Is a Merger Between Information Security and Data Governance Imminent?

see article formatted here: https://docs.google.com/document/d/13ndBJQOhHeAU1kmics7vkLskzwWBCC1j/edit?usp=sharing&ouid=114707231848613284515&rtpof=true&sd=true

Is a Merger Between Information Security and Data Governance Imminent?

Byline: George Tziahanas, Managing Director and Kevin Novak, Managing Director at Breakwater Solutions

Background

As with any merger, it is always difficult to predict an outcome until the final deal papers are signed, and press releases hit the wires. However, there are clear indications that a tie up between these two is essential, and we will all be the better for it. Data Governance has historically focused on the use of data in a business, legal and compliance context rather than how it should be protected, while the opposite is true for Information Security.

The idea of interweaving Data Governance and Information Security is not entirely new. Gartner discussed this in their Data Security Governance Model, EDRM integrated multiple stakeholders including Information Security, Privacy, Legal and Risk into an overarching Unified Data Governance model., and an integrated approach to Governance, Risk, and Compliance has long been an aspiration in the eGRC market. Organizations that have more mature programs are likely to have some level of integration between these functions already, but many continue to struggle with the idea and often treat them as separate, siloed programs.

As programs go, Information Security is ahead of Data Governance for its level of attention in the Boardroom; brought about primarily by news-worthy events that demonstrated what security and privacy practitioners had warning about for a long time. These critical risks to the public and private sectors inspired significant, sweeping frameworks and industry standards(PCI, NIST, ISO, ISACA, SOC2) and regulatory legislation (HIPAA, GDPR, NYDS), and gave Information Security Officers (CISOs) a platform for change.

By contrast, data governance has been more fragmented in its definition, organization, development, and funding. Many organizations accept the value of data governance, particularly as a proactive means to minimize risk, while enabling expansive use of information required in today’s business environment. However, enterprises still struggle to balance information risk and value, and establishing the right enablers and controls.

Drivers

Risks and affirmative obligations associated with information are the primary drivers for the intersection of data governance and information security. The reason that information security is so critical is that the loss ((through exfiltration or loss of access due to ransomware) of certain types of data carry legal and compliance consequences, along with impacting normal business operations. And a lack of effective legal and compliance controls often lead to increased information security and privacy risk.
Additional common drivers include:

Volume, velocity, mobility, and sensitivity of information
Volume and complexity of legal, compliance, and privacy requirements
Hybrid technology and business environments

Multinational governance models and operations
Headline and business interruption risks

Finally, an underlying driver is the need to leverage investments in technology, practices, and personnel across an organization. The interrelationships of so many information requirements simply demands a more coordinated approach.

Merging the Models

We chose Information Risk Management, to define a construct that encompasses the overarching disciplines and requirements. First, we did so because it places the focus on information. For example, the same piece of information that requires protection, may also have retention and discovery requirements. Second, risk management recognizes the need to balance the value and use of information from a business perspective, while also providing appropriate governance or protection. Risk management also serves as an important means to evaluate priorities in investment, resources, and audit functions.

Figure 1: Information Risk Management

The primary objective is to integrate processes, people, and solutions into a framework that addresses common requirements; and does so “in depth” for both. Security people, practices and technologies have long-been deployed at many levels (in-depth) to protect the organization. The same has not often been the case for governance (legal, compliance, and privacy) obligations. New practices and technologies are enablers for ntersecting programs, and support alignment amongst key constituencies, including Information Security, IT, Legal, Privacy, Risk and Compliance. Done right, this provides leverage in an organization’s human and technology investments, improves risk posture, and increases the rate and reach of new practices and solutions.

Meshing disciplines and elements of each program are not meant as a new organizational construct; rather, it should start with a firm understanding of information requirements from key stakeholders; and from there establish synergies. The list below, not meant to be exclusive, provides examples of shared enabling practices and technologies:

Conclusion

Integrating data governance, information security and privacy frameworks allows an enterprise to gain leverage from areas of common investment and provides a more comprehensive enterprise risk management strategy. By improving proactive information management, organizations increase preventative control effectiveness and decrease reliance on detection and response activities. It also develops cross functional capabilities across Privacy, Legal, Compliance, IT, and Information Security.

Security and privacy teams become more knowledgeable about business and upstream content creation, collaboration, and operational requirements, while legal and compliance teams gain better insight into the world of IT and Information Security. This provides increased scale and decreased time during incident response, broader analysis of potential enterprise risks, and improved efficacy and responsiveness during recovery activities. Overall developing a more integrated approach to information risk management provides a foundation for success in even the most tumultuous times of change.