Complying with InfoGov and eDiscovery Requirements in a Post-COVID WFH World

PART 3: OPSEC

Data insecurity is a substantial threat to your organization, with risk arising from insider actions as well as outside forces. Defensible disposition, paired with secure, strategic retention of critical assets, can go far in protecting your organization. The 3-phase checklist below can guide you in starting or improving defensible deletion and retention policies. By following this checklist, you will:

- ✓ Reduce unnecessary retention of expired data
- ✓ Reduce storage and litigation costs
- ✓ Reduce legal and compliance risks
- ✓ Create business value
- ✓ Withstand scrutiny in litigation or from a regulator with defensible disposition

When combined with the other Operation IG Revamp tools, this document will help you outline a comprehensive approach to upgrading your information governance and eDiscovery strategy.

3 PHASES OF DEFENSIBLE DELETION & RETENTION

1. Visibility
Your first step is to bring dark data into the light and compile an accurate picture of your data landscape. Doing so will equip you to mitigate compliance and regulatory risk, proactively monitor insider threats, and respond faster to security incidents and eDiscovery requests.

Key Actions:

- ❑ Roll out software to connect with and map content in locations such as:
  - ❑ Employee desktops and laptops
  - ❑ Network file storage
  - ❑ On-premises Exchange email
  - ❑ Microsoft 365 (email, archives, SharePoint, OneDrive)
  - ❑ Google Workspace
  - ❑ CRM
  - ❑ PST files
  - ❑ Box.com
  - ❑ Legacy systems
  - ❑ Backup files
- ❑ Tag message and file content for which retention guidelines do or should apply, with a focus on:
  - ❑ PCI (credit cards, bank accounts)

- ❑ PHI (medical codes and records, insurance information, etc.)
- ❑ PII (birthdates, addresses, social security numbers, HR/human resources)
- ❑ Proprietary information (internal processes, training resources, intellectual property, meeting recordings)
- ❑ Additional sensitive or risky data

2. Assessment

Next, assess what data is business critical (meaning it is vital to your ongoing success) and what is redundant, outdated, or trivial (ROT) and provides little to no business value. Business critical data must be protected and proactively managed, whereas ROT should be securely deleted on a regular basis.

Key Actions:

- ❑ Identify content that is 3-7 years old and over 7 years. Present data owners with that detail and allow them to select what could be eligible for disposition.
- ❑ Classify data as business critical only if it has:
  - ❑ Ongoing business value
  - ❑ Historical/archival business value
  - ❑ Legal or regulatory retention requirements, including litigation holds

3. Governance

Governance requires not only addressing urgent risks but also having an effective method for ongoing information governance. Fully protecting your organization will require software solutions that can reach disparate content and storage locations throughout the enterprise.

Key Actions:

- ❑ Immediately remediate identified sensitive and at-risk information according to existing policies and regulations
- ❑ Formulate, document, and implement enforceable rules to assess and manage content on a recurring basis so that you can
  - ❑ Maintain accurate data inventories and maps
  - ❑ Conduct proactive employee risk monitoring
  - ❑ Protect sensitive, business-critical information
  - ❑ Adhere to regulatory and privacy mandates such as PCI, GLBA and CCPA
  - ❑ Defensibly dispose of ROT

Want help with completing your IG Revamp?
Contact Gimmal at info@gimmal.com.