Information Management
©2017 ARMA International, *www.arma.org*

INFO SECURITY

Majority of Consumers Don't Believe Brands Will Protect Their Data

A study conducted by Gigya found that 68% of consumers do not trust brands to protect their personal data. The study, "2017 State of Consumer Privacy and Trust," also found that 69% worry about security and privacy risks posed by Internet of Things devices, including fitness trackers, smart watches, and connected cars.

Gigya, a customer identity and access management company, polled some 4,000 consumers on their views of personal data privacy and security.

"For brands, the findings highlight an impending crisis as they balance customer expectations and new privacy requirements with their need for customer data to deliver a more personalized online experience," the study said.

Among the other findings of the study:

- 67% of consumers believe that data security policies are not improving.
- 63% of consumers believe that protecting their own data privacy is primarily their responsibility rather than that of brands or government administrators.
- 62% took direct action to better protect their data security when a brand is breached by changing their passwords, while 32% added a second factor of authentication, and another 18% closed their account entirely.

The report also noted that the pending General Data Protection Regulation (GDPR), to be enacted next May, will likely exacerbate the problem of consumer trust: "brands will then face new hurdles in presenting and protecting their European customers' data."

PRIVACY

New Data Privacy Laws Are Launching in Asia in 2017

For several months the General Data Protection Regulation (GDPR) has soaked up a lot of ink, but it won't be in effect until May. Meanwhile, many e-discovery professionals are uninformed about new similar changes in Asia, according to an article on *LegalTechNews.com.*

In Japan, for instance, the Act on the Protection of Personal Information (APPI) was amended to address such common factors as the explosion in the volume of data, the risk in data breaches, and the illegal sale of private data.

The amendments took effect May 30; Japanese authorities expect all companies to follow them.

In part, the new provisions of the APPI create a Personal Information Protection Commission that will be independent and have enforcement power. Also new are the information classifications of *sensitive* and *anonymized*. Sensitive information (about a person's race, creed, social status, medical history, and so on) merits enhanced regulatory protection; anonymized data can be transmitted with restrictions but without the individual's consent. And, for the first time, any company transferring personal records beyond Japan will need the individual's consent.

In June, the People's Republic of China enacted its controversial Cybersecurity Law. Whereas Japan focuses on protecting data, China focuses more so on the network operators who manage data, according to the article.

In part, the new law insists that Chinese citizens' personal information and important data must be stored on servers within its borders. It also strengthens existing data privacy guidelines by saying network operators must obtain their customers' consent before collecting and disclosing personal data. Further, all network providers must pass a network security exam that includes requirements they must follow when buying network systems.

DIGITAL PRESERVATION

Archivists and Volunteers Rush to Preserve Videotapes

As reported on NPR's "All Things Considered," a group calling itself XFR Collective – composed of professional archivists, volunteers, and even children – is working to digitize as many videotapes as possible before the tapes succumb to the "magnetic media crisis" and are no longer viewable.

The collective on its home page describes itself as a "non-profit organization that partners with artists, activists, individuals, and groups to lower the barriers to preserving at-risk audiovisual media – especially unseen, unheard, or marginalized works – by providing low-cost digitization services and fostering a community of support for archiving and access through education, research, and cultural engagement."

With videotapes, as described in the NPR report, sounds and images are magnetized onto strips of tape, using the same principle as when you rub a piece of metal with a magnet and it retains that magnetism. But when you take the magnet away, the piece of metal slowly loses its magnetism. In the same way, the videotape slowly loses its magnetic properties.

"Once that magnetic field that's been imprinted into that tape has kind of faded too much, you won't be able to recover it back off the tape after a long period of time," says Howard Lukk, director of standards at the Society of Motion Picture and Television Engineers.

Most tapes were recorded in the 1980s and '90s, when video cameras first became widely available to Americans. That means even the best-kept tapes will eventually be unwatchable.

Lukk estimates there are billions of tapes sitting around. There are plenty of services out there to digitize tapes – local stores, online services, even public libraries and universities. Some services are free; some cost a lot of money.

Of course, digitizing the tapes doesn't guarantee they will be saved forever. Digital has its own problems, and Lukk says that some film preservationists argue we should be looking back to before magnetic media for stable preservation – many Hollywood films, for instance, are often stored on film in salt mines, where they can last a hundred years.

PRIVACY

Oregon Amends Law to Reinforce Importance of Following Privacy Policies

Oregon Governor Kate Brown recently signed into law H.B. 2090, which updates the state's Unlawful Trade Practices Act by holding companies liable for misrepresentations on their websites or in their consumer agreements about how they will use, disclose, collect, maintain, delete, or dispose of consumer information.

In a media release, the Oregon's attorney general, Ellen F. Rosenblum, praised the update, saying, "This new law does something very simple but important: If a business tells you it's privacy policy is going to treat your online information a certain way – and then it doesn't comply with what it told you – it's in violation of the Oregon consumer protection laws. We are living in an era where companies are happy to give out our personal data for the right price, and some are even completely disregarding their own online privacy policies."

PRIVACY

Expanded Guidance 'Highlights the Pitfalls' of Social Media Checks

DataGuidance.com reports that the Office of the Privacy Commissioner of British Columbia (OIPC) recently released guidance on conducting social media background checks of prospective employees, volunteers, and candidates. The release updates the guidance published in 2011 to help organizations collect and use information gleaned from such checks while complying with British Columbia's Personal Information Protection Act 2003 (PIPA).

Under PIPA, employers can use data collected without the individual's consent for certain employment purposes. The new guidance urges employers to identify the proper legal grounds for the collection of such data, assess the purposes of its collection and use, determine the categories of information collected, and identify any risks from actions that stem from inaccurate information.

Attorney Steve Winder told *DataGuidance* that some employers conduct ad hoc Internet searches on applicants because it's a simple way to screen them. "In many cases, they are unaware that they are collecting and using information that is subject to privacy laws, or mistakenly think that an applicant's consent makes these searches reasonable and permissible. The Guidance attempts to educate employers on these issues, and highlight the pitfalls of such searches and the risk of violating privacy laws," he said. "[A]n employer should conduct a Privacy Impact Assessment and consider, among other things, whether there are less intrusive means to obtain the same information. If there are, then in most cases social media searches on a potential candidate would not be considered reasonable."

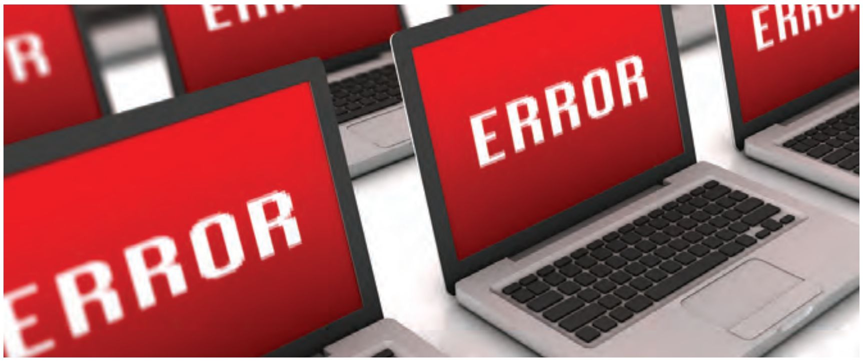
DIGITAL PRESERVATION

9 in 10 UK Directors Think Their Corporate Data Won't be Readable

Information-Age.com reports that more than 90% of company directors in Great Britain fear their crucial corporate information won't be readable in the future, according to a study commissioned by Crown Records Management, a global information management firm.

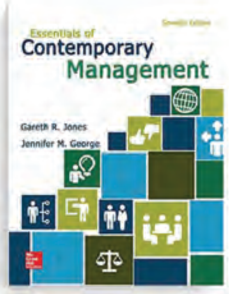
The survey also showed that nearly three in five IT decision makers believe it's vital to keep corporate records secure for more than 50 years. But only 35% said they regularly review the formats that hold their electronic data. Nearly a fifth of the IT executives said they have no systems to preserve electronic information stored for more than five years.

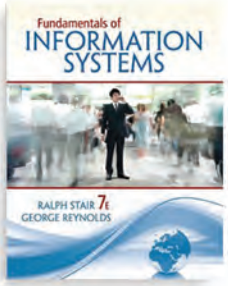
According to Dominic Johnstone of Crown Records Management, "Long-term digital preservation hasn't made big headlines so far but many companies may be in for a shock because the reality is that any information which is ten years old or more is seriously at risk. The speed at which software and hardware evolves is forcing old formats to quickly become obsolete and there is no guarantee they will be readable in future."

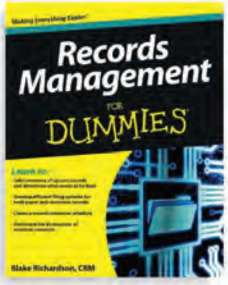


Files produced in Word Perfect or Lotus 123 are already in real danger of becoming unreadable soon, as are movie clips and photographs stored in the .MOV format and information on floppy disks.

Many companies might believe their information stored in the cloud is safe from such degradation, but Johnstone voices a warning: "It's not surprising that cloud storage is so popular – it's a relatively cheap and safe way to store information. But if the attached systems are not upgraded regularly and there is no lifecycle management in place there really is no guarantee all that information can be accessed and read when you really need it."







DIGITAL PRESERVATION

Is it Economical to Digitize Records? Illinois Seeks the Answer

Illinois lawmakers are critical of the state's costs for warehousing documents, according to a report on the *State Journal-Register's* site. But some experts say digitizing those documents may not be more economical.

Illinois law requires state agencies to maintain an essential records preservation program, but the statute doesn't dictate where the records should be stored. Ilinois is moving to digitize documents where it can. Gov. Bruce Rauner's new Illinois Department of Innovation & Technology (DoIT) is helping other departments do so.

Gary Dunn, records management officer at Southern Illinois University-Edwardsville, says digitizing records is not as simple as putting them into a scanner. The process can take years and requires periodic reviews to make sure the storage system is not degrading. Further, according to Dunn, the digitizing process can be expensive because more staff is needed to manage those digital documents.

"If you have a record that has to be maintained for 65 years, how many times are you going to have to (manage) that particular record?" he asks. "[Y]ou'll have to have an IT force in order to manage those records. I can't imagine the cost of everything that would go into that."

Sen. Tom Cullerton, D-Villa Park, who has been critical of the administration's handling of warehouse space, said the state should find the most efficient ways to store documents.

"The key is if you're going to spend $2.4 million just to rent and hold documents (at the Springfield warehouse), you're going to do that forever. At some point, if you're going to spend all this money to upgrade our systems, why wouldn't you take a little bit of that to make sure that we get rid of five or six warehouses that cost the state $2.4 million?" he said. "Wouldn't that cover the man hours it would cost to do it? I think technology is adapting well enough that as we continue to keep upgrading our systems, it would keep updating our data and archives as well."

Johnny Hadlock, executive director at the National Association of Government Archives & Records Administrators (NAGARA), said renting warehouses may be the most cost-effective way to store state documents.

"What the public may view as a waste of money by renting warehouses, may in fact be a cheaper option when compared to the expense and labor required to digitize everything." Hadlock said in a written statement.

CYBERSECURITY

UK Cybersecurity Expert Says Security Must Fit What People Do

Professor Angela Sasse, a director at the UK Research Institute in Science of Cyber Security, said good security is not so much about policies because a lot of security policies are counterproductive if they "do not work for people." The remarks were delivered at Infosecurity Europe 2017 and reported by *Infosecurity-Magazine.com.*

As a result, Sasse claimed it's time to stop thinking that the individual is the weakest link in security. She offered a three-step guide to getting security to work more effectively for people:

1. Accept that security is not the top priority for most end users. Accept also that it's the security experts' responsibility to design plans that fit with individuals' tasks and the business processes.
2. Make security communications NEAT: Necessary, Explained, Actionable, and Tested.
3. Realize that awareness and education alone are not the answers. There is no cure for a lack of "security hygiene" with unworkable policies or useless tools.

"What you want," she told the audience, "is a change in undesirable behaviors – this is neither a quick nor cheap option, and it's not a job for amateurs."

MOBILE DEVICES

Proliferation of BYOD Leads to E-Discovery Headaches

LegalTechNews.com recently reported on a 2017 study that emphasizes how the explosion in mobile devices in the workplace is problematic for corporate attorneys and e-discovery professionals.

The "2017 Executive Enterprise Mobility Report," by CITO Research and Apperian, queried more than 100 corporate managers and executives across 10 industries who manage mobile devices. More than half (57%) of respondents said they were most concerned about organizational data ending up on employee-owned mobile devices, as compared to 44% a year earlier. Roughly half of the executives cited mobile-based cybersecurity threats as a key concern, owing to the likelihood the devices are not protected against leaks. For 55%, the top challenge facing a data program was managing different mobile operating systems.

Mark Lorion, president of mobile app management firm Apperian, said the study suggests the challenges are becoming more pronounced. "[While] in years past it seems that the enterprise mobility projects were smaller-scale internal projects, this year, companies are hoping to roll out enterprise apps to much larger populations of users," he said.

Many organizations are allowing more mobile devices in the workplace in an effort to improve productivity, but Lorion suggests they're often failing to address legal and technical challenges that may occur when there's a need to acquire information from those devices.

Daniel Garrie of ZEK's cybersecurity practice believes employees will often be reluctant to give up their personal devices because they contain private information alongside corporate data.

Usually companies have agreements that allow full access to the employees' work devices. Adi Elliott of Epiq told *LegalTechNews* that "if you have a BYOD [bring your own device] policy and you are connecting [your phone] to the corporate network, and you sign something that said generally the corporation has access to it, people don't question that."

But discovering information on mobile devices, for example, is not as straightforward as it is from an e-mail server.

Lorion believes organizations can avoid many e-discovery barriers by limiting how corporate data can be accessed and stored on mobile devices. Solutions, he said, would "containerize" corporate data within a device and thus give IT "visibility and control over that content, even when it goes to a personal device."

PRIVACY

Alberta Privacy Chief Seeks Overhaul of Province's Privacy Law

As recently reported on *CalgarySun.com*, Alberta Privacy Commissioner Jilly Clayton says the wording of a major privacy law is hampering the efforts of her office to get information from the government in order to fulfill requests. She says many information requests from opposition parties, the media, and the public have been stymied, going back to 2012.

Clayton says the obstruction was the subject of a recent Supreme Court ruling that found the problem is with the wording of Alberta's Freedom of Information and Protection of Privacy law.

In April, her office tabled two reports in the legislature outlining the problems, including a request to change the law to make it effective.

"What should have been a relatively straightforward investigation has concluded under a shadow that brings the very notion of independent oversight of the executive branch of government into question and has the potential to erode public confidence in an open and accountable government," she said.

The commission says her office should have the authority to require the government to give it the records it requests and to determine if they are protected by legal privilege. She says the law must be updated so the public can get data in an affordable, timely way to keep the government accountable.

"Access to information is of fundamental importance to democracy and citizens participating in democracy. Citizens have a right to know what information the government has about them," she said.

E-MAIL MANAGEMENT

NARA Publishes First Round of Agencies' E-mail Records Reporting

As reported on *FederalNewsRadio.com,* the National Archives and Records Administration (NARA) recently published federal agency records management reports, including reports on how agencies manage their e-mails.

"Overall, at this point, the results are trending positive," said Laurence Brewer, chief records officer for the federal government. "Most agencies have taken action, but there is still a ways to go in many areas, including policy promulgation, systems implementation, and — important for NARA — transferring email to our agency for permanent preservation."

President Obama's 2011 directive on managing government records set forth certain requirements for the management of e-mail as records:

"Email records must be retained in an appropriate electronic system that supports records management and litigation requirements (which may include preservation-in-place models), including the capability to identify, retrieve and retain the records for as long as they are needed. Beginning one year after issuance of this directive, each agency must report annually to [the Office of Management and Budget] and NARA the status of its progress toward this goal."

In their reports, federal agencies answered questions on usability and retrievability of e-mails, establishment of retention schedules, categorization of e-mails, and the general state of their e-mail policies.

The maximum number of points for these four questions is 16. NARA achieved a top score because, according to its records officer, e-mails are easily and fully retrievable for requests, and employees are trained to manage them.

Agencies also received a maturity model score that determined whether the agency is at low, moderate, or high risk for not managing e-mail effectively.

Immigrations and Customs Enforcement (ICE), for one, received a score that indicated it has a high risk of not managing e-mail effectively. ICE claimed the questions "were poorly worded and did not allow for a proper response, forcing us to answer inaccurately regarding our agency's email management efforts."

The full agency reports can be viewed at *http://tinyurl.com/y7ktyz9b.*

ARMA INTERNATIONAL®

Take Our Latest Two-Minute *IM* Poll

We'd like to know what technology tools your organizations is using to manage its information assets. Please take two minutes to respond to our poll at ***http://imm.exploreamra.org/InfoTechTools.***

Read the article on page 22 that prompted this survey.

May/June 2017 IM poll respondents (347) said their information programs:

- Are valued by executive-level staff **(60.2%)**
- Have executive support in word and by example **(42%)**
- Get increased funding routinely when justified **(10.8%)**

Take or see results for previous polls at ***http://imm.explorearma.org/RIM_Polls.***

GOVERNMENT RECORDS

ND Attorney Scolds State Division for Deleting Staff E-mails

The Bismarck Tribune reports that last year nearly 39,000 employee e-mails from the State Oil and Gas Division were deleted improperly upon executive guidance to "remove unnecessary e-mails."

Bismarck, North Dakota, attorney Derrick Braaten said the division may have committed a Class C felony for destroying public records in May 2016, as instructed by Lynn Helms, executive director of the Department of Mineral Resources.

Acting on a tip, Braaten reportedly filed an open records request and learned the e-mails were deleted from staff inboxes and computer trash folders over a two-week period; about 7,000 of those messages were purged in a third, more technical, process.

The IT department was able to restore all messages and provide them to Braaten over the course of several months.

According to Braaten, the review suggests the agency was permanently destroying records that included inter-agency communications, reports and photos of oil spills from emergency managers and landowners, and reports of discrepancies in gas flaring data. The division's $8,900 fee for delivery of the e-mails was paid by oil patch landowners who were concerned about the loss of such records.

The attorney said the division was never able to turn over a document retention policy, leading him to believe the agency had none. In a statement, department spokeswoman Alison Ritter said the data within the e-mails is subject to state retention procedures and the department follows those procedures. She provided the *Tribune* with retention protocol for 112 records generated by the department, including e-mails. Ritter did not provide an explanation for why so many e-mails were deleted within the two-week timeframe.

Braaten said the lack of clarity makes it necessary that the Oil and Gas Division undergo a performance audit.

"Personally, what bothers me more are reports of documents being destroyed and misreporting of oil and gas numbers. I don't know why there's such resistance to an audit. We spent thousands of dollars to find out what's going on. You'd think Oil and Gas would want an audit," he said.

GOVERNMENT RECORDS

NM Clerk Uncovers Records on Death of Billy the Kid's Killer

USNews.com recently reported that an historic, century-old document was found inside a box of unarchived records during a preservation effort in a southern New Mexico county.

Found was a 1908 handwritten coroner's jury report concerning the probe into the death of Pat Garrett, who for a time served as sheriff in Lincoln and Dona Ana counties. Garrett had gained fame for killing the infamous outlaw Billy the Kid.

Signed by justices of the peace and coroners, the document says Garrett was reported dead in Dona Ana County in the territory of New Mexico about five miles northeast of Las Cruces. The document says "the deceased came to his death by gunshot wounds inflicted by one Wayne Brazel."

Some historians have said the single witness to the shooting never testified, and records show Brazel was acquitted after a one-day trial in which his attorney argued self-defense.

The document was found by Angelica Valenzuela, the records and filing supervisor with the county clerk's office, as part of a preservation effort that involved records spanning the last half of the 1800s through the mid-1960s.

"She knew as soon as she saw it that it was worth gold," county spokesman Jess Williams said of the signed jury report.

Touting this historic discovery, the county is seeking additional funding for its work to preserve historical records and make them more accessible.

Conversations and content at ARMA LIVE! 2017 will change the trajectory of the industry – and your career – for years to come.

And you will want to be a part of it!

Save $200 with Early Bird Registration! Deadline is August 25, 2017.

Special Thanks to Our Sponsors:

Access Information Protected. · docfinity · Hewlett Packard Enterprise · IBM · Iron Mountain · RecordPoint · VRC · ZASIO · ZLTECH

ARMA LIVE! 2017 Highlights (and there's so much more!)

KEYNOTE SPEAKERS

Jake Porway
Founder/Executive Director
DataKind™

Porway is a machine-learning and technology enthusiast who loves seeing good values in data. He founded DataKind™ in the hopes of creating a world in which every social organization has access to data capacity to better serve humanity. He was most recently the data scientist in the *New York Times* R&D lab and remains an active member of the data science community. He holds a B.S. in computer science from Columbia University and an M.S. and Ph.D. in statistics from UCLA.

Tim Callahan
CISO/Senior VP,
Global Security, Aflac

Callahan oversees Aflac's technology risk management, information asset protection, information security, threat and vulnerability management, and more.Earlier, as an executive at SunTrust Bank, he developed a unified approach to determining threats, developing mitigation strategies, and managing incidents. Callahan, a military veteran, was also the program manager for a command risk management function at a U.S. Air Force major command headquarters.

EDUCATION

Designation Academy

The sessions are half-day, one-day, or two-day programs that take place prior to conference, during the ARMA 2017 Designation Academy. They provide a unique opportunity for in-depth study of the latest topics in specialized fields related to RIM and IG. (Additional registration and fees are required.)

ICRM Exams Prep: Introduction and Parts 1-6 (ICRM)

Implementing IG: The Ins, Outs, Ups, and Downs of Program Development

Unvexing the Challenges of Shared Drives

Retention Program Development Certificate (ARMA)

Automating Electronic Records Management with Rules-Based Recordkeeping

Becoming a Certified Information Governance Professional

ARMA Flipped! Sessions

The flipped sessions consist of four practical web seminars with live text chat, SMEs, and solution providers in a virtual exhibit hall. Part one provides the content instruction in an online virtual conference on August 29, which you can attend from your home or office. Part two provides hands-on application of the online instruction in a follow-up, face-to-face workshop at the ARMA Live! 2017 conference. You must take part in the online virtual conference if you wish to participate in the ARMA Flipped! onsite workshops.

Anyone with a full conference registration is automatically registered for ARMA Flipped!

ARMA LIVE! EXPO

See the industry's emerging technologies presented by more than 100 exhibitors. Explore the top solutions in content management, e-discovery, cloud computing, e-mail management, archiving, and much, much more.

ARMA LIVE! Expo Hall includes:

FREE education sessions in the Expo Hall

FREE guidance at the Consultants Corner

FREE product demonstrations

FREE beverages during break times

FREE pub crawl in the Expo Hall Monday evening

WIN PRIZES! Register at selected vendor booths.

WIN CASH! Participate in the Big Money Giveaway game for the chance to win a cash prize.

Saturday Night Party

Please help us kick off the conference right! The party includes games, prizes, networking with peers, and a sneak peek of the Expo Hall. Your attendance is included with all registration options.

Agents of Change
ARMA LIVE! ORLANDO

OCTOBER 15-17 | MARRIOTT WORLD CENTER | ORLANDO, FL

Register now! ***conference.explorearma.org***

PRIVACY

HHS Settlement Shows the Risk of Not Understanding HIPAA

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI).

CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to the OCR that a workforce member's laptop was stolen from a vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's probe into the disclosure revealed that CardioNet had insufficient risk analysis and risk management processes at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania–based organization was unable to produce any final policies or procedures on the implementation of safeguards for ePHI, including those for mobile devices.

"Mobile devices in the health care sector remain particularly vulnerable to theft and loss," said Roger Severino, OCR director. "Failure to implement mobile device security by Covered Entities and Business Associates puts individuals' sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected."

The Resolution Agreement and Corrective Action Plan may be found on the OCR website at *http://tinyurl.com/ycarfd5d.*

CLOUD

Cloud Providers Serving India Government Must Store Data Locally

To help ensure that data is properly protected, India's Ministry of Electronics and Information Technology (MeitY) has mandated that all cloud service providers that handle government data store it on servers in India, as reported on *BankInfoSecurity.asia*.

The guidelines say cloud service providers' contracts with the government must state that all services and data will be guaranteed to reside in India. Additionally, cloud vendors' contracts must include details on the location of the data they're processing, storing, or hosting for the government.

To date, most cloud vendors have hosted websites and servers outside of India because they perceive there are cost advantages and business continuity benefits.

Experts believe the new guidelines are meant to keep data within India so that it's easier to take security and legal action in case of cyberattacks.

"The new guidelines will have a positive impact on the cloud service providers who can now take advantage of data localization and seek the government's support on any legal implications it might face," says Prashant Mali, a Mumbai-based attorney and international cybersecurity expert.

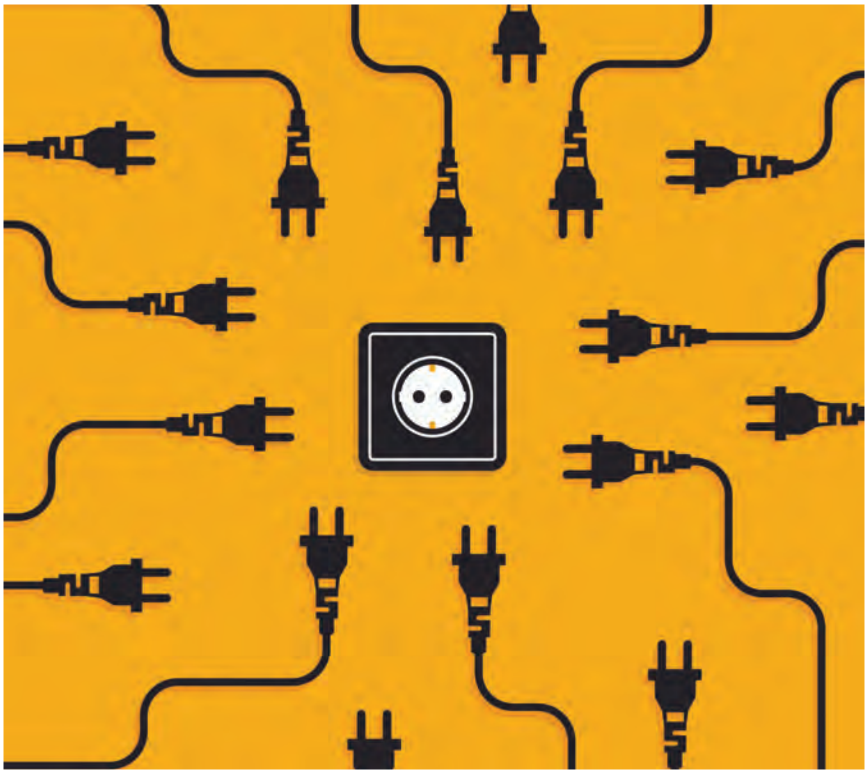
The mandate means that cloud providers must invest in infrastructure to store critical data and secure legacy applications.

In taking action to ensure data security, the government must look beyond entering contracts with the lowest-cost cloud services provider, one industry professional says.

"More often than not, lowest price is the criteria for purchase, impacting the quality of design, solution and services - which is not good for critical initiatives involving sensitive data," says S. Sriram, co-founder of a managed services provider.

CYBERSECURITY

Ukraine's Power Grid Attack a Possible Test Run



Was December's temporary shut-down of Ukraine's power grid a test run for attacks on other nations?

In June, cybersecurity firms Dragos and ESET sounded the alarm on what they described as the first ever malware designed specifically to attack the electric grid at scale. As reported on DarkReading.com, a threat group calling itself ELECTRUM used the malware – dubbed CrashOverride and Industroyer by the vendors – in an attack against Ukraine's power grid in December, resulting in areas of Kiev losing power for an hour.

The malware doesn't target any specific technology and doesn't leverage any specific vulnerability. Instead, it's designed to map, target, and attack grids by taking advantage of certain communication protocols. The malware uses the protocols in the manner they're designed for, which effectively counters the usual defensive measures, such as patching and other perimeter tools.

"The purpose for the malware is clear; cybersabotage, without a doubt," says Robert Lipovsky of ESET.

There's uncertainty about what the crybercrooks were hoping to accomplish with the Ukraine attacks; Lipovsky does believe the high levels of sophistication and the low impact suggest it was a test run for something larger.

"The potential impact of this threat is much greater, as the communication protocols and targeted hardware are used in critical infrastructure worldwide," he says.

Because the malware is not specific to vendors or configurations, it can be easily repurposed as a weapon against virtually any electric grid around the world.

"The most significant aspect about CrashOverride is that it is vendor-independent," says Sergio Caltagirone, director of threat intelligence at Dragos. "We are not saying everyone is going to get attacked. But this is a significant advancement in capabilities to attack power grids."

SECURITY

SIA Establishes Public Safety Working Group

TThe Security Industry Association (SIA) recently announced it had established the SIA Public Safety Working Group, to be chaired by Steve Surfaro of Axis Communications.

The group will recommend ways to improve the safety, security, and sustainability of cities and communities using technology, said SIA CEO Don Erickson.

SIA created the working group to focus on topics such as autonomous systems, unmanned vehicles, city surveillance, video analytics, body-worn cameras, and much more.

The SIA is a trade association for global security solution providers.

PRIVACY

Privacy Advocates Troubled by Spy Center's Use of Personal Data

According to *TheGlobeandMail.com,* an obscure center run by Canada's spy agency has long been using personal details gleaned from security clearance forms to help with national security probes.

In April, security experts said newly disclosed letters from within the Canadian Security Intelligence Service's (CSIS) Operational Data Analysis Centre stress the need for safeguards to rein in digital sleuthing.

The correspondence indicates that for at least five years the center has used private information that was provided during security assessments for employment and immigration purposes – applying it to efforts to combat terrorism and espionage.

The analysis centre became a focus of intense public concern last November when a federal judge said CSIS violated the law by keeping electronic data trails about people who were not actually under investigation.

The screening program helps the government prevent newcomers who pose a threat from entering Canada and acquiring legal status. It is also intended to ensure that people of security concern do not gain access to classified information, sensitive sites, or major events.

A 2011 privacy commissioner letter said that people should be told the data they provide to CSIS may be used "for purposes beyond the provision of security assessment services."

In November 2012, CSIS told the commissioner's office that while the data analysis center was using assessment data to help with security probes, existing measures addressed the privacy watchdog's concerns.

The intelligence service noted that people who need a federal security clearance must complete a screening form that says their personal information will be stored in a CSIS personal information bank. A publicly available description of that bank says the data may be used for data-matching or for the purpose of conducting lawful investigations, the CSIS letter added.

PRIVACY

Joint Review of Privacy Shield Set for September

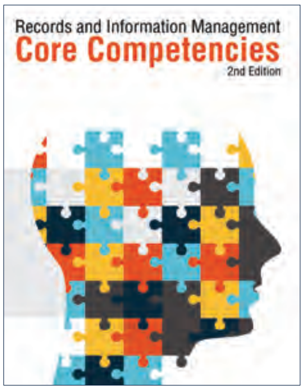
In September, a joint review of the EU-U.S. Privacy Shield will have the primary objective of monitoring the U.S. administration's work and steering the debate to prevent privacy safeguards from deteriorating, according to a recent report on the Hunton Privacy Blog.

According to the site, the review, to be held in Washington, will focus on two key points 1) the EU Commission will verify that the foundations of the Privacy Shield remain in place, in particular with respect to government access for national security reasons; and 2) the Commission will focus on the day-to-day implementation and robust follow-up of the Privacy Shield by companies that have self-certified.

Recently the European Parliament passed a resolution on the adequacy of the protection that's afforded by the Privacy Shield, highlighting these weaknesses to be fixed in the upcoming review: the lack of specific rules on automated decisions, the lack of a general right to object, the need for stricter guarantees on the independence and powers of the ombudsperson mechanism, and the lack of concrete assurances with respect to bulk collection of data.

Following the annual review, the EU Commission will issue a public report to the European Parliament and the Council.

Free to **ARMA Members!**

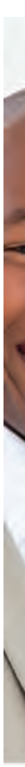


Records and Information Management
Core Competencies
2nd Edition

Download your free copy of ***Records and Information Management Core Competencies, 2nd Edition*** today at ***www.arma.org/go/prod/V5934.***

Not a Member? You should be. **Join Today!**

Invest in yourself by joining the thousands of ARMA members who are boosting their careers with the help of our education, events, publications, and more. Your small investment will pay for itself several times over when you take advantage of just a fraction of the benefits that membership offers. To find out more, visit ***www.arma.org/r1/membership/membership-benefits.***



INFO SECURITY

CQC to Fortify NHS Information Governance Inspections

Britain's Care Quality Commission (CQC) plans to beef up its own information governance assessments of National Health Service (NHS) hospitals, beginning this summer, as reported by *Healthcare.GovernmentComputing.com.* While the new inspection regime is not directly related to the May WannaCry intrusion, which affected some NHS trusts, inspectors are likely to scrutinize many aspects of NHS IT.

Even before the WannaCry exploit, the CQC was consulting on proposals for its future regulation of NHS hospitals, with the proposals planning to introduce a new "key line of enquiry" for inspectors to use to look more closely at "whether robust and appropriate information is being effectively processed and challenged."

Earlier, the CQC released "Safe Data Safe Care," a report on amendments to its inspection process to ensure "appropriate internal and external validation against the new data security standards have been carried out."

The report chronicles the review of 60 hospitals and medical practices to see whether personal health and care data is being used safely and is being protected appropriately. The CQC review focuses on patient data in the NHS and does not include providers of adult social care; nor does it examine IT systems.

The CQC review finds that while there is "evident widespread commitment to data security," staff at all levels face significant challenges in translating their commitment into reliable practice.

Included among the several issues the report finds are these:

- Lessons from data incidents are seldom learned or shared.
- The quality of training on data security varies greatly at all levels.
- Day-to-day practices often do not reflect the established policies and procedures.
- Data security tools and protocols are not user-friendly, which tempts the staff to find risky workarounds.

A CQC spokesperson said she expects providers to have robust arrangements for identifying and managing risk to their services: "We do look at this on inspection and as part our ongoing monitoring of services. Where an inspection finds concerns in those areas we would report our findings and require the provider to take appropriate action. Any extension to this remit would be a decision made by the Department of Health."

SECURITY

Archivists' Rep Speaks at PIPEDA Hearing

The Security Industry Association (SIA) recently announced it had established the SIA Public Safety Working Group, to be chaired by Steve Surfaro of Axis Communications.

On behalf of the Association of Canadian Archivists (ACA), Greg Kozak, records manager and adjunct professor, recently addressed Access to Information, Privacy and Ethics (ETHI) Committee on the ACA's views on the Personal Information Protection and Electronic Documents Act (PIPEDA).

In brief, Kozak focused on a few areas of interest in an effort to affect existing or proposed legislation concerning the life cycle of records:

1. *Trustworthiness of records.* Kozak cited factors that threaten privacy protections, including the use of visual analytics and algorithms to mine data, and the long-term management of such de-identifiers as tokenization.
2. *Preservation of records.* The ACA recommends preserving PIPEDA's mechanisms that permit private organizations to donate records containing personal information to archives for long-term preservation; allowing archival institutions falling under PIPEDA to acquire records containing personal information; and considering the implications of introducing a right to be forgotten or a right to erasure.
3. *The balance between the protection of an individual's reputation and the integrity and authenticity of the public record.* PIPEDA is already based on the principle that personal information be kept accurate, complete, and up-to-date. A wider application of this principle could rectify instances where incorrect or inaccurate personal information may result in reputational harm, reducing the need for a right to be forgotten.
4. *Cloud environment.* The ACA believes PIPEDA should make a definite statement on the issue of jurisdictional location of data of private individuals, otherwise what happens to them will be mostly decided by legal opinion rather than by clear, consistent rules. E