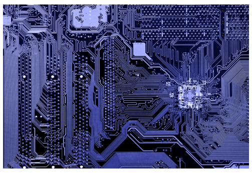
Why Data Loss Prevention is More of an Objective than a Data Security Solution for Most Companies



"Yes, we have a data loss prevention solution in place. We use firewalls and antivirus software."

These are the words that make sales reps both happy and sad when testing the market for customers of Data Loss Prevention (DLP) solutions. DLP can be very confusing; for most businesses, it ends up being more of a goal than a data security solution.

Let's explore three main reasons for why this is so.

1. **The Term Itself**

"Data Loss Prevention" doesn't sound like a typical software solution. It is a very general term and can be done any number of ways in practice. For instance, encryption helps to prevent data loss, but antivirus shares this goal. Indeed, there is a difference between "backup systems" and "data loss prevention" in that the latter is not sufficiently technical or specific. Maybe this is why Gartner has modified the term to "Content-Aware Data Loss Prevention" instead.

2. **The Vendors**

Some vendors use this concept for a suite of security solutions, including antivirus software, firewalls, device control features, Hard-Disk Encryption, Mobile Device Management, etc. Meanwhile, others use it in a more restricted sense, such as in reference to technology that filters company data through different storage devices, online applications and the cloud. Data Loss Prevention has grown tremendously, both as a concept and technology, in the past years. Even so, there is still no standard, no convention, so businesses can interpret DLP however they please. It is therefore up to us as vendors to do a better job explaining what we mean by this term.

3. **The Mentality**

As vendors, we still get a lot of invitations to cybersecurity events, and even today we still encounter skepticism from organizations regarding our products that help mitigate insider threats. Insiders cause most of today's data breaches, yet people think that the severest of cyber threats originate from external actors. This is not exactly an unreasonable mindset. Given the history of antivirus software and firewall solutions, it is justifiable to grant these technologies more of our attention than we do Data Loss Prevention, which is still a relatively new concept.

It is clear that it will take many years for people to understand DLP. Before that happens, it will still take a substantial amount of time for experts and vendors to arrive at an agreement regarding how to build and promote DLP solution suites.

This does not mean that DLP is meaningless now, however. In the meantime, no matter how they perceive it, organizations must begin to recognize Data Loss Prevention as an opportunity to protect their assets and ensure business continuity. This will better equip them to handle some of the threats of tomorrow.

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.

June 6, 2014