

# 10 SharePoint Security Mistakes You Probably Make

**Bradley Manning allegedly stole sensitive government cables destined for WikiLeaks from a SharePoint server. Are your information security controls tighter than the Army's were?**

By **Mathew J. Schwartz**  InformationWeek

January 31, 2012 09:45 AM

How important is it to secure and monitor Microsoft SharePoint? Consider the case of Bradley Manning, the Army intelligence analyst who's [accused of leaking 250,000 government cables](#) to WikiLeaks. According to an Army investigator who testified at a hearing to determine if Manning should face a court martial, one of Manning's laptops contained an Excel spreadsheet, containing a tab with multiple [Wget scripts](#)--designed to download large numbers of files--that "pointed to a Microsoft SharePoint server" that stored documents for the Guantanamo Bay Naval Base detention facility, [reported Wired](#). The investigator further testified that "he ran the scripts to download the documents, then downloaded the ones that WikiLeaks had published and found they were the same."

In other words, the [release of sensitive government cables](#) may have been partially prevented, had the military better [secured and monitored its SharePoint servers](#).

Similarly, any business that relies on SharePoint to store confidential--or even sensitive--information should know who's accessing that data, and why. What's the best way to make this happen? Start by avoiding these 10 stupid, but common, SharePoint security mistakes.

**1. Poor security training.** According to a [survey of 100 SharePoint users](#) conducted by security vendor Cryptzone at a November 2011 [SharePoint Saturday](#) conference, 92% agreed that removing information from SharePoint made it less secure, but 30% were willing to take that risk "if it helps me get the job done." Obviously, there's a disconnect at many

businesses between security and productivity. Worryingly, 34% of respondents also said they'd never even considered the security implications surrounding SharePoint.

**2. Collaboration barriers.** Likewise, the survey found that 45% of users regularly copied sensitive or confidential data from SharePoint to their hard drive, to a USB drive, or to email it to someone else. In the majority of cases (55%), this copying was to facilitate information-sharing with someone who lacked access to the SharePoint documents. This highlights the need for businesses to put clear policies in place regarding how information can be shared, and then to monitor access and enforce policy compliance.

**3. Unclear security oversight.** Who's responsible for SharePoint security? At 69% of businesses, the Cryptzone survey found that [access management responsibility](#) fell to in-house IT administrators. But 22% of respondents--which included SharePoint users, administrators, developers, and architects--didn't know who was responsible, which suggests that there's a lack of oversight and thus access accountability at their businesses.

**4. Overly broad access rights.** When it comes to access, less is typically more. "One of the most common issues we see with SharePoint is end users having access privileges that are far too broad," said Enterprise Management Associates (EMA) senior analyst Torsten Volk, via email. "It's a lot of work to properly create user roles and map them to Active Directory," and even more work to keep them updated, revised, and removed after employees depart. According to Scott Crawford, managing research director at EMA, this challenge "has given rise to vendors such as Aveksa, Varonis, and others" to analyze usage patterns and determine likely data custodians.

**5. Not watching watchers.** According to Cryptzone, meanwhile, 34% of IT administrators told Cryptzone that they'd "[sneaked a peek](#)" at documents they weren't authorized to view, including employee details (for 34% of respondents) and salary information (for 23%). In other words, too often there's insufficient separation of duties between security overseers and SharePoint administrators.

**6. Failure to encrypt.** Out of the box, SharePoint's SQL database is unencrypted, but adding encryption can be difficult, and may trigger performance issues. According to EMA's Volk, however, "leaving content in plaintext does leave it vulnerable to discovery and exploit--and could raise regulatory issues in environments subject to regulation governing the protection of sensitive data." To help, Volk said security vendors such as CipherPoint can ensure data confidentiality, which also helps maintain a

separation of duties between security teams and SharePoint administrators.

**7. Sloppy search indexing.** Too often, said Volk, SharePoint administrators use an admin account for the search indexer, "which causes the search to surface results that are not meant for everybody." While these documents can't be opened, searchers can see a two-line preview. According to Crawford, "this is an example of something that is far too common in many other aspects of IT, when administrative accounts are used needlessly for operations that really don't require it, resulting in far greater exposure to risk."

**8. Poor Internet Information Services maintenance.** "Microsoft IIS must be patched regularly to be secure," said Volk, yet many businesses fail to keep their [SharePoint server software updated](#). "Systems maintenance for security can be a challenge for any organization, but is a particular problem for SMBs, who often simply do not have enough people, time, or expertise to administer properly," said Crawford via email.

**9. Poor endpoint security.** "SharePoint Workspaces now allow users to synchronize with SharePoint libraries, so that they can have access to SharePoint content offline," said Volk. But what happens if that endpoint should become compromised? Accordingly, Crawford recommends strong [endpoint security tools](#), including [disk encryption](#), to prevent PC breaches from spilling SharePoint secrets.

**10. Failure to scan for viruses.** Many organizations fail "to scan files that are uploaded to the content libraries," said Volk. "This can lead to the dissemination of malware via SharePoint." Likewise, he said, many businesses also fail to account for SharePoint databases in their [disaster and recovery planning](#).

When it comes to administering SharePoint, Crawford said that not all of the above "would necessarily be considered 'mistakes.'" While some are, "others reflect the challenges of administering an environment where content--often sensitive--is shared," especially when the tools involved haven't been designed to work, out of the box, in locked-down mode. In other words, if your business uses SharePoint to store sensitive information, ignore taking the time to secure and monitor access to that data at your peril.