



Work Like Tomorrow.™

DOCUMENTS ARE YOUR BUSINESS

WORK LIKE TOMORROW: BALANCING DOCUMENT SECURITY WITH
WORKFORCE PRODUCTIVITY

CAN YOU PROTECT YOUR DOCUMENTS AS WELL AS YOUR CONTENT REPOSITORIES?

KOFAX

CONTENTS

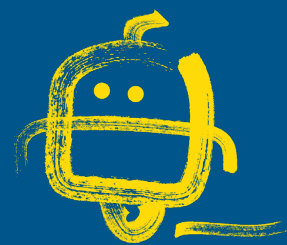
Information Reigns1

It isn't just Human Error2

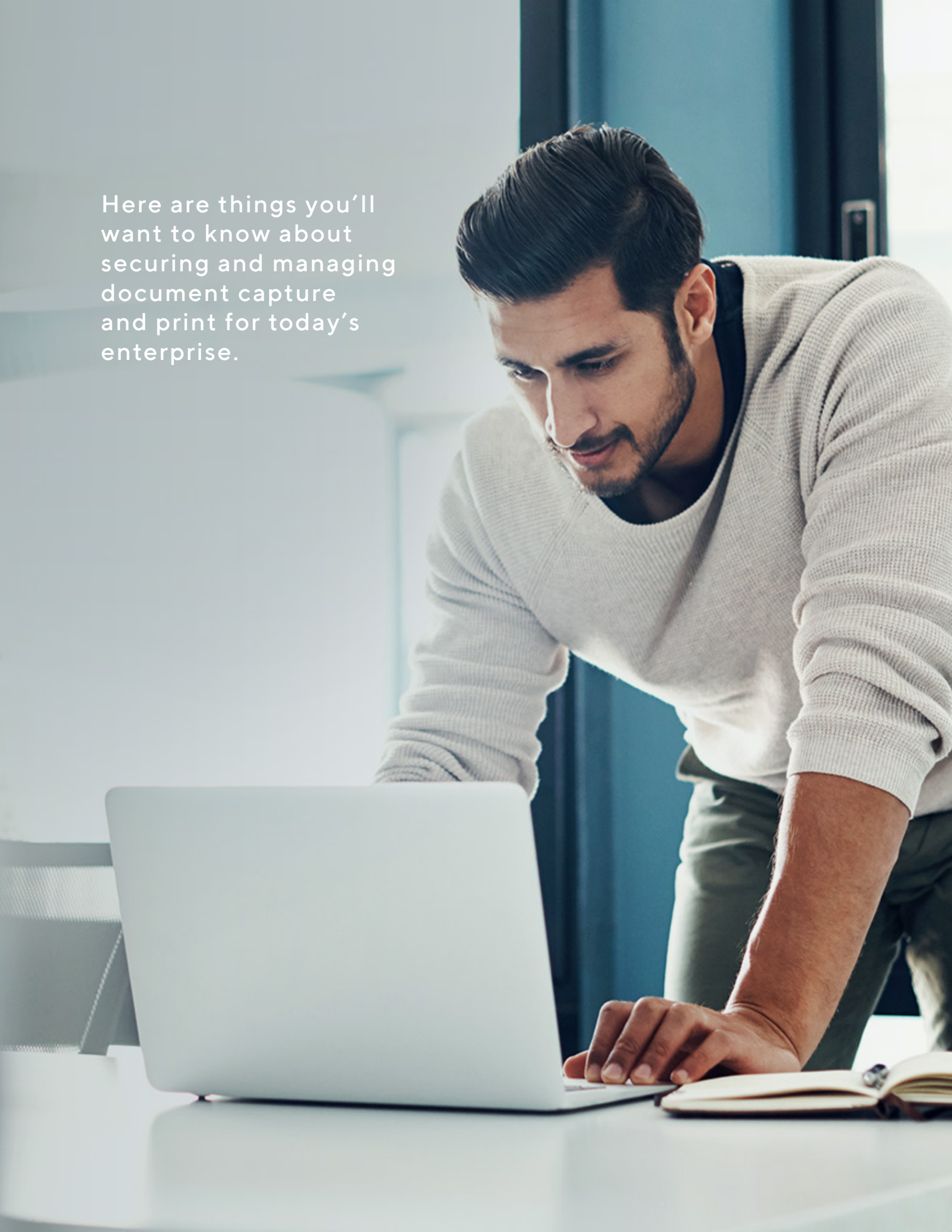
Is there a Way?.....3

It Isn't Hopeless4

Final Thoughts8



Here are things you'll want to know about securing and managing document capture and print for today's enterprise.





INFORMATION REIGNS

Your enterprise can't function without transmitting information, countless times every day, through documents—both physical and digital. And that's where trouble begins.

When was the last time you:

- ♦ Opened the cover of the copier to find that someone had been photocopying a customer's file in full color. And yes, the magenta cartridge is now empty.
- ♦ Found somebody's job offer letter on a printer tray.
- ♦ Pushed the button to make 25 copies and walked away—only to return, finding the copier had been set to 250.
- ♦ Spent 15 minutes composing an indignant retort to a rude customer email, another 15 minutes toning it down, and finally clicking send—only to realize you sent it to "reply all" instead of just "reply."
- ♦ Scanned in multiple customer files and meant to scan to your email, but sent to a broad distribution list exposing personally identifiable information to multiple employees.



**They are moments of humor and disgrace,
and everyone can name countless examples.
They happen every day in workplaces around the
world—but oftentimes, the results can be anything
but trivial.**

Just look at the [consequences](#) to one Australian government agency of mistakenly copying a journalist on an internal email. And physical documents are just as prone to mishandling. A senior staffer for the U.S. Department of Homeland Security accidentally [left documents on an airplane](#) containing drills for a biological warfare attack at the Super Bowl. (Also left behind? His travel itinerary and boarding pass.)



IT ISN'T JUST HUMAN ERROR

Stir cyberthreats into the mix: sophisticated actions by malicious parties to gain access to your information. There is a real and rising risk that, every day, the documents within your organization are the targets of cybercrooks.


A [2018 study of data breaches](#) by Verizon found that the top two assets from theft and loss breaches are paper documents and laptops. The most common location of theft was the victim's work area or employee-owned vehicle. Your organization is spending vast sums of money to protect applications—every company's crown jewels.

How can you possibly govern the internal and external spread of documents, both digital and physical?

With more than [75 billion devices](#) expected to be connected to the Internet worldwide by 2025, we have no choice but to find much better ways of protecting the information that flows throughout our organizations. Gartner expects we'll be spending [\\$3.1 billion on Internet of Things \(IoT\) security](#) alone by 2021.

SCAN THIS

In most enterprises today, "automated scans" means a scanner with a document feeder on top. But scans can be automatically routed to a storage repository the moment they're created. And targeted data can be automatically redacted, including hidden data. Your manual processes can be replaced today with automated solutions—without adding metadata to confuse document search capabilities.



The genie is out of the bottle. And we have no good solutions for corking it back in. So, perhaps the solution is to make the genie our friend?

IS THERE A WAY?

Nothing is as routinely mishandled, overlooked, abused, and subject to waste as documents. But we can't survive without them. In a very real sense, documents are your business. Did you know?

- ◆ 63% of organizations have reported print-related data breaches
- ◆ 90% of organizations have reported print-related data losses
- ◆ 71% of all cybersecurity incidents are caused by inadvertent employee actions
- ◆ 21% more security vulnerabilities have been detected in connected devices including printers, laptops & smartphones



And these challenges aren't diminishing. What about Bring Your Own Device (BYOD) initiatives? [Unsecured devices pose special threats](#) and often require additional layers of security. Are your workers more mobile than in prior years? Are they working remotely more often? Are your documents now being accessed and distributed globally? Mobile workers = mobile documents. And that equation puts you at even greater risk.

When your documents are not tightly managed and secured, you are exposing your business to a whole spectrum of risks:

- ◆ Are documents getting into the wrong hands through carelessness or breaches?
- ◆ Do your documents get to the right people at the right times to ensure business productivity?
- ◆ Can you accurately monitor and report on document movements throughout your organization to assure regulatory compliance?

ARE DATA BREACHES ALWAYS HIGH TECH?

Nearly ten years ago, a news organization conducted [an investigative report](#) in which they purchased four used copy machines and examined their contents. The results were horrifying. On one machine, documents were still on the copier glass from a police unit. Other finds from the same four machines?

- ◆ Documentation for domestic violence complaints and a list of targets in a drug raid
- ◆ Design plans for a building near Ground Zero in New York City
- ◆ 95 pages of pay stubs with names, addresses, and social security numbers
- ◆ \$40,000 in copied checks
- ◆ 300 pages of individual medical records, including drug prescriptions, blood test results, and a cancer diagnosis

Almost equally tragic: document security measures have changed very little in the past ten years, even though document capture, access, and portability have increased.



IT'S NOT HOPELESS.

We can get the genie under control. And it doesn't have to be expensive or difficult. You can mitigate security risks by creating document print and capture policies that are easy and intuitive for employees to work with.

POLICIES LIKE THESE:

- ◆ Follow-you-printing ensures workers can print and pick documents on-demand anywhere, anytime
- ◆ User-based authentication and access via mobile devices, touch screens, or card readers that control the production of multi-function printers (MFPs)
- ◆ Watermarking, encryption, and data conversions that are automated
- ◆ Know where your data is going and where it's been with automated audit trails, making failed document compliance audits a thing of the past

AND THERE'S MORE

- ◆ Automated file quarantine and other data loss prevention methods
- ◆ Track all print, capture, and routing activities in configurable reports
- ◆ Chain-of-custody documents track who has accessed or printed what information
- ◆ Automate workflows and information routing, eliminating "oops" and "gotcha" emails
- ◆ Smart business logic can dynamically route information to the right applications at the right times without user intervention
- ◆ Future proof your organization through highly-configurable workflows that adapt as your business infrastructure changes



If you're wincing at the potential costs of these new capabilities, never fear.

You can also leverage them to reduce hard costs—while equipping your fellow employees to become more productive, whether they're working with data in the cloud or on-premise.

- ◆ Diagnostics and controls can actively monitor and govern print usage and behaviors, by employee, department, and device
 - ◆ Your workforce can securely print, capture, process, and route documents and images from mobile devices
 - ◆ Automatically re-route print jobs within pre-defined parameters for automatic print failover
 - ◆ Print, capture, and route documents with a single, unified user experience, eliminating the learning curve for these new capabilities
 - ◆ A single installer for administering print, capture, and workflows, easing the burden on everyone
 - ◆ A single mobile app can be available for employees to use for print, capture, and routing
-

And you should be able to exercise these new capabilities and controls without ripping and replacing your costly machines, including those ubiquitous multi-function printing (MFP) fleets. Your document capture, distribution, and management solution should work across any hybrid environment.

- ◆ Simple solutions for centrally managing mixed MFP fleets, including a single, integrated authentication platform
- ◆ Easily control and enforce print, capture, and routing controls across all devices
- ◆ Give the business complete visibility into print and data capture behavior and costs
- ◆ Create consistent user experience across all devices

No single solution?
Not yet.





The U.S. Federal Trade Commission says,

“Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities.”

(“Protecting Personal Information: A Guide for Business”)

Your documents are at risk and under attack. And your vulnerabilities are so numerous and diverse, with more being spawned every day, you’re overdue a new solution. You need a new way to secure your documents, digital and physical, and their valuable information, including capture, distribution, and print.

We believe your documents and the information they contain are too valuable to be left to a patchwork quilt of methods, systems, interfaces, acts of forgetfulness, and even hostility. Someone needs to provide a better solution. And we’re stepping up.

Kofax will provide you with a solution that weaves data security, best practices, workflow management, and distribution monitoring and governance into a single strand. It actively manages, secures, governs, and monitors virtually every aspect of your documents’ lifecycles: printing, scanning, routing, storing, and tracking, across any combination of hybrid systems, technologies, and devices.

With the right Kofax solution, your organization will be equipped to engage today like the digital workforce of tomorrow.

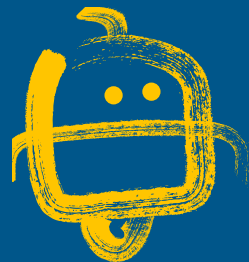
Kofax software enables organizations to
Work Like Tomorrow™—today.



**We know documents are
your business.**

**Ensuring they're safe, compliant,
and productive is ours.**

To learn more, visit WWW.KOFAX.COM/CONTROLSUITE.



Work Like Tomorrow.™

KOFAX

kofax.com

© 2019 Kofax. Kofax and the Kofax logo are trademarks of Kofax, registered in the United States and/or other countries. All other trademarks are the property of their respective owners.

