Using Information Governance to Help Avoid and Limit the Impact of Cyber Events

Information Governance often takes a back seat to other organizational initiatives. For example, when the General Data Protection Regulation (GDPR) was introduced, companies scrambled to address data privacy concerns because of a misunderstanding of the level of effort to comply. Now with the increase in other privacy regulations such as CCPA and the State Secrets law in China, and the increased criteria being imposed by insurance carriers to have a cyber policy, cyber security is now top of mind for organizations looking to invest in technologies to minimize the risk of a data breach. As companies continue to move to the cloud and reduce spend on information technology, creativity about where investments are made is becoming more important. Information Governance is an area of heavy investment for companies who want to reduce the risk associated with cyber events. **There are several components of Microsoft 365 ("M365") our clients often already own but do not take full advantage of.** Utilizing this technology allows an organization to leverage its investment better.

Typical Areas of Focus Include:

Data Classification

Implement sensitivity labels, sensitive information types, and trainable classifiers to accelerate Cyber Security readiness.

Microsoft Purview provides over 300 sensitive information types (SITs) to identify information such as social security, credit card, or bank account numbers. Microsoft Purview also has over 90 built-in classifiers to identify content based on existing data in your organization. These out-of-the-box classifiers can be customized to identify content specific to your organization as well. Classifying data allows you to take advantage of other M365 capabilities while reducing the risk associated with unclassified data. Knowing your data can play a key role in preventing its misuse and in defining your response and obligations should it ever be exposed or shared unintentionally.

Data Lifecycle Management

Leverage M365 retention policies and labels to apply retention to data and position the organization to defensibly delete data and reduce risks associated with the over-retention of data.

One of the best defenses against data getting into the wrong hands is deleting it so it is unavailable. Organizations may find it relatively easy to create a retention policy and a retention schedule, but operationalizing retention and deleting data is something that few companies do well. Eliminating redundant, obsolete, and trivial (ROT) information is a key Information Governance initiative that M365 can enable to reduce the volume of data in your organization and the risk associated with a data breach.

Records Management

The file plan capabilities and label policies within Microsoft Purview allow organizations to build a comprehensive solution to manage business-critical data in compliance with regulations, laws, and records retention policies.

M365 can mark items as records if needed and apply item-level retention to either automatically delete data at the end of a retention period or initiate a manual review for scenarios where human intervention is required. Good records management supports cyber security by ensuring records are managed throughout the information lifecycle.

Data Loss Prevention (DLP)

Implement sensitivity labels, sensitive information types, and trainable classifiers.

Making the investment to classify data in M365 will enable technologies such as Data Loss Prevention (DLP) to be more effective and potentially warn, catch, and even prevent data from being sent to bad actors across M365 services, including Exchange, OneDrive, SharePoint, and Teams. DLP can be configured to warn users from sharing sensitive information, block the activity, or audit information sharing.

Insider Risk Management

Insider risks are a top concern for security and compliance professionals.

Insider Risk Management helps minimize internal risks by enabling organizations to detect, investigate, and act on potentially malicious and inadvertent activities. With connectivity to a Human Resources Information System (HRIS), detection of end-of-employment, risky actors, event-driven populations, or other categories can automatically be used to monitor for nefarious activity.

Microsoft Priva

Proactively identify and protect against privacy risks.

Microsoft Priva is a tool that can help identify data transfers and data oversharing within M365. Microsoft Priva provides visibility into personal data storage and movement, enabling organizations to make informed data management decisions that comply with evolving data privacy regulations.

Information Barriers and Compliance Boundaries

Limit communication and collaboration between groups and create logical boundaries to manage content.

Information barriers can reduce cyber-related risks by restricting communications and collaboration between groups helping to prevent both intentional and unintentional sharing of sensitive data. Compliance boundaries are often used with large, multi-national organizations to segment geographies and meet eDiscovery requirements.

Why work with Epiq?

Epiq has worked with many organizations to advise on the important connection between Information Governance and Cyber Security, leveraging Microsoft Purview. Epiq has a global partnership with Microsoft providing advisory operational support services for select Microsoft compliance products to allow organizations to take advantage of their investment in M365 and potentially reduce the risk associated with data breaches. **Let us help you improve your privacy and security posture while also increasing your ROI on M365.**

Epiq's Awards and Recognition

Microsoft
2023 Partner of the Year
Winner
Compliance Award

Microsoft Security
Excellence Awards 2023
Microsoft Intelligent Security Association
FINALIST
Epiq
Security Customer Champion &
Compliance & Privacy
Trailblazer

Microsoft
Solutions Partner
Security
Specialist
Information Protection and
Governance