NUIX WHITE PAPER

# COUNTERING INSIDER THREATS IN eDISCOVERY

by Michael Chance
Nuix Business Threat Intelligence and Analysis Team

nuix
Simple. Powerful. Precise.

# CONTENTS

# EXECUTIVE SUMMARY

The eDiscovery process by its nature involves collecting and storing volumes of sensitive and valuable data. The data itself may be sensitive, in that intentional or accidental compromise could cause serious damage to your organisation's interests and reputation. The data also has a high inherent value to your organisation because it is essential to your ability to defend or prosecute a legal matter. When it comes to your data, if it's valuable, it's vulnerable.

The eDiscovery process allows many opportunities for unwanted disclosure or loss. To mitigate this risk you need a better understanding of current vulnerabilities and risks that insiders pose, and a strategy to secure data throughout the eDiscovery lifecycle. This requires a holistic approach that combines technical and non-technical methods to deter and detect potential insider threats. Is your organisation prepared?

When it comes to your data, if it's valuable, it's vulnerable

# SECURING CRITICAL VALUE DATA FROM INSIDER THREATS DURING eDISCOVERY

Data derived for eDiscovery, whether for litigation or regulatory compliance, is unique in that it contains specific information requested by entities outside your organisation to resolve a legal matter. Uncontrolled disclosure of this information can be particularly damaging. This class of data requires a focused set of process controls to prevent unauthorised insiders from accessing and deliberately or inadvertently releasing it.

Proper handling of ESI is critical because lost or stolen data may prevent you from fulfilling your disclosure obligations

Electronic discovery is an iterative process that involves identifying, collecting, analysing, reviewing and releasing information. In many cases, this includes confidential information that is crucial to the operation of the organisation or detrimental to its market value and reputation. In all cases, the data collected is essential to your ability to defend or prosecute the legal matter at hand.

Due to the sensitive nature of the electronically stored information (ESI) involved in eDiscovery matters and the length of time you may need to retain this data, we recommend you identify and safeguard these materials as critical value data (CVD).

There are many opportunities, throughout the discovery process, for data to be lost or to fall into the wrong hands:

- In the early stages (preservation and collection), the data is vulnerable at rest after it has been collected.
- It is also vulnerable in the mid to late stages (processing, review and analysis), which often involve making working copies of the data.
- Additionally, any ESI is at risk in motion. Data sets may be moved or copied when they need to be processed or sent to a third party for review or further processing.

Your ESI is vulnerable and needs to be secured at all points during the discovery lifecycle. Proper handling of ESI is critical because lost or stolen data may prevent you from fulfilling your disclosure obligations. Despite these dangers, protecting eDiscovery data sets and materials from malicious insiders is something organisations rarely consider or address.

## CASE STUDY

### Hacked data provides unfair advantage in litigation

In 2005 and 2006, litigation was underway in the UK courts between international aluminium companies. During the discovery phase, the claimant noticed that the defendant was answering its interrogatories far too quickly, almost as if its legal team had prior knowledge of the questions. The claimant launched a cybersecurity investigation and discovered that its network had been penetrated – and that it could connect the hack to the defendant. It emerged that the defendant's access to the claimant's network included eDiscovery data pertinent to the case. The claimant counter-sued and the case was settled out of court, but this rare public example highlights the vulnerability of data involved in litigation.

*The claimant counter-sued and the case was settled out of court, but this rare public example highlights the vulnerability of data involved in litigation*

# KEY POINTS IN COUNTERING INSIDER THREATS IN eDISCOVERY

Critical value data must be identified, secured and safeguarded throughout the eDiscovery process. There are many opportunities throughout the process where a trusted insider may destroy, alter or steal important data. It is your organisation's responsibility to take reasonable steps to safeguard this data.

While technical safeguards are paramount, it is equally important to have a supporting information governance structure. Implementing policies and procedures that directly address these issues can mitigate the risk of an insider threat.

## Questions to ask:

For each eDiscovery project, your organisation must be able to answer these questions.

*Who is collecting the data?* It should be only designated personnel who have been vetted through a full background investigation that was initiated when they were hired.

*Where is the data stored?* Collections should be stored in a central repository that has dedicated secure servers with limited access and the ability to monitor access.

*Who has access to it?* Only designated, vetted individuals who are part of the eDiscovery process should have access.

*Where does this data reside while it is being processed?* Use dedicated workstations that can only be accessed by vetted and authorised individuals. Apply specialised software to monitor who is doing what.

*How should we transport the data to third parties?* Data sets should be encrypted before being burned to CD or transferred online. The password should be sent separately.

*Who are the people authorised to receive and work with the data?* These names should be vetted by inside counsel and the eDiscovery counsel.

*What are the access controls?* Any systems that store this sensitive data should have role-based access with defined roles and responsibilities. They should use dedicated hardware with limited, monitored access.

*Is the data or media encrypted?* Data should be encrypted in transit with the password sent separately using a different method.

*Who in the organisation is accountable to monitor and guide the access, production and flow of data?* This should be led by the eDiscovery counsel and a small group of designated stakeholders.

## Vet your personnel

When it comes to insider threats, security is not an IT problem, it's a people problem. Your employees are your primary concern but you should also scrutinise business partners.

### EMPLOYEES

Employees involved in the eDiscovery process should be trusted, designated personnel who have authorised access commensurate with their functions. Any employee who has the 'keys to the kingdom' poses a significant insider threat to an organisation if they abuse their rights, privileges and access.

New employees should be properly vetted before hiring. The type of background check and level of scrutiny should match the prospective new hire's role, responsibilities and level of access to critical value data. The checks would generally include previous employers, references, criminal record, credit checks and verifying professional licences, certifications and degrees or accreditations. Background checks also should be conducted:

- At fixed periodic intervals (for example, annually)
- When an employee's responsibilities or access to CVD are elevated (for example, if they are promoted or transferred)
- If employee displays signs of distressed or disgruntled behaviour.

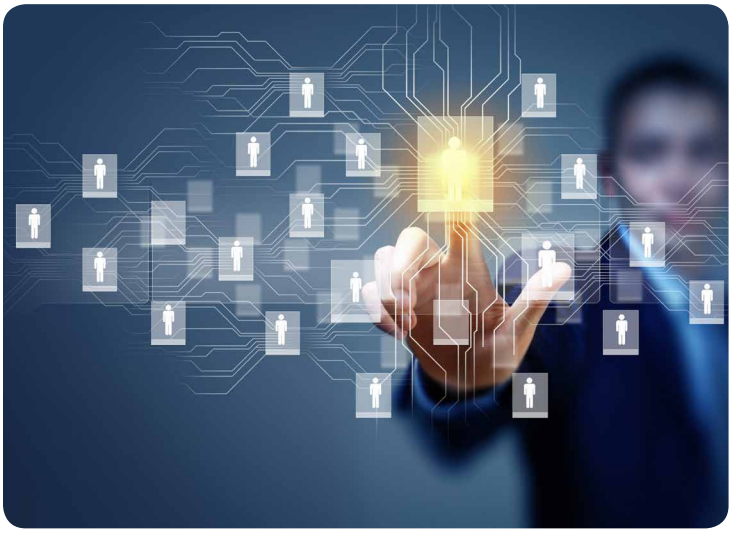
It is equally important to define who are the key stakeholders in the eDiscovery process – most likely they will include inside counsel, records management, the eDiscovery team, IT infrastructure, compliance and outside counsel. Clearly defining each individual's roles and responsibilities assigns accountability and establishes a baseline for determining when someone is attempting to operate out of scope.

### VENDORS, CONTRACTORS AND BUSINESS PARTNERS

Businesses generally evaluate their vendors, contractors and business partners on criteria such as level of service, price, unique need and return on investment. However, if these third parties will have access to a company's critical value data, it's essential to consider additional criteria for trustworthiness and adequate information security.

Conducting public records searches, contacting listed customers and gathering open source intelligence may help you determine if a business partner may pose a potential insider threat.

Contract personnel, whether they work onsite or access your data remotely, should be run through the same vetting processes as regular employees and subject to the same policies and procedures. Business partners must have solid nondisclosure agreements in place. It is worthwhile developing long-term relationships with reputable vendors and business partners in whom you can maintain confidence.



## Educate employees on the insider threat

Establishing and enforcing an insider threat awareness training program will promote an organisational culture that is less likely to allow insider threat activities to go unnoticed. Awareness begins with a comprehensive new employee orientation program. This program should explicitly state:

- Activities that are acceptable and prohibited while using the organisation's assets and infrastructure.
- What employees can expect when accessing, handling, using and protecting the organisation's data.
- Employees' duty to report violations of organisational policy and acceptable usage while using the organisation's assets and infrastructure.
- Employees' expectation of privacy while using the organisation's assets and infrastructure.
- The organisation's right to monitor and collect any information or activity that occurs on its computing assets and network infrastructure. It is important to explain that the organisation will observe and protect employees' privacy and civil liberties except in situations that involve prohibited activities or malfeasance.
- The organisation's right to enforce and execute disciplinary action, at its discretion, including the range of disciplinary actions available to the organisation.
- Additional organisational, legal or government policies and guidelines specific to that workplace.

It is important to update and reinforce the information presented in the orientation program through mandatory annual awareness training for all employees.

Vendors, contractors and business partners should also receive this orientation information as an onboarding or pre-engagement briefing. They should be required to sign an acknowledgement that they have received the briefing. In addition, these personnel should be required to complete, acknowledge and sign off on the organisation's annual awareness training.

You should also provide specific training for eDiscovery personnel on the potential vulnerabilities during the discovery lifecycle to ensure they properly handle ESI and understand the risks of unwanted disclosure.
Topics should include:

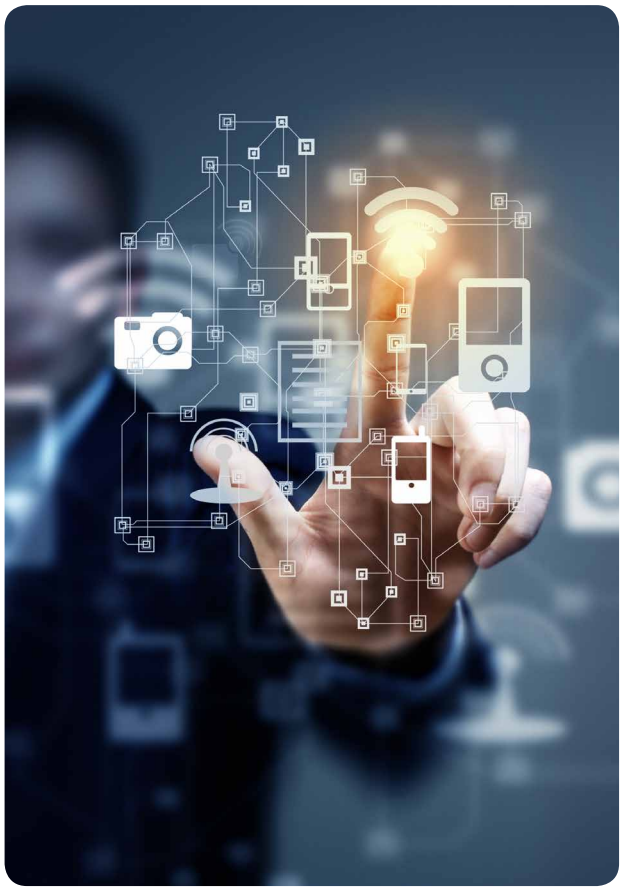
- Why information governance is important in detecting and deterring insider threats
  - Why limiting access to ESI is important
  - Defining the key stakeholders and their roles and responsibilities
- The importance of collecting and preserving ESI securely
- Identifying when data is at risk during the discovery process
  - How to securely store and manage the data through all stages
- Preparing ESI for delivery to third parties, including encrypting data in motion.

Establishing and enforcing an awareness training program will promote an organisational culture that is less likely to allow insider threat activities to go unnoticed

## Map your environment

During the identification phase of eDiscovery, the first step in securing your critical value data from insiders is to create a functional overview of your organisation's computing environment. Valuable information can be stored on workstations, email servers, file shares, collaboration systems such as Microsoft SharePoint, portable storage and mobile devices. It is important to identify potential sources of ESI and who has access to them in order to secure it from potential insider threats.

Knowing where your data is stored will help identify and secure all locations that contain or provide access to ESI, define the data owners and enforce data owners' accountability to control data access and integrity.



## Secure your data collections

The preservation and collection stages of eDiscovery place data at significant risk. This process must:

- Be executed by vetted, trusted, designated individuals
- Use forensically sound methodologies that meet or exceed industry best practices
- Be fully documented to provide continuity and accountability.

Once targeted data is properly collected, documented and accounted for, it should be immediately stored in a dedicated, secure central data repository. To maintain the integrity of the collected data:

- The ability to write data to the secured repository should be restricted to limited, monitored access only for the designated data collectors, and it should be 'write-only' access
- The hardware, software and operating systems that comprise the secured repository must be updated and patched regularly to decrease vulnerabilities that an insider might exploit
- An appropriately scoped and scaled case management system will give key stakeholders better control of what is stored, where it is stored, data owners, data access and activity.

Non-technical considerations include adhering to the guidelines that apply for that jurisdiction and matter type, and ensuring retention schedules are not enforced on the collected data or are suspended. For example, Rule 26 of the Federal Rules of Civil Procedure protects trade secrets and other confidential research information. If disclosure of critical value data is not necessary in a particular matter then it should not be collected in the first place.

Retention schedules ensure that specified data sets are appropriately discarded as prescribed by regulations or organisational policy. By lawfully limiting the legacy ESI residing on data stores and thus excluding that data from collection in the first place, an organisation will significantly limit an insider threat's attack surface.

## Implement access controls

Physical security, strong policy and robust technical controls are all part of reducing the insider threat. All eDiscovery data stores require controls that restrict and log all activity pertaining to ESI. Role-based permissions are a way to limit individuals' logical access to data based upon their job function or the sensitivity of the information. A pragmatic approach to limiting logical access to ESI reduces risk.

Enterprise-wide technical controls – such as disabling portable storage device usage for people with certain job roles – can mitigate a common avenue of spoliation or exfiltration. You can significantly reduce the opportunity for insider activity to go unnoticed by:

- Placing physical controls such as multi-factor authentication or security access cards to enter areas of the organisation where ESI is stored
- Only allowing designated individuals to access ESI.

Ensuring that only vetted, authorised individuals are granted access, at any level, strengthens an organisation's insider threat security posture. This is further strengthened by clearly defined roles, responsibilities, authority and accountability for all stakeholders.

## Limit exposure during the discovery process

The discovery process involves numerous phases of establishing the facts of the collected data and reducing the volume to relevant data sets. This process typically requires carefully honed criteria, filters and analytics such as keywords, date ranges and file types.

If the work product of developing these criteria or culled findings were disclosed or accessed, with the assistance of an insider, this would give opposing counsel a significant advantage. Thus it is important to carefully handle the documentation behind processing efforts to mitigate the insider threat as well as to maintain accountability.

Ensure you retain working copies of image files and the original evidence in a secure central repository. Treat all copies of ESI the same way you would original evidence. Make sure authorised, designated personnel are accountable to document any intentional or unintentional ESI manipulation.

The discovery process by its nature involves searching and compiling data that is sensitive and important to the organisation

## Know your electronically stored information

ESI may likely contain an organisation's critical value data and privileged information. It may reside anywhere on an organisation's network. It is incumbent upon an organisation to have a current working knowledge of what that ESI is and where it is located when required to produce it. It is equally important to understand what and where ESI resides for the purpose of protecting it.

An important aspect of ESI commonly overlooked by an organisation when considering insider threat is the 'sum of parts'. Organisations typically evaluate the sensitivity of ESI based upon its current contents, state and location on the network. It is not uncommon for low-value ESI, when combined with other low-value information, to result in critical value data. However, due to the ESI's relative low value, it is typically less regarded, secure, access-limited and scrutinised. For these reasons, the seemingly low value ESI is a common target of malicious insiders. An organisation must have the ability and foresight to identify and appropriately safeguard information that presents this risk.

## Understand the potential insider

Throughout the discovery process, there are many ways an individual could become an insider threat, either witting or unwitting. An insider may act recklessly or maliciously for personal gain or to damage the reputation of an organisation. They may be coerced by, or seeking to collaborate with, a nation state or a competitor.

The insider threat is a most often an opportunistic act. Reducing the risk requires an organisation to remove opportunity by implementing and enforcing robust policy, sound technical controls, comprehensive identification of critical value data, restrictive access controls, secure data repositories, stringent hiring practices and informative insider threat awareness education. It is every organisation's responsibility to operate with due diligence and safeguard all critical value data with which it has been entrusted.

## ARE YOU PREPARED?

There are no singular solutions for protecting ESI derived from litigation or regulatory request. The discovery process by its nature involves searching and compiling data that is sensitive and important to the organisation. As such, you must protect it diligently. But no single technical solution or policy will result in a successful defence. You must take appropriate measures, creating a holistic approach to potential insider threats, before and during the discovery process to ensure that data collected remains secure and ready to support the company's legal requirements. Mitigating the insider threat is a key element of protecting critical value data during the discovery process.

*Are you prepared?*

## ABOUT THE AUTHOR


### Michael Chance

Director, Business Threat Intelligence and Analysis, Nuix


Michael has fifteen years of experience in advanced computer forensics, incident response, eDiscovery and insider threat assessment for local law enforcement, federal law enforcement, the federal government and Fortune 100 companies. His recent assignments include managing internal threats for Cigna Healthcare, leading forensic investigations for the CSIRT at the U.S. Food and Drug Administration and serving as an agent on the FBI's New Haven, CT Computer Crimes Task Force. Prior to that, Michael was Lead Detective on Computer Crimes Unit at the Waterbury, CT Police Department.


The author would like to thank Angela Bunting,
Vice President – eDiscovery at Nuix for her contribution to this paper.


To find out more visit:

# nuix.com/insider-threat

## ABOUT NUIX

Nuix protects, informs and empowers society in the knowledge age. Leading organisations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management and other essential challenges.


**North America**
USA: +1 877 470 6849
» Email: sales@nuix.com

**EMEA**
UK: +44 203 786 3160
» Web: nuix.com

**APAC**
Australia: +61 2 9280 0699
» Twitter: @nuix



ED1605UK1