Canon

```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror mod
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the act
    #mirror_ob.select = 0
```

SECURING CLIENT DATA IN A DIGITAL AGE

WHY DOCUMENTS ARE AT RISK, AND WHAT YOU CAN DO ABOUT IT.

Law firm data breaches and lawsuits related to those breaches have surged. Clearly, protection of client data must be a priority. However, studies show that, while nearly three-quarters of law firms believe they are more secure than their industry peers, actual results show significant security gaps across firms of all sizes.[1]

New Threats Move Fast

Activist groups, disgruntled employees, and cybercriminals know that law practices own rich repositories of information chronicling mergers and acquisitions, civil and criminal cases, real estate transactions, and more. Given the sensitive nature of legal data, attorneys may be more willing to pay ransomware demands rather than risk a firm's reputation or delay time-sensitive matters.

Unfortunately, lack of standardization, outdated equipment, and innocent mistakes can put law firms at risk of exposing client data. But many firms still do not have an overarching information governance strategy in place to comprehensively control document creation, access, and flow.

3 Reasons Why Law Firms Need to Make Information Governance a Priority

Trust

The American Bar Association's *Rule 1.6: Confidentiality of Information* expressly states "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." This rule is the cornerstone of attorney-client privilege and puts the onus on lawyers to protect sensitive data.

Litigation

As cyberattacks become increasingly sophisticated and widespread, the number of class action lawsuits against corporations and law firms is growing. According to Law.com, the monthly average of data breach lawsuits was 44.5 through the end of August 2023—more than double the average in 2022.[2]

Client Expectations

According to the American Bar Association, clients are more proactive than ever about stipulating specific security guidelines that law firms must meet as part of their Outside Counsel Guidelines (OCGs). Ensuring that information governance processes are aligned with client data privacy requirements is essential for law firms of all sizes.[3]

[1] ***Source:*** *ILTA/Conversant Group, "Security at Issue: State of Cybersecurity in Law Firms", 2023 Available from: https://higherlogicdownload.s3.amazonaws.com/ILTANET/ce7f3e74-fb70-402e-a1b3-5dc0abe72260/UploadedFiles/z5DmBwjTmSXTUVzImRWc_ILTA_CG_Exec_Summary_FINAL.pdf*

[2] ***Source:*** *Law.com Radar*

[3] ***Source:*** *2022 ABA Legal Technology Survey Report*

TOP WAYS TO HELP SECURE CLIENT DOCUMENTS

Every day, firms handle tremendous amounts of sensitive documents containing private client information. Those documents are created, uploaded, downloaded, shared, copied, printed, and filed. This fast-moving connection of workflows must be secured, but also organized and controlled for productive operations.

Here are five ways to help secure your document ecosystem:

1. CENTRALIZE THE CAPTURE OF CLIENT DATA

Ensure paper and electronic files are immediately captured, processed, and stored in a secure centralized document repository that incorporates multifactor authentication, password protection, and role-based access controls.

2. MAINTAIN DETAILED AUDIT TRAILS

Implement a document management system that can provide extensive audit trails to record the date of document creation, modifications, deletions, who performed an action, when it was performed, and more. Limit and prevent information from being modified beyond authorized parameters through built-in anti-tamper measures such as a unique digital signature.

3. ENSURE BACKUP AND RECOVERY

Maintain a document management system that can automatically save mission-critical files in primary and backup storage areas. This enables firms to recover data in the event of a ransomware attack or other unexpected event.

4. AUTOMATE DOCUMENT RETENTION

Set up automated retention policies for sensitive financial, personal, and client matter documents that align with client agreements and local, state, and federal policies. Utilizing a flexible document management system rather than a practice management system can help support a uniform data management policy across the enterprise.

5. EMPLOY A CLOUD-BASED PRINT AND SCAN MANAGEMENT PLATFORM

Incorporate a cloud-based print and scan management platform to track all print and scan activity—whether it occurs onsite or remotely.

LACK OF DATA OVERSIGHT CAN BE COSTLY

$4.88 MILLION

The global average cost of a data breach in the professional services industry in 2024.[4]

Take a Unified Approach

Securing and controlling document workflows doesn't have to slow down day-to-day operations or impede client services. In fact, document management solutions like uniFLOW and Therefore from Canon can help enable firms to create a secure document ecosystem by incorporating a consolidated platform for document capture, processing, storage, and output.

The reality is that many points of potential exposure exist in the life of any active client document. Having visibility and control of document workflow can help law firms reduce risk while continuing to provide clients with stellar service.

[4]***Source:*** *2024 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.*

1-844-50-CANON
usa.canon.com/business

Learn how Canon can help provide
security surrounding your document management.

Canon U.S.A. do not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21, or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrants any third-party product or feature referenced hereunder.