When picturing the relationship between the information security and the records information management (RIM) teams in many organizations, Aunt Eller, from the Broadway play Oklahoma, singing “The farmer and the cowboy should be friends” comes to mind. Both the farmer and the cowboy had similar interests and could have likely benefited from some collaborative endeavor; however, in many organizations, the tendency has been to fixate on the differences between information security and RIM rather than the mutual benefits.

In many organizations, there has been limited interaction between the information security and the RIM teams. While there may be myriad explanations for this lack of partnership, the most likely cause is a combination of the following erroneous assumptions:

- Most information security practitioners believe that RIM is primarily focused around management of archival hard copy records, rather than active electronic records.
- Many RIM professionals have limited backgrounds in IT.
- There is a desire by both groups to avoid conflict by not infringing on the other's turf (i.e., peaceful coexistence).
- Differences exist in the backgrounds of practitioners. Many information security professionals come from IT, where RIM staff often have library science backgrounds.

Information security and IT organizations seem more naturally aligned because the technical focus of many information security initiatives and tools necessitates their mutual involvement. Many information security practitioners view their IT peers as natural extensions of their team. Put simply, information security sees IT as “us” rather than “them.”

Fewer information security professionals view their RIM counterparts as potential players on their team. Conversely, RIM professionals seldom regard information security as prospective stakeholders on their projects. When communication is required between the two teams, the approach is often to send an envoy to fetch the necessary information rather than to initiate continuing exchanges.

Despite the historical gaps that exist between RIM and information security, there has been increased outreach between professional associations, such as ARMA International and (ISC)², as well as significant research initiatives that form a junction between the two disciplines. This effort to form a bridge between information security and RIM comes from an increasing recognition between risk and compliance professionals of the requirement to manage information securely from its creation to its ultimate destruction.

The current regulatory environment and growing concerns around data privacy create an opportunity for information security and RIM to forge a new relationship that draws on the strengths of both groups to yield innovative approaches to managing the increasingly complex business requirements to provide cradle-to-grave protection for information assets. A significant example of this fusion of information security and RIM requirements is the Massachusetts Data Privacy Law (M.G.L. c.93 H ~ Regulation 201 CMR 17.00). This data-protection statute is one of the toughest of the state privacy laws. The Massachusetts law requires the identification of records containing personally identifiable information (PII). For those uninitiated in RIM practices, this provision means having a current, sustainable and accurate electronic records inventory that intermingles security-related attributes. The law’s focus on records is no surprise given that it owes its creation to a series of data breaches that involved both security issues and storage of a significant amount of PII retained far past its useful existence.
While it is tempting to believe that RIM and information security can deal with the recent regulatory challenges and proceed down their separate and parallel paths, this would waste an opportunity to forge a synergistic affiliation that has the potential to yield invaluable benefits in the protection of information.

An organization can introduce a series of related practices to construct a collaborative partnership between the RIM and information security function within an organization. It may be preferable to introduce each practice in succession to obtain its full benefits. It is not necessary to implement all practices into an organization; however, developing a sustainable approach to electronic records inventory is the foundation upon which the other practices are dependent.

All practices have been implemented successfully in a production environment. Different combinations of practices have been implemented depending on the cultural environment and level of organizational maturity of the client enterprise. Utilizing all nine practices is best suited for larger enterprises, based upon the author’s experience implementing this strategic approach. Smaller organizations experienced a better outcome employing the first practice, as well as by employing several other of the practices based upon a risk-based analysis of the organizations’ environments. The success of this approach is dependent on senior management’s commitment to the project and buy-in from the RIM and information security teams. Because implementing all practices requires the availability of resources, the outcome is dependent upon the ongoing commitment of all key stakeholders to this strategic approach.

The practices are as follows:

1. Develop a sustainable approach to electronic records inventory. Records inventories have long been one of the most tedious and resource-intensive tasks facing records managers. Most methodologies have a hard copy focus and require an extremely detailed analysis of the records population under inventory. This works for hard copy records that tend to have fewer varieties and lend themselves to a simpler classification scheme. Unfortunately, electronic records can present a significantly more challenging inventory project.

Electronic records come in a diverse array of formats related to different hardware and software platforms, various development approaches, an assortment of database types, and diverse storage media formats, just to name a few. In most enterprises, structured electronic records are invariably linked to specific applications, rather than just a record type. Modern applications utilize numerous types of records, many of which have no records retention implications, such as intermediate work files. Using a traditional records inventory approach would require evaluating a plethora of files to make a determination about what files constitute actual records (i.e., official records). Without an approach to categorize record types at a higher level of significance, inventorying a single application could seem like trying to boil the ocean. This means developing a records inventory methodology specifically designed to handle structured electronic records. While these methodologies exist, they are not widely utilized outside of RIM consulting firms. The basic idea is application of the Pareto principle (i.e., the 80–20 rule) to the electronic inventory process. Rather than attempting to inventory the entire universe of files associated with an application, the inventory looks for specific categories of electronic records that represent the official records associated with an application, such as databases, marketing reports or third-party extracts. This process will yield a manageable inventory and offers a risk-based approach to inventory management.

This approach to electronic records inventories lends itself to scripts based on application profiles, such as enterprise mainframe systems or web-based applications. These scripts could provide for automated inventory gathering from application support staff. This approach makes an inventory of electronic records feasible, cost-effective and sustainable on a continuous basis.
This approach, in combination with the application of network scanning and discovery tools to inventory unstructured electronic records, has the potential to provide a continuous inventory of the electronic records of an enterprise.

2. **Introduce a governance, risk management and compliance (GRC) approach to address the broad universe of risk and compliance issues, including vendor risks and PII exposures.** A great deal of overlap exists between the myriad of risk teams within an enterprise. The need to manage risk associated with stored electronic information is a common challenge for each group. Currently, each team seeks to manage a portion of the electronic records risk associated with their specific function. For example, RIM looks to maximize the disposal of obsolete electronic records to minimize potential e-discovery risk. Information security also seeks to avoid the retention of unnecessary electronic information to mitigate any potential data privacy issues. This divided approach often leads to redundancy in some areas with other risk going unaddressed.

A GRC approach can facilitate records being used to drive corporate compliance rather than as a component of several risk management initiatives. One of the easiest ways to incorporate GRC into RIM is by extending the records inventory process to include other threats and vulnerabilities. These risk attributes would simply become additional attributes of the records inventory, such as outsourcing/vendor records storage, presence of PII, use of encryption tools, and retention beyond scheduled destruction. Using this centralized records inventory would facilitate a comprehensive assessment of records-related risk across the organization and encourage the adoption of strategies that mitigate several categories of risk utilizing shared solutions.

3. **Encourage collaboration on RIM policies and procedures that expedite the disposal of obsolete records with a destruction priority given to high-risk electronic records containing PII or personally identifiable health information (PIHI).** The excessive retention of obsolete records is associated with two significant areas of risk. Changes in e-discovery rules since 2006 have placed a greater requirement on organizations to produce electronic records as part of the discovery procedures in legal actions. Retention of electronic records beyond their retention requirement or useful life can escalate the cost of discovery action into the hundreds of thousands of US dollars.

Excessive retention of obsolete records including PII can also magnify the results of a security breach. Storing these records in an unencrypted format increases the risk associated with excess records retention.

The simplest way to diminish excessive retention risk is the development of an effective electronic records disposal process. Effective disposal is dependent on a current inventory of electronic records that includes the location and storage format of the information scheduled for destruction. Inclusion of a PII attribute in the records inventory can provide a means of expediting the disposal of electronic records containing sensitive data.

A joint effort between the RIM and information security teams can yield complementary policies that ensure that the records disposal procedure expedites higher-risk records, especially those with a PII component intended to decrease the potential consequences of a security breach.

4. **Stimulate innovation in the development of records life cycle that guides data through a defined pathway, from creation to destruction, based on its assigned risk-based profile (i.e., a records ecosystem approach).** The optimal way to reduce risk from both a RIM and information security perspective is to ensure that records do not exist beyond their planned destruction date, barring legal restrictions such as a records hold that might extend a record’s retention period. Unfortunately, this rarely occurs. RIM professionals have referenced decades-old media sitting in their offsite storage facilities because it was not a high priority to destroy these records. The trend toward a lower storage cost for electronic media has made it more economically viable to keep older records than actively work to dispose of them. Some industries, especially in the financial services sector, have placed general records holds on their records inventories after several industry scandals. After the lifting of the general hold actions, many disposal programs remained relatively inactive. There is also a tendency among some executives to maintain obsolete records because “they might be needed someday,” despite the reality that restoring these records is likely technically and economically infeasible. This “hoarder” mind-set could be immensely expensive if future e-discovery requests involve archaic records formats.
RIM and information security teams need to work collaboratively to establish a records ecosystem in which the establishment of an electronic records expiration date occurs at the record’s creation.

Most information security organizations require data classification labeling based on information risk profiles. The information security team can work with RIM peers to add an expiration date to the existing data classification process. In addition, the current tools used to identify information with sensitive content, such as PII, could perform a discovery analysis to add date information to the search criterion. The net result of this extension of an information security tool set into the RIM concerns would produce a listing of obsolete PII records with the potential for immediate disposal. This type of data clean-up project, reminiscent of similar information security efforts to remove dormant user accounts, would result in a tangible reduction in risks and costs.

5. **Create a united front on compliance projects with a strategic goal of obtaining resources.** In a recessionary economic period, most organizations seek to maximize their investments to protect revenues. Compliance initiatives can find it difficult to compete for resources with revenue enhancement proposals. There exists the potential for an exacerbation of this situation when multiple compliance-related functions submit similar budgetary requests to manage different aspects of the same risk, e.g., complying with a new data privacy law such as the Massachusetts Data Privacy Law. RIM and information security might improve their prospect of gaining necessary funding by linking their efforts into a single initiative that provides broader risk-mitigation coverage. This approach might also yield the most considerable cost savings as a result of the joint deployment of automated solutions that offer RIM and information security benefits.

6. **Establish new strategies for responding to records retrieval requests.** One of the best strategies for gaining funding for a project is to position its potential to reduce costs or increase efficiency. Joint RIM and information security projects have the potential to accomplish both of these objectives. After changes to the e-discovery rules in 2006, the costs associated with electronic records discovery requests have escalated. A large component of these costs involves the location of electronic data stores. An effective continuous approach to electronic record inventories would simplify the fulfillment of e-discovery requests, resulting in considerable savings in legal discovery tasks and avoidance of negative judgments when critical information is missing.

7. **Provide a timely assessment of the impact of security breaches.** After a security breach occurs, an organization needs to initiate its response in a very short time frame. A perpetual approach to electronic records inventories could provide critical data to assist in the identification of electronic data containing PII. A comprehensive records inventory can also determine the security controls, such as encryption, associated with these records, which might avoid reporting a potential breach or at least provide peace of mind for affected parties.

8. **Provide one-stop shopping for risk assessment using a centralized records information repository.** Currently, attempting to determine the risk associated with data in an organization will generate myriad responses, depending on who is asked. One of the primary reasons for the difference in response is that different disciplines concentrate on a narrow spectrum of risk attributes. Within a risk discipline, a narrow but deep approach to risk assessment may make sense, but it may also fail to recognize the synergic impact that different risk attributes may have upon each other. One only has to review past security breach incidents to understand that many events result from the presence of multiple factors that combine into “a perfect storm.”

A good example of this synergy of risk to create a sizeable security breach occurred with a major retail chain. The major cause of the breach was a wireless infrastructure, but an investigation uncovered multiple points of unauthorized access, including unsecured wireless communications and unencrypted PII data.

Forensic investigation usually reveals the causes of the breach to allow for remediation of identified issues. However, the use of a multidisciplinary risk assessment may prevent a breach from occurring or may mitigate its impact. One natural starting point for this risk assessment is with the records themselves. Rather than using an electronic records inventory as an end in itself, a joint effort between the information security and RIM teams could extend the value of the inventory data by creation.
of a multidimensional risk assessment tool that includes compliance-related attributes, such as PII content, location, regulatory requirements, encryption, storage format and technology used. There is a potential to incorporate application and business criticality risks to create a records repository capable of providing data for a variety of risk assessments. This repository can support diverse risk assessment needs, such as the impact of new policies or compliance with new regulatory requirements.

9. Simplify end-user compliance education and awareness efforts. One of the biggest complaints of end users is that they do not have the time to attend training. Some of this objection comes from multiple uncoordinated training efforts from various risk functions that touch upon the same topics from slightly different perspectives. This approach also creates confusion around compliance because of similar terminology applied with slightly different meanings. An integrated education effort between the RIM and information security teams would provide the end user with a comprehensive understanding of how to handle records under their control from data protection and records retention standpoints during their daily work activities. It also decreases overall training cost and time for the organization.

CONCLUSION
One approach to cultivating a robust relationship between information security and RIM is the establishment of human outposts within each other’s teams. These human outposts would be rotating roles fully integrated into the daily operations of their assigned team. Some participants might elect to become permanent members of these teams. Other participants will go back to their original assignments with new insights into the issues of their peers, thus becoming subject matter experts (SMEs). This exchange endeavor could be an approach to the creation of a new class of hybrid professionals with core competencies that span both RIM and information security disciplines. These hybrid professionals could become indispensable resources on data protection strategies and on managing the current trend toward greater privacy regulation.

Corporate governance boards provide another avenue to develop closer integration between the RIM and information security teams by inclusion of both groups in regular meetings and cross-pollinating project teams among both teams’ members.

In the past decade, information security professionals have proactively sought their peers in business areas to build relationships and provide value to the organization. Information security management may need to take the lead in establishing a closer alignment between the two complementary risk functions.

Albert Einstein said, “We cannot solve our problems with the same thinking we used when we created them.” The closer alignment between RIM and information security may provide an approach to managing increasing data protection concerns and tough privacy regulations rather than maintaining the separation between these critical compliance functions.

ENDNOTES