5 Similarities Between Data Loss Prevention Solutions And Business Practices

Most of the time, Data Loss Prevention (DLP) is a concept discussed in a meeting room with a handful of people: IT administrator, IT manager, and vendor representative (maybe a reseller or distributor). Usually, business managers are not part of the group, but they should be because a significant part of the confidential data that could be leaked is represented by business data: financial indicators, employee information, know-how, reports, data bases, etc. If there is one person in an organization that knows which information has to be protected against data loss or theft, the business manager is it.

Here are five instances where the business and the DLP worlds collide:

1. Business environment vs. Data Loss Prevention

Just like analyzing the internal environment (people skills, product and services, etc.), or the external environment (market trends, economy, competitors, etc.), business managers should consider DLP as a technology that identifies the biggest threat and enables them to take steps to prevent sensitive data from leaking. Inside vulnerabilities usually present more risk for data loss than external factors. If employees aren't motivated or trained about DLP the business is at risk, regardless of industry. In fact, studies show that simple human error is the most common cause of data loss. Lost or stolen USB thumb drives containing highly confidential data, files sent to the wrong recipients, data uploaded to the cloud or transferred by Skype or other applications, are to blame for some of the most infamous data breaches.

2. Business investments vs. DLP formats

If a business manager wants to buy a fleet of cars to transport merchandise, he or she will buy pick-up trucks, but if they want to get to the destination fast and get noticed, sports cars will be purchased. The same goes for DLP. An IT administrator will choose a cloud-based solution to set up policies for staff to work securely from a coffee house or home. If he has a virtualization infrastructure, he will definitely choose a virtual appliance. It all goes down to making the right choices, depending on the purpose and environment.

3. Physical security vs. data security

To protect a company against burglars, the weakest points are secured: doors, windows, garage doors. Some companies resort to installing video surveillance cameras. In information security, the most vulnerable exit points are: portable storage devices, cloud services, instant messaging applications and e-mail. Data Loss Prevention solutions can block transfers to removable devices and online application and simultaneously, in real-time, monitor the users' activity to detect any unusual data transfers.

4. Organizational chart vs. DLP policies

The creation of an organizational chart enables management to establish clear workflows and delineate authority, which leads to operational efficiency. Data Loss Prevention software allows different security permissions to be set for data transfers and the use of portable storage devices. Similar to an organizational chart, it establishes which employees have the authority to transfer which information outside the company. Rights can be set for groups, computers, users or devices and different filters created. For example, some users can be blocked from copying Excel files to external HDDs, others from uploading a document containing credit card numbers on Gmail, and other staff prevented from transferring documents containing the word "salary." Employees can be stopped even if they copy and paste data that contains confidential words set by the administrator or if they try to make screen captures.

5. Business compliance vs data protection compliance

Companies must comply with legal, economical and other laws. Tax evasion, illegal laborers, and the violation of quality standards are all punishable by huge fines or even prison time. Data protection laws have been in place for some time now, and regulations like PCI (Payment Card Industry), HIPAA (Health Insurance Portability and Accountability Act), PII (Personally Identifiable Information) are very strict. Non-compliance with such legislation can lead to fines ranging from thousands of Euros to millions. On top of this, a data breach or data protection violation can end up in press and badly affect a company's image (like retailers Target or Neiman Marcus). What has been built in years of work can be destroyed in a matter of seconds.

By Roman Foeckl, CEO and Founder of at CoSoSys

Roman is the Founder and CEO of CoSoSys. Before founding the company in 2004, Roman worked for Goldman Sachs in Frankfurt, Germany and Paris, France. He studied business in Wiesbaden, Germany. After the acquisition of CoSoSys by Astaro and the subsequent acquisition of Astaro through Sophos, Roman together with Michael Bauner took the company private again in a Management Buyout (July 2011), with the goal to build CoSoSys and its Endpoint Protector product family in the leading content aware Data Loss Prevention (DLP) and Mobile Device Management (MDM) offering on the market. Roman's vision is to offer an easy to use and implement Data Loss Prevention Solution that covers all popular platforms, from Mac OS to Windows and Linux, so large and small businesses can protect their data against accidental loss or intentional data theft.

March 25, 2014