PRIVACY

FCC Rules Would Restrict Use of Consumers' Private Data

Internet service providers (ISPs) that provide broadband Internet access service to consumers have extraordinarily broad access "to very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interest, physical presence, and fears," according to the Federal Communications Commission (FCC).

ISPs can follow their customer's Internet activity by collecting individualized data and develop highly specific profiles of where each user goes and what services are acquired upon arrival at their Internet destinations, according to *The New York Law Journal*. That is why the FCC adopted, by a 3-to-2 vote, Notice of Proposed Rule Making (NPRM) that, if adopted, will address consumers' rights to have notice, choice, and security when their private information is used by broadband providers.

The FCC said in a statement that the NPRM proposes rules that would give broadband customers "the tools they need to make informed decisions about how their information is used by their ISPs"

and whether and for what purposes ISPs may share their customers' information with third parties.

The FCC's proposal allows for certain data collection that is necessary to provide broadband services and for marketing those services, as well as for public safety; this would not require customer consent beyond creation of the customer-ISP relationship. All other uses and sharing of consumer data would require "express, affirmative 'opt-in' consent from customers."

The NPRM defines the data to be protected as customer proprietary information, which would include both "customer proprietary network information" and personally identifiable information collected by broadband providers through their provision of services.

Because there is no uniform federal breach notification standard, the NPRM proposes that broadband providers notify affected customers within 10 days of discovering a breach that triggers customer notification requirements. The NPRM requires that the FCC be notified of all data breaches and that other federal law enforcement be informed of breaches that impact more than 5,000 customers within seven days of their discovery and three days before notification to the customer, the *New York Law Journal* reported.

PRIVACY

GDPR, Privacy Shield Will Impact Businesses, Survey Finds

According to the "2016 EU GDPR and EU-U.S. Privacy Shield Survey" by Baker & McKenzie, 84% of privacy professionals who responded said they expect the new General Data Protection Regulation (GDPR) recently adopted by the EU to impact their organizations.

Of the 100 respondents surveyed, between 60% and 70% said their organizations will need to spend at least some or significantly more of their budget in an effort to comply with the GDPR. The requirements that will call for additional attention include consent, data mapping, and cross-border data transfer, according to the survey.

Lawyers say preparing for the GDPR and Privacy Shield regulations calls for creating readiness plans and data maps, and the majority of organizations do not believe they have the tools and solutions necessary "to meet all of the requirements," Theo Ling, an attorney at Baker & McKenzie, told *Legaltech News*. In fact, the survey revealed that 45% of respondents said they either do not have the tools or could obtain them only at significant cost.

The good news is that more than 80% of the respondents said they are at least somewhat familiar with all of the major GDPR requirements. That's good, because the GDPR allows non-compliance fines of up to €20 million ($22.79 million U.S.) or 4% of an organization's total global annual turnover.

PRIVACY

EU Approves GDPR

The EU Parliament passed the General Data Protection Regulation (GDPR), overhauling the Data Protection Directive rules established in 1995. The rules apply to all organizations and businesses targeting EU consumers, regardless of their geographic location.

According to *Legaltech News*, the legislation defines new data and privacy rights for EU consumers, regulates the transfers and processing of EU data, and establishes more stringent enforcement of data handling, allowing organizations to be fined up to 4% of its total worldwide revenue for violating GDPR regulations.

GDPR is meant to replace the patchwork of EU member states' national laws so that businesses accessing EU data will have only one centralized supervisory authority to follow. The EU estimates that savings from this standardization will hit €2.3 billion ($2.6 billion U.S.) per year, *Legaltech News* reported.

The GDPR is effective now, but member states have two years to translate the regulations into their national laws. The UK and Ireland will follow the regulation on a limited basis because of their special "home affairs and justice legislation" status. Denmark will vote on the adoption of the GDPR within six months.

The GDPR:

- Allows an EU citizen's right to be forgotten, which means data controllers, processers, and Internet third parties must remove the personal data of an EU citizen upon request if there are no legitimate reasons to retain such information, such as historical, statistical, public health, scientific need, a right to free expression, or legal or contractual obligations
- Requires clear and affirmative consent, such as an EU citizen "ticking a box" on a website allowing it to retain or process his or her personal data
- Gives EU citizens the right to data portability, which allows them to transfer personal data between service providers easily, such as moving contact information from one e-mail provider to another

- Requires clear, plain language in Internet and business privacy policies
- Requires EU businesses and providers to expedite notifying their national supervisory authority of "serious" data breaches
- Limits the use of "profiling," which is collecting an individual's personal information in order to predict his or her behavior, without the expressed consent of the individual, or that of a law or contract
- Requires parental consent for children between the ages of 13 and 16 to open social media accounts, although the exact age varies among EU member states. Such laws are already in place in most EU countries.

The GDPR was also passed with a new EU directive on cross-border data processing and handling in criminal and judicial investigations, *Legaltech News* reported. The directive sets minimum standards for data processing by law enforcement agencies, defines EU citizens' rights and data transfer limitations in criminal or judicial processes, and enables cooperation between member state law enforcement agencies.

E-DISCOVERY

EDRM Releases E-Discovery Glossary

EDRM has released a free, downloadable PDF version of its *EDRM Glossary*, a comprehensive glossary of e-discovery terms. At more than 330 pages, the glossary is the industry's most comprehensive listing of electronic discovery terms.

"Experienced legal and e-discovery professionals have developed a fairly broad understanding of the processes and terms related to our craft," says George Socha, EDRM co-founder, "but none of us knows it all, and the technologies and language surrounding e-discovery continue to advance. Our goal with the glossary is to provide a tool that will enhance e-discovery knowledge and understanding, and evolve with the industry."

First launched in 2006, the *EDRM Glossary* includes terms from specialized glossaries on collection, metrics, search, and information governance, as well as glossary content on search and predictive coding from Herb Roitblat and from the Grossman-Cormack glossary on technology-assisted review.

The complete EDRM glossary can be downloaded at *www.edrm.net/resources/glossaries/glossary*.

PROFESSIONAL DEVELOPMENT

Survey: U.S. Government Not Prepared for Future IM Requirements

Many federal information management (IM) professionals feel unprepared to handle the future requirements of their jobs, according to the recent Iron Mountain survey report "Constructing the Next Generation Information Management Professional."

Iron Mountain said it conducted the study to identify the government's IM priorities for the next three to five years, share agency respondents' feedback on where gaps exist, and offer suggestions on how to improve on the necessary skillsets.

The survey asked these professionals what skills would be required for future effectiveness. More than half (56%) said they believe information security and access control will be in greatest demand from IM professionals, followed by data quality management (39%) and analytics capabilities – including data sourcing and integration (39%).

In addition, projects related to data privacy (34%), records and information management (RIM) (31%), and data analytics (30%) are thought to be in the greatest demand over the next three to five years.

"This survey provides an important view into the state of federal records and information management, both where the government is now in terms of capabilities and, more importantly, where agencies need to focus their information management practices in the future," said Michael J. Lewis, vice president and general manager, Iron Mountain Government Services.

The survey of 200 federal employees identified some key focus areas for future success, including:

- *Areas for improvement:* Risk management (34%) is most often cited, followed by electronic records retention (24%) and RIM practices (24%).
- *Most desired skill sets:* Risk management/security/data privacy (54%), analytics (42%), and content/records management (33%)
- *Technical and soft skills in demand:* Information security (52%), innovative thinking (39%), and fostering stakeholder buy-in and delivering C-level and stakeholder communications (15%)
- Ensuring compliance (32%), physical and IT records format management integration (26%), and information and data valuation assessment (24%)

The data suggests significant gaps between the skills RIM professionals currently have and what they believe they will need in the future. As such, Iron Mountain said agencies should consider focusing on the following in order to close that gap:

- Promote a more holistic approach to IM and sell it internally
- Meet the demand for specialized skills with a focus on information security, quality management, and analytics
- Focus on soft and technical skills in need of improvement and understand why improvement is needed
- Leverage the knowledge and mentoring skills of older staff before they retire
- Provide professional development training in the formats employees most prefer
- Create a forum for sharing ideas and best practices

The report is available at *www.ironmountain.com/NextGenIMPro*.

INFO SECURITY

Tennessee Enacts Tough Data Breach Law

This month, Tennessee becomes the first state to abolish the "encryption safe harbor" rule, giving it the honor of having the strictest data breach law in the United States, according to data privacy experts.

Encryption safe harbor requires companies who suffer a data breach to notify customers only if the exposed data was unencrypted. Tennessee's amended Identity Theft Deterrence Act of 1999, which became effective July 1, requires notification even if the breached data was encrypted, according to a *Corporate Counsel* report. The rule requires notice of a data breach to be reported to affected individuals within 45 days unless law enforcement needs more time to investigate. Only a few states have established a set notification time period.

Lastly, the bill amends the statute to specify that an "unauthorized person" includes an employee of the information holder who is discovered to have obtained personal information and intentionally used it for an unlawful purpose. According to the Jackson Lewis law firm, this amendment is likely focused on people who failed to provide notification of data breaches that resulted from improper access by employees.

Some lawyers believe the revised rules will place an undue burden on companies.

"If you're a company with a laptop stolen in Tennessee, you really have to ask yourself how you're going to demonstrate that the bad guys" aren't going to get access to certain information. Whereas in every other state, "you just have to show that the data is encrypted," Stephen Embry of Frost Brown Todd told *Corporate Counsel*.

The law doesn't require notice without question in all circumstances, but experts say the law in Tennessee now makes a distinction between strong and weak encryption that other states are not making, *Corporate Counsel* reported.

GOVERNMENT RECORDS

B.C. Revising its Freedom of Information System

British Columbia (B.C.) will revamp its Freedom of Information (FOI) system by releasing more documents proactively, restricting interference from political staff, and better helping the public access important records, according to B.C. Finance Minister Mike de Jong.

According to *The Vancouver Sun*, de Jong also suggested legislation to force government officials to better document their decisions, and he left open the possibility of eliminating FOI fees altogether as part of changes he said will increase confidence in the government's recordkeeping.

"If we are spending public money then the public deserves to know," he said, adding that contracts, calendars, and scanned receipts for ministerial travel now will be routinely posted online.

De Jong said non-partisan civil servants will oversee the gathering and release of records from the partisan offices of cabinet ministers, and ministers won't be able to delay signing off on records for more than five days.

"If anything, what we are trying to move to is a system that eliminates entirely the political level of oversight particularly with respect to minister's offices," said de Jong.

The federal government recently announced that it would eliminate FOI fees, charging only $5 per application. De Jong said he's pondering how to reform B.C.'s fee structure but is considering waiving all fees. The *Vancouver Sun* reported that the B.C. government collects approximately $60,000 a year in fees on an FOI system that costs $15.3 million to administer. The government added an additional $3 million into the FOI system in April, and de Jong said he'd like to see faster FOI responses as a result.

INFO SECURITY

Distrust of Vendors Raises Security, Compliance Questions

Many companies don't trust the vendors they share confidential data with, according to a recent Ponemon Institute survey.

The survey of 600 individuals across industries found that more than a third of U.S. businesses (37%) believe that their primary third-party vendors wouldn't notify them in the event of a security breach involving "sensitive and confidential information." In addition, 73% of respondents said that fourth-party to "nth"-party [an unknown number in a series of numbers] vendors – subcontractors or indirect service providers employed by a third-party vendor – would "fail to notify" if a breach occurred.

The survey, "Data Risk in the Third Party Ecosystem," was commissioned by law firm BuckleySandler and Treliant Risk Advisors to reveal the challenges facing firms trying to protect client information when sharing data with third parties, according to *Legaltech News*. Companies surveyed have a vendor data risk management program and were asked to consider only their outsourcing relationships in which they share "sensitive or confidential information or involve processes" that require vendor access to that data.

The survey revealed difficulties with "mitigating, detecting and minimizing" risks posed by third parties handling company data. According to the survey, companies lack faith in outside data handling and are not able to properly manage it. The findings show:

- About half (49%) of companies said they experienced a breach caused by vendors, while 16% said they weren't sure if a vendor was to blame.
- 73% of companies said they see vendor-related cybersecurity incidents increasing.
- Most companies find it difficult to manage vendor-related cyber incidents, with 65% saying they "don't have the internal resources to check or verify" when evaluating vendors' security and privacy practices.
- 58% of companies said they cannot determine whether vendor "safeguards and security policies are sufficient to prevent a data breach," leaving 41% who said they are sufficient.

"The reliance solely upon contractual agreements instead of audits and assessments to evaluate the security and privacy practices creates significant risk," Margo H.K. Tank, partner with BuckleySandler, told *Legaltech News*. "Companies will need to establish and track metrics regarding the effectiveness of the vendor risk management program and establish vendor risk management committees."

According to the survey, for many companies, information governance in vendor relations should be strengthened. For example, only 31% view their vendor risk management program as "highly effective," while 38% said they don't track metrics on their programs' effectiveness. In addition, the majority (62%) admitted that "their boards of directors do not require assurances that vendor risk is being assessed, managed, or monitored appropriately, or they are unsure."

"Companies must understand managing data risk is not merely a compliance and contract issue but a fundamental strategic challenge in which personal data, intellectual property and transactional records must be protected from third, fourth and nth-party risk," Tank said.

GOVERNMENT RECORDS

U.S. National Archives Appoints Permanent Chief Records Officer

Brewer

Laurence Brewer, the acting chief records officer (CRO) for the U.S. government, has been appointed to fill the position permanently, Archivist of the United States David Ferriero announced in late April.

Brewer's responsibilities include issuing federal records management policy and guidance; serving as a liaison to the Office of Management and Budget, Congress, the Government CIO Council, and other stakeholders on records management issues; and serving as an ombudsman between agencies and the U.S. archivist to ensure that the National Archives and Records Administration (NARA) and the agencies it serves meet their statutory mandates and records management requirements.

Brewer became the acting CRO in October 2015 when the previous CRO, Paul Wester, left NARA to become the director of the U.S. National Agricultural Library. He joined NARA in 1999 as an appraisal archivist and later worked as an electronic records policy analyst. He previously served as a records management consultant at the Environmental Protection Agency and the Virginia Department of Transportation.

MOBILE DEVICES

Security Issues May Hamper BYOD Adoption

Analysts are predicting that the global bring your own device (BYOD) and enterprise mobility market will hit $360 billion by 2020. While BYOD policies are boosting employee productivity and flexibility, security issues may be impeding their growth and implementation, according to a recent survey.

Crowd Research Partners surveyed 800 cybersecurity professionals for the "2016 BYOD and Mobile Security Report." Around three-quarters of those surveyed reported that their companies implemented BYOD policies for employees, 23% allowed BYOD for contractors, and 16% set up their policies on the company's partners' devices. In addition, 14% extended the service to their customers.

More than half of respondents noted that BYOD policies at their companies increased employee mobility, satisfaction, and productivity, while just under half cited reduced costs as an added benefit.

The survey also found, though, that security risks and mobile data breaches are increasing. It revealed that 39% of employees are worried about BYOD security, and 12% have concerns about the privacy of their data. More than 70% of the cybersecurity professionals surveyed cited data leakage or loss as their top BYOD concerns, while a little more than half also cited unauthorized access, user downloads of unsafe apps or content, and malware.

The survey revealed additional key insights on BYOD adoption and risks, including:

- Almost 40% of respondents noted that BYOD devices or corporate devices have downloaded malware, while 21% noted that mobile devices were involved in security breaches at their companies. About 25% said these devices had connected to a malicious WiFi network.
- One in five organizations suffered a mobile security breach, mainly driven by malware and malicious WiFi.
- Security threats to BYOD imposed heavy burdens on organizations' IT resources (35%) and helpdesk workloads (27%).
- Despite increasing mobile security threats, data breaches, and new regulations, only 30% of organizations are increasing security budgets for BYOD in the next year; 37% have no plans to change their security budgets.

The majority of respondents (80%) said malware protection and the ability to log, monitor, and report devices were key requirements for confronting mobile security threats. But just 63% said they had password protections for BYOD devices, while fewer than half had remote wipe capabilities (49%) or device encryption (43%).

"While these threats can significantly impact the success of BYOD initiatives and place a burden on IT support staff, this is also an opportunity for organizations to implement effective cybersecurity solutions to strengthen their security posture and capitalize on the promise of enterprise mobility," said Holger Schulze, the founder of the 300,000-member Information Security Community on LinkedIn, in a news release.

PRIVACY

Canada Joins Asia-Pacific Privacy Regime

Canada will join the Cross-Border Privacy Rules (CBPR) System, which requires Canadian entities doing business in Asia-Pacific Economic Cooperation (APEC) member economies to comply with minimum requirements regarding cross-border data privacy procedures. The requirements are outlined in the APEC Privacy Framework, published in December 2005, which seeks to provide clear guidance and direction to businesses on common privacy issues and their impact on the conduct of legitimate business.

APEC is a 21-country regional economic forum that seeks to promote economic integration and prosperity for the Asia-Pacific region. A joint oversight panel of the APEC CBPR system submitted a report in April 2015 confirming that Canada met the conditions for participating in the system. That report noted that Canada's Personal Information Protection and Electronic Documents Act contains provisions relevant to the enforceability of each of the 50 CBPR program requirements.

The United States, Mexico, and Japan have also been certified to participate in the system, and other APEC countries are evaluating their ability to meet the system's compliance and enforcement requirements.

BUSINESS CONTINUITY

More Businesses Moving to the Cloud for Data Backup

An increasing number of organizations are looking to the cloud to back up their company data, according to Kroll Ontrack research.

Kroll studied the data backup practices of more than 500 companies in North America, Asia, and Europe that have suffered data losses. According to the survey, among companies with no data backup plans, 51% are still considering hard drives for primary data backup, while 23% are considering moving their backup data to the cloud.

When compared to the results of the same survey conducted in 2015, Kroll found that businesses are slowly moving away from external hard drives (down 17% from the previous year) and toward cloud consideration, which has increased by 5%.

Most organizations have procedures in place to back up their data, but challenges remain.

"Maintaining a traditional backup solution takes time and due diligence. For instance, think about the exponential growth in data volumes that IT teams are handling and backing up. That growing volume translates into time – significant time," said Todd Johnson, vice president of data and storage technologies at Kroll Ontrack. "And it's not a 'set it and forget it' process. Backup health requires regular testing and auditing to not only ensure the backup is working properly, but to confirm it includes all the necessary media to meet preservation and compliance requirements. It's a huge balancing act, particularly for smaller to midsize organizations with limited IT support infrastructure."

Interestingly, Kroll found that at the time of data loss, 14% of companies did not have a data backup in place. Perhaps not surprisingly, 58% relied on external hard drive solutions while about 16% used the cloud. Eleven percent said they used network-attached storage.

Of those without backup solutions, 54% said not having enough time for administration and research was their reason for not implementing a solution. Notably, fewer companies cited expense as a reason for not backing up data than in 2015 – a 7% decline, according to Kroll.

DIGITAL PRESERVATION

Microsoft Experimenting with DNA for Digital Storage

Microsoft said it plans to acquire 10 million strands of DNA from Twist Bioscience to use for digital storage experiments. Twist Bioscience is a San Francisco-based biology startup that makes synthetic, storage-ready DNA, according to *Tech Times*.

"As our digital data continues to expand exponentially, we need new methods for long-term, secure data storage," said Doug Carmean, a Microsoft partner architect in its Technology and Research organization. "The initial test phase with Twist demonstrated that we could encode and recover 100% of the digital data from synthetic DNA. We're still years away from a commercially viable product, but our early tests with Twist demonstrate that in the future we'll be able to substantially increase the density and durability of data storage."

Compared to traditional storage systems, the data density offered by DNA is significantly higher. According to *Tech Times*, 1 gram of DNA is equivalent to nearly 1 billion terabytes (or 1 zettabyte) of data. It also is far more robust than conventional storage systems as is evidenced by the fact that DNA fragments that are several thousand years old can be sequenced successfully.

Another advantage of DNA is that it will stay unharmed and readable for between 1,000 to 10,000 years.

Microsoft research estimates that 1 cubic millimeter of DNA can store 1 exabyte, or 1 billion gigabytes, worth of data, making the use of DNA for digital data archival a viable option long term, *Tech Times* reported.

EHRs

U.S. Nears 100% EHR Adoption

Ninety-six percent of U.S. hospitals are using certified electronic health records (EHRs), compared with 72% in 2011, revealed a survey released at the 2016 annual meeting of the Office of the National Coordinator for Health Information Technology (ONC) in Washington, D.C.

"Data showing the nearly universal adoption of certified electronic health records are an indication of how far we have come for clinicians and individuals since the HITECH Act was passed," National Coordinator for Health Information Technology and Acting Assistant Secretary for Health Karen DeSalvo said in a statement.

Introduced in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act has led to an increase in the adoption of health IT, *eweek.com* reported.

According to the survey, just 9% of non-federal, acute-care hospitals used basic EHRs in 2008, while 84% use them today; in 2011, 72% used certified EHRs, and today 96% do.

Small, rural, and critical-access hospitals are not as up to speed; however, since 2014, small, rural hospitals have increased their adoption of basic EHRs by 14%, and critical-access hospitals have increased adoption by 18%, *eweek* said.

The rate at which information – such as radiology reports, care summaries, and lab results – is being exchanged has doubled since 2008, from 41% to 82% in 2015, the report found. And even between 2014 and 2015, the percentage of hospitals using, sending, receiving, and finding key clinical information "grew significantly," from 23% to 26%.

E-DISCOVERY

U.S. Appeals Court Allows Search of Old PC Files

In a closely watched case, a U.S. appeals court has ruled that federal agents acted in good faith when executing a warrant to search records that had been seized two and a half years earlier.

The 12-to-1 decision by the Second U.S. Circuit Court of Appeals in New York restored a Connecticut accountant's 2011 jury conviction and two-year prison sentence for tax evasion, Reuters reported. A three-judge panel had overturned both in June 2014.

Stavros Ganias' computer files were seized in November 2003 by U.S. Army investigators examining possible overbilling by a military contractor that had employed Ganias as an accountant, according to Reuters. But instead of purging unnecessary files, the government held onto them, and in April 2006 got a warrant to search them for evidence of unrelated tax evasion by Ganias.

While the appeals court decision tested how long the government can keep a criminal suspect's computer data, the court did not answer the question of whether keeping the records for that long violated the suspect's Fourth Amendment rights.

In the 2014 ruling that voided the jury verdict, Circuit Judge Denny Chin, who was the lone dissenter in the most recent decision, said the government went too far by searching computer records it had long considered irrelevant for evidence of a new crime.

The majority, in its 60-page opinion, did not address that issue but did warn law enforcement to be more careful, citing "significant" privacy concerns and Fourth Amendment issues arising when the government retains hard drives and other digital media containing vast troves of personal information, "much of which may be entirely irrelevant to the criminal investigation that led to the seizure," Reuters reported.

Chin, in his 40-page dissent, said the "cloud" that has hung over Ganias' head for the last 13 years should be lifted.

"The government did precisely what the Fourth Amendment forbids: it entered Ganias' premises with a warrant to seize certain papers and indiscriminately seized – and retained – all papers instead," he wrote.

Ganias' lawyer said he was reviewing the decision and might appeal to the U.S. Supreme Court.

INFO GOV PROGRAMS

Firms Must Focus More on Information Governance, Lawyers Say

Firms just aren't paying enough attention to information governance (IG), according to corporate in-house counsel interviewed for Kroll's 2016 Corporate Risk Survey.

The 170 lawyers taking part in the survey cited the following as the most pressing issues facing their firms: data security, cybersecurity, and privacy risks, including the loss of personally identifiable information.

Almost half of respondents (47%) said their companies do not have an IG program in place. According to the survey, another 26% think their programs lack the resources needed to be effective.

The survey also found that 59% of lawyers reported that their organization's data breach or incident response plans are inadequate or non-existent.

Other findings include:

- Data security is "the most significant risk facing modern corporations." Most (76%) in-house counsel said there are effective safeguards in place to protect their organization's intellectual property, but only 41% said their company's plan is regularly updated and tested.
- Two-thirds of respondents said their firms are more at risk of external fraud, while 33% believe their risk of internal fraud is higher.
- For fraud, 85% of organizations conduct due diligence on proposed business partners and 76% maintain internal resources to investigate fraud in the United States. But almost two-thirds lack the internal resources needed to investigate global fraud incidents.
- Organizations are using most of their compliance budgets for risk assessments and policy creation and management. In-house counsel said they want to spend additional funds on compliance training and technology systems to facilitate compliance screening.

According to Kroll, the survey shows that "organizations are making noteworthy strides as a result of the new risks facing the enterprise. Nevertheless, the survey also reveals that organizations have additional room to evolve if they seek to combat these modern risks in an efficient, cost-effective manner."

INFO GOV PROGRAMS

Survey: Unstructured Data a Growing Challenge

While most companies are aware of the importance of information governance (IG), many do not have insight or control over employee-produced data, according to a recent survey from Acaveo and Osterman Research.

They surveyed more than 100 organizations that stored an average 20 TB of unstructured data and found that only 37% of them regularly audited the amount of data employees or business units produce. Just 35% said they had a budget in place to deal with unstructured data challenges.

Overall, while many companies admitted to struggling with governing unstructured data, only half of the surveyed companies said they have an IG program in place to help deal with it.

But they do understand the importance, as 70% cited regulatory risks and 66% cited the need to avoid any data risks as reasons to adopt an IG program. In addition, 75% of respondents noted the savings IG can bring to storage costs. Other findings include:

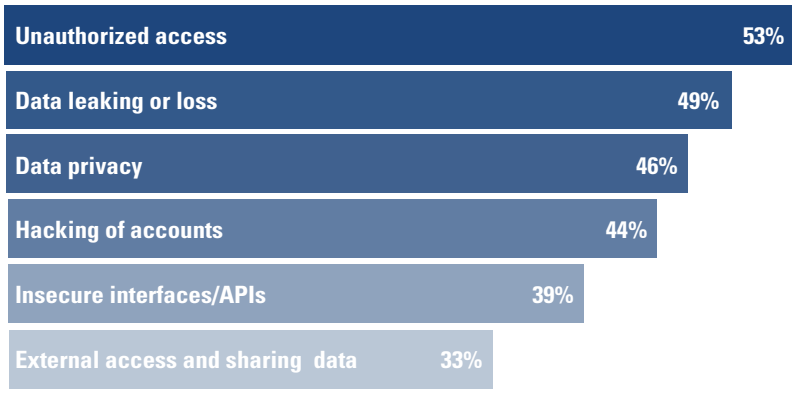
- 55% of organizations perform regular file share cleanup exercises.
- 40% of organizations have a "defensible deletion" program in place.
- Of the companies that have an IG program, 75% justify the program based on storage costs.

Notably, the survey predicts that the proportion of unstructured data stored in-house will increase from 22% currently to 25% in just two years, while cloud storage will comprise a bit less than half of an organization's information repositories in at least five years.

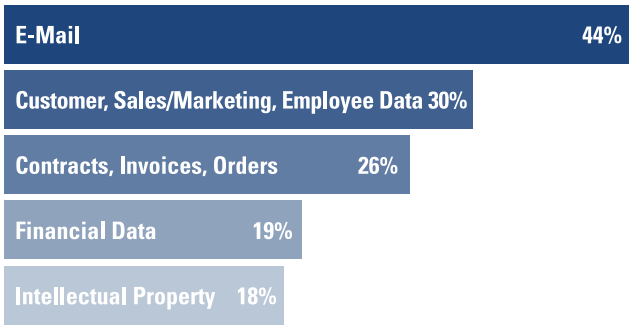
CLOUD COMPUTING

Are Cloud Security Concerns Overblown?

Greatest Threats to Cloud Security
More than 2,000 professionals surveyed by Cloud Research Partners cited the following obstacles to cloud security:



Percentage of Companies Storing These Data Types in the Cloud



While security concerns over cloud adoption are the greatest barrier to adoption among businesses, a recent survey found that few have actually suffered a cloud-related security incident.

The *Cloud Security Spotlight Report* by Crowd Research Partners surveyed 2,200 consultants, specialists, executives, IT, and other professionals across a variety of industries and found that more than half (53%) of respondents expressed concern over the security of their data in the cloud, an increase from 45% in 2015, *Legaltech News* reported.

Interestingly, however, when asked if they had suffered a cloud-related security incident, only 9% said yes, while 36% could not disclose or did not know of any incident, and 55% said they had not had any cloud-related security issues, the survey found.

If the survey findings are any indication, respondents may be confused about how secure the cloud really is. For example, 22% of respondents said there was a lower risk of breaches from the cloud compared to data hosted on premises servers, while 21% said the opposite, and 27% said they believed security for cloud and on-premises storage was about the same.

Legal and regulatory compliance concerns were also cited as a barrier to cloud adoption by 42% of respondents in 2016, up from 29% in 2015. The survey noted, however, that "the rise in specific concerns about compliance and integration suggests that companies are moving from theoretical exploration of cloud models to actual implementation."

According to *Legaltech News,* factors driving these concerns include the recently approved General Data Protection Regulation in Europe and cybersecurity disclosure and data regulations, which require companies to consider where their data is being stored and processed. The full report may be downloaded at *www.crowdresearchpartners.com/portfolio_item/cloud-security.* **END**

CISCO® GLOBAL CLOUD INDEX

Data Center Virtualization and Cloud Computing Growth

- By 2019, 86% of workloads will be processed by cloud data centers; 14% will be processed by traditional data centers.
- Overall data center workloads will more than double from 2014 to 2019; cloud workloads will more than triple (3.3-fold) over the same period.
- The workload density (that is, workloads per physical server) for cloud data centers was 5.1 in 2014; it will grow to 8.4 by 2019. Traditional data centers' workload density was 2.0 in 2014 and will grow to 3.2 by 2019.