

```
def operation == "MIRROR_X":  
    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 active  
mirror_ob.select = 0  
new = bpy.context.selected_objects[0]  
new.data.objects[0].parent = mirror_ob
```

# SECURING CLIENT DATA IN A DIGITAL AGE



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

Law firms have many priorities to manage. Protection of client data should be at the top of the list. And even if it is already, document flow and management are not usually among the highest security priorities. They should be, because private client information in any document that law teams handle is at risk of exposure, a disaster that could harm a firm's reputation and cost millions of dollars to rectify.

### New Threats Move Fast

Activist groups, disgruntled employees or clients, and cybercriminals have new means of accessing client information. They could be taking client documents from anywhere at any time: a desktop, a laptop, a mobile device, a table in a copier room, or during a file-sharing session.

Lack of standardization, outdated equipment, and innocent mistakes can put law firms at risk of exposing client data when document creation, access, and flow aren't controlled and secured.

### Today's Top 10 Cyber Security Threats

In no particular order, here are today's top 10 threats:

1. Lack of Pervasive Security Mindset
2. Security Issues With Third Party Providers And Cloud Systems
3. Ransomware
4. Rogue Employees
5. Hactivists
6. Nation-State Espionage
7. Accidental Exposure By Well-Intentioned Employees
8. Technology Obsolescence
9. Password Management Being Weak Or Non-Existent
10. Reduced Security Standards For Remote Workers

# SIX TOP WAYS TO 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 six ways to help secure your document ecosystem:

## 1. CAPTURE NEW & INCOMING FILES

Ensure every incoming client document immediately enters the same document management system. Use an encryption method to protect documents when they are in digital storage or being transferred digitally.

## 2. USE INTEGRATED TECHNOLOGY

Use an integrated hardware-software solution for document management so that users can share information without leaving the secure ecosystem.

## 3. USE SECURE ACCESS CONTROL

Require user authentication at points in a workflow where documents will leave the secure ecosystem; for example, when documents are transferred via mobile file sharing.

## 4. EMBED ACTIVITY TRACKING AND REPORTING

Having visibility to active document workflows can enable monitoring for abnormal activity or unauthorized access.

## 5. PLAN FOR USER ENGAGEMENT

Security protocols should be intuitive and easy to follow to promote user adherence to firm policies, and can help reduce firm liabilities.

## 6. BALANCE ACCESS WITH SECURITY

A proactive approach to security involves a balance of document availability, confidentiality, and integrity, because a security plan should be aligned to business drivers and outcomes or it won't be effective.

# LACK OF PREVENTION IS COSTLY

**\$8.19 MILLION**

**Average cost of breach of private data for U.S. organizations in 2019**

## 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, solutions like uniFLOW from Canon can help enable firms to contribute to a secure document ecosystem by providing a consolidated platform for collecting documents and managing document 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.

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

The Canon logo is displayed in a bold, red, serif font.

CANON SOLUTIONS AMERICA

1-800-815-4000 [CSA.CANON.COM](https://www.csa.canon.com)

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

Canon U.S.A. and Canon Solutions America 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., Canon U.S.A., Inc. nor Canon Solutions America, Inc. represents or warrants any third-party product or feature referenced hereunder.

©2020 Canon U.S.A., Inc. All rights reserved.

1/20/19-1124-3967