In particular, those transition points, such as document scanning and printing, can ...

Jan. 25, 2017

When taking steps to protect online privacy, companies shouldn't overlook documents that transition between paper and digital formats during their lifecycle. In particular, those transition points, such as document scanning and printing, can introduce risk that threatens data privacy. Documents from employers, banks, vendors and more can include sensitive information such as social security numbers, bank account information and birth dates.

#1: Avoid Data Leakage

One way data privacy can be compromised is through documents that have been scanned and distributed by email. This unwanted "data leakage" occurs often when people have uncontrolled access to scanning combined with access to sensitive content.

"Safeguard privacy by placing filters within scanning applications to restrict document access. These content filters can search for specific words or character strings like 'confidential' or 'non-disclosure' once they are transformed to searchable format during the scanning process. After terms are identified, the software can take any number of actions, including automatically encrypting the file prior to sending, or perhaps quarantine or delete the file altogether." – Chris Strammiello, Vice President of Global Alliances & Strategic Marketing, Nuance Communications

#2: Protect Against Unauthorized Access

Oftentimes, companies make the mistake of attempting to cover up private information, like a social security number, by using a drawing markup tool, such as a rectangle with solid fill. That's a path to redaction failure.

“The only secure way to do redaction is with a redaction tool, commonly found in

industries, face mandated reporting requirements to avoid additional penalties. Printing is a data privacy tactic that is notoriously overlooked in this regard. Due to the non-searchable format of printed documents, they can be difficult to track and dangerous to store. Plus, consider the human error involved; accidentally taking the wrong document from the printer or maliciously distributing copies outside of an organization can be just as damaging as a hacker or malware. Establishing a robust print and capture log can help with these protection efforts.

“Studies show that 20 percent of all print jobs are never retrieved by the original user. Print management software can prevent exposure of information by holding your print job in a secure print queue until you authorize its output when you are at the printer. This protected print release allows you to print from anywhere on your network and pick up the documents when and where you want.” – Chris Strammiello, Vice President of Global Alliances & Strategic Marketing, Nuance Communications

———-

Chris Strammiello directs the worldwide Marketing and Global Alliances for Nuance’s Document Imaging Division.

Firm Management

Sponsors.