Does Dropbox scare you?

Based upon seeing the following article on the ease of sharing files with Dropbox, http://www.macworld.com/article/164477/2011/12/share_files_with_dropbox.html , I wrote the following post to my own LinkedIn account, "Does Dropbox scare you as much as me? Serious security, privacy and eDiscovery concerns with this highly used cloud service..."

Now I hesitated seriously prior to posting as I never want to disparage a technology without having personally used it unsuccessfully first, and that is not the case here. I am not a day-to-day Dropbox user, although I have received a video from a friend via Dropbox and was easily able to see the streaming content sent to me, considering it was larger than a traditional email could support. My problem is not with the technology itself, in fact the technology works so well that is the problem, not its lack of functionality, but rather the ease of use and depth of its capabilities.

My concerns for security with this technology go beyond reading an article. I have firsthand knowledge of field use of Dropbox by a friend of mine from high school. This friend went to business school, then MBA, and works for a multinational conglomerate F100 corporation, based in NYC. My friend has no concern for security, eDiscovery, Information Governance, those are foreign terms to a high-level sales executive, his concern is having the right content when and where he needs it, and being able to access everything from his iPad while on the road or at home, away from the office.

All we were doing was discussing a day in his life and he starts going on and on about how easy it is for him to use this Dropbox application. He goes to the office on Monday, and drops everything he might need for the week into his Dropbox account for use during the week. Now the concern I have for my friend has to do with the ease of sharing files using Dropbox. As indicated earlier it is so easy to use that a person can just drag and drop files. What type of security is built in that would prevent a user from inadvertently dragging in a file that contained sensitive data or NPPI.

I am not worried about my high school friend as a security concern. According to an Computer Economics
study in 2009 analyzing Security Threats and Employee Misuse of IT Resources, 57% of employees mishandled Portable Storage Devices.
http://www.computereconomics.com/article.cfm?id=1436
Which leads me to be worried about employees who are malicious, and are looking to steal IP or PII from his/her employer. I am worried that Dropbox enables the user to move large files outside of a firewall without security protocols preventing this from occurring. We must not forget "
Bradley E. Manning,
a US Army soldier who was arrested in May 2010 in Iraq on suspicion of having passed restricted material to the website Wikileaks. He was charged in July that year with transferring classified data onto his personal computer, and communicating national defense information to an unauthorized source. Manning had been assigned in October 2009 to a unit of the 10th Mountain Division, based near Baghdad. There he had access to the Secret Internet Protocol Router Network (SIPRnet), used by the United States government to transmit classified information."
http://en.wikipedia.org/wiki/Bradley_Manning

What is the difference between burning CDs, printing out confidential documents and emails, or emailing corporate information to yourself to avoid a paper trail, and using Dropbox to evade corporate policy? Nothing.

So, what should you do to prevent a situation like Wikileaks from occurring with your corporate data? Have policies in place proactively, but make sure you can enforce those policies. Put security controls in place to monitor the content that employees are placing into collaboration tools such as Dropbox for restricted materials on your network. Take a closer look at the rights and permissions granted to different users. Invest in Data Loss Prevention (DLP) technology, and monitor it. Organize and categorize your business records and set up tighter controls on sensitive materials. Stay vigilant. Assume the worst, but hope for the best of intentions from your employees. Do not be afraid to safeguard your information. Information is the lifeblood of your organization and it should be protected at all costs.