SURVEY

Businesses Not Taking Advantage of Information

According to a new survey from PricewaterhouseCoopers (PwC) and Iron Mountain, all businesses want to maximize the value of their information, but most lack the skills, technology, and culture necessary to do so.

In fact, the survey, "Seizing the Information Advantage," reveals that two-thirds of businesses are unable to extract value from their information, and one-quarter derive no benefit at all. Only 4% of businesses can extract full value from the information they hold; more than one-third (36%) lack the tools and skills to do so. As a result, 43% obtain little tangible benefit from their information, and 23% derive no benefit whatsoever, according to the survey.

The survey also found a consistent lack of focus when it comes to organizational investment in the right analytical talent, tools, information-led solutions, and value-driven information strategies.

Surveys were completed by 1,800 senior business leaders in Canada, the United States, France, Germany, Spain, the Netherlands, and the UK. Each was assigned an "Information Value Index," a score from 1 to 100 measuring the business's information usage and governance framework. On average, the study reveals, businesses scored a 50.1, which the study authors called "disappointing, though perhaps not unexpected." According to the index, European businesses scored 47.3%; North America (NA) businesses fared a little better, at 52.9%.

The index confirms that the vast majority of businesses, regardless of geography or sector, have a long way to go before they can realize the value from their information.

For example:

- 23% overall (23% in Europe, 21% in NA) lack the data interpretation skills and 23% overall (25% Europe, 22% NA) lack the capabilities required to deliver a return on information.
- 16%-18% in Europe and 12% in NA don't believe the organization knows what information it holds.
- 28% (32% Europe, 23% NA) don't believe it knows how information flows through the business and where it is most valuable.
- 21% (21% Europe, 20% NA) don't believe it knows how information flows through the business and where it is most vulnerable.

Companies should use the disappointing results as an opportunity, according to Richard Petley, director of risk and assurance at PwC.

"The opportunities for competitive advantage through data are very real," he wrote. "The better organizations have made the value of data tangible and are exploiting it and protecting it in equal measure. What makes these organizations distinctive? The survey demonstrates that this comes from a platform of strong senior leadership, investment in data governance, and best use of analytics both in terms of technology and people."

LEGAL DECISION

Goldman Sachs Fined $50M Over Stolen Documents

Goldman Sachs has been hit with a $50 million fine, and an ex-banker will plead guilty to federal criminal charges that he took confidential documents from the Federal Reserve Bank of New York, according to media reports.

The civil penalties against the banking giant are among the harshest ever doled out by New York. The charges against ex-banker Rohit Bansal and the source of the documents, New York Fed banker Jason Gross, were filed by Manhattan U.S. Attorney Preet Bharara, the *New York Times* reported. The two could be sentenced to up to a year behind bars.

Bansal and his supervisor were fired when the leak was discovered in 2013, and the DFS has punished Goldman with a three-year ban that will bar the bank from participating in new regulatory consulting in the state.

"We have zero tolerance for improper handling of confidential information," Goldman spokesman Michael DuVally said. "We have reviewed our policies regarding hiring from governmental institutions and have implemented changes to make them appropriately robust."

GOVERNMENT RECORDS

Australia Public Service Bans Paper in Boxes

A new policy for the Australia Public Service (APS) directs all federal agencies to shift their work practices from paper to entirely digital. The "Digital Continuity 2020 Policy," released by the National Archives of Australia, signals a death knell for recordkeeping methods used for the past century.

The policy will force agencies to manage their information as an asset, ensuring it is created and managed for as long as required, considering business and other needs and risks, the *Sydney Morning Herald* said.

Agencies will transition to entirely digital work processes, meaning business processes, including authorizations and approvals, will be processed digitally, and that information will be created and managed in digital format.

According to the *Herald*, agencies will have "interoperable" systems of recordkeeping so their information can be found easily and shared with other agencies.

By June, agencies must have information governance committees established and by the end of 2016 must announce plans for how they will deal with their information. By the end of 2020, the APS expects the transition to the new era of recordkeeping to be complete.

National Archives Director-General David Fricker said information stored by the government needs to outlive technical obsolescence and that public servants can no longer "entomb pieces of paper in boxes."

According to the policy, developing end-to-end digital work processes will offer opportunities for agencies to establish more mature, efficient procedures and services that engage the public directly and effectively.

"Work processes that create and collect digital information and keep it in an accessible digital form can enable better productivity and responsiveness to client and government behaviour," the policy states. "Digital information kept in paper and other analogue forms can result in inefficiencies such as unnecessary duplication, increased storage costs, and unreliable or inaccessible information that cannot be easily found and cost-effectively shared or backed up for business continuity."

Agencies have been instructed to report back to the National Archives annually via a survey. Public servants will attend training sessions to help them make changes, the *Herald* reported.

LEGAL DECISION

New Zealand Supreme Court: Digital Files Constitute Property

The New Zealand Supreme Court has determined for the first time that digital files constitute property under the Crimes Act.

The case, involving a bouncer who released video from a Queenstown bar, has changed the law in New Zealand. Previously, information and software were not considered property. In light of the recent decision, some incidents of information theft, as well as copyright infringement, now might be considered criminal acts. Taking non-confidential information in digital form may also be considered a crime as a result of the decision.

During the Rugby World Cup 2011, the English rugby team spent a night out in Queenstown. According to media reports, at some point that night, player Mike Tindall, whose wife is Queen Elizabeth II's granddaughter, had an encounter with a woman. A bouncer at that bar, Jonathan Dixon, took a copy of the CCTV footage of Tindall from the bar and tried to sell it. When he was unable to do so, he uploaded it to YouTube.

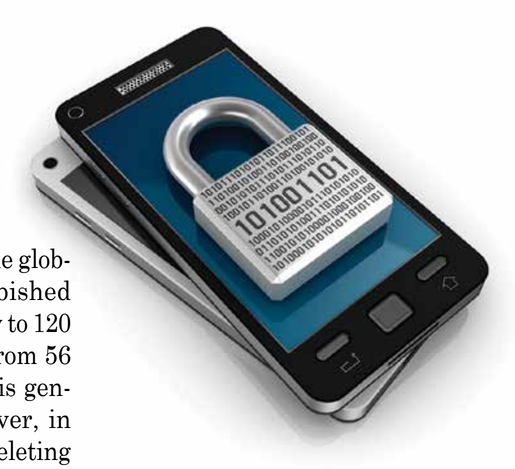
Dixon was convicted of accessing a computer system for a dishonest purpose under section 249 of the Crimes Act, which makes it a crime to "directly or indirectly, [access] any computer system and thereby, dishonestly or by deception, and without claim of right, [obtain] any property, privilege, service, pecuniary advantage, benefit, or valuable consideration."

Dixon was originally convicted on the basis that he obtained "property." He appealed, and the Court of Appeal determined that the digital file taken by Dixon could not be considered property. The conviction was changed to state Dixon had obtained a "benefit" under section 249. However, the Supreme Court reviewed the relevant laws from New Zealand, the United States, and the UK and found that the digital file was property, so the original conviction was reinstated.

The Supreme Court reasoned that it was a fundamental characteristic of property that it was something capable of being owned and transferred. The digital files taken by Dixon were capable of being sold and, therefore, they constituted "property." It noted the Crimes Act's definition of "document" included an electronic file and if a Microsoft Word document is property, then so are other forms of digital files.

INFO SECURITY

Used Smartphones Often Hold Past Users' Data



Gartner Inc. predicts the global market for refurbished smartphones will grow to 120 million units by 2017, up from 56 million in 2014. Recycling is generally a good thing; however, in this case, it may be risky. Deleting data on smartphones is not always easy and often is not done properly.

Recent research conducted by Blancco Technology Group and Kroll Ontrack studied the prevalence of data "ghosting" on resold devices and found that more than one-third of secondhand smartphones contain information created by past users.

According to that survey, "In an examination of 122 pieces of second-hand equipment, 48% of the hard disk drives and solid state drives contained residual data, while thousands of leftover emails, call logs, texts/SMS/IMs, photos, and videos were retrieved from 35% of the mobile devices."

In addition, the research found that 57% of used mobile devices and 75% of used hard drives purchased from Amazon, eBay, and Gazelle had previous unsuccessful deletion attempts.

These figures are worrisome given the growing secondhand marketplace for used devices and even more so within the context of increasing bring-your-own-device (BYOD)-policy prevalence, *Legaltech News* said. For example, without secure management of BYOD-enabled devices, data contained on resold employee devices may escape from company-secured networks.

"One of the more glaring discoveries from our study is that most people attempt in some way or another to delete their data from electronic equipment," Paul Henry, IT security consultant for Blancco, said in an announcement. "But while those deletion methods are common and seem reliable, they aren't always effective at removing data permanently and they don't comply with regulatory standards."

The survey also reveals that on 11% of the devices reviewed, only basic delete functions were performed before the device was resold. Researchers also found that often-used "quick-formatting" processes are unreliable, having been performed on 61% of the drives with data still present.

Needless to say, these survey results should capture the attention of records and information management professionals – on both a personal and corporate basis. Several concerns should be addressed in their organization's policies and procedures:

- **BYOD policies:** Does your BYOD policy address the segregation of personal and organizational information? Does the organization have the technology capability to manage this segregation and to enable deletion of organizational information while retaining the personal information?
- **Employee separation practices:** Is your human resources department collecting company-owned phones and other portable devices as part of the exit procedure? How does the BYOD policy address the segregation of personal from organization information?
- **Organization-owned devices:** Does the policy allow for recycling or selling used devices when replacing them? Does IT wipe data from the devices or does it rely on a third party? What process and checklists are used in the process?

E-DISCOVERY

E-Discovery Growing Worldwide

E-discovery is spreading even in countries that have no laws to require the practice, according to a recent report by Kroll Ontrack.

In France, formal e-discovery does not exist, but it is seen in such circumstances as "reviewing data seized by the European Commission and national competition authorities during dawn raids," the "The New Frontiers" study found.

In the Asia-Pacific region, e-discovery is often used in varied cases, too. "While the majority of cases stem from U.S. or EU litigation, a large portion of APAC e-discovery results from cases that involve regulatory requests, internal investigations (most often relating to the Foreign Corrupt Practices Act in the US or the UK Bribery Act), and company-driven internal compliance reviews," the report reveals.

Also, the survey found the "most challenging e-discovery environments" may be in South Korea or China, "which have undeveloped or very restrictive climates."

E-RECORDS

30% of IT Professionals Not Sure What Tape Archives Hold

New research from Kroll Ontrack reveals that despite the large volume of legacy data organizations often have stored on archive tapes, many IT departments don't have strong plans for managing it, leaving their organizations vulnerable to compliance and regulatory risks.

The study also found that 30% of more than 700 IT administrators surveyed from corporate and service provider IT shops around the world don't know what specific information is stored within their tape archives – even though 30% of them get daily or weekly requests for information stored there that is critical to e-discovery or internal audit.

The research suggests the combination of frequent backup data requests and poor data maps led to 22% of participants being unable to respond to restore requests from their organizations. They also admitted difficulty in consistently locating and accessing the data needed to facilitate critical business operations.

"Most organizations are required by law to keep and maintain access to regulated data for a designated period of time. Therefore, maintaining access to legacy data and having the ability to quickly respond to data requests is crucial," Todd Johnson, vice president of data and storage technologies at Kroll Ontrack, said.

This problem was also identified in a study from Iron Mountain and the International Data Corp. (IDC); 49% of those respondents said that lines of business lose significant productivity searching for archived information that is difficult to access.

INFO SECURITY

Employees, Vendors Threaten Corporate Data

A global survey of 347 corporate privacy professionals identifies employees and vendors as two huge sources of risk that corporations are failing to manage properly.

Conducted by Bloomberg Law and the International Association of Privacy Professionals (IAPP), the survey "Assessing and Mitigating Privacy Risk Starts at the Top" reveals key threats to a company's data security and highlights the importance of corporate buy-in to mitigating the risk of a data breach.

While 55% of respondents said they consider their corporation's performance relating to privacy and risk as excellent or almost excellent, they were less confident in how they specifically address some of the most critical privacy issues. Only 35% rated their company's employee monitoring program excellent, and only 30% gave the same rating to their vendor management program.

While insider risk frequently is attributed to disgruntled employees, the findings of the survey point to lack of education as a much bigger cause. If employees are not correctly educated in their responsibilities, it can be easy for them to mishandle private data.

David Perla, president of Bloomberg Law, said, "One thing that jumped out at me is the sense of insecurity that organizations have about their employees being properly trained. The risk is not so much one of intentional insider threat as it is that people are not aware of their own ability to impact and protect data, as a result of their lapse in training."

Brian Kudowitz, Bloomberg Law's commercial product director for privacy and data security, added, "If you have a base of employees from top to bottom who don't understand any of this, it's not going to be just about breach responses – you're going to create problems for HR, and other normal business operations like communications and vendor selection as well."

Survey participants identified the support of corporate leadership as the most important factor in reducing the risk of a data breach, with 89% considering it "important" or "very important." Kudowitz told *Legaltech News* that buy-in is the "glue that holds everything together."

PRIVACY

Study: No Expectation of Privacy in Massachusetts Schools

A recent study conducted by the American Civil Liberties Union (ACLU) of Massachusetts found that most school districts in the state give students "no expectation of privacy" online or on their devices.

The ACLU study of 35 Massachusetts K-12 school districts, "Back to the Drawing Board," reveals that many schools in the state use technology to monitor students, as well as to collect and share their data. Ten districts said they have the right to inspect devices without notice or consent, eight districts said students have "no expectation of privacy," and two reserve the right to periodic searches.

The report also shows that students' personal data is often shared with third parties. Eight districts reported using third-party applications that gather personal data to be shared with corporations or law enforcement agencies without consent. Only one district said it does not share data with third parties.

In response, the Massachusetts department of secondary and elementary education said, "We agree that student privacy is important, and we also know that schools want to ensure students are using technology appropriately. Most of the policies related to student use of technology are made at the school or district level. We have offered guidance in that area and will continue to look for best practices and ways to improve how schools approach these issues."

Others have come under fire for their mishandling of data related to minors. For example, a Philadelphia-area school district was hit with two lawsuits after capturing thousands of webcam photographs and screenshots of student laptops in an attempt to locate missing computers. The district later settled both lawsuits for $610,000.

Google also faced a lawsuit dealing with children's privacy, after the company acknowledged scanning the contents of millions of e-mail messages in its Apps for Education tool. Google said it no longer practices the e-mail scanning.

Still, many organizations have not improved privacy standards for children. A study released in September from the Global Privacy Enforcement Network found that 67% of the websites reviewed collected personal information from children. Only 31% of websites and apps actually featured controls to limit this collection, and only 24% encouraged parental involvement in browsing the website or app.

CYBERSECURITY

Report Predicts Cybersecurity Trends, Threats for 2016

Intel Security's McAfee Labs report "2016 Threats Predictions" predicts several new methods and trends for cybersecurity in 2016 and beyond, and it offers insight into what will impact organizations in the near future.

It mentions nine specific areas associated with cybersecurity likely to become more prominent in 2016:

1. Hardware-based attacks
2. Ransomware
3. Wearable attacks
4. Employee systems attacks
5. Cloud service attacks
6. Smart car attacks
7. Data warehouse attacks
8. Integrity attacks
9. The sharing of attack information with other victims

According to the research, in 2016, researchers, IT security vendors, and automakers will work together to develop standards, guidance, and solutions for "potential exploit scenarios for connected automobile systems lacking foundational security capabilities or failing to meet best practice security policies." Vulnerable systems include vehicle access system engine control units (ECUs), driver assistance system ECUs, remote key and passive keyless entry, smartphone access, and others.

In addition, wearables devices could provide access to a user's personal data. The report said that the devices contain only a small amount of information, but they could offer access to a broader network of devices and larger stores of potentially sensitive information.

INFO GOVERNANCE

IG for Making Good Big Data Decisions

According to a recent *Legaltech News* report, the challenge for organizations in our *app-ified* world – in which we are "addicted to the predictive, persuasive, instant gratification that that the Digital Trinity [mobility, social media and advanced analytics] delivers" – is not the volume of data being produced; it is consumers' growing expectations that organizations act upon their data.

To remain relevant, organizations must use data to provide better customer service, personalized offers, and highly targeted ads. At the same time, they must avoid doing anything that might be considered too invasive or manipulative. So how do they exploit the value of data without alienating the people with whom they're trying to connect more personally and deeply?

Legaltech News says organizations should consider how their use of customer data can affect their offerings, their reputation, and their brand. The report offers the following guidelines for that decision-making process:

1. **Establish appropriate-use guidelines.** Consider creating a cross-sectional committee of stakeholders, including marketing, legal, HR, and customers, to ensure that data use is consistent with the organization's values, societal norms, and customer expectations. Consumers often won't provide their data to entities they don't trust.
2. **Be transparent.** Policies for collecting and using data should be transparent, understandable, enforceable, and current. Real-time notification should be standard, and customers should be told how and when their data is being used.
3. **Establish meaningful information governance.** Establish an information governance (IG) structure that reflects the value of individual data. It should include guidelines for information use, asset tracking, security, risk management, and lifecycle management, and the program should have executive oversight, just like capital governance processes do.
4. **Acknowledge the trade-offs.** Organizations that use customer data to drive business should provide customers value in return for that use. Although most understand that free services come at a cost – usually personal data – wise companies ensure that customers benefit from their participation and that the organization's use of customer data is not far removed from the purpose for which it was collected.
5. **Provide recourse and control.** Give customers some degree of control over the collection and use of their data by making opting in or out easy and effective and by providing a way for them to correct their information.

Companies that thoughtfully manage their use of data, treating it as they would any other mission-critical asset, are more likely to achieve the goal of remaining relevant to their customers.

E-STORAGE

Useless Data Clogging Worldwide Storage

Veritas Technologies' "Databerg Report 2015" reveals that public and private sector companies in South Africa, Europe, the Middle East, and Africa have created a "databerg," a massive block of "dark, useless, and expensive data" that is clogging up storage facilities at businesses worldwide.

The report identified three major causes for databerg growth:

1. Data volumes disproportionately affecting IT strategy
2. Vendor hype driving the widespread adoption of currently free storage
3. Employees putting corporate data at risk through their own actions and becoming data hoarders

The report advises companies :

- Identify dark data, expose risk, and recognize valuable information
- Eliminate redundant, obsolete, and trivial data promptly to reduce wasted costs
- Define a workable information governance strategy for unstructured data
- Increase business agility by using cloud storage environments

MOBILE DEVICES

Half of U.S. Firms Lack Formal BYOD Policy

A survey of 447 U.S. businesses of all sizes conducted in mid-2015 by systems integrator Champion Solutions Group found that 53% haven't implemented a formal bring-your-own-device (BYOD) policy to protect their data, while more than one-fourth admitted to having no systematic security approach, according to *Computerworld*.

The findings reported in "Mobile Device Security Practices" are "ridiculous … surprising," said Champion CEO Chris Pyle in an interview with *Computerworld*. Experts and security firms have suggested mobile security best practices for more than a decade.

Companies understand the advantages of allowing workers to use their personal smartphones and tablets while at work, including increased productivity because workers use applications and services they personalize to become more efficient. But, Pyle said, there must be a framework for protecting them.

In addition to the lack of formal BYOD policies, the survey found that only 21% of businesses use multifactor authentication (MFA) to verify a user's identity when granting access to critical enterprise applications and data. MFA covers a wide category of techniques to require two or more methods of authentication to allow a person to log in from a device.

While many newer phones use fingerprint scanners to allow users to access them, companies are just beginning to consider using scanners to allow access to enterprise apps or data, Jason Milgram, director of software development for Champion, said. Some companies are relying on partitioning of personal from work data within the operating system of some newer phones, but even that approach may not be secure enough, he said, depending on the level of risk a company can tolerate.

The survey also noted that 23% of companies don't lock out mobile access after a repeated number of sign-in failures, and 30% don't even require basic alphanumeric passwords.

E-DISCOVERY

What Does FRCP Rule 37(e) Mean Now?

Changes in the U.S. Federal Rules of Civil Procedure (FRCP) went into effect December 1, and many experts predict they will accelerate the pace of litigation and provide cost savings.

In particular, Rule 37(e) addresses spoliation within e-discovery, and the changes were designed to address the disparity among different courts on the effects of failing to preserve, as well as the risks parties face with spoliation sanctions.

"What 37(e) tried to do is develop a uniform standard of imposing sanctions when a party fails to preserve this information," Mark Michels, director at Deloitte, told *Legaltech News*. "The intent of the rule is that only in the most severe situation, where someone actually acts willfully, should they face more severe sanctions."

Rule 37(e), "Failure to Preserve Electronically Stored Information," states that if data is lost "because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery," the court has two options:

1. Upon finding prejudice to another party from loss of the information, the court may order measures no greater than necessary to cure the prejudice.
2. Only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation, the court may:
   - Presume that the lost information was unfavorable to the party;
   - Instruct the jury that it may or must presume the information was unfavorable to the party; or
   - Dismiss the action or enter a default judgment.

Michels said that the rule changes are meant to provide uniformity, which should particularly help parties with large amounts of electronic data save on costs.

"The impact of the rules and decisions in New York would be different than, say, in Texas. The challenge that companies that have a lot of data are concerned about is that if they didn't preserve – or some might say over-preserve – there was this risk years later that they could face fairly severe sanctions or remedies," he said. "A number of corporations in particular came forward and demonstrated the significant cost of over-preservation of information."

As a result, according to *Legaltech News*, the Advisory Committee and Rules Committee tried to revise a spoliation standard closer to the more lenient Texas version than New York's.

The jury is still out on how the new rules will affect e-discovery and court decisions. But, in theory, the best way to avoid spoliation is by implementing more distinct processes and procedures to preserve in a repeatable way.

CYBERSECURITY

SEC Warns CCOs About Cybersecurity Lapses

Gartner Inc. predicts that the importance of the personal cloud will continue to grow and that those responsible for building the digital workplace will be increasingly challenged as the personal cloud continues to evolve and intersect with IT initiatives.

The Securities and Exchange Commission (SEC) has put chief compliance officers (CCOs) on notice to carefully review and implement, where appropriate, the agency's latest cybersecurity guidance. Two recent remarks by SEC officials may have been a warning that the SEC plans to focus more on cybersecurity offenses and likely grabbed the attention of CCOs everywhere.

First, SEC Chief of Staff Andrew J. Donohue indicated that the SEC will continue to bring enforcement actions against CCOs for not addressing compliance issues, including cybersecurity. He challenged them to be "proactive" in their work and pointed to three recent SEC enforcement actions against CCOs on the grounds that they failed to implement compliance programs reasonably tailored to the specific needs of their firms.

Two days after Donohue's speech, SEC Chair Mary Jo White announced: "While cybersecurity attacks cannot be entirely eliminated, it is incumbent upon private fund advisers to employ robust, state-of-the-art plans to prevent, detect, and respond to such intrusions."

Another message from the SEC came in the form of its recent enforcement action against investment advisor R.T. Jones Capital Equities Management for allegedly failing to establish cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of about 100,000 individuals. As a result of these alleged violations, R.T. Jones agreed to pay a $75,000 penalty and undertake remedial efforts, including:

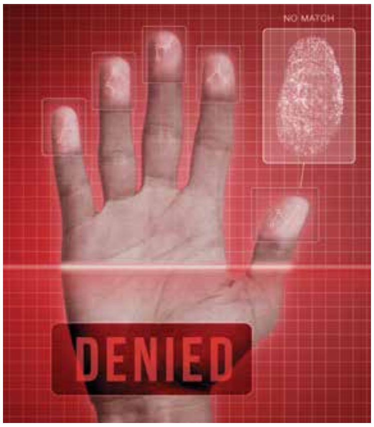
- Retaining multiple cybersecurity firms to assess the scope of the breach
- Removing all PII from its web server and encrypting all PII on its internal network
- Installing a new firewall and logging system
- Appointing an information security manager and implementing a written information security policy
- Notifying the affected individuals (advisory clients and third parties) of the breach and providing them with free identity monitoring

According to *Legaltech News,* this was the first officially titled SEC cybersecurity enforcement action – and it appears to be the SEC's long-awaited "message case" on this issue. Indeed, in the release announcing the settlement with R.T. Jones, co-chief of the SEC Enforcement Division's Asset Management Unit Marshall S. Sprung stated: "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

Experts say CCOs should have already incorporated into their firms' compliance programs the SEC's cybersecurity guidance released in 2015, which recommends the following measures:

- Periodically assess the firms' (a) information and processes, (b) internal and external cybersecurity threats and vulnerabilities, (c) security controls and processes, (e) impact of cyber-related events, and (v) governance structures.
- Devise cybersecurity strategy to (a) control access to systems and data, (b) encrypt data, (c) restrict use of removable media, (d) deploy monitoring software, (e) employ data backup and retrieval, and (f) develop an incident response plan.
- Implement written policy and procedures and training to provide appropriate guidance.
- Assess cybersecurity measures of vendors and business partners.

Though directed at investment companies and investment advisers, this guidance is applicable to all financial firms.



GOVERNMENT RECORDS

Vancouver's FOI Practices Scrutinized

British Columbia's Office of the Information and Privacy Commissioner (OIPC) announced it is investigating the city of Vancouver for its freedom of information (FOI) practices.

Information and Privacy Commissioner Elizabeth Denham recently released a damning report on the province's illegal practice of permanently deleting e-mails, revealing that the government had encouraged, "willfully or negligently," a culture of permanently deleting or not even creating necessary records. The report detailed how political staff members are exploiting the ability to permanently "triple-delete" e-mail records before they are backed up to government servers, effectively erasing the only copy of what could be an important government record.

Denham also accused the government and senior staff of sidestepping the FOI law by not writing things down, deleting e-mails en masse, and narrowing the scope of people's FOI requests so they produce no records, according to *The Vancouver Sun.*

Director of Communications Cara McGregor told the *Sun* that OIPC staff will interview stakeholders and review internal files, including complaints, requests for review, and breaches. They also will analyze information collected from other entities and consider other investigations and policy projects recently completed, currently underway, or about to be initiated.

Last year, according to the *Sun*, Mayor Gregor Robertson promised greater transparency. His administration had been criticized by residents for being inaccessible and secretive. Media also criticized the city's practices of centralizing and vetting all responses through the city manager's office. Some also have reported problems when filing FOI requests, discovering that records they believe should exist either weren't created or no longer existed.

Acting City Manager Sadhu Johnston said the city already has a robust system for dealing with FOI requests and welcomes the audit.

PRIVACY

Handling Foreign Data in a Post-Safe Harbor World

When the European Court of Justice (ECJ) invalidated the Safe Harbor agreement, it didn't mention a grace period to allow governments or companies to transfer from a world with data handling guidelines to one without.

In a recent webcast, "No Safe Harbor: Five Strategies for Cross-Border eDiscovery," four e-discovery experts from Recommind suggested how firms can protect themselves from violating EU privacy laws in the new environment:

1. **Limit collection.** Ways to do this include leveraging mobile early case assessment and collections technology, indexing files on-location in the country for a text-based search of the data, and filtering aggressively via metadata, the experts said.
2. **Process and host locally.** Take advantage of multinational data centers to meet standards.
3. **Segment data.** Use this three-step process: 1) Apply analytics, specifically using software to auto-segment the data. 2) Have an EU team review it to confirm proper segmentation and that private data is not being moved. 3) Share the confirmed safe data across the border with a U.S. team to conduct review.
4. **Restrict access.** When U.S. access to potentially private data is absolutely essential, keep the data access truly remote with technology such as Citrix that allows remote control of a computer or program. Also use IP restrictions to control who views potentially private information.
5. **Redact globally.** Redaction software can help ensure that a team does not miss any possible personal information. Some software can redact PII, payment card information, entities, and other personal information automatically, using search and "regular expressions" to block out data. E-discovery professionals can take a responsive document, look for patterns of PII, and use those patterns to block out private information among all documents.

INFO GOVERNANCE

Who Owns Data Management? IT, Legal Disagree

Recent research conducted by Iron Mountain and the International Data Corp. (IDC) shows that IT and legal departments often disagree about who should oversee data management.

According to "Mining for Insight: Rediscovering the Data Archive," 45% of legal and compliance respondents said they believe they should be responsible for determining what to archive, but only 25% of IT respondents agreed. Additionally, only 38% of legal and compliance respondents said they view archives as enhancing revenue, compared to 70% of IT respondents.

John Sharpe, Iron Mountain's director of product management, data management, noted that the disparity likely stems from the fundamental difference in each group's goals for data management.

"Legal's need to access data drives cases, whereas IT often has more of a support function; it doesn't necessarily have the same urgency … Legal has high expectations for IT to accomplish their data objectives, and that is a disconnect. They don't care about 1s and 0s; they care about emails and messages, the two are not necessarily aligned," he said.

According to the research, legal's data requirements are for specific content, while IT's focus is on storing and supporting all data. This misalignment creates misunderstandings between the two groups and impairs their ability to meet expectations.

Although storage costs continue to decrease, the associated costs of growing data volumes and the risks of potentially mismanaging these volumes mean legal and IT must be more strongly aligned. A good first step is for them to work together to define clear processes.

This could also help solve another problem the study identified: difficulty in accessing information. According to the research, 49% of respondents said significant productivity is lost in the search for difficult-to-access archived information.

These numbers highlight the importance of what many in the industry refer to as "unified information governance" (IG). Legal and IT aren't the only parts of the organization that have a disconnect; the same dynamic can occur between privacy and security groups. The greatest disconnect in the organization, though, is the disconnect from business units, which are generally focused on the organization's mission-critical functions.

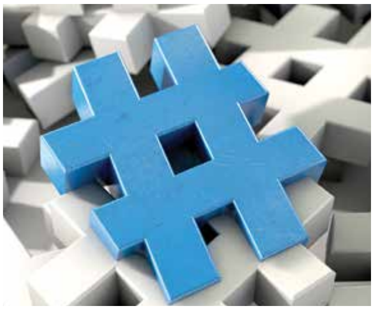
The business units' records and information are the lifeblood of the organization's success and must be drawn into the IG process. Which brings us to the other missing piece from this survey – the records and information management (RIM) group.

Unified IG calls for a steering committee to coordinate the viewpoints and needs of ALL stakeholders into a set of policies and procedures that serves the needs of all. A robust RIM program brings the viewpoints and needs together and provides a solid foundation for enhancing the organization's overall governance structure.

Unified IG has the goals of increasing business efficiency and effectiveness while mitigating risk and ensuring compliance. Achieving these goals requires forethought and routine implementation of defined procedures. In short, an organization that waits until litigation hits has waited too long.

INFO TECHNOLOGY

Gartner's Top 10 Technology Trends for 2016



According to Gartner Inc., data analytics has been a top area for technology investment in 2015 and is likely to be so again in 2016. David Cearley, vice president and Gartner Fellow at Gartner Group, shared his thoughts with *Information Management* on the "Top 10 Strategic Technology Trends" that will affect IT leaders and data analytics in the coming year.

1. **The Device Mesh:** According to Cearley, this is "the expanding set of endpoints people use to access applications and information or to interact with other people, social communities, governments, and business."
2. **Ambient User Experience**: Cearley says this is "one continuous, seamless digital experience for the user that blends device, time, and space, and combines the user's physical environment with the virtual and electronic environments."
3. **D Printing Materials:** 3D printing technology advances will cause it to be used more widely in new industries, Cearley says. For example, he says, there will emerge over the next two decades more materials that can be printed, improved printing speed, and new models to print and assemble composite parts.
4. **Information of Everything:** Cearley says, "Advances in semantic tools such as graph databases as well as other emerging data classification and information analysis techniques will bring meaning to the often chaotic deluge of information."
5. **Advanced Machine Learning:** Manual classification and analysis will not be feasible or affordable due to the growth of data sources and information complexity, Cearley says, so "deep neural nets" will automate these tasks and will address challenges related to the Information of Everything.
6. **Autonomous Agents and Things:** Machine learning will give rise to a "spectrum of smart machine implementations," Cearley says, including "robots, autonomous vehicles, virtual personal assistants, and smart advisors, all acting in an autonomous (or at least semiautonomous) manner."
7. **Adaptive Security Architecture:** Cearley says that particularly because of more cloud-based data and applications, perimeter defense will no longer be enough. IT leaders must focus more on detecting threats than on reacting to them.
8. **Advanced System Architecture:** The digital mesh and smart machines will require advanced computing architectures that function more like human brains, Cearley says.
9. **Mesh App and Service Architecture:** According to Cearley, application designs will take a loosely coupled integrative approach "to deliver agile, flexible, and dynamic cloud-based applications with agile, flexible, and dynamic user experiences that span the digital mesh."
10. **Internet of Things (IoT) Platforms:** Organizations embracing the IoT will need an IoT platform strategy, Cearley says, but "incomplete competing IoT vendor approaches will make standardization difficult through 2018." **END**