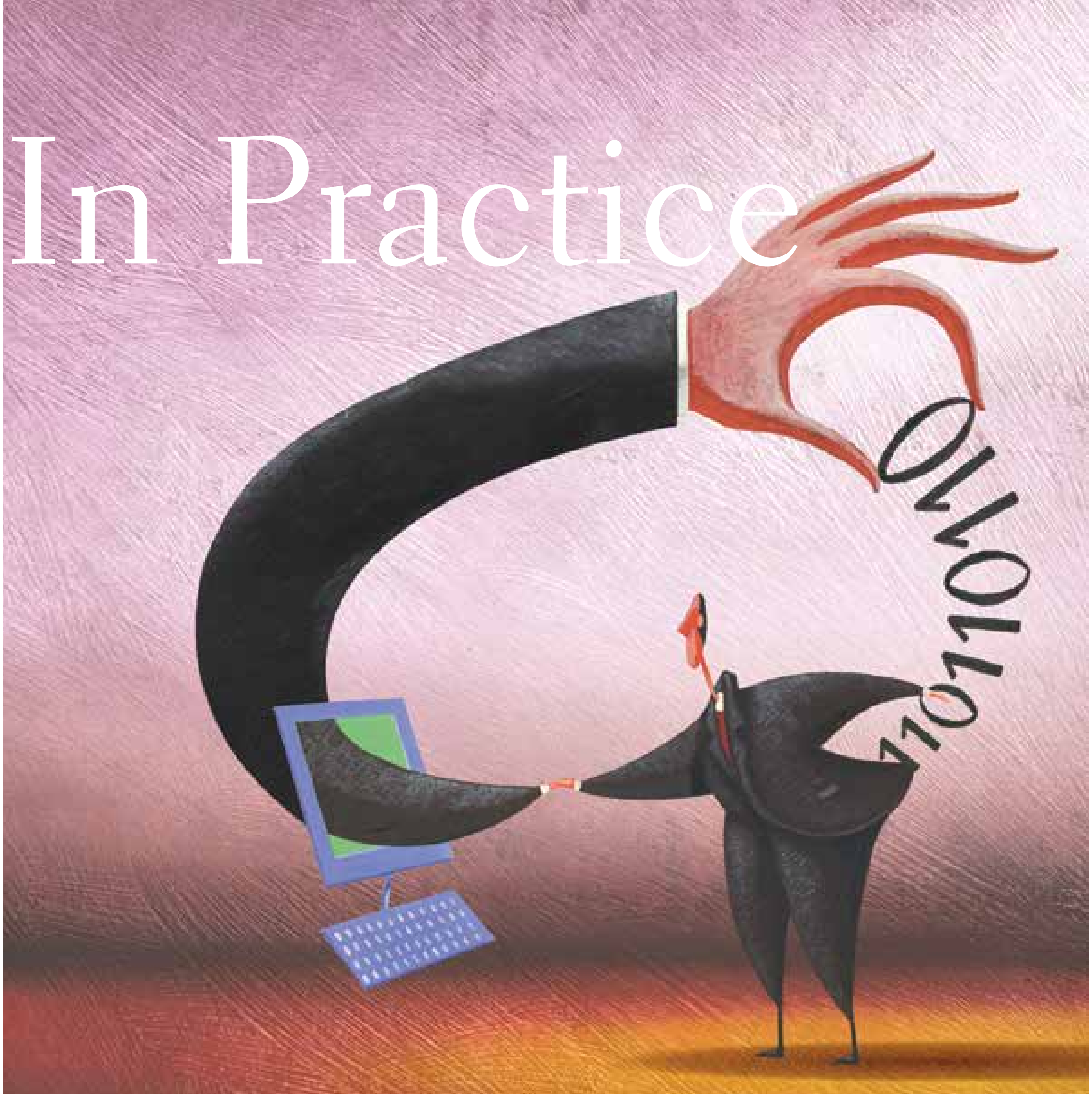
In Practice



Avoiding the Digital Dark Age and Remaining Competitive

How to protect proprietary information against disclosure or misuse.

By Charles R. Ragan

In today's business environment, information is a powerful and valuable asset. Organizations that use information wisely and strategically can reach customers faster and with more precision. But in today's highly regulated environment, information carries substantial risk, and, with the deluge of new media types, organizations that do not use information wisely may be thrown into a digital dark age.

Senior management and directors are responsible for navigating the strategic shoals the organization faces, including those of information assets and their myriad risks. Failure to do so may lead to losses and, in the extreme case of unconsidered failure to act, even liability. On the other hand, an organization can compete more effectively and with greater trust across disciplines when senior management and boards decide to confront these issues head-on and insist that the determination of acceptable risks and necessary costs are aligned with the organization's long-term strategy and mission.

This article identifies the main risks associated with modern information assets, asserts that the responsibility for charting a course through those risks lies with boards and senior management, discusses a vehicle to aid the navigation, and suggests a path organizations can follow to safety that leverages existing frameworks for dealing with risk.

Information Risks

For decades, businesses have been sold on the proposition that "storage is cheap," so there is no harm in keeping information forever. That is no longer true, if it ever was. In 2011, it was estimated that 90 percent of the data in the world had been created in the

BRUNO BUDROVIC/ILLUSTRATION SOURCE

prior two years, and for most organizations, information volume doubles every 18 to 24 months. With avalanches of information, the absolute cost to store and manage it is actually increasing in most organizations.

Absent investment in costly search technologies capable of federated searches across platforms and storage containers, these volumes jeopardize the ability of the organization to retrieve valuable information efficiently, and strategic opportunities may be lost. Only 15 percent of the information created in most organizations has value over time, but most organizations do not dispose of useless or outdated information, and an organization may incur substantial costs to process such information in litigation or investigations.

These risks, however, are only the tip of the armada of information-risk icebergs awaiting the sleeping captains of today's corporate ships.

The specific information-related risks an organization faces will vary depending on such factors as the industry, geographic reach, and the organization's information technology (IT) infrastructure.

Briefly stated, the risks associated with information in the modern enterprise include:

Contractually protected information. When considering new business arrangements or technologies, non-disclosure agreements typically require that information exchanged be protected from misuse.

Enhanced risk of security breaches. A 2012 survey of chief legal officers and directors found that 48 percent of directors and 55 percent of general counsel (of more than 13,000 surveyed) rated data security as their most prevalent concern. Another study estimated the median annualized cost of cyber crime per company at $5.9 million. But these direct costs related to a data breach (Sony reportedly spent more than $170 million to address multiple breaches in 2011) pale in comparison to the total injury including that to the company's reputation (estimated for Sony at more than $1 billion). Some of the cybersecurity risk can be attributed to criminal activity (e.g., identity theft), and some apparently is the result of international espionage (e.g., attacks on university networks seeking to obtain high-value research, or on corporations seeking to learn strategies for ongoing negotiations) or politically motivated retaliation. Indeed, if a recent Kaspersky Lab survey is accurate, most organizations have suffered *and acknowledged* at least one cyber attack in the past 12 months.

Data protection and privacy. The United States has followed a reactive, sectoral approach to privacy regulation at the federal level. In addition, almost all states have adopted legislation imposing notice and other obligations on organizations that experience a security breach and the loss of personal information. Numerous jurisdictions outside the United States have adopted comprehensive regulations for data protection and privacy regarding "personally identifiable information." In fact, to date, more than 80 nations have adopted privacy regimes—half of them in this century. Given the diversity and evolving nature of these laws and regulations, global organizations face a web of potentially conflicting and constantly changing privacy obligations that must be comprehended and addressed.

Challenges to sound record-keeping practices. Organizations should ensure that information of value to the business is maintained in order to ensure its accuracy, integrity, and availability for later use. Conversely, organizations should avoid keeping excessive volumes of unnecessary information, which only adds to cost and risk. Individual employees, however, should not spend more than one-third of their time at work managing e-mail, as surveys have found they do.

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. IT systems are complex and ever changing, making compliance challenging, absent thoughtful advance preparation.

Challenges in developing and implementing retention policy schedules. Separate from any litigation or investigation duty to preserve information, an organization must keep different categories of information for various periods, depending on the laws where it does business and the nature of those businesses. Ascertaining and assessing these diverse obligations—which often conflict—can be daunting.

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.) 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 will be freely exchanged during discovery.

Trend to allow workers to BYOD. In order to attract the best and the brightest young talent, many organizations are succumbing to pressures to allow employees to Bring Your Own Devices (BYOD) to work. The introduction of these devices into the workplace presents a host of security issues for an organization's central technology function.

Movement to cloud alternatives. Many organizations, in order to take advantage of economies of scale and the resulting economic savings, either have moved or are considering moving their data into "the cloud," where it may be commingled with the data of other organizations, and is not under the immediate possession or control of the organization. The economics of cloud operations can be incredibly attractive (if not compelling), but there are also a variety of risks, including mid- to long-term costs. For example, is the cloud provider capable of (a) preserving and providing data to the owner as quickly as the owner may need to respond to discovery requests, or (b) disposing of data in accordance with the owner's retention policy? These risks and costs should be considered and addressed so that the organization understands the total cost of owning information in the cloud.

Legacy or "debris" data that has no "owner" or continuing value. As noted, 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 rather allows it to linger, the organization will be spending money to store and manage information that has no business value—and that information may be subject to costly future discovery requests. This legacy or "debris" data poses a significant risk and problem for many organizations.

Big data. On the other hand, many large organizations are grappling with the issue of so-called big data (i.e., whether to keep lots of data and subject it to sophisticated algorithms and analytical techniques that can produce significant business opportunities and sales). Big data can produce substantial benefits and revenues, but that possibility does not mean that every organization should keep all information, without understanding all the other attendant risks and costs.

Finally—and this is by no means a small concern—organizations that have addressed these risks in the past typically have done so episodically and not as part of a comprehensive program. The result is a hodge-podge of policies and procedures, which rarely if ever present a coherent whole to the workforce. Many organizations have adopted a code of conduct in the wake of Sarbanes-Oxley that typically asserts that the organization complies with all applicable rules and regulations. But the reality is that the smorgasbord of policies and complex tapestry of regulations that global organizations face make such compliance doubtful.

All constituents with legitimate interests in information-related assets should have a voice in the governance process.

Recent surveys confirm the reality of improper information governance. One survey found that lack of proper management of information was affecting business productivity and creating costs and liabilities. Another found that 74 percent of respondents reported valuable information was being lost, 73 percent said their organizations missed business opportunities because they could not access information efficiently, and 88 percent said they had large stores of legacy data.

The Responsibility

The board is generally responsible for overseeing and directing the business of 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 duties to the owners of the corporation (its shareholders) that 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.

In *Caremark International Inc. Derivative Litigation*, the claim was 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." While acknowledging that the business judgment rule insulates directors in many cases, the court 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."

The issue thus squarely posed 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 information governance processes. As one commentator observed: "There 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 law but rather due to lax risk management."

It therefore follows that directors exercising their fiduciary duties of care should attempt in good faith to ensure that the organization's IT systems and procedures are reasonable and adequate to address the risks surrounding information-related assets.

Two areas deserve special attention. First, if intellectual property is not properly safeguarded, its value and the organization's competitive edge may be lost. Second, when protected personal information is accessed or lost in an attack, it often leads to expensive class action litigation or a governmental investigation that results in long-term governmental monitoring. More important, an October 2013 survey by Harris Interactive for Experian establishes that post-breach reputational damage is far from hypothetical.

The Securities and Exchange Commission (SEC) has issued guidance as to how corporations may use social networks consistent with their SEC obligations and what they should say in public filings about information security. So the issues are clearly ripe for board action.

The Vehicle

How then does an organization ensure that it gets value from its information without undue cost or risk? The answer is through a risk-based information governance program directed from the top and aligned with the organization's strategy, mission, and objectives.

Because the risks are diverse and vary from one organization to another, and because IT may be spread among different business units, the task of aligning risks, assets, and costs should not be left to the IT department. That group should know the systems and applications (the pipes), and the associated costs, but it will not know the value of the information (the content) or the risks of continuing to maintain it in its current state.

Accordingly, key business units should be involved in the project. The program team should also include those with the subject matter expertise (e.g., legal, privacy, records and information management, security, systems architects, internal audit, compliance) to conduct the necessary requirements and risks analyses. In short, all constituents with legitimate interests in information-related assets should have a voice in the governance process, but all need not be present at every meeting. Rather, for efficiency purposes, the program can proceed along a hub-and-spoke model, with a core group of people and oversight by senior management in the core disciplines. No single discipline should control the decision making: the choices should serve the organization's business strategies, mission, and objectives. Lawyers and other specialists can assess obligations and consequences, but senior business executives and board members determine the organization's tolerance for risk.

Senior management also needs to provide clear messaging that information governance is important to the organization, and supply appropriate resources including funding.

A Path Forward

In designing an information governance program and prioritizing specific enhancement projects, the organization may leverage other existing risk-based assessment methodologies, such as COSO's framework for assessing financial risks and the recently released security framework by the National Institute of Standards and Technology. Such tools enable participants to share a common vocabulary and methodology for assessing requirements, vulnerabilities, probabilities of a loss, and options to mitigate, avoid, or accept risk.

Because the risks associated with information assets are so diverse and potentially severe, management may not demand a complete business case or a hard return on investment to launch an information governance project (i.e., to assemble the necessary players and conduct the initial assessment).

The risks an organization faces will be many, some will have hard dollars associated with them, but few senior managers will want to assume the Risk of Infamy associated with a multi-million-user cybersecurity breach and its attendant reputational damage. Nor are they likely to accept the risk of being sued for an unconsidered failure to act.

On the other hand, once the initial assessment is completed, business cases for individual projects should be readily available—and aid in the prioritization process. Of course, senior management (and/or the board) can and should assist in ensuring that the projects selected align with the organization's risk tolerance and go-forward strategies.

The benefits of a comprehensive information governance program can be substantial. Rationalizing information storage and using smart analytics to remediate legacy data can yield savings in the tens or even hundreds of millions of dollars. A Deloitte survey found that companies with boards that are actively involved with IT matters perform better financially.

A good information governance program can also sew up some of the seams in an organization's systems that are targets for cyber attacks. If policies and procedures for handling information assets are simplified and harmonized, the organization may expect compliance and employee morale to increase, leading in turn to greater productivity and bottom-line results. And organizations that choose to move in this direction will be shining a light on their dark data challenges. D

Charles R. Ragan is an adjunct associate professor at the University of Minnesota School of Law and the UC Hastings College of Law and serves as special counsel at Zelle Hofmann Voelbel & Mason LLP. The author acknowledges and expresses his appreciation to Jason R. Baron for his review and comment on an earlier draft of this article.