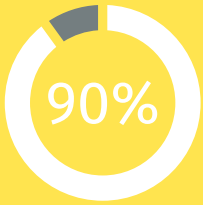
5 Hard Copy Data Security Risks in Every Office

Is your printed information secure?

Despite all the hype about the paperless office, hard copy documents still exist in every business.

As our dependency on printed documents continues to be challenged by new technologies, it's vital to make sure your sensitive data on paper is secure.

A 2019 Global Print Security Landscape Report revealed that small to medium-sized businesses are becoming increasingly concerned about print security.



of businesses have had a security breach in the last year caused by hard copy documents."

– The Digital Generation

are concerned about print-related security breaches." – Quorica

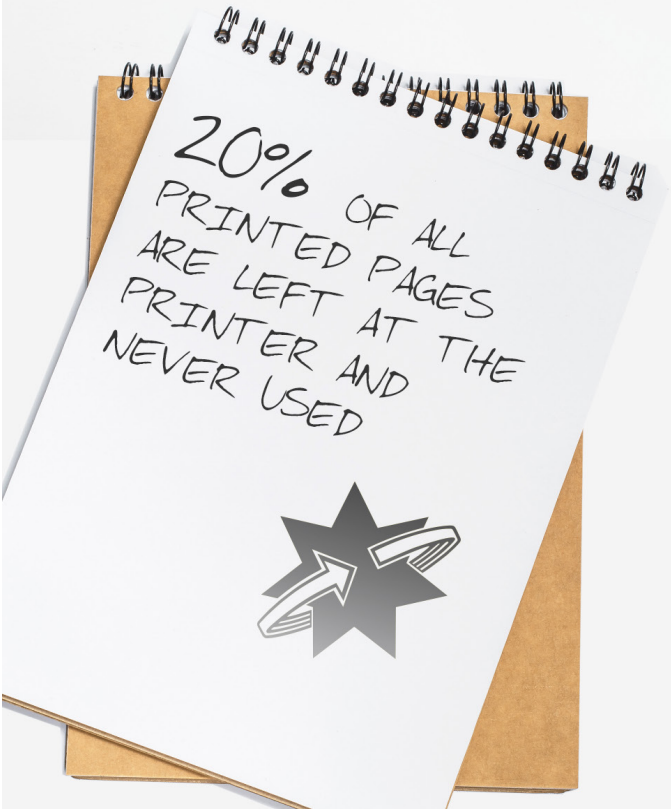
of print security incidents are caused by internal users." – Quorica

of business information still exists in hard copy format in most businesses." – Coopers & Lybrand

of business processes still require paper documents."

– Managed Print Consulting

More awareness of where confidential information may be exposed, will help you prevent security breaches.



Popular printed document targets include:

- Payroll Figures
- Financial Reports
- Bank Statements
- Employee Records
- Client Information

5 Common Hard Copy Security Risks

1. Copier/Printer Output Trays

Have you ever seen a stack of paper sitting in the office printer's output tray? It's a common sight. It would take virtually no effort for someone to see potentially sensitive information that they shouldn't. The time between when the job is printed and when the pages are picked up leaves confidential documents exposed to anyone walking by or picking up another print job. In fact, recent studies suggest that roughly 20% of all printed pages are left at the printer and never used. Be aware of your printer output tray, it could cause more data security breaches than you think

Document Security Tip: The simplest way to protect confidential information may be to place a dedicated printer in the executive office or high risk departments like Human Resources, Accounting, etc.. If you place a printer in an open area, newer technologies have the ability to restrict access to people given special permission or just the person who sent the job to print. A worker sends the request to the printer then punches an access code into the printer interface or even swipes their employee ID badge to retrieve their printed documents. This helps keep unauthorized eyes from seeing your sensitive information.

2. Filing Cabinets

Who has access to your filing cabinets? Are they locked or in a secure location? Unattended or unlocked filing cabinets present obvious risks of unapproved access. Unless your organization has a secure storage area or pays to have paper files stored offsite, chances are your confidential documents are left exposed. Those with malicious intent could access employee information, financial records, and client files.

Document Security Tip: Think about how your business stores documents and if there are any unsecured filing cabinets. Technology has advanced to the point that invoices, HR files, and other documents are easily scanned into a digital

3. Recycling Bins

Have you looked at what's in your office's recycling box lately? Some don't think twice about dropping paper documents into the office recycling bin since it's the right thing for the environment. This is especially true when 20% of printed pages are never used and the average life span of a printed page is less than five minutes. This is why office recycling bins can be a prime source of security breaches. Leaving paper in a blue box may make you feel good about helping the environment, but it could be providing easy access for people with the wrong intentions.

Document Security Tip: Walk around your office and look at the kinds of documents that are being placed in recycling bins. Ensure the disposal procedures are complying with data security laws. If not, create a policy for you and your employees to follow when discarding sensitive data.

4. Personal Workspaces

In a busy workplace it's easy to leave confidential information exposed to wandering eyes. This includes documents left on top of desks and in unlocked desk drawers as well. Having documents handy while working is great, but precautions need to be taken to keep this information secure. Keep in mind that fellow office workers and third-party contractors may have access to your office space during or after business hours. You and your employees should make a habit of tidying your workspace of documents anytime you're going to be away from your desk for any amount of time.

Document Security Tip: Create a simple document security policy that outlines how people should protect confidential information in their workspaces. Enforce it with random checks but make it a little competition with incentive to comply with the policy.

5. Dumpster Bins

Data thieves don't need access to your office for this one! When trash is removed from your office, where does it go? Printed pages are often mixed in with everyday garbage and thrown into a dumpster behind the office building. This opens up another vulnerability to your private information. Savvy thieves can easily access this information and leave you open to a host of liabilities.

Document Security Tip: Take the initiative to remind your staff of the proper way to discard paper documents and don't assume that everyone knows your disposal policies. Knowledge is power when it comes to preventing data breaches from improper document disposal.

BONUS TIP: Don't Forget the Printer Hard Drive

Did you know that the hard drive in your printer stores data from recently printed documents? Most people don't think about what could be exposed when discarding an office printer. If you don't remove or destroy the hard drive, it's not difficult for the wrong person to extract your data in seconds.

Document Security Tip: When you are ready to upgrade to a new printer or copier, make sure to ask your provider about erasing the printer's hard drive properly to ensure no one can access a digital version of you're the confidential documents you recently printed.

Need help with document security?

Ask a local Cartridge World for your free, no-obligation printer assessment. With the right printer program or managed print services, you'll streamline your printing and identify processes that will secure your documents and stay on top of newer printer technology.