Addressing Security Concerns: The Expanding Role of Information Governance

Andrew Altepeter

Over the past decade, cyber security has become a major concern in the public consciousness. From WikiLeaks, to state-sponsored attempts to steal valuable intellectual property, to highly publicized retail companies' credit card breaches, information professionals face a constant barrage of threats to their organizations' information.

These threats erode an organization's ability to prosper and threaten American competitiveness as a whole. While traditionally, information professionals have focused on helping the organization meet legal, regulatory, and business requirements, the equally pressing concern of securing information assets provides them new opportunities.

Protecting these assets are not only the responsibilities of the firewall administrators, network architects, and others who sit in IT. In his book *Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets*, Robert F. Smallwood argues an important piece of this strategy must be information governance.

While acknowledging that there are several competing definitions of *information governance*, Smallwood characterizes it as an interdisciplinary subset of corporate governance: the melding of records management, IT governance, e-discovery, business continuity, disaster recovery, information security, and privacy. Its ultimate aims are to manage and control the output of IT through policies and tools that control access to and use of information.

Although Smallwood is not the first to use this definition of information governance, it is a relatively new approach that greatly expands the scope of what until quite recently has been a field primarily rooted in the disciplines of records management and e-discovery.

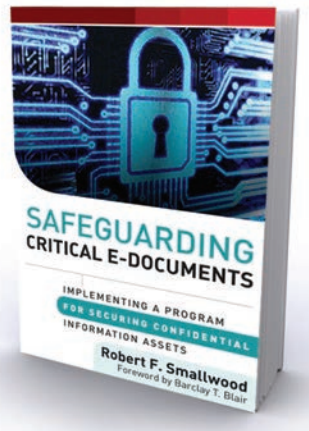
Smallwood's book is divided into five parts. He first outlines the major security problems and risks organizations face and introduces basic information governance principles. In Part II he describes the risks and countermeasures that can be taken for specific platforms, such as unstructured content, e-mail, instant messaging, social media, mobile devices, and cloud computing. Part III is devoted solely to e-records management issues, specifically defining and protecting vital records and long-term preservation of electronic records. Part IV introduces technologies that can help protect information assets, such as encryption, digital signatures, data loss prevention tools, and information rights management. The final part of the book provides strategies for obtaining executive sponsorship, managing projects, and selecting vendors.

Readers will find helpful the concrete steps the book gives for rolling out and maintaining a secure environment for information assets. Each chapter has text boxes that outline key points and chapter summaries that reinforce the main takeaways.

Non-technical readers will find Smallwood's descriptions of information governance technology tools easy to understand. Appendices give standards for digital signatures, regulations for records management, and lists of technology and service providers. Chapter endnotes provide readers with additional resources.

In total, Smallwood's book gives readers a solid foundation for making informed governance decisions and presenting them in a way that upper management will find appealing.

The book would be strengthened by a more robust discussion of the "low-tech" ways organizations can help secure their environment, such as employee training, awareness presentations, newsletters, portal messaging, and office posters; these are all important pieces of an information protection program.



Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets
Author: **Robert F. Smallwood**
Publisher: **John Wiley & Sons**
Publication Date: **2012**
Length: **263 pages**
Price: **$75**
ISBN-13: **978-1-118-15908-8**
Source: ***www.arma.org/bookstore***

The book also largely neglects the most common entryways of data breaches, such as phishing and social engineering scams, although Smallwood does devote some discussion to insider threats, such as careless or malicious employees. Nevertheless, more emphasis should be given to the fact that while technology is necessary to secure information, employee vigilance is the first step.

Despite these omissions, *Safeguarding Critical E-Documents* is an important call to arms for information professionals. To stay relevant, the profession must expand beyond the established business justifications of improved efficiency, regulatory compliance, and legal retention requirements. Protecting information from security threats is a way to add significant value to the organization by addressing a concern that is on the mind of every executive in the country.

For American businesses to stay competitive with the rest of the world, organizations must continually be vigilant in protecting their information assets. Proper information governance policy and controls are important elements in any security strategy. **END**

Andrew Altepeter can be reached at andrew.altepeter@gmail.com. *See his bio on page 47.*