SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Leveraging ILM for Convergence and Compliance

Mike Calero, CISM, PMP

Originally Published in Security InfoWatch

October 2008

Leveraging ILM for Convergence and Compliance

Protecting the confidentiality, integrity and availability of information assets should be a convergence endeavor. The Information Lifecycle Management (ILM) strategy ensures protection and enables compliance with both information and physical requirements of existing laws, rules and regulations.

The Storage Network Industry Association (SNIA) defines ILM as the policies, processes, practices, services and tools used to align the business value of information with the most appropriate and cost-effective infrastructure — from the time information is created through its final disposition. While ILM has its roots in the storage industry, approaching compliance from an ILM perspective enables the convergence of areas such as information classification policy with incident response processes, and physical access control services with audit log management tools.

Information has always followed a lifecycle; organizations have always used document management, content management and records management methods, all of which are functions inherent to ILM. Documents have business value, physical records must be warehoused and content is retained and/or disposed. SNIA makes sure security convergence is inherent to ILM through the work of publications such as its Security Technical Work Group's (TWG) *Storage Security Best Current Practices (BCPs)*.

In this document, SNIA 's Security TWG addresses the "convergence of the storage, networking, and security disciplines, technologies, and methodologies for the purpose of protecting and securing information assets." It presents the BCPs as the means to a holistic approach for organizations to secure their storage systems and/or ecosystems. " SNIA also sponsors security forums such as the Storage Security Industry Forum (SSIF) that promote collaboration between members, volunteers and other groups. The resources they produce, such as the SSIF Risk Assessment Toolkit, the Cryptographic Use Cases and the Rationale for End-to-End

Security tutorial, provide the perspective for organizations to have converged security and achieve compliance.

SNIA counts on its 10 years in existence and a membership that includes major vendors to bolster its credibility and promote the adoption of its standards. Nonetheless, the association's standing has been recently counterbalanced by criticism of its leadership and membership structure, which skews voting power toward larger vendors — those with the largest membership fees.

Coincidentally, it is these larger members that, in an effort to distinguish their offerings from the competition's, increase market share, introduce non-standard terminology (e.g. , Intelligent Information Management). Beyond SNIA, vendor definitions, processes, practices and services have become even more divergent: ILM is now synonymous with DLM (D referring to data). In acknowledgment to the importance — and (marketability?) — of security, data becomes protected, yielding PDLM.

Inconsistency prevails outside the vendor realm as well. The British Computer Society (BCS), a chartered organization with a membership 60,000-strong across 100 countries, uses Intelligent Infrastructure Management (IIM). The Government of Canada defines information lifecycle in its Framework for the Management of Information (FMI) as "the steps that information passes through in the course of conducting business activities: collect/create/receive/capture, organize, use/disseminate, maintain/preserve, disposition."

Issues such as these increase the challenge security groups face in pursuing an ILM-based security strategy; nonetheless, the case for ILM as a catalyst for convergence and compliance is strong; stronger when considering the *quantitative* risk of non-compliance with laws, regulations and rules, and the significant investment of resources necessary to implement the supporting organizational change.

Even partial adoption of unified security policies, processes, practices and services will yield improvement. Leveraging ILM for security convergence will yield the true benefit: Protection of information assets. With security in place, compliance will follow.
Resources:

www.snia.org/home

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com