CLOUD

Forrester: Cloud Technology in a 'Hypergrowth Phase'

Cloud service revenues will reach $236 billion in the private sector by 2020, predicts Forrester Research. That total exceeds Forrester's 2014 forecast by 23%.

According to the Forrester study, public cloud will become the dominant technology model by 2020. The growth won't come from a huge influx of new customers, but from portfolio expansion and new application scenarios, the study predicts.

Cloud technology, according to Forrester, is currently in a "hypergrowth phase" that will gain speed for the next four years for cloud platforms, cloud applications, and cloud business services.

The increasingly strong market for software-as-a-service (SaaS) and dramatic increases in infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) will continue, according to the study. By 2020, Forrester predicts SaaS will comprise more than two-thirds of spending on customer relationship management, human resource management, e-commerce, and e-purchasing.

Forrester says it has been "astonishing" how cloud service providers, including Amazon Web Services, Microsoft Azure, IBM, Google, and Salesforce, have already affected sales of on-premises servers and storage devices. By 2018, Forrester's research suggests, North American and European companies will run 18% of their custom-built application software on public cloud platforms.

INFO SECURITY

Pokémon Go Proves that Companies Need Strong BYOD Policies

The Pokémon Go game has become an insanely popular hit worldwide, enticing millions of players to find, catch, battle, and train virtual monsters that pop up at real-world landmarks. But it's also a huge security risk for organizations everywhere, underscoring their need for a strong "Bring Your Own Device" (BYOD) program.

According to *Legaltech News,* although many BYOD policies separate corporate data from personal activities, they cannot restrict employees from downloading to their personal devices games like Pokémon Go, which by default has full access to players' Google e-mail, files, and location data. According to Pokémon Go's privacy policy, the "data it collects – including personal information – is an asset of the developer."

This popularity of Pokémon Go likely means that such games will become the norm. Here's how to keep your organization safe, according to a *Legaltech News* report:

- Implement a written BYOD policy, enforce restrictions, and make sure you have the tools to do so. Train staff on cybersecurity and appropriate digital device usage.
- Verify that your employees' personal devices have not been "jail broken" before allowing them onto your network. According to *Legaltech News*, this means that a user has gained access to a device's operating system (usually in Apple devices) in order to run unauthorized applications.
- Encrypt all devices and data used for work purposes.
- Restrict network access for employees who don't want to install security tools on their personal devices.

INFO SECURITY

Data Breaches Cost More than Money

According to a recent *Journal of Accountancy* article, a new report by Deloitte & Touche LLP lists 14 impact factors of a cyberattack, including seven that might not be readily apparent:

1. Higher insurance premiums: Deloitte says companies may face premium increases of 200% for the same coverage, or they may be denied coverage until they prove to the insurer that they have shored up their cyber defenses. Insurers may tell a company what to fix before coverage will be continued.
2. Increased cost to raise debt: After a data breach, a company's credit rating can be lowered, which will affect its ability to raise debt or renegotiate its existing debt, Deloitte said. Deloitte's analysis said credit ratings agencies typically downgrade by one level companies that have experienced a cyber incident.
3. Business disruption: When normal business operations are disrupted, a company suffers financially. If a company's e-commerce site must be shut down temporarily, for example, the company will lose current and possibly future business when customers move to a competitor.
4. Lost customer relationships: Customers may not return to a business that suffers a breach. Deloitte's hypothetical analysis showed that customer attrition rate increases 30% after a cyber incident and doesn't return to normal for three years.
5. Lost contract revenue: Negotiating contracts with other entities is harder after a data breach, and contracts may be terminated as a result of a cyberattack.
6. Devaluation of trade name: If a company's business is offering services to other companies, those companies will be less likely to seek additional services from a company that has suffered a data breach. Most companies will need to rebuild brand loyalty after a breach.
7. Loss of intellectual property: This can be the most crippling effect of a data breach. The effects could be long-lasting or potentially fatal to the company's survival, depending on what type of intellectual property is lost. "If you lose plans, if you lose designs, or lose [research and development] that you've been working on for months or years, and that then is brought to market by another organization faster and cheaper than you can do it, that impact can be reverberating for decades," said Emily Mossburg, principal in Deloitte & Touche's cyber risk practice and a report author.

INFO SECURITY

Connecting Phones to Rental Cars May Expose Data, FTC Warns

Automotive IT systems that connect smartphones with onboard media players may put your private data at risk when you're driving a rental car, the Federal Trade Commission has warned.

Lisa Weintraub Schifferle, an attorney in the FTC's Division of Consumer and Business Education, said that when you return the car, those connected systems might reveal your private data to those who know where to find it, according to an article on *FCW.com*.

For example, the car's GPS device can store the locations you visited, which may include a rental car user's workplace and home. By connecting a smartphone to any of the systems in the vehicle, someone could find telephone numbers, call and message logs, contacts, and text messages, Schifferle wrote.

If you connect to any system in a rented vehicle, you must proactively delete the data to keep it from being accessed by the next driver or by hackers, she warned.

Schifferle said even charging a smartphone on a rental car's USB port could automatically transfer data to the onboard systems. She recommends charging a smartphone on an adapter instead; checking onboard screens for options to limit access to connected devices; and deleting your devices from the list when you return the vehicle.

GOVERNMENT RECORDS

OMB Updates Rules to Protect Government Data

After a spate of large breaches involving federal agencies, the Office of Management and Budget (OMB) has revised its rules to promote data protection in the federal government.

OMB released an 85-page update to Circular A-130 highlighting how the OMB "recognizes the need for strong data governance that encourages agencies to proactively identify risks, determine practical and implementable solutions to address said risks, and implement and continually test the solutions," according to a *Legaltech News* report.

The document, which was sent to the heads of all federal departments and agencies, is designed to establish general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.

With its circular, the OMB is sending a message to government agencies – in the form of a framework – that they need to develop a culture of privacy and security protection.

Bart Lazar, attorney at Seyfarth Shaw, told *Legaltech News* that for years the private sector has been encouraged to establish a C-suite level champion within each company for data privacy and security. "Without support from the top, it is difficult, if not impossible, to get the budget and resources allocated in order to develop a culture of data privacy and security compliance. This circular, coming from OMB in the White House, in some ways is the U.S. government's C-suite support for developing, implementing, and maintaining that culture of compliance," he said.

In response to the document, federal agencies need to make changes, including creating a risk management framework, maintaining a continuous privacy monitoring program, implementing an overall privacy awareness program, and training staff and vendors on how to handle data breaches, *Legaltech News* said.

"It is hard for the U.S. government to expect businesses in the private sector to do something the government does not do itself, the whole 'talk the talk, walk the walk,'" Lazar said.

PRIVACY

Illinois Public Employees' Private Messages May Be Made Public

Illinois Attorney General Lisa Madigan recently issued a binding decision that the personal e-mail accounts of many types of public employees are subject to Freedom of Information Act (FOIA) requests if those e-mails contain public business, the Illinois News Network reported. The decision is the result of a CNN request to the Chicago Police Department to turn over any personal e-mails that officers may have made concerning the Laquan McDonald shooting.

Legal experts said the ruling will affect municipalities across the state. "Sometimes the easiest thing to do is to pull out a smartphone to text a colleague for a public works project or something similar," Mark Burkland, Holland & Knight senior counsel, said. "If a water main breaks at 2 a.m., is the public works director not supposed to use their personal device to call or to text someone to get out and fix it?"

An attorney for CNN argued that granting public employees' private e-mails immunity from FOIA requests would undermine current disclosure laws because it would give them reason to use those accounts to hide sensitive information.

The rule doesn't apply to elected officials and their private accounts.

Burkland said public bodies should make rules to establish a way to get to their employees' private accounts should they need to.

At time of publication, it was unclear whether the city of Chicago would appeal the decision.

PRIVACY

Facebook Cannot Collect Data on WhatsApp Users in Germany

WhatsApp angered some users when it announced in August that in an effort to provide better service, it would begin sharing users' phone numbers and analytics data with Facebook – which acquired WhatsApp in 2014.

The city of Hamburg, Germany's data protection commissioner, Johannes Caspar, has ordered Facebook to stop collecting and storing data on WhatsApp users in Germany and to delete all information on about 35 million German users that already had been forwarded from WhatsApp. The Hamburg regulator has authority over Facebook's activities in Germany because the company's German subsidiary is based in the city, according to the *New York Times*.

Caspar said that neither WhatsApp nor Facebook had received individuals' permission to share the information and had potentially misled people over how their data would be used in the future. He added that millions of people whose contact details had been uploaded to WhatsApp could now see that information shared with Facebook against their will, which would infringe German law.

"It has to be their decision, whether they want to connect their account with Facebook," Caspar said in a statement. "Therefore, Facebook has to ask for their permission in advance. This has not happened."

After the order was issued, Facebook said it had complied with Europe's privacy rules and was willing to work with the regulator to address its concerns.

"Facebook's answer, that this has merely not been done for the time being, is cause for concern that the gravity of the data protection breach" will have a more severe impact, Caspar said.

GOVERNMENT RECORDS

Federal CIOs Focused on Cybersecurity, Survey Shows

Cybersecurity is the top priority and challenge for U.S. federal chief information officers (CIOs) and chief information security officers (CISOs), according to the 26th annual Professional Services Council survey, conducted with Grant Thornton.

This year's survey, "Federal CIOs: Delivering Results While Preparing for Transition," highlights federal IT leaders' efforts to modernize outdated IT infrastructure, raise the bar on cybersecurity, reform IT acquisition processes, deliver on the promise of innovation, and address the ongoing war for top IT talent in both government and industry.

"Today's government IT leaders need to wear many hats as demands increase and budgets shrink," said George DelPrete, principal with Grant Thornton Public Sector and leader of its Information Technology Service line. "They face a number of daunting challenges, but it is reassuring to see how they are being creative in using technology and new strategies to keep their agencies agile and responsive."

While cyberattacks on government systems continue to make headlines, overall, survey respondents report that government is making progress coordinating on cyber issues. The cyber sprint conducted in the summer of 2015 was helpful for them to gain insights into their own cyber risks and improve communication within the CIO community on threats and mitigations to common cybersecurity risks.

CIOs and CISOs who responded to the survey also said:

- Cybersecurity challenges are exacerbated as federal legacy systems and infrastructure continue to age, and that additional investment is required to address this crucial issue.
- Hiring rules need to change to make it easier to recruit and offer competitive pay to new cybersecurity talent. Skills in greatest demand include cybersecurity, agile development, cloud expertise, and digital services skills.

There is a need to modernize federal IT legacy systems, reduce network footprints, rationalize and modernize applications, and migrate to the cloud. Modernizing the IT environment is needed to close security gaps, refresh infrastructure to improve IT performance, reduce spending on outdated equipment or software, take advantage of fast-changing technology improvements, and better manage, consolidate, and analyze the increasingly large volumes of government data.

PRIVACY

How to Prepare for the EU's General Data Protection Regulation

The European Union's (EU's) General Data Protection Regulation (GDPR) provides specific guidelines for how to classify, secure, and manage EU individuals' private data. They affect companies operating there, as well as any organization that does business there or that collects data on EU citizens.

The GDPR aims to give individuals more control over their personal information by clarifying the law relating to the clear and affirmative consent to data processing, how and where data can be stored, and individuals' right to be forgotten, according to *Legaltech News*.

GDPR mandates that organizations must proactively classify data and have tools in place to take action on this information, including applying governance policies, detecting and responding to data breaches, and optimizing backup and recovery. According to the new rules, organizations must understand their data and where it resides, as well as protect it in use, in transit, and in storage.

Organizations have a May 2018 deadline to comply with the GDPR or face significant fines, sanctions, and lawsuits.

Joe Garber, vice president of marketing at Hewlett Packard Enterprise, recently provided *Legaltech News* with the following tips to help organizations prepare for the GDPR:

Understand your data. If your organization is subject to GDPR, first assess your data:

- What and where is the information that falls under GDPR regulations?
- How do I identify information in accordance with "right to be forgotten?"
- How do I apply and enforce policies to manage information in use, in transit, and at rest?
- How can I quickly and cost-effectively respond to investigations or legal matters requiring information under management?
- How can I mitigate the risk of a data breach? What is my plan of action if one occurs?

Assess technology platforms to ensure compliance. The cloud hasn't been as widely adopted in the EU as in the United States because of data sovereignty issues, but many EU organizations are now re-thinking their cloud strategy, Garber says. Those companies need to ask:

- Is data stored and processed within the European Economic Area?
- What security measures does the cloud provider have to protect data as it relates specifically to GDPR?
- How can I access this information for investigations and litigation, if necessary?
- Will these cloud-based technologies provide broad enough tools to address the full scope of GDPR, or will I have to switch to other capabilities over time?

Break down the GDPR into simple use cases. The GDPR has more teeth and specificity than many requirements that have come before it, Garber said, so playing the "wait and see" game is not a good idea. If organizations wait until right before the May 2018 deadline to prepare, they may not be fully compliant when the requirements kick in, leaving them and their customers' information at risk.

Garber says the smart approach is to take GDPR compliance in a methodical, modular way. There are specific use cases mapped out by certain technology vendors that align directly to GDPR requirements.

E-DISCOVERY

Report: 2016 a Good Year for E-Discovery

2016 is shaping up to be an eventful year for e-discovery, according to a mid-year report.

With the U.S. Federal Rules of Civil Procedure (FRCP) amendments in effect and plenty of new technologies, Gibson, Dunn & Crutcher's "2016 Mid-Year Electronic Discovery Update" describes e-discovery as evolving, ripe for innovative technologies, struggling to keep pace with new sources of discoverable information, and watchful of post-FRCP changes.

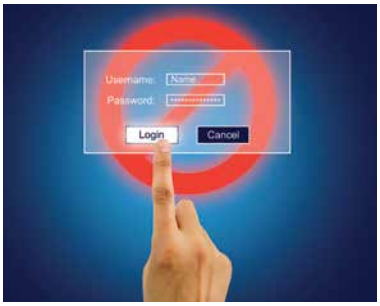
E-discovery looks "much better" than in years past, in part because FRCP Rules 26(b)(1) (discovery must be relevant and proportional) and 37(e) (preservation responsibilities and sanctions for failure to preserve) have "for the most part" had "their intended effects," noted co-author Gareth Evans, litigation partner at Gibson Dunn. This is a stark change from the 2006 amendment to Rule 37(e), which was not applied as intended, he added.

According to the report, the positives include the following:

- In the first six months of 2016, Rule 37(e) was applied in 32 decisions, with 13 granting sanctions and 19 denying them. This is a "substantially slower" pace than in past years, the report says (150 sanctions in federal courts in 2011 and 120 in 2012). The report says the reduction is likely due to a growing awareness of preservation duties.
- A rational, easy-to-apply set of criteria in amended FRCP 37(e) for imposing sanctions for failure to preserve discoverable electronically stored information (ESI) seems to have resulted in shorter sanctions decisions that are faithful to the amended rule, as well as in substantially fewer sanctions motions and decisions.
- Courts also appear to be faithfully implementing the requirement of amended Rule 26(b)(1) that discovery must be both relevant and proportional, with courts repeatedly holding that merely establishing relevancy but not proportionality is not enough. Despite once implicitly allowing broad "fishing expeditions," courts are now explicitly prohibiting them.
- What appears to be a dramatic reduction in the number of sanctions decisions likely is due, in part, to greater awareness among litigants of preservation duties, as well as improved legal hold practices. But it is almost certainly also a result of a clearer, more consistent legal framework, which should discourage sanctions motions that do not satisfy each of the criteria set forth in the amended rule – particularly the elimination of the harshest sanctions where there was no intent to deprive other parties of the lost information.

The report also identified several challenges to consider:

- New sources of potentially discoverable ESI, such as text messaging and social media, have created new risks and difficulties for identification and for legal hold preservation and collection, and, further, have made it difficult to determine just what is discoverable. Indeed, many of the sanctions decisions so far in 2016 have involved failures to preserve text messages on mobile devices, the report found.
- The potential of predictive coding to greatly reduce costs and increase accuracy and review speeds remains largely unfulfilled, hampered by several factors, including a lack of awareness of the technology, lawyers' comfort with traditional keyword searches, obstacles raised by those opposing its use (such as demanding access to irrelevant documents in training sets), and the limited availability of the latest predictive coding software.
- Vendors have yet to put together a single, full suite of "best in breed" software for companies to handle e-discovery tasks internally from beginning to end (legal holds through production). It is likely only a matter of time before they do so, however, the authors noted.



FOIA

NJ May Deny Public Records Access, Court Says

Government agencies in New Jersey may deny access to public records by saying they can "neither confirm nor deny" their existence when they receive an information request under the state's Open Public Records Act (OPRA), New Jersey's state appeals court has ruled.

The decision makes New Jersey the second state to adopt as law what one media lawyer has called "a broad and damaging secrecy tool" first used by the U.S. government during the Cold War to protect its national security interests. The other state, Indiana, authorized "neither confirm nor deny" responses through a statute, not a court ruling.

The ruling was made against North Jersey Media Group, a division of Gannett that publishes several newspapers, including *The Record*. The New Jersey appeals court allowed what is known as a "Glomar" response, which some U.S. agencies have used since the 1970s to block requests for public records submitted under the U.S. Freedom of Information Act.

"Glomar responses are used under FOIA in two contexts: where confirming or denying raises national security issues or privacy issues," said Erwin Chemerisnky, a First Amendment expert and dean of the law school at the University of California, Irvine. "But even then, agencies must present as much as possible. It is essential that Glomar responses be limited or they could be used to undermine public records laws."

In 2013, a reporter for North Jersey Media Group filed a request under OPRA and the common law seeking from the Bergen County Prosecutor's Office recordings or transcripts of 911 calls, complaints, and other documents regarding a Catholic priest who has never been arrested or charged with a crime.

To protect the priest's privacy, the prosecutor's office neither confirmed nor denied the records existed. "Exposing information regarding individuals who have not been arrested or charged with any crime is an invasion of privacy and could have devastating repercussions," the office stated.

When the dispute went to trial, Superior Court Judge Peter Doyne ruled for the first time in New Jersey that a government agency could answer a request for public records by neither confirming nor denying the existence of relevant documents, according to media reports.

Doyne based his ruling on the state constitution's right to privacy. The appeals court upheld the response from the prosecutor but its decision was even more specific.

Judge Marianne Espinosa wrote for the appellate court that although "there is no language in OPRA that explicitly permits an agency to decline to confirm or deny the existence of responsive records," that law does allow agencies to respond to public records requests by stating that they are "unable to comply." Those agencies, however, should be prepared to show a court a "sufficient basis" for neither confirming nor denying the existence of relevant documents, Espinosa added.

"It is obvious that, in order to protect the confidentiality of persons who have been the subject of investigation but not charged with any offense, the prosecutor must respond to requests for such records uniformly," Espinosa wrote. "To deny records exist in some cases and to issue no denial in others would implicitly confirm the existence of records in a particular case, entirely defeating any effort to protect the confidentiality interest at stake."

E-DISCOVERY

Sedona Releases Draft E-Discovery Publication

The Sedona Conference® recently released the public comment version of *Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*. The publication addresses the tension between the principle of party-controlled discovery and the need for accountability in the discovery process. It establishes a series of reasonable expectations and provides practical guidance to meet these competing interests.

The overriding goal of the principles and guidelines set forth in this commentary is to reduce the cost and burden typically associated with modern discovery by helping litigants prepare for – or, better yet, avoid – challenges to their discovery processes, and by providing guidance to the courts in the (ideally) rare instances they are called upon to examine a party's discovery conduct.

The commentary may be downloaded free from The Sedona Conference® website. The public comment period closes November 15. Questions and comments may be sent to *comments@sedonaconference.org*.

PRIVACY

More Than 100 U.S. Companies Earn Privacy Shield Certification

The European Commission recently said that more than 100 U.S. companies have been certified by the U.S. Department of Commerce as having privacy policies that comply with the data protection standards required by the U.S.-EU Privacy Shield.

"I'm pleased that many companies have already signed up and brought their privacy policies in line with the Privacy Shield," Vera Jourová, the EU's commissioner for Justice, Consumers and Gender Equality, said in the announcement. "I encourage many others to continue to do so to ensure Europeans can have full confidence in the protection of their personal data when transferred to the U.S."

The European Commission announcement also notes that the U.S. Commerce Department is reviewing the privacy policies of another 190 companies that have signed up for the Privacy Shield and that another 250 companies are submitting applications. In contrast, more than 4,000 companies had been certified under the Safe Harbor that was invalidated by the European Court of Justice in 2015.

The Privacy Shield program, which became available to U.S. organizations on August 1, provides companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States.

E-DISCOVERY

ESI Infrastructure Still Frustrates E-Government

Government agencies have hired additional e-discovery experts to help manage their data volumes, but most still struggle with electronically stored information (ESI) infrastructure and processes, according to consulting firm Deloitte.

Deloitte's 10th annual benchmarking study on the use of e-discovery by government agencies found that internal systems and processes remain the most pressing challenge agencies face in their e-discovery practices.

In "Study of Electronic Discovery Practice for Government Agencies - 2016," 35% of 210 respondents reported that "internal systems and processes" created the biggest challenges in handling, processing, reviewing, or producing ESI. The category has been ranked the top challenge for respondents of the survey five years running.

Surprisingly, the report also found that government agencies rarely request social media data, with only 19% of legal experts polled saying they requested social media data from opposing counsel, down slightly from 23% last year.

"Social media data – while important on some matters – is not a source of information in most federal litigation matters," Patrick McColloch, managing director in the government sector discovery practice of Deloitte Transactions and Business Analytics, told *Legaltech News*.

McColloch said agency staff has taken some measures over the last decade to mitigate these concerns. For example, agencies have hired specific e-discovery counsel to specialize in technology and issues surrounding ESI within their general counsel offices.

McColloch noted that the Department of Justice has also added to its own e-discovery staff and resources in an attempt to better support agencies during litigation.

McColloch suggested that agencies start to invest more heavily in supporting ESI needs, despite budgetary constraints.

"Agencies need to view investments in internal systems and processes as they would any other investment," he said. "With the expanding volumes and complexities of data, and without investing in the systems in processes, government agencies are forced to tackle the issue with more manpower or potentially face litigation risks."

E-DISCOVERY

Court Orders a $3 Million Fine for E-Discovery Misconduct

Legal experts have called the recent *GN Netcom v. Plantronics* decision a "teaching opinion" for how e-discovery should be conducted and one of the more significant opinions since the enactment of the U.S. Federal Rules of Civil Procedure (FRCP) amendments in December 2015.

In the antitrust case, the District of Delaware issued a scathing opinion relating to the scope of sanctions that may be applied for e-discovery misconduct. A senior manager for Plantronics Inc. instructed employees to delete e-mails and deleted messages from his own account. After the establishment of a litigation hold, the senior manager deleted as many as 90,000 unrecoverable e-mails, of which 6.5% were estimated to be responsive.

The court imposed sanctions on Plantronics, including the fees and costs incurred for bringing the motion, $3 million in punitive damages, possible evidentiary sanctions to be determined at a later date, and an adverse inference jury instruction, according to *Legaltech News*.

The court said that although Plantronics may have taken reasonable, and even extensive, steps to preserve documents, the organization was still responsible for the failure of one of its managers to follow preservation procedures. The court said the senior manager's actions were the opposite of reasonable and were inexcusable, even though he believed that IT personnel would continue to have access to his deleted e-mails.

Further, the court made a finding of bad faith on the part of the senior manager and Plantronics. The court also found that the deleted e-mails and deprivation of discovery caused prejudice to the plaintiff, a point which Plantronics failed to disprove in its argument.

Chief Judge Leonard Stark noted in his decision that the behavior of Plantronics' senior manager requires a "perverse interpretation" of Rule 37(e), a finding that might place a strict precedent for those who choose to participate in evidence spoliation.

INFO SECURITY

Canada's Police Chiefs Want Access to Encryption Keys, Passwords

At its annual conference in Ottawa, the Canadian Association of Chiefs of Police adopted a resolution seeking "a legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement."

According to the resolution, Internet and computer-related crime threatens the privacy and security interests of Canadian citizens, and law enforcement authorities have been unable to complete investigations of serious criminal activity as a result of their inability to execute judicially authorized services of electronic devices. The resolution contends that legislative authority to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device is needed to support legitimate law enforcement interests.

"Canadian police are fighting an uphill battle," wrote cybersecurity analyst Eric Jacksch in an online column for IT in *Canadaonline*. "Their recent request for new legislation to compel people to disclose passwords and encryption keys demonstrates both desperation and lack of cybersecurity savvy."

Jacksch contends the authority could be rendered ineffective by technical controls, and it "could be used to bully those who cannot afford legal representation and appeals into allowing police to rifle through their digital lives at an unprecedented level."

He added that it "seems highly unlikely" that the Canadian government could draft a law to force people to disclose passwords and encryption keys without violating their constitutional rights.

REGULATORY ACTION

Utility Fined $25.6 Million for Recordkeeping Violations

California regulators hit PG&E with a $25.6 million fine for many recordkeeping violations that resulted in the San Bruno natural gas explosion that killed eight people in 2010.

The state Public Utilities Commission (PUC) voted unanimously to punish the utility for failing to keep accurate records on its aging natural gas pipeline system, the *East Bay Times* reported.

In June, PUC Administrative Law Judge Maribeth Bushey noted that PG&E was guilty of widespread deficiencies in its recordkeeping.

"These inaccurate records were relied on for locating and marking underground facilities in anticipation of excavation," Bushey wrote in the proposed ruling. "The inaccurately mapped and consequently inaccurately marked facilities led to excavators damaging the distribution system in several instances."

Six incidents, from September 2010 to March 2014, prompted regulators to open a formal probe into PG&E's recordkeeping. Most of the incidents resulted in leaks and service interruptions. In one incident, natural gas leaked into an empty home that eventually blew up.

A National Transportation Safety Board (NTSB) investigation concluded that PG&E's recordkeeping played a major role in the 2010 San Bruno explosion, in which eight people died and dozens of homes were destroyed. The NTSB determined that inadequate pipeline maintenance by PG&E and lazy oversight by the PUC were also key contributors to the explosion.

In April 2015, the PUC fined PG&E $1.6 billion for causing the San Bruno disaster, the largest financial punishment ever levied on an American utility. In August 2016, a federal jury found PG&E guilty of six felony charges, including five violations of U.S. pipeline safety rules before the San Bruno blast and one count of obstructing the government's investigation.

CLOUD

10 Tips for Effective Cloud Service Agreements

Legal experts in a *LegalTech News* article recommend 10 best practices for those who negotiate and write cloud service agreements:

1. Require service providers to comply with all applicable privacy and data security laws, regulations, and industry standards.
2. Identify a minimum standard of care for privacy and data security to meet the organization's particular needs, and require service providers to meet it.
3. Allow cloud providers to access the organization's IT systems and use its data only as required to perform the agreed-on services or as authorized for other purposes.
4. Restrict cloud providers from disclosing the organization's data to third parties except as specifically authorized. Address how the provider will handle any data requests from government authorities.
5. Require cloud providers to impose the same privacy and data security mandates on their subcontractors and to monitor them to ensure compliance.
6. Include privacy and data security performance expectations and measures in service level agreements, including timeframes for addressing risks and reporting security incidents.
7. Require cloud providers to return or destroy, at the organization's request, all copies of the organization's data when the service agreement ends.
8. Define specific security incident reporting and response requirements, including timeframes, cost allocation, and responsibilities for handling data breaches and any ensuing liabilities.
9. Obtain the right to audit or otherwise regularly assess and review the cloud provider's privacy and data security practices using common assessment methods, such as direct audits, vendor self-assessments, and independent third-party audits, assessments, or certifications.
10. Address risk allocation, especially if a security incident occurs. Service agreements should cover responsibility and cost allocation for regulatory penalties or other liabilities if service providers fail to meet privacy and data security requirements. Also consider requiring cloud providers to maintain cyber insurance coverage.

CYBERSECURITY

Yahoo Says Hackers Stole Data on 500 Million Users in 2014

Experts have called it the biggest data breach to date. At least 500 million Yahoo users' account information was stolen by hackers in 2014.

In a statement, Yahoo said user information – including names, e-mail addresses, telephone numbers, birth dates, encrypted passwords, and, in some cases, security questions – was compromised in 2014 by what it believes was a "state-sponsored actor."

According to the *New York Times*, Yahoo is one of the Internet's busiest sites, with one billion monthly users and one of the oldest free e-mail services. Many users have built their digital identities around it, from bank accounts to photo albums and even medical data.

"The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family," said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground web.

"This is one of the biggest breaches of people's privacy and very far-reaching."

Upon discovering the breach – two years after it occurred – Yahoo instructed users to change their passwords and stay vigilant over their other online accounts. Yahoo said it was working with law enforcement agencies in their investigations.

Yahoo said it learned of the data breach this summer after hackers posted to underground forums and online marketplaces what they claimed was stolen Yahoo data, the *Times* reported. A Yahoo security team eventually found the breach.

According to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify such an attack is 191 days, and the average time to contain a breach is 58 days after discovery.

Security experts told the *Times* that the breach could result in class-action lawsuits on top of other costs. An annual report by the Ponemon Institute released in July found that remediating a data breach costs $221 per stolen record. In Yahoo's case, that would total more than $4.8 billion – the price Verizon Communications is purchasing Yahoo for. The *Times* said it was not clear how the breach would affect the acquisition.

Sen. Mark R. Warner, a Democrat from Virginia and former technology executive, issued a statement that said the "seriousness of this breach at Yahoo is huge."

He has called for a federal "breach notification standard" to replace data notification laws that vary by state. Warner added that he was "most troubled" that the public was only learning of the incident two years after it happened.

END