3 essential steps to prevent employees from using unsanctioned file-sharing tools

If your employees use cloud-based file-sharing tools that you prohibit, you're likely aware of the challenges this creates within your organization and your information strategy. In a recent AIIM research report, **What's happening with file sync and share?**, organizations shared their three biggest areas of concern:

- Lack of visibility into what's being shared and where it's located
- Inability to control who is sharing and accessing your information
- Risk of unintentional access being granted

With these challenges in mind, how can you empower your employees to get their jobs done while preventing them from using unsanctioned tools? Beyond the obvious step of restricting access to URLs for certain cloud-based products, there are three essential steps you can take to ensure safe content sharing.

1 STEP 1: EDUCATE YOUR EMPLOYEES

When asked how their organizations address information-sharing challenges today, a staggering 65 percent of respondents in the AIIM study cited education as their primary method of defense.

Interestingly, as this research points out, organizations rely on education more so than other tangible solutions like the use of technology or strict policy enforcement.

With this in mind, how can you empower someone to do something while making them aware of the risks of a bad decision? Through the right education, of course.

It's like the lesson we all learned as children, "Stop, look and listen." You can tailor this conversation to help your employees **stop and think before they share information with others**.

ShareBase® by Hyland

2 STEP 2: PROVIDE A VIABLE, CORPORATE-APPROVED TOOL FOR EMPLOYEES (NOT JUST EMAIL)

In the world of content sharing, email is a tool you can't ignore. In fact, 85 percent of respondents in the AIIM survey cited using email to share, putting it at the top of the list – even above cloud-based sharing applications.

So, why are cloud-based sharing tools becoming so popular if email has been there all along? While frequently used, email presents the exact same concerns as cloud-based sharing tools but without the many benefits of a secure sharing platform.

First, there's a lack of visibility into what's being shared and where it is. Sure, email might provide some ability to track down who shared what and with whom; however, no one would argue that this is a cumbersome task at best.

Does email give you the ability to control who is sharing and accessing your information or mitigate the risk of granting unintentional access? Absolutely not. As soon as an email leaves your server, it can get into anyone's hands.

On the opposite end of the spectrum, other forms of sharing include sending a password-encrypted USB drive or setting up an FTP download site. While these methods address some concerns and might be perfectly valid for some situations, they are both slower methods of secure document sharing.

Clearly, a viable, secure file-sharing alternative is needed to address these challenges, offering the speed of email but the same security and control as FTP sites and USB drives.

3 STEP 3: ASSIGN A CLEAR OWNER FOR THE PROBLEM

In the AIIM survey, when asked, "Who, if anyone, is responsible for ensuring the proper use of content sharing tools, policies and procedures?" the answers revealed an important insight: There's no clear standard across organizations.

In fact, 45 percent of organizations said it was the responsibility of IT staff; 33 percent said line-of-business executive, department head or process owner; 21 percent said information governance manager/director; 11 percent said chief compliance officer; and the rest said either the CIO, COO or other.

The 32 percent who have someone dedicated to information governance or compliance are due a congratulations. This is an excellent role and/or department to own this area as they can look holistically at how information is managed across all tools.

For those organizations unable to staff a dedicated governance or compliance position, you have some decisions to make. The key step is to choose someone who you will hold accountable for the content sharing problem, and then make sure everyone in your organization is aware where the responsibility lies.

While there are many challenges, there is a clear path to combat the content sharing quandary and prevent your employees from using unsanctioned tools: Educate them, provide a viable alternative and assign ownership over the issue.

Remember, you can't stop employees from sharing content, but you can help them stop, think and then choose the right tool to share.

ShareBase® by Hyland