

9 HARDCOPY DOCUMENT SECURITY RISKS

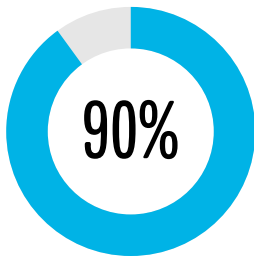
DOCUMENT MANAGEMENT SECURITY GUIDE



ALLIED
BUSINESS SOLUTIONS

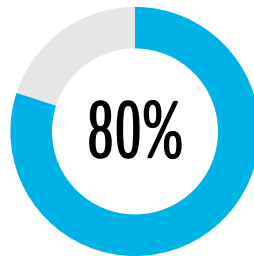
IS YOUR DATA SECURE?

Hardcopy and digital documents exist in every office. Most with business relevant information you need to advance a business process, make a business decision or serve your customers better. The typical unorthodox blend of paper and digital documents can be difficult to manage and as a result, create security risks you need to be aware of.



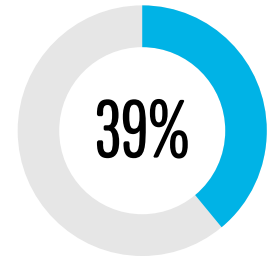
“90% of companies have had a **security breach** in the last year from **people accessing hardcopy documents.**”

- The Digital Generation



“80% of business information still **exists in a hardcopy** format in most businesses.”

- Coopers & Lybrand



“39% of business processes still require **paper documents.**”

- MPS Consulting

By managing documents better, organizations can make their knowledge workers more productive, reduce document related expenses and boost the security protection of sensitive information.

In most cases, this is achieved by merging paper documents into digital workflows with today's multifunction systems and easy to use software that restricts user access, enhances version control and eliminates the risk of loss or damage associated with a hardcopy document. It's never been easier to make your information more secure yet so few organizations prioritize this area of concern until it's too late.

ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCATELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

A FEW QUESTIONS TO CONSIDER....



What % of your organization's processes still require **hardcopy documents**?



Are you leveraging scanning to create **digital documents**?



Do you have people in your office that could **pose a threat**?

Popular Hardcopy Targets

-  • Payroll Figures
-  • Company Financials
-  • Bank Statements
-  • Employee Records
-  • Customer Information
-  • Proprietary Data



ALLIED.tech

BOISE • ONTARIO • IDAHO FALLS • POCA TELLO • SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

RISK 1 **FILING CABINETS**

How do you prevent access to hardcopy files? Unattended or unlocked filing cabinets present obvious risks of unapproved access in most offices. Unless your organization has a secure storage area or adopted a digital document management system, chances are unauthorized people may gain access to confidential employee information, financial records and sensitive customer information.



RISK 2 **RECYCLING AND DISPOSAL PRACTICES**

How do you dispose of confidential hardcopy documents? Private information that is not shredded or disposed of properly provides easy access for people with the wrong intentions.



RISK 3 **UNAUTHORIZED COMPUTER ACCESS**

Do people in your office take information security seriously? Without proper access controls in place, unsecured computers can be a major access point for confidential information when a person is away from their desk, before or after hours.



ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

RISK 4

OFFICE PRINTER HARD DRIVES

Did you know data is often stored on the hard drive of your desktop printers and MFPs? Today's printers have internal hard drives that retain confidential information and malicious people have developed software to extract the images of printed pages if the device lacks basic security protection. Also, before disposing any print device, it is highly recommended that you or your imaging partner remove all data from the hard drive to prevent access to previously printed files.



RISK 5

PRINTER OUTPUT TRAYS

Have you ever looked at someone else's printed pages? Delays in picking up print jobs leaves confidential information exposed in an unattended output tray available to anyone walking by. Newer technologies allow print jobs to wait to be released until the user arrives at the print device.



RISK 6

NETWORKED MFPs

Did you know hackers can use MFPs to gain access to your network? Like any network enabled device, proper precautions should be taken to protect your office MFPs with the same protection you use to protect computers to avoid malware and accessibility by hackers.



ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCATELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

RISK 7

CLOUD STORAGE

How do you prevent access to hardcopy files? Unattended or unlocked filing cabinets present obvious risks of unapproved access in most offices. Unless your organization has a secure storage area or adopted a digital document management system, chances are unauthorized people may gain access to confidential employee information, financial records and sensitive customer information.



RISK 8

MOBILE PRINTING

How do you dispose of confidential hardcopy documents? Private information that is not shredded or disposed of properly provides easy access for people with the wrong intentions.



RISK 9

WI-FI CONNECTIVITY

Do people in your office take information security seriously? Without proper access controls in place, unsecured computers can be a major access point for confidential information when a person is away from their desk, before or after hours.



ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

LET'S AVOID A BREACH IN YOUR OFFICE

ALLIED is open to helping you mitigate these document related risks with our new technology solutions designed to:

-  Prevent wrongful exposure
-  Improve productivity
-  Reduce document related costs



Contact us today to learn more about our complementary document assessment service that includes quick and easy ways to identify potential risks and highlight areas to improve.



ALLIED.*tech*

BOISE · ONTARIO · IDAHO FALLS · POCATELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY