Richmond Journal of Law and Technology

Volume 19 | Issue 4 Article 1

2013

Information Governance: It's a Duty and It's Smart Business

Charles R. Ragan

INFORMATION GOVERNANCE: IT'S A DUTY AND IT'S SMART BUSINESS

By Charles R. Ragan*

Cite as: Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12 (2013), *available at* http://jolt.richmond.edu/v19i4/article12.pdf.

I. INTRODUCTION

[1] A scant generation ago (twenty-five years), the World Wide Web—"an internet-based hypermedia initiative for global information sharing" —was largely a laboratory phenomenon.[1] In 1994, the Clinton Administration urged world leaders to develop a global information superhighway,[2] and the Information Age raced upon us. Now, Facebook

* Charles R. Ragan has practiced in high stakes commercial litigation for 30-plus years, and in the field of information management and electronic discovery for more than a decade. He was an original participant in Working Group 1 of The Sedona Conference, and has contributed to many of its publications, including: The Sedona Principles (2004 and 2007, and its Annotated Versions in 2004, 2005 and 2007), The Sedona Guidelines (2005), and The Case for Cooperation (2009). He has advised Fortune 500 companies, as well as emerging companies, on electronic discovery and records and information management issues. He is also an Adjunct Associate Professor at the University of Minnesota Law School, where he teaches a seminar on Information Governance. He is licensed to practice law in California, Minnesota, and New York. The author thanks and acknowledges the editorial assistance of his colleague and friend, M. Kate Chaffee, in reviewing earlier drafts of this article, but he remains responsible for any error.

[1] *Tim Berners-Lee*, W3C, http://www.w3.org/People/Berners-Lee/ (last visited Feb. 23, 2013) (dating the invention of the World Wide to 1989).

[2] *See* Jube Shiver Jr., *Gore to Call for Global Information Age*, L.A. TIMES (Mar. 17, 1994), http://articles.latimes.com/1994-03-17/business/fi-35298_1_economic-development.

has more than one billion accounts and most of us are constantly deluged by volumes of electronic information through e-mail, texts, social media, the Internet, cable systems, and others.

[2] Information is among the most valuable assets for most organizations—public or private. For some, the value may lie in priceless intellectual property, such as patents or trade secrets. For others, it may be a customer database built up over decades of sales or the brainchild of a Harvard student aggregating faces. For still others, it may be complex workflows or systems for transmitting demand for power from individual customers onto a regional grid for the distribution of electricity. Last but not least, and increasingly so, it may be a set of algorithms for assessing vast volumes of data and discerning what trades are most likely to succeed, or what products may appeal to a customer with discretionary income.

[3] For most of the Information Age, it has been relatively risk-free to allow these volumes of information to accumulate—even after their normal useful life – because storage devices have been cheap. In fact, the cost of unit storage declined approximately ninety-nine percent from 2000 to 2010.[3] So far, as the saying goes, this is "all good." But recently, three important caveats have injected themselves into that bromide. First, the total worldwide costs to store and manage the ever increasing volumes of information being generated and retained in organizations are *increasing*.[4] The increase in volumes is truly staggering. It was estimated in 2011 that

[3] Barclay T. Blair, *Today's PowerPoint Slide: The Origin of Information Governance By the Numbers*, BARCLAY T. BLAIR (Oct. 28, 2010), http://barclaytblair.com/2010/10/28/origins-of-information-governance-powerpoint/ (referring to data from the IDC *Quarterly Storage Software Tracker, Worldwide Quarterly Disk Storage Tracker* and *Costs of Hard Drives 1956 – 2010*).

[4] *See id*. While the worldwide expenditures on storage hardware remained the same, expenditures on storage software more than doubled between 2000 and 2010.

ninety percent of the data in the world had been created in the prior two years and for most organizations, information volume doubles every eighteen to twenty-four months.[5]

[4] Second, absent investment in costly search technologies capable of federated searches across platforms and storage containers, these volumes of information may jeopardize the organization's ability to retrieve valuable information efficiently such that strategic opportunities are lost. Third, if information is retained past its useful life (*i.e.*, after its business function is fulfilled and while there is no other legal obligation to keep it), that information could be subject to future requests in litigation or governmental investigation.[6] As a recent article notes, while the basic cost to manage a terabyte of information may be about $5,000, if that terabyte is retained unnecessarily and becomes the subject of discovery (and collection, processing, analysis, and review), that unneeded data may cost the organization an extra $15,000.[7] For an organization that has petabytes of information (roughly 1,000 times a terabyte), or in the case of our

[5] DEIDRE PAKNAD & RANI HUBLOU, CGOC, INFORMATION LIFECYCLE GOVERNANCE LEADER REFERENCE GUIDE 5 (2012), *available at* https://www.cgoc.com/files/CGOC_ILG_LeaderReferenceGuide.pdf.

[6] *See* Thomas M. Jones et al., *Going Global: Mapping an International Records Retention Strategy*, ZASIO ENTERPRISES 2, http://www.zasio.com/pdfs/consulting_goingglobal.pdf (last visited Feb. 24, 2013).

[7] Jake Frazier & Anthony Diana, '*Hoarders': The Corporate Data Edition*, LAW TECH. NEWS (Dec. 19, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202581938140&Hoarders_The_Corporate_Data_Edition&slreturn=20130109125622. Actually, the number cited in the article is probably low, as the author's calculation appears to assume equal volumes are collected, processed, and reviewed; when in fact far more data is collected and processed than is reviewed.

largest organizations, scores of petabytes, the "electronic discovery tax" poses a horrific and unnecessary risk.[8]

[5] For some in senior management (*i.e.*, those in the Boomer generation), the problem of unnecessary data causing substantial costs in litigation will sound familiar. In fact, as a result of expensive paper discovery experiences in the 1970s and 1980s, many organizations developed policies falling under the euphemistic label of "document retention" or "record retention" policies.[9] Under these policies, an organization established how long they *had* to keep certain information due to laws or regulations, how long they *wanted* to keep information due to business value or need, and destroyed what they did not have or want to keep.[10] The Supreme Court famously ruled in *Arthur Andersen*, a case that grew out of the Enron scandal, that such policies are perfectly lawful.[11] In fact, the Court in that case recognized that such policies are "created in part to keep certain information from getting into the hands of others, including the Government," and stated that a manager may instruct his employees to comply with a valid document retention policy under normal circumstances.[12] In the day of paper records, relatively small

[8] For an organization with 40 petabytes of data under management, the potential "tax" would be $600 million! (40 *times* 1,000 *times* $15,000 = $600,000,000).

[9] *Cf.* STEVE PALOMINO & ART VANCIL, AICPA, A PRACTICE AID FOR RECORDS RETENTION (2012), *available at* http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/BusinessIntelligence/DownloadableDocuments/Records_Retention_Mktg.pdf (discussing the importance of record retention policies and suggesting practice tips for implementing such policies).

[10] *See id.* at 5.

[11] Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005).

[12] *Id.* Once litigation or government inquiry is reasonably anticipated, however, one ventures into the realm of circumstances that are not "normal." *See, e.g.*, Hynix

staffs with administrative assistance in local offices could administer such policies.

[6] By the late 1980s and early 1990s, however, competitive pressures of globalization forced many organizations in the United States to go lean; consequently, many records functions were cut as expendable.[13] More problematic, however, were the advent of the Information Age and the proliferation of "road warriors" who wanted all of their potentially relevant files stored on their laptops. Few organizations took immediate steps to update their retention policies to account for the influx of electronic records. Further, in those organizations that sought to maintain "retention" policies for all information regardless of the media, those developments turned most employees into *de facto* records managers without any additional compensation or training in the discipline.[14] Some workers tried to remain faithful to the policies, but as the volumes exploded in recent years, knowledge workers were spending more than a quarter of their time managing e-mail.[15] In a competitive global economy,

Semiconductor, Inc. v. Rambus, Inc., 645 F.3d 1336, 1344 (Fed. Cir. 2011); Micron Tech., Inc. v. Rambus, Inc., 645 F.3d 1311, 1319 (Fed. Cir. 2011).

[13] *Cf.* Jones et al., *supra* note 6 ("An organization's goal should be to retain *only* those records needed to conduct business, to comply with the law . . . and to reasonably preserve archival documentation.") (emphasis added).

[14] *See* R. Thomas Howell & Rae N. Cogar, *Records Retention – An Essential Part of Corporate Compliance*, *in* RECORD RETENTION AND DESTRUCTION CURRENT BEST PRACTICES 1, 4 (Am. Bar Ass'n ed., 2003), *available at* http://www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf (noting a widely applied rule that the creator of electronic documents has the responsibility for retaining the document).

[15] Published estimates range from 28% to 50%. *Compare* Laura Vanderkam, *Stop Checking Your Email, Now.*, CNN MONEY (Oct. 8, 2012, 11:14 AM), http://management.fortune.cnn.com/2012/10/08/stop-checking-your-email-now/, *with* Courtney Rubin, *Study: Employees Are Unproductive Half the Day*, INC. (Mar. 2, 2011),

this is a not a model of efficiency. As Jason Baron, the 2011 recipient of the prestigious Emmett Leahy award, persuasively urged, "[W]e need to declare an official end to the end-user being expected to act as *de facto* records manager."[16]

[7] The glut of information arriving randomly also interferes with productivity. One study showed that, on average, knowledge workers are interrupted every three minutes and it takes a half hour to return to the pre-interruption level of concentration.[17] This is no small problem. Indeed, the problem has led senior researchers at some of the world's leading technology companies to form (and incorporate) the Information Overload Research Group.[18]

[8] Another exacerbating factor in the modern organization is that some users who are newer to the workplace have not received training about the risks of quickly (and informally) generating information that might prove problematic for the organization in litigation.[19]

---

http://www.inc.com/news/articles/201103/workers-spend-half-day-being-unproductive.html (finding that employees at small and medium-sized businesses spend half their day working un unproductive tasks such as filtering information and correspondence).

[16] *See* Jason R. Baron, Acceptance of the 2011 Emmett Leahy Award 7 (Sept. 15, 2011), *available at* http://www.emmettleahyaward.org/uploads/Proceedings_2011.pdf.

[17] *See* L. Gordon Crovitz, *The Information Age: Unloading Information Overload*, WALL ST. J., July 7, 2008, at A11.

[18] *See id.*; *About IORG*, INFO. OVERLOAD RES. GROUP, http://iorgforum.org/about-iorg/ (last visited Feb. 20, 2013).

[19] *Cf.* Teresa Schoch, *Turning the Ship Around with Four-Generation Crew*, INFO. MGMT. MAG., July-Aug. 2012, at 28 (noting the importance for younger generations to realize "how critical the implementation of record capture procedures is to the organization's long-term well-being").

[9] Finally, the challenge of dealing with information in the modern organization is a dynamic, not stationary, target because the technologies that generate and deliver information are constantly changing. Witness, for example, the quick sprint from paper documents and phone-message slips, to e-mail and voicemail, through universal messaging, or instant messaging and chat, and to Facebook, LinkedIn, and Twitter.[20]

[10] Something new—and at least a *little* different—is needed if we are to avoid what Baron and others have called "the coming 'digital Dark Ages'" in which we cannot see clear paths forward due to the glut of information before us.[21] Thus far, those who labor principally in the fields of law and records management have started to discuss these issues, but have found difficulty gaining traction or budget, usually for want of either a champion or a clear business case with an indisputable return on investment. As discussed below, senior management in all organizations and corporate boards of directors need to recognize that assessing and overseeing management of the risks posed by information overload *is* a necessary part of their existing duties.

II. THE FOUNDATIONS OF THE DUTIES

[11] The board of directors of a corporation is generally responsible for overseeing the business of and helping to set strategy for the corporation so as to minimize unnecessary risks. Senior management is generally responsible for managing the company and executing in accordance with the organization's strategic direction. Board members have fiduciary

[20] Even Pope Benedit XVI was on Twitter—in eight languages. *See* Gaia Pianigiani & Rachel Donadio, *Twitter Has a New User: The Pope*, N.Y. TIMES (Dec. 3, 2012), http://www.nytimes.com/2012/12/04/world/europe/follow-the-pope-on-twitter-he-follows-no-one.html?_r=0. Pope Francis has also joined Twitter. *See Pope Francis*, TWITTER, twitter.com/Pontifex (last visited May 13, 2013).

[21] Jason R. Baron, *supra* note 16, at 8.

duties to the owners of the corporation (its shareholders), which include the duty of care, the duty to remain informed, and the duty of loyalty, as typically circumscribed by the so-called "business judgment rule."[22]

[12] Several courts have elaborated on these duties in factual circumstances not stemming from an organization's management of information-related issues, but in terms that are directly relevant to the current state of information governance in many organizations.[23] The principles thus enunciated raise the specter of potential liability if officers and directors utterly fail to ensure the adequacy of information systems. For example, in *Caremark International Inc. Derivative Litigation*, plaintiffs claimed that "directors allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in doing so they violated a duty to be active monitors of corporate performance."[24] The Delaware Chancery Court, noting that the theory advanced was "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment," nonetheless agreed that director liability for breach of the duty of care could arise either from a board decision that resulted in loss or "from an *unconsidered failure of the board to act* in circumstances in which due attention would, arguably, have prevented the loss."[25] In discussing the "business judgment rule" limitations on these principles, Chancellor Allen concluded, in line with Judge Learned Hand's analysis, "the core element of any corporate law duty of care inquiry [is] *whether there was good faith effort to be informed*

[22] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967-68 (Del. Ch. 1996). Under the business judgment rule, directors are generally insulated if they have considered an issue in good faith or through a rational and informed process.

[23] *See generally id.*; *in re* Abbott Labs. Derivative S'holder Litig., 325 F.3d 795 (7th Cir. 2003).

[24] .*See* 698 A.2d at 967.

[25] *Id.*

and exercise judgment."[26] With respect to potential liability for failure to monitor, Chancellor Allen stated:

> [A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.[27]

[13] In the years since *Caremark* was decided, much has happened in the world of corporate governance. The case has been cited more than 3,000 times;[28] many courts have embraced the decision, a few have commented negatively or distinguished the case, and some have found on the facts before them the "unconsidered failure of the board to act" required for liability.[29]

[14] Perhaps even more important, Americans have already witnessed two separate periods of corporate malfeasance in this century. The first of

[26] *Id.* at 968 (citing Barnes v. Andrews, 298 F. 614, 618 (S.D.N.Y. 1924)) (emphasis added). In *Barnes*, Judge Learned Hand noted that directors are not specialists; rather, they are "the general advisors of the business, and if they faithfully give such ability as they have to their charge, it would not be lawful to hold them liable." *Barnes*, 298 F. at 618.

[27] 698 A.2d at 970. The *Caremark* court concluded that the board had followed procedures to inform themselves regarding contracts with health care providers, so as to be protected by the business judgment rule, and approved the settlement in issue.

[28] As of April 23, 2013, Westlaw's Keycite shows 3,234 citations to the case, including 260 cases.

[29] *E.g.*, *In re* Abbott Lab. Derivative S'holder Litig., 325 F.3d 795, 808-809 (7th Cir. 2003) (finding that six years of noncompliance established lack of good faith).

these periods included such fiascos as Enron and WorldCom[30] while the second stemmed from the overvaluation and trading of subprime mortgages, which led to the demise of several major financial institutions and the global financial crisis of 2008.[31] Both led to outcries for heightened scrutiny on corporate America and each led to new legislation imposing new requirements on corporations. The first led to the passage of the Sarbanes-Oxley legislation[32] and the second led to the passage of the Dodd-Frank legislation.[33]

[15] Posed squarely, the issue is whether the risks attending information systems in the modern enterprise are such that directors and senior management may safely ignore them and fail to take steps to enhance

[30] *See* MARK JICKING & BOB LYKE, CONG. RES. SERV., RS21253, WORLDCOM: THE ACCOUNTING SCANDAL 1-2 (2002), *available at* http://www.iwar.org.uk/news-archive/crs/13384.pdf.

[31] *See generally*, KATALINA M. BIANCO, CCH, THE SUBPRIME LENDING CRISIS: CAUSES AND EFFECTS OF THE MORTGAGE MELTDOWN (2008), *available at* http://www.business.cch.com/bankingfinance/focus/news/Subprime_WP_rev.pdf.

[32] *See generally* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

[33] *See generally* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010). The act applies not just to financial institutions, but to all organizations doing business in the financial, capital, and credit markets, including energy companies, electric and natural gas utilities, chemical companies, mining and mineral companies, airlines, agribusinesses, and consumer products companies. *See* Fred Pulzello & Sonali Bhavsar, *Dodd-Frank Act Puts Focus on Information Governance*, INFO. MGMT. MAG., Nov.-Dec. 2011, at 42, *available at* http://content.arma.org/IMM/Libraries/Nov-Dec_2011_PDFs/IMM_1111_business_matters_dodd_frank_act_puts_focus_on_info_gov.sflb.ashx. As recently as December 2012, the Government Accountability Office estimated that rulemaking under the Dodd-Frank legislation was only half complete. *See Fragmented U.S. Regulatory System Stalls Dodd-Frank Rules-GAO*, REUTERS (Jan. 23, 2013), http://www.reuters.com/article/2013/01/23/financial-regulation-gao-idUSL1N0ASHV320130123.

information governance processes.[34] The short answer, I submit, is a resounding "no." As one commentator observed, "[t]here is no doctrinal reason Caremark claims should not lie in cases in which the corporation suffered losses, not due to a failure to comply with applicable laws, but rather due to lax risk management."[35] The three following sections, respectively, (a) describe those risks,[36] which include some conflicting obligations, (b) suggest a logical approach for addressing the risks, and (c) identify the opportunities with existing mechanisms for addressing them.

III. RISKS ASSOCIATED WITH INFORMATION IN THE MODERN ENTERPRISE

A. The Risks Are Many and Diverse

[16] The risks associated with information in the modern enterprise are numerous, varied, and conflicting. At the outset, one should also note that almost all information is now created electronically[37] and because

[34] The problem is not limited to business organizations. Indeed, in a 2011 memorandum on managing government records, President Obama warned that "if records management policies and practices are not updated for a digital age, the surge in information could overwhelm agency systems, leading to higher costs and lost records." Memorandum from President Barack Obama on Managing Gov't Records for Heads of Exec. Dep'ts and Agencies (Nov. 28, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records. The government initiative is certainly needed and welcome, but there should be no mistake that the problem is not limited to a records management issue.

[35] Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. CORP. L. 967, 968 (2009).

[36] Bainbridge further observes, "risk management does not differ in kind from legal compliance or accounting controls." *Id.* at 981.

[37] Recent estimates suggest that more than ninety-nine percent of all information is now generated electronically. *See* ROBERT M. VERCRUYSSE & GREGORY V. MURRAY,

electronic information has significant differences from paper documents, former processes and paradigms are no longer 1:1 analogs.[38] Briefly stated, the risks associated with information in the modern enterprise include[39]:

- Proprietary information. Information that has competitive value must be protected against disclosure or misuse. In most organizations, there will be several levels of confidentiality or protection requiring different treatments (*e.g.*, company-private, confidential, highly confidential, etc.).[40]

- Contractually protected information. When considering new business arrangements or technologies, organizations often receive information under the terms of non-disclosure agreements. Such contractual obligations with third parties

VERCRUYSSE MURRAY & CALZONE, P.C., ELECTRONICALLY STORED INFORMATION AND THE NEW FEDERAL RULES OF CIVIL PROCEDURE REGARDING DISCOVERY 1 (2007), *available at* http://www.vmclaw.com/articles/3_Electronic_discovery.pdf.

[38] *See generally Introduction* to THE SEDONA CONFERENCE®, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (2nd ed. 2007), https://thesedonaconference.org/download-pub/81 [hereinafter "The Sedona Principles"] (providing a brief but informative survey of differences between paper and electronic information).

[39] This is an illustrative—not an exhaustive—list.

[40] *See Excerpt from Dupont Records Management Guide, in* RECORDS RETENTION AND DESTRUCTION CURRENT BEST PRACTICES 22, 28 (Am. Bar Ass'n ed., 2003), available at http://www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf.

also require protection of such information from misuse or theft.[41]

- Challenges to sound record keeping practices. Information that has business value to an organization should be maintained in such a manner as to ensure its accuracy, integrity, and availability for later use, but also protected against alteration. Keeping excessive volumes of information, which might not adequately distinguish drafts from finals, undermines these objectives.[42]

- E-Discovery. Information that may be responsive to requests in U.S. litigation or investigation must be identified quickly and preserved once a claim (or inquiry) is reasonably anticipated.[43]

- Challenges in developing and implementing retention policy schedules. Separate from any litigation or investigation obligation to retain information, an organization is required to retain different categories of information for various periods, depending on the jurisdictions where the organization does business and the nature of those businesses. Determining the retention

[41] *See* JERE M. WEBB, A PRACTITIONER'S GUIDE TO CONFIDENTIALITY AGREEMENTS 1 (1985), *available at* http://www.stoel.com/files/confidentialityagreementguide.pdf.

[42] *See generally The Generally Accepted Recordkeeping Principles*, ARMA (Feb. 17, 2013), http://www.arma.org/garp/index.cfm. These Principles were previously marketed under the term GARP; ARMA recently has shied away from referring to them as "GARP" because of trade name issues raised by the Global Association of Risk Professionals.

[43] *See* The Sedona Conference®, *The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 267 (2010).

schedule for a given organization through traditional methods of legal research is a labor-intensive and expensive effort.[44] In the case of a global enterprise, for example one doing business in 130 countries, the expense could easily exceed one million dollars and the retention requirements found for different jurisdictions often conflict, even for a single category of information. Finally, traditional means for categorizing information into record series that can be manually segregated, stored, retrieved, and eventually destroyed do not translate well or efficiently into the world of electronic storage, retrieval, and disposition.

- Data protection and privacy. Numerous jurisdictions outside the United States have adopted comprehensive regulations for data protection and privacy regarding "personally identifiable information," which is broadly defined to include even information in an e-mail header.[45] The best known of these regimes is in the European Union and its constituent nation states.[46] Legislation or initiatives have also been launched in Asia (Singapore, South Korea,

[44] In the author's experience, a client could easily spend $10,000 per state jurisdiction in legal fees for this research. *See also* Charles Ragan, *How to Avoid the Information Management Dark Ages*, LAW TECH. NEWS 1, 2 (Dec. 16, 2011), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202535755654&How_to_Avoid_the_Information_Management_Dark_Ages.

[45] Gail Lasprogata, et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH L. REV 4, ¶ 14 (2004) *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_4. *See generally* ERIKA MCCALLISTER ET AL., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION § 2-2 (2010).

[46] Lasprogata, *supra* note 45, at ¶ 113.

Taiwan, Malaysia, India, Vietnam, New Zealand, Hong Kong, and China) and Latin America (Brazil, Mexico, Peru, Colombia, Uruguay, and Costa Rico).[47] Typically, such information should be retained only as long as necessary to fulfill its purpose, but enforcement of privacy regulations varies widely from one jurisdiction to another (and even within the European Union).[48] In the United States, there is a patch quilt of federal and state, non-uniform legislation (and some state constitutions) protection of privacy interests in specific areas.[49] In addition, most states have adopted legislation specifying what steps an organization must take in the event that its information systems with consumer information are breached.[50] In short, most organizations face a web of

[47] *See generally* Matthew Glynn, *Australia: Data Privacy Compliance in Asia Pacific*, MONDAQ (Nov. 17, 2012), http://www.mondaq.com/australia/x/206518/data+protection/DATA+PRIVACY+COMPLIANCE+IN+ASIA+PACIFIC; Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 INT'L L. NEWS 4 (2012), http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html.

[48] *See generally European Data Privacy Obligations Impact On U.S. Businesses*, NICOLAI LAW GROUP, P.C. (Aug. 1, 2001), www.niclawgrp.com/Resource-Materials/Monthly-Memo/European-Data-Privacy-Obligations-Impact-On-U-s-Businesses.shtml.

[49] *See, e.g.*, The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2006); Electronic Communication Privacy Act of 1986, 18 U.S.C. §§ 2510-2511 (2006); The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320a-7c; Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 17931, 17937 (2006 & Supp. III 2010).

[50] *See* GINA STEVENS, DATA SECURITY BREACH NOTIFICATION LAWS, Summary (2012), *available at* https://www.fas.org/sgp/crs/misc/R42475.pdf.

potentially conflicting and constantly changing privacy obligations that must be comprehended and respected.

- Conflict between data protection regulation and traditional U.S. expectations of "liberal" pretrial discovery. The privacy or data protection rules and regulations of many jurisdictions do not permit "processing" or "transfer" of personal information without the consent of the data subject. (A proposed data protection reform in the European Union would ensure that explicit consent be given before a company could process a data subject's personal data.[51]) These regulations often conflict with the expectations of judges in the United States that all information relevant to the claims and defenses in an action (if not the subject matter of the litigation) will be freely exchanged during discovery.[52]

- Enhanced risk of security breaches, and attendant release of personal information, including health and financial information.[53]

- Ever-changing landscape of technologies that enhances business communications and confounds management of electronically stored information. Modern technologies—including social media and smart devices (*i.e.*, tablets and

[51] *See* EUROPEAN COMM'N, HOW DOES THE DATA PROTECTION REFORM STRENGTHEN CITIZENS' RIGHTS? 1 (2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf.

[52] *See* AMERICAN BAR ASSOCIATION SECTION OF INTERNATIONAL LAW, REPORT TO THE HOUSE OF DELEGATES 103, 1-2 (2012), *available at* http://www.abanow.org/2012/01/2012mm103/.

[53] *See infra* Part IV.B.3.

smartphones)—allow for the immediate transfer of data and images to unlimited numbers of people who are virtually in any place on the planet with just a few clicks or swipes of the finger. These developments pose obvious risks to sensitive organizational information, including trade secrets and other intellectual property.[54]

- Trend to allow workers to BYOD. In order to attract the best and brightest young talent, many organizations are succumbing to pressures to allow employees to Bring Your Own Devices to work.[55] The introduction of these devices into the workplace presents a host of issues for an organization's central technology function.[56] In the past, for example, the organization could concentrate on a few technology platforms running a particular operating system that relied on a dedicated backend server environment. The

[54] *See* PRICEWATERHOUSECOOPERS LLP, SECURITY FOR SOCIAL NETWORKING 1 (2008), available at http://www.pwc.com/en_US/us/it-risk-security/assets/social-networking-final.pdf.

[55] *See generally* Brittany Bolster, *BYOD: Bring Your Own Device to Work*, AMERICA'S REMOTE HELP DESK BLOG (Dec. 5, 2012), http://www.remotehelpdesk.com/uncategorized/byod-bring-your-own-device-to-work/.

[56] *See, e.g.*, Emily Maltby, *Many Gadgets, Many Risks*, WALL ST. J. (Nov. 11, 2012), *available at* http://professional.wsj.com/article/SB10001424052970204840504578087311857039762.html?mg=reno64-wsj (noting that smaller companies may be earlier adopters of BYOD policies in part because that helps them lower IT costs). *See generally* Brent Gatewood, *The Nuts and Bolts of Making BYOD Work*, INFO. MGMT. MAG. (Nov./Dec. 2012), *available at* http://content.arma.org/IMM/Libraries/Nov-Dec_2012_PDFs/IMM_1112_Making_BYOD_Work.sflb.ashx; Nancy D. Barnes & Frederick Barnes, *Smartphone Technologies Shine Spotlight on Information Governance*, INFO. MGMT. MAG. (May/June 2012), *available at* http://content.arma.org/IMM/Libraries/May-June_2012/IMM_0512_Tech_Trends_Smartphone_Technologies.sflb.ashx.

proliferation of smart devices, however, introduces the need for some conversancy with Apple and Android operating systems and the development of new security protocols to account for them. In addition, to the extent information on such devices may be called for in litigation or investigation, the organization (or its vendors) will have to become familiar with an array of ESI harvesting techniques because collection techniques typically vary from device to device and from operating system to operating system.[57]

- Movement to cloud alternatives. Some organizations, in order to take advantage of economies of scale and resulting economic savings, have considered moving their data "into the cloud" where it may be commingled with data of other organizations and is not under the immediate possession or control of the organization (which may impair the ability to respond to requests in litigation or evaluate claims of internal malfeasance).[58] The economics of cloud operations can be incredibly attractive (if not compelling) for some organizations and/or functions, but there are also a

[57] *See* Greg Buckles, *A Quick Forensics Lesson: The Smart Phone Is Much More than Just a Hard Drive*, LEGAL IT PROF'LS (July 17, 2012), http://www.legalitprofessionals.com/index.php/col/guest-columns/4471-a-quick-forensics-lesson-the-smart-phone-is-much-more-than-just-a-hard-drive.

[58] Rackspace Support, *Moving Your Infrastructure to the Cloud: How to Maximize Benefits and Avoid Pitfalls*, RACKSPACE, http://www.rackspace.com/knowledge_center/whitepaper/moving-your-infrastructure-to-the-cloud-how-to-maximize-benefits-and-avoid-pitfalls (last updated Sept. 12, 2012).

variety of risks—including mid- to long-term costs—that should be analyzed and evaluated.[59]

- Legacy or "debris" data that has no "owner" or continuing value. As noted above, if the organization does not dispose of data and information after its useful life (and when it is not subject to a duty to preserve for litigation or investigation), but instead allows it to linger, the organization will be spending money to store and manage information with no business value[60] *and* that information may be subject to costly future discovery requests. Because "storage has traditionally been cheap"[61]—at least in relative terms—this legacy or "debris" data is a significant risk and problem for many organizations.

- "Big Data." Lastly, and taking the opposite side from the last point, several large organizations are grappling with the issue of so-called Big Data, *i.e.*, whether or not to keep lots of data and subject it to sophisticated algorithms and searching techniques that can produce significant business opportunities and sales.[62]

[59] For example, is the cloud provider capable of (a) preserving and providing data to the owner quickly enough for the owner to respond to discovery requests, or (b) disposing of data in accordance with the owner's retention policy.

[60] The costs of managing information include the cost of labor and equipment to backup data pursuant to disaster recovery and business continuity protocols. Those organizations that do not know what information they have in their legacy systems are paying to backup valueless information.

[61] Mary E. Shacklett, *'Big Data' Calls for an IT Culture Change*, INTERNET EVOLUTION (Mar. 11, 2010), http://www.internetevolution.com/author.asp?section_id=562&doc_id=188999.

[17] From this recitation it should be apparent that while these issues may be present for most organizations, the strategies one organization may choose to follow, and the acceptance or mitigation of particular information-related risks, will differ from the next, depending on each organization's business objectives, specific legal obligations, and its tolerance for risk. For example, a company like Google or Facebook may have an interest in maximum retention of personal demographic information so as to match the ads it displays in sidebars to a particular user, while a manufacturer of heavy equipment might not wish to capture and retain user information for every visit to a webpage advertising forklifts. Senior management and corporate boards have a responsibility to ensure that the organization considers these diverse information-related issues and the optional approaches surrounding them so that the organization addresses them in line with its overall goals and strategies, rather than in an ad hoc manner driven by a single (or even a spare few) disciplinary biases.

[62] Analysis of big data may result in enormous potential savings. For example, the *Economist Outlook for 2012* refers to a McKinsey Global Institute study indicating that analysis of health care data could yield $300 billion worth of savings in the United States alone. Ludwig Siegele, *Big Welcome to the Yotta World*, ECONOMIST (Nov. 17, 2011), http://www.economist.com/node/21537922. Big data also has a wide variety of uses. *See, e.g.*, Joseph Walker, *Meet the New Boss: Big Data*, WALL ST. J. (Sept. 20, 2012, 11:16 AM), http://online.wsj.com/article/SB10000872396390443890304578006252019616768.html (hiring employees); Catherine Dunn, *IBM's New Privacy Chief Eyes Big Data, Analytics*, LAW (Oct. 17, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1350226328616&rss=rss_ltn_news (tailoring customer offers and services); Evgeny Morozov, *The Tyranny of Algorithms*, WALL ST. J. (Sept. 20, 2012, 12:15 AM), http://online.wsj.com/article/SB10000872396390443686004577633491013088640.html (picking the next pop-music star).

B. Organizations Often Assert that They Handle All Information Appropriately

[18] In response to heightened scrutiny of corporate behavior, many organizations have "gone on offense" to assure shareholders that their interests are being managed well.[63] Thus, many organizations have adopted "codes of conduct" that recognize that a global company must comply with the laws of many countries and that each employee is responsible for knowing and complying with the letter and spirit of applicable laws or regulations.[64] Many organizations also speak in their public materials about the duty to protect confidential information and to take precautions before sharing it with anyone,[65] the need to protect company assets to guard its competitive advantage in the marketplace, the importance of "us[ing] electronic communications wisely," and the expectation that each employee is responsible for maintaining accurate records and complying with company policies and procedures for recordkeeping.[66] Some even recognize that employees have a "right to

[63] *See, e.g.*, James E. Rohr, *Message from the Chairman*, PNC (Mar. 7, 2012), *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=107246&p=irol-chairman2012 (follow "Annual Letter to Shareholders" hyperlink) ("At PNC we manage our business with the goal of creating opportunities for increased shareholder value over the long term.").

[64] *See, e.g.*, *Code of Conduct*, JPMORGAN CHASE & CO. (Mar. 15, 2012), *available at* http://www.jpmorganchase.com/corporate/About-JPMC/document/2012CodeofConduct_05_15_12_ada.pdf [hereinafter JPMorgan Chase Code] (discussing compliance with the law in section 1.3); *Intel Code of Conduct*, INTEL (Jan. 2013), *available at* http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-code-conduct-corporate-information.pdf (requiring employees to conduct business with honesty and integrity and to follow the letter and spirit of the law).

[65] *E.g.*, JPMorgan Chase Code. *supra* note 64, at 5.

[66] *Id.* at 22-23.

engage in social, professional and political dialogue outside the workplace" through, for example, social media.[67]

[19] These broad statements[68] set a high bar of expectations. The next obvious questions are whether there are mechanisms in place to facilitate compliance by individual employees or associates, and whether the board has attempted to assure itself that they are adequate.

C. Surveys Strongly Indicate That the Reality Is Far from the Promise

[20] Surveys of knowledgeable persons suggest that reality falls far below the publicly stated promise. For example, a recent survey found that lack of proper management of information was "impacting business productivity and creating costs and liabilities."[69] As Baron and others have observed, employees are spending too much time searching and managing information and recreating desired information that is not readily retrievable.[70] In fact, one recent survey reported that seventy-four percent of respondents reported that valuable information was being lost, and seventy-three percent said that their organizations missed business opportunities because they could not access information efficiently.[71] Virtually all organizations responding to the survey acknowledged rapid

[67] *Id*. at 31, 34 (outlining employees' responsibilities).

[68] In the author's experience, such statements are typical of large organizations and can readily be found in corporate governance materials on the Internet.

[69] *The Information Explosion: How Organizations Are Dealing with It*, COUNCIL FOR INFO. AUTO-CLASSIFICATION 3 (Oct. 2011), http://www.infoautoclassification.org/survey.php.

[70] *Id.*

[71] *Id.* at 5.

volume growth of electronic information: eighty-one percent said document management environments were challenging to manage, seventy-eight percent admitted increased IT infrastructure costs, and eighty-eight percent said they had large stores of legacy data.[72]

[21] Significantly, an increasing and sizeable percentage of senior corporate personnel recognize that their valuable information is *not* secure. For example, in a 2010 study, thirty-seven percent said they were not confident that their electronic records had not been modified, deleted, or inappropriately accessed.[73] Just two years later, forty-eight percent of directors and fifty-five percent of general counsel (of more than 13,000 surveyed) cited data security as an issue of concern, making it the most referenced concern.[74] Another study estimated the median annualized cost of cyber crime per company at $5.9 million.[75] But these direct costs related to a data breach (Sony reportedly spent more than $170 million to address multiple breaches in 2011[76]) pale in comparison to the total injury, including that to the company's reputation.[77]

[72] *Id.* at 4-7. Legacy data is the term used to describe information past its useful life, or with no clearly identifiable owner.

[73] *E-Discovery and ERM: How Is Records Management Performing in the New Spotlight?*, AIIM MARKET INTELLIGENCE, 4 (2010), http://www.aiim.org/Research-and-Publications/Research/Industry-Watch/ERM-and-eDiscovery-2010.

[74] CORPORATE BOARD MEMBER, LEGAL RISKS ON THE RADAR 2 (2012), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf.

[75] *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*, PONEMON INSTITUTE 1 (2011), http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[76] *See* Mathew J. Schwartz, *Sony Data Break Cleanup To Cost $171 Million*, INFORMATIONWEEK (May 23, 2011),

[22] Some of the cybersecurity risk can be attributed to criminal activity (*e.g.*, identity theft), but some apparently is the result of international espionage or politically motivated retaliation.[78] Further, in 2013, several major news organizations acknowledged that their systems had been hacked and their journalists' e-mail passwords compromised by Chinese authorities seeking to monitor Chinese issues, including the news

http://www.informationweek.com/security/attacks/sony-data-breach-cleanup-to-cost-171-mil/229625379.

[77] *See* Juro Osawa, *As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill*, WALL ST. J. (May 6, 2011), http://professional.wsj.com/article/SB10001424052748703859304576307664174667924.html?mg=reno64-wsj.

[78] *See* Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 ("Since September [2012], intruders have caused major disruptions to the online banking sites of Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC."); *White House Confirms Cyber-Attack on "Unclassified" System*, BBC NEWS (Oct. 1, 2012), http://www.bbc.co.uk/news/world-us-canada-19794745. As this article was being finalized, there were cyber attacks on the U.S. Department of Justice, the Federal Reserve, and the e-mail of the Presidents Bush. *See Anonymous Launches Major Cyberattack Against US Justice Dept!!*, THE LORINOV REPORT (Jan. 26, 2013), http://lorinovsreport.wordpress.com/2013/01/26/anonymous-launches-major-cyberattack-against-us-justice-dept/; *Federal Reserve Hit by Cyber* Attack, MARKET WATCH (Feb. 6, 2013), http://www.marketwatch.com/story/federal-reserve-hit-by-cyber-attack-2013-02-06; Molly Hennessy-Fiske, *Bush Family Emails Hacked; "Can Happen to Anyone," Experts Say*, LATIMES.COM (Feb. 8, 2013, 1:31 PM), http://www.latimes.com/news/nation/nationnow/la-na-nn-texas-bush-email-hacked-20130208,0,4693210.story.

organizations' investigations into the affairs of high-ranking Chinese government figures.[79]

D. The "Current State" Is Usually the Result of Policies or Procedures Adopted in Silos, Often in Fire-Drill Mode

[23] How did so many organizations arrive at this state of affairs? Based on the author's experience with several Fortune 100 companies during the last decade, the answer is quite simple. Rarely, if ever, are an organization's information-related policies and procedures the result of an integrated harmonized approach. Rather, the policies and procedures emerge through accretion with different departments or functions taking the lead at different times for different documenting efforts, sometimes in response to a perceived urgent need. The result is a hodgepodge of policies and procedures, which rarely present to the workforce a coherent whole.

[24] Thus, an organization may have separate documentation addressing each of the following information-related subjects:

- Code of Conduct or Ethics
- Information Security
- Confidentiality (Proprietary Information)
- Disaster Recovery

[79] Nicole Perlroth, *Washington Post Joins List of News Media Hacked by Chinese*, N.Y. TIMES (Feb. 1, 2013), http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0; Nicole Perlroth; *Hackers in China Attacked the Times for Last 4 Months,* N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all*; see also* David E. Sanger, *China's Military Is Accused by U.S. in Cyberattacks*,NY TIMES (May 7, 2013), http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all.

- Privacy
- Media Handling
- Social Media
- Bring Your Own Device (to work)
- Outsourced Systems (including Cloud)
- USB and other peripheral devices (whether they can be connected to company systems)
- Access Control (who has access to different systems)
- Records Retention (or Records & Information Management)
- Legal Hold
- Electronic Signatures
- Electronic Communications
- Acceptable Use (of company equipment, and/or social media)
- Home Computers (whether they can be used for company business)
- User Backup
- PC Maintenance
- Virus Protection

[25] As one can discern from a simple review of this list, some subjects are highly technical, some relate to legal obligations, and many relate to business strategies. However, as the discussion of the illustrative codes of conduct above demonstrates, management often proclaims that employees shall comply with all.[80]

[26] Therefore, the obvious question that should be asked is: Is it realistic to believe that employees can comprehend and comply with such diverse requirements? The Chase Code purports to give guidance where local law, the local custom, the corporate Code, or the business unit

[80] *See supra* Part III.B.

policies may differ.[81] But how should employees retain electronic employment-related information if there are twenty different federally mandated retention periods?[82] Or, if an American employee is based in Europe, but the retention obligations there differ, which rule governs? Or, how is a privacy officer in Germany to respond to a U.S. lawyer's request for personally identifiable information concerning a Singaporean citizen working in Berlin if the laws of those three countries (U.S., Singapore, and Germany) are inconsistent? While these are just illustrative conflicts, they lead, however, ineluctably to alternative questions. Is it more likely that employees will substantially ignore the hodgepodge of written policies and instead behave as they personally believe may be exigent to the business circumstances? If the answer to this last question is, as the author submits, more likely in the affirmative, does that present a significant additional risk—namely that courts or agencies asked to respect a policy will conclude that there is, in fact, no effective one present? For example, in the context of litigation, a court may find that when litigation is reasonably anticipated, an organization has a duty not only to issue a legal hold notice promptly to persons likely to have relevant information, but also to provide adequate guidance and assistance, or even monitoring, to ensure that individual recipients of the notices can comply.[83]

[81] JPMorgan Chase Code, *supra* note 64, at 5.

[82] *See* Ragan, *supra* note 44 (noting that one analysis of federal employment retention obligations listed more than twenty sets of regulations mandating document retention).

[83] *See, e.g.*, Apple Inc. v. Samsung Elecs. Co., 881 F. Supp. 2d 1132, 1147, 1150 (N.D. Cal. 2012) (finding that, in the absence of such individual guidance, relevant material was likely lost and an adverse inference was warranted).

IV. AN INFORMATION GOVERNANCE PROGRAM IS THE LOGICAL AND APPROPRIATE MEANS TO DEAL WITH THESE DIVERSE INFORMATION-RELATED RISKS AND INTERESTS

[27] As stated at the outset, information is one of an organization's most valuable assets and can be the source of enormous competitive power. But if the risks associated with information are not managed in accordance with the organization's main objectives and strategies (which may evolve over time), information can also be the source of enormous and unnecessary costs, liability, and damage to reputation.

[28] Many organizations have an individual with the title of Chief Information Officer (CIO). But as the descriptions above manifest, information-related issues in today's organizations touch numerous different disciplines, and no matter how talented, the CIO cannot be solely responsible for governing all information issues. Moreover, recent litigation experience with trying to find *a* "person most knowledgeable" about today's complex information technology systems and applications has demonstrated that no *one* person can competently speak authoritatively about an organization's information technologies and their functionality.[84] Something different is needed and that something is an "information governance" program.

[29] While much has been written recently under the "information governance" headline, one should note that definitions of the term differ in

[84] *See* Hopson v. Mayor & City Council of Balt., 232 F.R.D. 228, 245 (D. Md. 2005) (designating persons (plural) as being knowledgeable in the information technology systems); *In re* Vivendi Universal, S.A. Sec. Litig., No. 02 CIV.5571 RJH, 2004 WL 3019766, at *1 (S.D.N.Y. Dec. 30, 2004) (order granting deposition) (designating two individuals to provide information on information technology systems). *See generally* David A. Reif et al., *Reviewing and Producing ESI*, *in* MASSACHUSETTS CONTINUING LEGAL EDUCATION, A PRACTICAL GUIDE TO DISCOVERY & DEPOSITIONS IN CONNECTICUT § 13.4 (2011).

some respects and proponents may also differ as to the main driving forces in favor of adopting an information governance program. The subsections that follow address the various definitions and points of commonality in addition to the business cases that can be made for such a program, including potential hidden "wins."

A. Proposed Definitions for "Information Governance"

[30] Gartner, the information technology research and advisory company, defines "information governance" as:

> the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.[85]

[31] Gartner goes on to explain that the definition is derived from the firm's definition of IT (information technology) governance, involving processes that ensure effective and efficient use of IT in enabling an organization to achieve its goals.[86] IBM (which has products addressing many information-related issues) defines "information governance" as "a holistic approach to managing and leveraging information for business benefits and encompasses information quality, information protection and

[85] *See Information Governance*, GARTNER, http://www.gartner.com/it-glossary/information-governance/ (last visited Feb. 21, 2013).

[86] Debra Logan, *What is Information Governance? And Why is it So Hard?*, GARTNER, (Jan. 11, 2010), http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard.

information life cycle management." [87] Other vendors (RSD and Autonomy among them) have also proposed formulations.[88]

[32] Barclay Blair, a leading contributor to the literature, has said that information governance is a "new approach" that "builds upon and adapts disciplines like records management and retention, archiving business analytics, and IT governance to create an integrated model for harnessing

[87] *See* JUDITH R. DAVIS, INFORMATION GOVERNANCE AS A HOLISTIC APPROACH TO MANAGING AND LEVERAGING INFORMATION 1 (2010), *available at* ftp://public.dhe.ibm.com/software/os/systemz/IBM_Information_Governance_Survey_Report.pdf (reporting on the results of an online survey). SearchCompliance.com, which describes itself as "a free online resource for IT professionals seeking cost-saving strategies and information on how to create a manageable compliance infrastructure," *About Us*, SEARCHCOMPLIANCE, http://searchcompliance.techtarget.com/about (last visited Apr. 21, 2013), similarly defines the term as "a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset." *Information Governance*, SEARCHCOMPLIANCE (Mar. 2011), http://searchcompliance.techtarget.com/definition/information-governance; *see also Information Governance Benchmark Report in Global 1000 Companies*, CGOC 1, 8 (2010), https://www.cgoc.com/register/benchmark-survey-information-governance-fortune-1000-companies (defining information governance as "the discipline of managing information according to its legal obligations and its business value, which enables defensible disposal of data and lowers the cost of legal compliance"). The report was prepared under the joint auspices of the EDRM project and the Compliance, Governance and Oversight Council (hereinafter "CGOC") founded by Deidre Paknad, who is also the President and CEO of PSS Systems now an IBM company. *CGOC Speakers: Deidre Paknad*, CGOC, https://www.cgoc.com/events/speakers/deidrepaknad (last visited Mar. 5, 2013).

[88] *See* AUTONOMY CORP., AUTONOMY INFORMATION GOVERNANCE 2-3 (2009), *available at* http://www.aiim.org/pdfdocuments/37234.pdf; Tamir Sigal, *Information Governance versus Records Management- What's the Difference?*, RSD (Mar. 26, 2010, 7:52), http://www.rsd.com/en/blog/201003/infomration-governance-versus-records-management-what-difference.

and controlling enterprise information. . . . [I]t is an evolutionary model that requires organizations to make real changes."[89]

[33] While the available definitions and described scope of an information governance program may vary,[90] most of the commentators seem to agree that a well-functioning program will require the proverbial "village" of constituents who can help identify, assess, and prioritize values, costs, and risks associated with different categories of information.[91] That village should include at least personnel from the following functions:

- **Business leaders**, who understand the business value of information;

- **Legal personnel**, who can identify obligations (including those for records retention purposes) and some risks associated with information (including those that may arise with discovery in litigation or investigations, or importantly, risks that may arise as the result of adopting new technologies);

[89] Barclay T. Blair, *Why Information Governance*, *in* INFORMATION GOVERNANCE EXECUTIVE BRIEFING BOOK 7 (2011), *available at* http://mimage.opentext.com/alt_content/binary/pdf/Information-Governance-Executive-Brief-Book-OpenText.pdf.

[90] As the previous paragraph confirms, many of the early definitions of the term were technology-centric, in part growing out of the "data governance" teachings and discipline. *See, e.g.*, SUNIL SOARES, THE IBM DATA GOVERNANCE PROCESS 3 (2010), *available at* http://public.dhe.ibm.com/common/ssi/ecm/en/imm14074usen/IMM14074USEN.PDF. Much of the current discussion is being driven by vendors who purport to have solutions to address *some* of the issues around information management.

[91] *See, e.g.*, *Using the IGRM Model*, EDRM.NET, http://www.edrm.net/resources/guides/igrm/using-model (last visited Feb. 23, 2013).

- **Records & information managers** (to the extent the function exists), who can identify retention periods and how information may be stored;

- **IT** (including its storage experts and system architects), who can explain system volumes, costs, auto-delete functionality, how systems tie together, alternative storage strategies, and the organization's current capabilities to search for objects across platforms;

- **Privacy** (which may be part of legal, or separate), who can explain what information is subject to data protection obligations in different jurisdictions;

- **Security**, who can explain access protocols, perceived threats (such as to trade secrets), and current approaches and challenges;

- **Internal audit**, who can explain practices for assessing fraud controls and internal risks associated with information;

- **Risk**, who can provide existing methods for assessing, measuring, and evaluating defined risks; and

- **Compliance**, who have experience with the organization's general compliance efforts and history and usually at least a dotted line to the audit committee (in the case of a corporation).[92]

[92] The EDRM group based in Minnesota recently published an Information Governance Reference Model v3.0 that suggests inclusion of some (*i.e.*, legal, IT, business, records, privacy and security), but not all, of the groups identified in the text above. *See id.* The early materials from this group seek to emphasize that the project does not aim solely to build out the Information Management node on the far left of the earlier Electronic

[34] Like other villages, not all citizens of the information governance village need to be present at all times or for all meetings. But, also like other villages, what is essential in order for the information governance village to function well is one or more distinguished "elders" who can set a tone and ensure that the villagers understand that the elders are committed to the goals and will expect compliance with the path charted.

[35] Stated otherwise, senior management (and even the board) must make clear to employees not only that the organization means what it says in its Code of Conduct or other similar document, but also that the organization through its information governance program will provide employees with the tools—and the time—necessary to ensure that compliance with stated objectives is possible and achievable. This last statement does not mean that an information governance program requires immediate investment in new and expensive technologies with attendant training and education of the workforce. Indeed, one might question whether an information governance program will succeed if it begins with a project to acquire an expensive new tool to address some of the symptoms (*e.g.*, management of electronic records) rather than the information-related needs and interests of the organization as a whole, such as what information should be retained and managed in line with the organization's strategies and objectives. What must be recognized is that achieving a successful information governance program is a process that requires time and such a program will evolve and mature over time. During this process, priorities may change, as will available technologies, and the organization's approaches to various information-related issues will mature. Along the timeline tracking those changes, the organization should reevaluate its needs, its appetite for information-related risks, and

Discovery Reference Model (EDRM). The IGRM is a welcome addition to the literature on information-related issues. To date the model notably includes neither the link between basic law of corporate responsibility and the duty to manage information-related risks, nor guidance on how an organization should conduct the overall risk assessment. *Cf. id.*

its ability to bring on attractive technological tools, all of which should align with the strategic direction charted by the board and senior management.

B. Business Cases that Can Be Made for an Information Governance Program

[36] The advantages of maintaining an information governance program are many and vary depending upon the information-related issues (and risks) the particular organization faces[93] in addition to the extent to which an organization has already addressed records and information management, including the need to suspend normal retention and disposition schedules in the event of litigation or investigation.[94] Stated differently, organizations that have not updated retention policies to account for the proliferation of electronic information or that have not established a litigation response plan that includes hold notice procedures and a comprehensive data atlas may find an information governance program the path to quick "wins" on these fronts. Or, where a legal department has worried about the risk large stores of legacy data pose, an information governance program that establishes the total cost of owning legacy data may propel the organization to needed action. Indeed, it is not surprising that much of the recent talk about a need for information governance stems from costly experiences with electronic discovery challenges and risks.[95]

[93] *See supra* Part III.A.

[94] *See generally* THE SEDONA CONFERENCE®, THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 44-51 (2d ed. 2007).

[95] *See* Barry Murphy, *The State of Information Governance*, FORBES (Apr. 19, 2012, 2:11 PM), http://www.forbes.com/sites/barrymurphy/2012/04/19/the-state-of-information-governance/.

[37] Fear certainly can be a motivator, but it usually is not the best rationale to persuade a business executive to spend scarce resources. Executives have a tendency to think that the "sky may be falling, but it is not falling on our house." Moreover, businesses typically are not organized for the purpose of conducting litigation[96] and, therefore, may not readily accept soft-dollar, litigation-related "benefits" as key motivators for action.

[38] Business organizations are created to conduct business and executives understand that executing strategies well depends in part on identifying valuable information and leveraging it through technologies in order to compete efficiently.[97] Accordingly, the rationales more likely to persuade senior management to push forward with an information governance program are those that hold the promise for the organization to conduct its business more efficiently, less expensively, with less risk, and with less grumbling from employees and customers. In this author's view, the potential benefits from an information governance program address all these objectives and will usually be a mix of the following consequences, which virtually all organizations should embrace: business performance improvements, cost reduction, risk mitigation, including enhanced compliance with legal obligations, and improved employee morale and customer satisfaction.

[39] In the subsections that follow, the author outlines how and where an organization may look for these benefits. Preliminarily, however, two

[96] A recent exception is the establishment of companies that do not make products themselves and whose main purpose is to aggregate patents and sue to collect royalties or license fees for them. *See generally* Allen W. Wang, Note, *Rise of the Patent Intermediaries*, 25 BERKLEY TECH. L.J. 159 (2010).

[97] *See How Do You Leverage Information and Technology for Competitive Advantage?*, INSPIRION CONSULTING, http://inspirionconsulting.com/overview/how-do-you-leverage-information-and-technology-for-competitive-advantage/ (last visited Apr. 22, 2013).

points are worth highlighting. First, the conclusion of a Deloitte survey of corporate boards was that "[o]rganizations whose boards are actively involved with IT matters perform better financially."[98] Second, while it may be difficult at the outset and before an assessment of risks is completed to identify hard dollar savings and a concrete ROI, measurable ROIs for particular action steps or projects should be determinable once the program gets underway and the initial risk analysis is completed. Let us consider how this might work in practice.

1. Business Performance Improvements

[40] The goal of an information governance program is to optimize the value of information within the organization. The obvious first step in any such program, therefore, is to understand what "information exists, where it exists, and how to access and leverage it."[99] In large organizations, some knowledge of what information exists and where it is located will be available from a central IT function, but some will also be known only at the local or departmental level. Thus, for example, the central IT function may have an asset inventory for centrally administered systems and applications that can be leveraged. In addition, representatives of key business functions should be queried as to the systems and applications

[98] Deloitte T. Tohmatsu, *Introduction* to THE TECH-INTELLIGENT BOARD: PRIORITIES FOR TECH-SAVVY DIRECTORS AS THEY OVERSEE IT RISK AND STRATEGY 1 (2011), *available at* http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Board%20Governance/Information%20Quality%20and%20Technology/Tech-Intelligent%20Board_Deloitte%20Global%20Center_021111.pdf (reporting on 2007 survey conducted by Deloitte Touche Tohmatsu in conjunction with Corporate Board Members).

[99] The Sedona Conference®, *The Sedona Conference Commentary on Finding the Hidden ROI in Information Assets*, 13 SEDONA CONF. J. 267, 273 (Feb. 2011) [hereinafter *Finding Hidden ROI*], *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Finding%20the%20Hidden%20ROI%20in%20Information%20Assets.

upon which they principally rely to perform their function. The result of merging the central IT knowledge with the local business function expertise is an understanding of the systems and applications used to drive the business.

a. "Option Value"

[41] Several quick benefits can be recognized from such an analysis. First, as the *Finding Hidden RIO* paper sets forth, such canvassing of valuable information within an organization may help identify a source of information created in one function that can be repurposed without additional cost and reused by another function to help it meet its business objectives and enhance revenue for the organization as a whole (so-called "option value").[100] Conversely, such an analysis may determine that existing technologies (as opposed to the content harnessed by technologies) can be used for alternative purposes to improve efficiencies, again without additional cost. Indeed, a recent Gartner survey of CIOs found that "technology is only used to 43 percent of its potential" and suggests such "optional technology use" could be a significant boost to business performance.[101]

[100] *Id*. at 274-76 (providing several concrete examples).

[101] Evan Koblentz, *Gartner Finds Corporate IT in "Crisis Mode"*, LAW TECH. NEWS (Feb. 5, 2013), http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202587086400 (reporting that only nine percent of 2,054 CIOs who responded to the survey included as part of their top two concerns the general field of information governance, risk management, and compliance). Given what directors and general counsel said in response to FTI's survey, this suggests a significant and troubling disconnect. *See* CORPORATE BOARD MEMBER, *supra* note 74. Or, as Gartner vice president Mark McDonald was quoted in the article as saying, "There's a 'quiet crisis' being that CIOs as a whole, the entire industry, and their practice of it, is in need of reform." Koblentz, *supra*.

b. Litigation Response, Records, and Information Management

[42] Second, through the information assessment process, the organization may establish a comprehensive data atlas that can be used for purposes of responding to most litigation or investigation requests.[102] Third, this very kind of business process mapping is a linchpin in many modern information management programs and can jump-start the updating of an organization's retention program to address electronic information.

[43] Fourth, assessing what information has value to different business functions will also provide insight as to the quality of the record-keeping practices at the organization. With such insights, the organization can determine whether the integrity of information is maintained and whether users are able to reliably identify and retrieve valuable information efficiently. If they are not, the organization may choose to enhance its record-keeping systems so that employees do not waste time retrieving or re-creating information, thereby delaying execution and potentially undermining customer satisfaction.

2. Managing "Non-Value" or "Low Value" Information Can Lead to Substantial Cost Reductions

[44] One commentator has cautioned that the *Finding Hidden ROI* paper is an important contribution to the literature, "but it omits many of the details that can make or break the proposed option value information governance initiative, including details about issues of confidentiality and security, considerations for managing 'non-value' information, and the significant differences in managing and mining structured versus

[102] Note that the suggestion is not to "map" every system and application in use, but those upon which the function principally relies.

unstructured information." [103] In many organizations, however, confidentiality and security issues will not be unknowns, but likely will have been part of the risk assessment necessary to prepare Risk Factor sections of the organization's public filings (*e.g.*, 10Ks). If so, the information governance program can leverage that analysis too.

[45] Considerations for managing "non-value" information, as Juhnke suggests, definitely should be a key part of the information governance program. [104] Indeed, when the organization as a whole analyzes and understands how much information it stores and manages that has no current business value in addition to the total costs of owning that information (currently and prospectively), the organization will likely identify huge potential savings. How is it, you may ask, that such savings are not more apparent? The answers are obvious and nearly universal (in the absence of an information governance program). In the typical organization, an IT department is not motivated to look for such savings on its own; rather, IT has traditionally lived in fear of being criticized for not maintaining certain information. In some instances, the organization may have encouraged executives to rely on IT to be able to find information inadvertently deleted during an "oops moment." In others, IT may have been a scapegoat for the loss of information when a litigation hold was not properly communicated and enforced.

[46] Moreover, IT is tasked with storing and maintaining the information technologies and, in virtually all cases, will not understand the content of the information stored, much less its value to the organization as a whole. On the other hand, the business functions know the value of

[103] Deborah H. Juhnke, *In Review: Effective Information Governance is Power*, INFO. MGMT. MAG. 44 (May-June 2012), *available at* http://content.arma.org/IMM/Libraries/May-June_2012/IMM_0512_In_Review_Hidden_ROI.sflb.ashx.

[104] *Id.*

the information, but rarely understand the total costs of owning the information. The associated risk managers (*e.g.*, in legal, records, and privacy) may not know the business value of the information or alternative storage techniques that may be available, but can assess the risks associated with different categories of information.

[47] In the typical organization, cross-discipline discussions to assess these various angles have not occurred. Consequently, huge volumes of information for which the business generator has no current use and has simply forgotten remain under management. For example, a telecom company established that $100 million could be saved through an application retirement program and a U.S. bank expected a $400 million spend reduction over thirty-six months from an IT transformation plan.[105]

[48] An information governance program can accelerate the process of identifying such opportunities and provide the incentive to proceed in steps. For example, the program may identify some valueless information that is subject to legal hold and decide to move that data to cheaper storage. Similarly, the program may identify some stores of information that have continuing value, but which can also be moved to cheaper storage with less immediate retrieval times. Finally, such programs may provide an incentive for the organization to review legal holds placed long ago, lift those that are no longer truly required, and thereafter dispose of the valueless data.

[105] PowerPoint presentation from webinar given Nov. 1, 2012 by George Socha & Deidre Paknad on *IGRM v3.0 Security & Privacy Addition*, slide 15 (on file with the author). The presenters noted that the telecom project was on hold for want of clarity as to data retention and legal requirements. It is unclear whether the forecasted spend reduction was for storage and maintenance only, or also included what Frazier and Diana called the "EDD tax." Frazier & Diana, *supra* note 7. In fact, both costs would be eliminated or saved if the organization is able to dispose of such data.

3. Other Risk Mitigation Including Enhanced Compliance with Legal Obligations

[49] Section III above outlined several diverse information-related risks. Without repeating that discussion, it suffices to say that a functioning information governance program can assess these various risks and with senior management input, chart a course that aligns decisions with the organization's overall strategy and risk tolerance. Thus, as the program matures, the organization should find that:

- Valuable information is reliably and readily accessible;
- Confidential and proprietary information is protected in accordance with the organization's policies and legal duties;
- The organization avoids substantial risks of not retaining information in accordance with legal regulations and in connection with litigation or investigations;
- Personally identifiable information is retained only so long as necessary and in manners that guard against unlawful access;
- The costs of keeping information is optimized, *i.e.*, information is kept only so long as necessary for legal or business purposes, and at storage costs appropriate to its use and needs; and
- The organization meets its duties to avoid waste and to ensure that appropriate information and reporting systems are in place to provide management with timely and accurate information.

[50] Analysis of the systems that store and transmit personal information will also help the organization to identify the potential for breaches to its systems by hackers or others and to adopt appropriate mitigation strategies.

[51] As with the cost-reduction issues discussed above, prudence dictates that information-related risk issues be considered in a multidisciplinary forum such as an information governance program. For example, bringing social media and smart devices into the workplace represents only a recent and not the last new technology with business applications. There will be others and as those new technologies are proposed, the information governance framework will provide a forum in which to evaluate the relative opportunities that the new technology promises and the risks that may arise from deploying it. In many business situations, opportunity will trump risk, but at least with a proper forum in place for considering risks, the organization can take appropriate steps to mitigate.

[52] As another example of what many organizations have experienced recently, if IT alone considers the potential savings and economies of moving data to a cloud environment, a positive decision can be expected quickly. But if legal, privacy, records, and other specialists are brought into the evaluation, they can point out risks that should be addressed in negotiations with the cloud provider. For example, how will internal auditors conduct an investigation under the radar if they do not have direct access to data in the cloud? How quickly will data be available for discovery requests? Will the data be stored in one location and how will data privacy authorities in EU states view that storage? Will the cloud provider be able to dispose of the information when it is no longer needed? On each of these issues, a considered collective evaluation is more likely to reach a conclusion in line with strategy for the organization as a whole and its risk profile.

[53] Through a comprehensive cross-function or cross-disciplinary analysis of the organization's various information-related policies and procedures, the organization should also assess whether one can reasonably expect employees to understand and comply with the various information-related policies and procedures that the organization has in place to address such risks or whether that documentation should be updated, harmonized, rationalized, and put into more comprehensible formats. In line with the maxim that less is more, having a concise and cohesive set of policies would no doubt enhance the prospect that employees could follow the stated policies.[106] In an era where public companies face the potential for more scrutiny[107] and recognizing that having an effective compliance program can under the Federal Sentencing

[106] In his 2013 State of the State address, the Governor of California made a similar point:

> Montaigne, the great French writer of the 16th Century, in his Essay on Experience, wisely wrote: "There is little relation between our actions, which are in perpetual mutation, and fixed and immutable laws. The most desirable laws are those that are the rarest, simplest, and most general; and I even think that it would be better to have none at all than to have them in such numbers as we have."

Jerry Brown, State of the State Address, (Jan. 24, 2013), *available at* http://gov.ca.gov/home.php.

[107] *See supra* text accompanying notes 30-33. As a Gartner vice president said, "The recent global financial crisis has put information governance in the spotlight. Information governance is a priority of IT and business leaders as a result of various pressures, including regulatory compliance mandates and the urgent need to improve decision-making." Press Release, Gartner Says Master Data Management Is Critical to Achieving Effective Information Governance, (Jan. 19, 2012), *available at* http://www.gartner.com/newsroom/id/1898914. If an exclamation point for this finding were needed, it may be found in a recent survey in which a vast majority of respondents reported that seventy-five percent (or more) of IT spend did not add value to the business. DOUG MILES, AIIM, INFORMATION GOVERNANCE–RECORDS, RISKS AND RETENTION IN THE LITIGATION AGE 12 (2013), *available at* http://www.aiim.org/Research-and-Publications/Research/Industry-Watch/InfoGov-2013.

Guidelines reduce the risk that an organization will be held criminally liable for the acts of a rogue employee, it is foreseeable that more organizations may be interested in ensuring their policies are harmonized and clarified.[108]

4. Improved Employee Morale and Customer Satisfaction

[54] When an organization has a set of policies and procedures that align with its business goals and strategies, employees are more likely not only to understand and comply with the policies, but also, and just as important, to understand the mission of the organization and move forward as a unified team seeking clear and commonly held purposes. In such harmony, employee morale soars.[109] Finally, when an organization can reliably and quickly access and leverage information through technology, it will respond to customers more quickly and with better results, likely leading to increased customer satisfaction. Conversely, when customer data is breached or the customer gets inconsistent information slowly from the organization, sales suffer.

[108] Christian Lipfert, *Making the 'Business Case' for Information Governance*, LAW TECH. NEWS (Oct. 1, 2011). *See generally* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (2011); Paul Fiorelli & Ann Marie Tracey, *Why Comply? Organizational Guidelines Offer a Safer Harbor in the Storm*, 32 J. CORP. L. 467 (2007), *available at* http://blogs.law.uiowa.edu/jcl/wp-content/uploads/2012/01/Fiorelli-FINAL-smf.pdf.

[109] *See* Bruce W. Dearstyne, *Groundbreaking Trends: The Foundation for Meeting Information Challenges and Opportunities,* INFO. MGMT. MAG. 28 (Mar.-Apr. 2010), *available at* http://content.arma.org/IMM/Libraries/March-April_2010_PDFs/IMM_0310_groundbreaking_trends.sflb.ashx ("People like collaborating when they have a deep commitment to the company, product, service, or to the collaborating community itself.").

[55] In short, multiple business cases can be made in support of an information governance program. Which elements a particular organization emphasizes will depend on the particular industry in which the organization does business and the extent to which it has addressed information-related issues.[110] And, as stated earlier, senior management in virtually all organizations should understand that information governance is not only the right thing to do for the organization, but also something that cannot be ignored under *Caremark* and its progeny.[111]

V. MOST ORGANIZATIONS HAVE IN PLACE METHODOLOGIES THAT CAN BE LEVERAGED TO ACHIEVE ENHANCED STATES OF INFORMATION GOVERNANCE

[56] A central thesis of this article is that senior management of organizations and corporate boards have duties to ensure that information-related issues are considered and evaluated for risk. This idea is not a radically novel contribution, but as a rationale for organizations to adopt information governance programs, it has not been a central focus of the recent information governance discussions.[112] Given the current (post-financial crisis) emphasis on corporate compliance programs, it should be.

[110] *See generally* SUNIL SOARES, SELLING INFORMATION GOVERNANCE TO THE BUSINESS (2011) (listing sample business cases for ten different organizational types, nine different business functions).

[111] *See supra* text accompanying notes 22-29.

[112] In 2005, the Business Law section of the American Bar Association published a small book which included the statement: "Those Directors who defer or delegate to specialized personnel their understanding and command of data governance will be at increasing risk of incurring personal liability for failing to fulfill their fiduciary duty of care to ensure that their companies comply with rapidly emerging legal requirements concerning deficiencies in data governance." E. MICHAEL POWER & RONALD L. TROPE, SAILING IN DANGEROUS WATERS: A DIRECTOR'S GUIDE TO DATA GOVERNANCE 1-2 (2005). Many of the issues that Power and Trope identify as creating "dangerous waters" remain; but, to maintain the analogy, the exponentially increased volumes of information

[57] Equally as important, *initiating* an information governance program need not entail a herculean effort or fundamentally different and foreign concepts. Many organizations have established cross-disciplinary teams in recent years to cope with obligations to report risks, especially around financial reporting. In addition, many organizations have launched cross-disciplinary efforts to deal with the challenges of electronic discovery response. Financial reporting risk evaluations have enlisted joint efforts of risk managers and compliance officers, finance functions, and business personnel that understand the organization's business operations. E-discovery litigation response efforts have entailed joint efforts of at least the IT, legal, and records functions, and in cross-border matters, privacy. In an organization that has addressed some of these information-related issues, the first steps to establishing an information governance program may be as simple as: (1) aggregating personnel to round out the roster of knowledgeable constituents,[113] and (2) having senior management (and the board) communicate forcefully its full support and encouragement for the launch of the program.

[58] Further, in conducting the next significant and essential effort of such a program—a comprehensive assessment of information-related risks—the organization need not start from scratch, but can leverage existing techniques and methodologies employed is assessing financial reporting risks.[114] Thus, to deal with Sarbanes-Oxley and other recent

and the array of challenges and risks posed by new technologies combine to form a Sandy-like superstorm. *Id*. at 7.

[113] *See supra* Part IV.A..

[114] Senior management and directors may be able to avoid liability under the business judgment rule; however, in order to benefit under this rule, they may not utterly fail to consider the issues. Within the risk assessment and implementation phases of an information governance program, if the organization acts reasonably and in good faith, courts and other deciding bodies should be reluctant to second guess or find fault. The author is unaware of clear authority to support the latter proposition, but it would seem to

regulations, many organizations have adopted methods for identifying risks, evaluating them, and seeking to mitigate the more important ones.[115] In October 2012, the Committee of Sponsoring Organizations (COSO)[116] published a guide on *Risk Assessment in Practice*.[117] This guide provides

flow from the *Arthur Andersen* decision, as well and logic and common sense. *See generally* Arthur Andersen LLP v. United States, 544 U.S. 696 (2005).

[115] *See, e.g.*, Mark Anderson, *Sarbanes-Oxley Still Raises Ire, But it Has Fans, Too*, SACRAMENTO BUS. J. (Jan. 23, 2012), http://www.bizjournals.com/sacramento/print-edition/2012/01/20/sarbanes-oxley-raises-ire-but-has-fans.html?page=all; Charlsie Dewey, *Sarbanes-Oxley Act Impacts Privately Held Companies*, GRBJ.COM (Nov. 12, 2012), http://www.grbj.com/articles/74764-sarbanes-oxley-act-impacts-privately-held-companies.

[116] *See About Us*, COMMITTEE OF SPONSORING ORGANIZATIONS, http://www.coso.org/aboutus.htm (last visited Feb. 16, 2013) ("COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. The National Commission was sponsored jointly by five major professional associations headquartered in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]).").

[117] *See* Scott McCallum, *COSO Releases ERM Thought Paper Dealing with Latest Thinking on Risk Assessment Approaches and Techniques*, COMM. SPONSORING ORGS. (Oct. 26, 2012), *available at* http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO%20Release%20ERM%20Risk%20Assessment%20Paper%20Oct%202012.pdf. For those readers with records and information management backgrounds, it is worth noting that when this guide speaks of ERM, it means "enterprise-wide risk management," and not "electronic records management." *See generally id.* The 2012 guide builds upon COSO's *Enterprise Risk Assessment—Integrated Framework*, which was first published in September 2004, to help organizations deal with the (then-fairly new) reporting requirements of Sarbanes-Oxley.

a framework with advice on navigating through the risk assessment process—from developing assessment criteria, assessing risks with a common vocabulary that is established for the particular enterprise, including the interactions of various risks,[118] and prioritizing risks in accordance with the enterprise strategy. The guide recognizes that all organizations face risk and successful competition usually requires the organization to accept some risk.[119] With respect to risk evaluations, it suggests that the organization establish several scales for potential risks, specifically a five-point impact scale (ranging from "incidental" to "extreme"), a five-point likelihood scale (ranging from "rare" to "frequent"), a five-point vulnerability scale (ranging from "very low" to "very high"), and a five-point speed of onset scale (ranging from "very low" to "very high").[120] The guide also offers several ideas on how to obtain input from different functions or departments.[121]

See generally PricewaterhouseCoopers LLP, *Enterprise Risk Assessment—Integrated Framework*, COMM. SPONSORING ORG. TREADWAY COMMISSION (Sept. 2004), http://www.coso.org/documents/coso_erm_executivesummary.pdf.

[118] For example, in assessing information-related risks, the organization should consider the interaction of risks associated with failing to comply with discovery obligations and of having to comply with restrictive data privacy regimes.

[119] Patchin Curtis & Mark Carey, Deloitte & Touche LLP, *Risk Assessment in Practice*, COSO 1 (2012), http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf.

[120] *See id.* at 4-7.

[121] *See id.* at 9.

[59] COSO is not the only source of readily available assistance. The Open Compliance and Ethics Group (OCEG) is a nonprofit that provides standards and resources to aid the achievement of principled performance through integrated governance, risk, and compliance.[122] Under the GRC (governance, risk, and compliance) tag, OCEG has published a wealth of materials, such as charts and guides that can also help an organization navigate these information governance waters. For example, the GRC charts vividly demonstrate the costs to organizations that operate in silos with ineffective oversight—namely, disjointed strategy, poor integration, duplication, high costs, unnecessary complexity, lack of integrity, and wasted resources.[123]

[60] CGOC also has developed materials that will aid an organization's understanding of the interplay between and among several of the necessary constituents—specifically, legal, records, IT, and business—and how each of those groups can "give" and "get" something of value to and from the other groups.[124]

[61] In short, an organization can leverage the lines of communications, techniques, and lessons learned from recent compliance efforts to create the formula for successful information governance. Moreover, following

[122] *See About OCEG*, OCEG, http://www.oceg.org/view/About.

[123] Other materials published by GRC professionals and aimed principally at Compliance officers can also be extremely helpful. *See* Michael Rasmussen, *The Evolving Role of Chief Ethics and Compliance Officer: Managing Compliance and Ethics in the New Era*, CORP. INTEGRITY NEWSLETTER (2012) (describing an eight step approach to risk-based compliance).

[124] With the involvement of CGOC's leadership in the recent rollout of IGRM v.3.0, one can anticipate that CGOC will soon be expanding its materials to include privacy and security functions. *See* Doug Austin, *EDRM Announces Version 3 of the IGRM for Information Governance—eDiscovery Trends*, EDISCOVERY DAILY BLOG (Oct. 11, 2012), http://www.ediscoverydaily.com/2012/10/edrm-announces-version-3-of-the-igrm-for-information-governance-ediscovery-trends.html.

a risk-based approach to information governance aligns tightly with traditional notions of corporate management, performance optimization, and risk avoidance.

VI. CONCLUSION

[62] Virtually any organization can achieve significant benefits—in terms of better utilization of valuable information, hard dollar savings, softer-dollar risk mitigation, and unquantifiable improvements to employee morale and customer satisfaction—from an information governance program. Commitment from the top is essential to establish and maintain a successful program, but as explained above, ensuring that such a program is established to consider information-related risks is part of the fundamental obligations of senior management and corporate boards. Moreover, most public companies in the United States will already have in place frameworks and methodologies for proceeding with an information governance program. Doing so is not rocket science, but it makes good business sense and should be embraced.