RICOH
imagine. change.

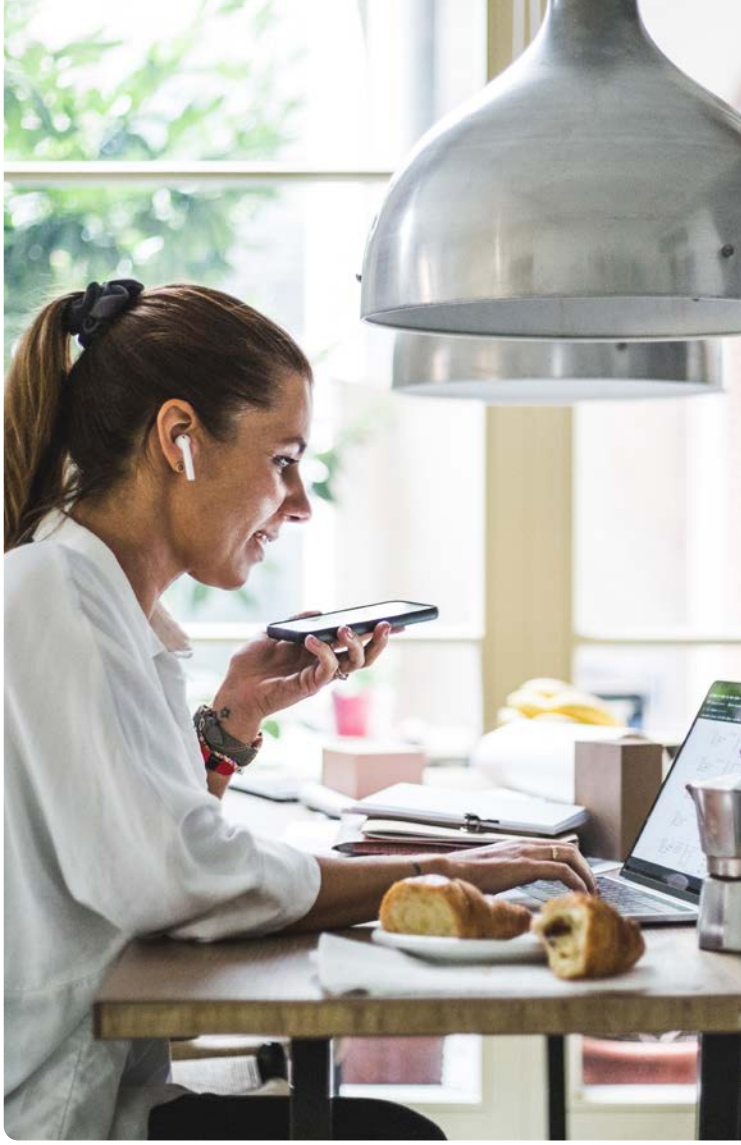
Navigating through eDiscovery challenges in the **hybrid workplace**

A guide to defensible collection and preservation of ESI in today's distributed workforce.

DATA CREATION, USE AND STORAGE IN HYBRID WORK

Shifting from traditional workplaces to hybrid models has become the new way of working for many organizations. This rapid change has created dispersed teams working remotely from any location and using a variety of devices, and applications to communicate, collaborate, and access and share company information. This brings new challenges and potential complications in the eDiscovery process of collection and preservation of electronically stored information (ESI) across multiple environments.

In a hybrid work environment, the process of collecting and preserving digital evidence needs to evolve to take into consideration the dispersed location of employees that may be working from locations with unsecured networks, such as their homes or even from different geographical areas. Furthermore, this also presents challenges in enforcing legal holds, especially when employees use their own personal devices and applications instead of company-issued devices, and company-sanctioned communication and collaboration platforms.



Centrally managed Microsoft environment

- Cloud Platform (M365)
- MS Office
- MS Teams
- Archived Data
- Cloud Storage (M365, Azure)
- Data Backups

Commonly untracked unsecured environments

- Home Computers (WFH)
- Mobile Devices (BYOD)
- Mobile & Web Applications
- USB, Portable Drives

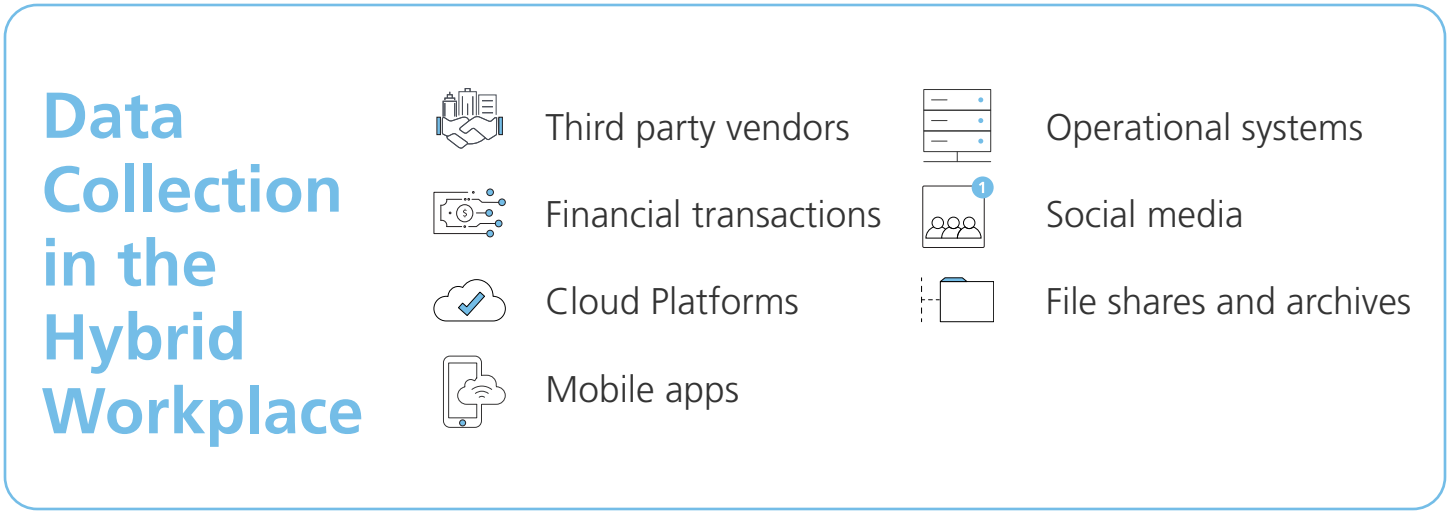
64% of employees use a personal device for work but only 43% of those devices are securely enabled.[1]

[1]2022 Endpoint Ecosystem Study

COLLECTION

Navigating the complexity of data collection in multiple environments

Accessing and collecting evidence for litigation in the hybrid world of work can seem daunting with distributed users creating, storing and accessing data in a number of different ways – from BYOB devices to social media, mobile apps, cloud platforms, data-sharing platforms and more – each presenting varying levels of accessibility and unique challenges.



Comprehensive access and collection of digital evidence

The variety and availability of collaboration and communication platforms will continuously grow and with it, the increasing range of data format, structure, accessibility and location – which can challenge the conventional concept of the collection process as data stored in these platforms must remain uncompromised. Furthermore, the rapid acceleration and advancement of these platforms may have little to no consideration for legal or compliance requirements, and may have not been designed to take into account eDiscovery requirements.

Today's collaboration and communication platforms, especially when used for hybrid work, are often cloud-based and hosted by third-party vendors. Due to the flexibility requirements of enabling employees to work from anywhere, the demand for cloud-based collaboration platforms that can be accessed across multiple devices such as M365, or virtual communication platforms such as Zoom and Microsoft Teams has accelerated. As such, when collecting defensible data, organizations need to have the ability to extract information from a wide variety of data types, formats and volumes.

Defensible chain of custody

The movement of digital evidence from the time it is collected till it is presented in court needs to have a thorough and reliable process or documentation that demonstrates its authenticity and disproves any potential claim of data tampering. The movement trail of the digital evidence must be able to provide details on the custodian, date, and time when it was placed on hold, as well as the data collected and details about the administrator who executed the legal hold. In addition, more detailed information such as the metadata on when the data was created, modified, and last updated is very important and must be included during the collection process and documentation.

For digital evidence, preserving the chain of custody during the collection process that is admissible in court presents more complications as digital files can be easily altered, deleted and fabricated. During the collection process, legal counsel and IT teams commonly preserve or authenticate the chain of custody of digital evidence using manual methods such as taking screenshots of the data collected to preserve the information. Manual methods are not only time-consuming but can potentially result in the dismissal of critical evidence in court as it fails to maintain a defensible trail for chain of custody and ESI authentication requirements.

Leverage AI-based forensics for reliable and defensible ESI collection

When collecting ESI during the eDiscovery process, consider mapping out the data types and sources you will need, and develop a strategy to enable the legal counsel and IT teams to effectively review and collect the data. Automated solutions such as APIs or solutions with dynamic mapping technology can capture data in its native form and from complex data sources to help ensure its accuracy and admissibility in court. This technology can capture and store data in an unalterable way that provides a defensible audit trail, including the data's hash value for the complete collection of the metadata.

However, while in-house applications go a long way in automating collection, the complexities a hybrid work environment presents may require a combination of outsourced expert services and advanced forensics. Consider outsourcing your collection needs to digital forensic experts who can perform both on-site and remote online collection for your convenience, and use cutting-edge technologies such as Relativity and ActiveNav to ensure nothing is missed and collection is highly defensible and auditable.

Leveraging the expertise of outsourced digital forensic experts can also help you determine what types of data are most important to help support you in preparing for litigation and eDiscovery.

PRESERVATION

Preservation of data across multiple environments

Hybrid work blends the boundaries between professional and personal data, particularly on mobile devices, and in communication and collaboration apps. Employees are working in different environments and utilizing new technologies to drive better efficiency and collaboration. Sometimes these technologies aren't approved and managed by the IT department, referred to as 'shadow IT'. This presents risks when it comes to preserving case-critical communications from being destroyed, deleted, lost, or altered in any way.

Locate and preserve relevant data effectively

Preservation in a hybrid work environment makes collecting relevant digital evidence more difficult to identify, locate and protect as it can be located on multiple platforms – from employees' personal devices and applications to cloud-based applications, internal servers and more. Furthermore, data is constantly being created, modified and deleted, and when digital evidence that should have been preserved is spoliated or lost and cannot be restored, legal sanctions and compliance issues can ensue.

Preserving digital evidence requires an in-depth understanding of cloud-based platforms such as M365 and its built-in retention policies for litigation holds. Additionally, awareness of what applications are in use and how information is being assessed and stored, especially in a remote work environment. Consider conducting a regular review of systems and applications that is in use within your organization and be proactive in adopting new communication and collaboration technologies to support the hybrid workforce. By doing so, you can mitigate employees utilizing unsanctioned apps and devices, and it also enables your IT team to implement security and capture controls to ensure your organization is meeting data compliance and regulatory expectations.

Preventing spoliation

The use of digital messaging platforms in hybrid work is increasingly on the rise and presents challenges in data retention, especially for platforms that have auto-deletion settings. Furthermore, with employee resignations, organizations must be proactive in setting up protocols on quickly and effectively preserving employee data should it be relevant for litigation.

With many communication and collaboration platforms being cloud-based and employees working remotely from anywhere, organizations must also have a firm understanding and comply with jurisdictional privacy laws and legal requirements from where the data originates, is stored and processed. When using cloud-based tools and platforms, backup failure can be a common occurrence and can happen due to a number of reasons, from human errors to software update issues, network infrastructure failure and cyber attacks or threats. Therefore, having a good backup strategy combined with intelligent cyber security solutions embedded into your network infrastructure can go a long way in preventing data loss, as well as in being an integral part of any data protection strategy.

Data security and protection

Ensure your IT department and third-party cloud providers implement technical and administrative controls and data-mapping technology to protect your data. Develop a comprehensive strategy for security and privacy measures for data retention and disposition, such as MFA and cloud-based file transfers with end-to-end encryption and tracking. You may also consider working with an outsourced eDiscovery partner who uses advanced AI-based technologies and expert techniques to preserve and retrieve case-critical data on-site or remotely. For organizations with BYOD policies in place, consider utilizing mobile device management solutions such as Microsoft Intune to simplify the management of employees' personally owned devices, and ensure they are compliant with your organization's configurations, and data compliance and regulations.

EFFICIENT COLLECTION AND PRESERVATION FOR A HIGHLY DEFENSIBLE AND AUDITABLE PROCESS

Today's digital solutions are constantly changing to support employees and legal professionals working from various locations, which means eDiscovery collection and preservation processes need to evolve. Today's remote collaboration and communication platforms offer convenience, flexibility and scalability that is required for hybrid work. However, with its increased adoption, so is the growing volume of ESI and cyber security risks and challenges – and it can be overwhelming to manage everything on your own – from adhering to EDRM best practices to ensuring that ESI collection and preservation are defensible.

You need powerful and agile technology that can evolve, and scale along with your eDiscovery needs to ensure secure, efficient and defensible litigation preparedness. Consider outsourcing to an expert partner like Ricoh for complete eDiscovery management solutions.

Digital Forensics Services
Comprehensive solutions for fast, reliable, and defensible ESI collection.
Find out more >

RelativityOne
Your complete and secure platform for eDiscovery.
Find out more >

Mobile Device Management
Simplified device management and deployment to help ensure data security and protection.
Find out more >

Managed Backup & Recovery Services
Customized backup, restore and recovery plans protect data and ensure business continuity.
Find out more >

Managed Cyber Security Services
A cost-effective, scalable approach to ongoing cyber security monitoring and management.
Find out more >

For more information, get in touch with a Ricoh solutions consultant.

RICOH
imagine. change.

Ricoh Canada Inc., 100-5560 Explorer Drive, Mississauga, ON L4W 5M3, 1-888-742-6417