leaks of information. In 1% of cases, it was senior executives of organizations.

As of the situation with data leaks in India, InfoWatch Analytical center has not released a separate research on this market so far. However, since India is the country where many sectors in the economy are now in active transition from paperwork to digital documents workflow, InfoWatch analysts expect India to experience a significant growth in the number of data leaks in the nearest 3 years. This trend was demonstrated by all emerging markets, which have experience a process of data digitalization.

With the rise of mobile devices in the corporate environment and targeted attacks on such devices becoming more rampant. How can DLP help CIOs address such issues?

The rise of mobile devices in the corporate environment poses a serious threat to confidentiality of corporate data. There are more than 4000 different modifications and platforms for smartphones and tablets. If the company chooses Bring your Own Device concept, it allows its' employees to bring any device from this 4000 list. There is no security solution in the world which would support them all. According to researches of global analysts and InfoWatch client polling, 67% of respondents are worried about confidential data leaks from mobile devices and 68% of respondents note the absence of effective security solutions for mobile devices. Two factors, a high risk of data loss through mobiles and a big number of mobile modifications make the concept of BYOD very risky for an enterprise, which values its information.

There are several approaches which can be implemented in regard to the device usage. First is to allow the staff to choose from a short list of smartphone modifications, which company's security products support. The second is to provide the staff with corporate devices with monitoring security systems preinstalled. The third one is to forbid the usage of all devices in corporate perimeter which is unfavourable for business, but for sure very secure. The forth is to allow anyone to use whatever (the above-mentioned BYOD) and accept data leaks.

I would still recommend using some type of security solutions, like content filtering, mobile device management, etc. InfoWatch is now developing a DLP solution with integrated module for data protection on mobile. The solution will allow intercepting and analysing all web traffic, camera snapshots, and all correspondence from smartphones on server level.

What are your plans for the Indian market in the next 12-18 months?

Firstly, InfoWatch plans to establish a number of offices in India (Delhi and Mumbai) which will add very good technical back-up for the market. This is very important for proper support of DLP projects during whole project life-cycle and InfoWatch offers here the best possible support. We already have two strong partnership networks in West India (Mumbai) and in North (Delhi). These networks are in active business development and very open for new cooperation's in terms of more partners and opportunities development. Secondly, we will proceed with active expansion to the South of India because while New Delhi is a capital of manufacturing and government industries and Mumbai is a financial hub, South India is the heart of IT sector, an important user of our security products, so it is a good region for development. Finally, with our current partner strength at 30+ and several distributors in northern India, and considerable amount of partners in western India, we are looking to build a strong partner network in the country.

Source