potential to pose truly disastrous results for a company and its clients. For instance, in 2012, a public accounting firm was contracted to perform financial statement auditing services for a client.

May. 22, 2013

From the June 2013 issue.

About 72% of the 855 data breaches worldwide analyzed in 2011 by Verizon Communications Inc.'s forensic analysis unit were at companies with 100 or fewer employees. That represents an increase of 63% of the 761 data breaches it analyzed in 2010.

The figures included investigations conducted by Verizon's team, as well as data-breach investigations by various law-enforcement groups around the globe, including the U.S. Secret Service and the Australian Federal Police.

For many CPA firms, data leakage is becoming an increasing problem, with the potential to pose truly disastrous results for a company and its clients. For instance, in 2012, a public accounting firm was contracted to perform financial statement auditing services for a client.

An employee of the accounting firm accidentally removed several CD-ROMs from the office containing a list of the client's workers' compensation claimants and a list of equity shareholders in the client's company, that were later reportedly stolen from the employee's vehicle.

The workers' compensation information contained names, claim numbers, medical status, and date of loss, and the medical status information included the employees' claim for injuries or illnesses.

While larger organizations generally face greater risk, any level of data leakage can

Accounting for the Human Factor

No matter how robust an organization's security protocols are, human error remains the greatest risk of all. This risk is magnified in the age of BYOD (Bring Your Own Device) and collaboration tools. When employees open files on their personal devices, those documents are only protected to the extent of the devices' personal security settings — or lack thereof.

Personal devices tend to be insecure and more open to hacking and theft than company devices. In addition, an employee could lose a device with important information and put the company at risk.

Collaboration tools are simple to use, but likewise leave a lot to be desired when it comes to content control. The most common items of reported theft and loss include email attachments, USB drives and documents residing on collaboration/sharing platforms like DropBox, which is less secure than many other platforms when it comes to regular in-house usage.

It loses even more security when used as a collaboration tool for outsourcers, partner businesses, and other third parties. Add mobile devices into the mix and combine them with the ways that data is commonly lost, as well as the fact that Dropbox's contents can be easily accessed by tapping on a folder icon, and you'll see why many businesses are choosing other content security solutions.

Working with clients near and far often requires transmitting information both inside and outside of the firm itself, which can increase your risks for losing control of sensitive data. Without the right safeguards in place, collaborating with other parties can expose the organization to major theft and lost competitive advantages.

However, new technologies exist that enable enterprises to simply and securely share

Olson delivered her annual report to Congress, and the findings were startling: as of September 2012, the IRS maintains more than 650,000 unresolved cases of identity theft.

Perhaps even worse is that in 2012, the most common tax-related complaint from members was that they could not file a return electronically because a Social Security Number (SSN) listed on the return had already been received by the IRS on another return.

Mapping the path of content delivery, tracking content usage and having the ability to terminate content access from anywhere are all keys to content security. If these three capabilities are in place, content can remain secure no matter where it is sent across the cloud.

The first step is establishing a protocol and utilizing tools to ensure content security from inception to disposal. Your organization needs to map out the typical flow of content and then implement the use of tools that will help you maintain security throughout that flow.

Secondly, you need to have tools for tracking content usage. In many cases, the increased risk of data breaches described in the NTA report can be avoided if there are tools in place to track and manage content usage. Being able to see how, when and where content is being used can help organizations stop a breach before it starts or at least control the spread of information.

Finally, termination of content access can be a line of defense between corporations and data thieves. Regardless of whether the threat is coming from an internal or external part or even a third party source, terminating content access remotely and automatically can stop a data breach in progress.

Content security issues are going to become more commonplace unless

Firm Management • Security