Best Practices for Data Loss Prevention

By Roman Foeckl, Founder & CEO, CoSoSys — November 30, 2014

CSOs and CISOs know it takes just one weak spot for someone to steal data or cause harm. The increasing role of mobile devices in business, and BYOD and cloud-based file sharing services, also increase the risks because critical information can more easily leave the physical confines of your company.

Mobile and portable storage devices, and online collaboration tools, are huge risks for data leakage. However, adopting best practices in Data Loss Prevention (DLP) can make securing your data very manageable.

Training and educating employees to protect data are important, but if you allow access to data via USB storage and mobile devices, or through non-enterprise grade applications, that is not enough.

Robust DLP and MDM solutions enable control of use of removable devices, filter data transfers through online applications, while securing and managing mobile devices. Encrypting key data is absolutely vital.

There are many DLP solutions, yet their complexity—or perceived complexity—delays adoption. A solution offering ease of use and AES 256-bit strength encryption will encourage more adoption. Such a solution must integrate with your device control solution to turn any USB stick into a trusted device. If the encryption is tampered with, it will automatically delete any data on the USB stick.

In addition to encryption, here some best practices:

- **Evaluate DLP solution forms.** The popular options (hardware appliance, virtual appliance, cloud-based/SaaS and Amazon Web Services) each have strong pros and cons and should be properly evaluated.
- **Choose a cross-platform solution**. Pick a solution that works on Apple OSes and Windows. Build a platform with the flexibility to handle evolving and changing needs. Build to adjust for future developments to limit potential operational overhauls.
- **Set authorization levels according to departmental and task requirements** .Controlling and managing data loss prevention is easier when access to key data is determined by user, workstation, device or group. Ensure that two users on the same device can have two completely different levels of authorization for transferring data. This flexibility marries convenience with security.
- **Establish and communicate clear policies regarding mobile devices.** To protect mobile data, enroll each device with an MDM solution. This weds the productivity advantages of mobile devices with the security of MDM solutions (i.e., remote lock, remote wipe, establish secure passwords, etc.). Ensure mobile users know your policies for storing company data and the consequences of non-adherence.
- **Test a variety of risk scenarios, such as content and portable device threats** . Focus on threats from newer technologies, but remain aware that older technologies (CDs/DVDs) can still cause losses. Risks to unencrypted data in a local folder and data stored in the cloud are also at risk.
- **Consider resources for advanced features**. Before you deploy a DLP solution, consider the resources required to execute advanced features like file tracing and file shadowing; the amount of data being monitored and the number of copies stored could quickly absorb a sizable part of your resources if you activate all features.
- **Look at cloud-managed DLP**. A cloud-based DLP solution offers easy evaluation, implementation and scalability. It's a good way to safely reap the benefits of the cloud while protecting data.

Adopting and maintaining best practices in data loss prevention offers strong ROI if carefully planned and executed. There is no universal DLP solution. Best practices can be modified to meet your unique needs. Data loss can damage your operations and brand.

Manage your exposure to risks by following a sound DLP strategy and executing it effectively. Do you want to commit the time and resources to minimize exposure, or deal with massive damage after a loss?

Be proactive. Make the right moves today to protect your employees, data and business.