INFOLOCK

CASE STUDY:

ULLICO

INFOLOCK DELIVERS FULL DATA RISK MANAGEMENT PROGRAM FOR ULLICO

CUSTOMER PROFILE

Ullico

SOLUTIONS FOR THE UNION WORKPLACE

LOCATION

Washington, DC - USA

INDUSTRY

Financial Services

ORGANIZATIONAL SIZE

200+ Employees

ORGANIZATIONAL FOOTPRINT

$7.1 billion

Ullico manages more than $7.1 billion in assets

2.2 million

Ullico insures over 2.2 million people

140+

Ullico gives to over 140 non-profits and community groups

Founded in 1927, Ullico (formerly Union Labor Life Insurance Company) is a privately held insurance and financial services company headquartered in Washington, D.C.

Ullico's mission is to provide financial security for union workers and their families, manage investments, and support charitable organizations. The company insures over 2.2 million people, manages $6.4 billion in assets, and has annual revenue of approximately $300 million.

PROJECT BACKGROUND

Ullico first engaged Infolock to implement a data loss prevention (DLP) program, as documented in a previous case study. During this previous engagement, Infolock:

- Applied the DataRAMP™ risk management framework to optimize user behavior analytics and data loss prevention
- Launched company's first-ever proactive testing for data exfiltration risks
- Detected and managed ~47,000 data risk events
- Transformed data risk management into a holistic integration of people, technology, and processes
- Introduced a Data Risk Index to guide information governance, track data risks, and drive business decisions

Infolock's DLP program achieved Ullico's goals for identifying and protecting sensitive data, retaining data per policy requirements, and meeting regulatory mandates for financial and personal data. As a result of Infolock's efforts, Ullico realized many DLP benefits, including:

- Unprecedented visibility of data access and use
- Better-defined data risks, prioritized for mitigation
- More informed procedures to enforce data governance
- Reduced risk of data exposure in every state: at rest, in transit, and in use

> *"Infolock dramatically improved the quality of our DLP program and saved us a lot of time and money."*
>
> **Marc Zinsmeister**
> Chief Information Officer

NEW CHALLENGES AND GOALS

Infolock's DLP program succeeded in identifying, measuring, and reducing enterprise data risk for Ullico. However, DLP is typically one of many tools in a more extensive, strategic **Data Risk Management (DRM) program**. Infolock helped CIO Zinsmeister look beyond DLP to see that a comprehensive DRM strategy would enable Ullico to:

1. Better understand specific business values of data and judge technical risks accordingly.
2. Define normal and abnormal use of business-critical data within each business unit.
3. Deploy a stronger information governance model for continuous improvement of data risk management and maturity.
4. Deter employees from leaving the company with unauthorized, business-critical data.

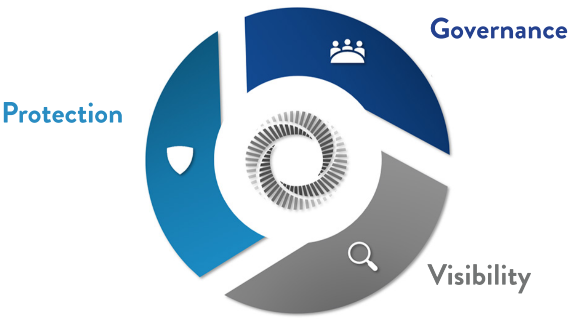
Preventing data from "breaking out" was especially important for Ullico — as important as stopping cyber criminals from breaking in. Ullico needed to control its customer lists, intellectual property, and other proprietary data.

SOLUTIONS

Infolock's Advisory Services team helped Ullico set up a DRM program based on Infolock's data risk management framework, DataRAMP™.

DataRAMP is an industry-first set of principles and best practices that provides a common language to assess and control data risk. DataRAMP takes a detailed, prescriptive approach to data risk management, including evaluating Ullico's Governance, Visibility, and Protection.

DataRAMP's Prescriptive Approach



Governance *looks at the organization's structure with a primary focus on program ownership and charter guidance in the form of policies and standards, risk metrics, goals, reporting, and resourcing.*

Visibility *focuses on turning Governance into technical ability (i.e., how to find the right types of data, how data is used, and who is using data).*

Protection *focuses on consistently enforcing data security requirements, verifying data is appropriately secured, and providing response and remediation as incidents occur.*

Data risk management is effective only if an organization commits to it from the top down. So, the first step for Infolock was to set up a formal **Data Risk Management Body (DRMB)**, led by CIO Zinsmeister. Infolock educated the group on DRM processes and empowered it to define and enforce data risk policies.

Infolock then conducted a meticulous **business risk assessment**, collaborating with every business unit to fully understand the human side of data risk at Ullico. This process enabled Infolock to identify, classify, and prioritize the risks to each business unit's data. Using these findings, Infolock:

1. Guided the DRMB in defining policies to address specific, prioritized risks
2. Helped Ullico consolidate/replace technical tools for a more cohesive data control architecture
3. Utilized the DRI to provide further insight into data tasks

Infolock also implemented proactive testing in Ullico's environment to help mitigate risks. For example, Infolock regularly attempts to exfiltrate test data to determine if policies and controls work properly. This practice is especially important to get ahead of potential issues caused by software updates.

THE DATA RISK INDEX

One of the cornerstones of Infolock's DRM program is a detailed **Data Risk Index (DRI)**, which tracks priorities and progress in reducing data risk. The DRI provides metrics that enable users to:

- Monitor all data with contractual, regulatory, or other business critical importance.
- Break out data by business unit, category, risk factors, and many other parameters.
- Prioritize each data element based on the risk and potential impact of adverse events.
- Measure the effectiveness of individual data controls and overall control efficacy.

THE RESULTS

Infolock transformed Ullico’s management of data risk into a holistic practice that integrates people, technology, and processes to address both external and internal risks. Results from this endeavor include:

- Efficient routines now guide information governance, track data risks, and drive business decisions about data. The program’s governance-to-metrics feedback loop continuously drives process improvement and reduces business risk.
- Ullico’s risk management leaders meet regularly — using Infolock’s DRI as their “bible” — to prioritize and take action on an ever-changing data risk landscape (for example, to timely address new rules for SOX and HIPAA data).
- By gaining a better understanding of what data is important and how it should be used, Ullico consolidated and optimized the effectiveness of its data security technology.
- Under DataRAMP, DRI metrics translate into actionable intelligence needed to configure and optimize user behavior analytics (UBA) and DLP.
- Infolock’s dedicated Incident Response (IR) team also uses DRI metrics for early identification and remediation of emerging risk issues.
- For the first time in its history, Ullico proactively tests data exfiltration risks — enabling effective pre-incident mitigation instead of post-incident damage control.

4TB

Scanned 4TB of unstructured data at rest — identified ~700,000 files unused in 7 years

25%

Identified ~90 sensitive data types — over 25% tied to a single, critical application

~47k

Detected and managed ~47,0000 data risk events

~80%

Implemented effective new controls for ~80% of all data risk vectors

INFOLOCK

Learn more at infolock.com