Information Management

INFO SECURITY

Senators to Introduce Bill to Secure Internet of Things

Reuters recently reported that a bipartisan group of U.S. senators is drafting legislation that seeks to address vulnerabilities in computing devices that belong to the Internet of things. The bill would require all government vendors that provide Internet-connected equipment to confirm their products comply with industry security standards. Additionally, the bill would ban vendors from supplying devices that have unchangeable passwords or known security vulnerabilities.

The legislation is sponsored by Cory Gardner (R-Colo.), Steve Daines (R-Mont.), Mark Warner (D-Va.), and Ron Wyden (D-Ore.). It was drafted with the help of technology experts at the Atlantic Council and Harvard University.

"We're trying to take the lightest touch possible," Warner told Reuters. He said the bill is intended to remedy an "obvious market failure" that has left device manufacturers with little incentive to build with security in mind.

The legislation would permit federal agencies to ask the U.S. Office of Management and Budget for permission to buy non-compliant devices if other controls, such as network segmentation, are in place. Further, it would expand legal protections for cyber researchers working in "good faith" to hack equipment to find vulnerabilities so manufacturers can patch previously unknown flaws.

Security experts have long said the proliferating array of online devices such as cars, appliances, speakers, and medical equipment are not adequately protected from hackers. As many as 30 billion devices are expected to be connected to the Internet by 2020, researchers estimate, with a large percentage of them insecure.

A Senate aide who helped write the bill said companion legislation in the House was expected soon.

GOVERNMENT RECORDS

Audit Criticizes IRS on Records Management Issues

Fedweek says an audit of the IRS has found areas of concern for the ways it manages and retains records. Among the issues is the agency's responses to Freedom of Information Act requests, which often cite that documents have been lost or destroyed.

According to the audit, "the IRS's ability to adequately respond to federal records requests is essential in maintaining the public's trust and ensuring transparency in government."

The audit claims the agency's e-mail retention policies are inadequate because e-mails are not archived automatically for all employees; staff are instructed to take manual actions to archive the messages by saving them on computer hard drives or network shared drives. The report says the policy has led to lost records when hard drives are destroyed or damaged.

According to *Fedweek*, IRS management has voiced agreement with the audit's recommendations for remediation, saying a new enterprise-wide e-mail system is being deployed that should help the agency comply with records management requirements.

PRESERVATION

Videographer Strives to Preserve Old Film Rolls

Our July/August edition of "Up Front" included a report on an NPR "All Things Considered" story that featured the XFR Collective, a group of professional archivists and volunteers who are digitizing as many videotapes as possible before the tapes succumb to the "magnetic media crisis" and become unviewable.

More recently, the public radio program covered a similar effort that seeks to preserve film. Featured in the report is a Boise, Idaho, man named Levi Bettwieser who scours real estate sales and vintage shops for undeveloped film and then posts his findings on a website he calls Rescued Film Project. His mission is to reunite film owners with their photos.

"I figured all the cameras had been opened and all the film was destroyed or it was too old," he says.

But he found out otherwise; Bettwieser saw that the rolls typically contained home movie fare that would be important to some people.

"And so I figured, *You know what?* I need to start finding more rolls of film to process, because there's more memories out there," he told the program.

By day he is a videographer, but in his off hours he works for the Rescued Film Project, taking undeveloped film, often from decades ago, and chronicling it in a digital archive for preservation purposes.

About 10 years ago, an engineer formerly associated with NASA began a preservation project of his own. Dennis Wingo calls it the Lunar Orbiter Image Recovery Project. His goal is to resurrect high-resolution pictures of the moon taken by the orbiter in the 1960s. To do so, he has to unlock images that have been kept on magnetic tapes that can be read only by that era's technology.

Wingo has successfully saved images of the moon that helped the Apollo missions, just as the Rescued Film Project is salvaging photos of past Christmases.

Says Bettwieser: "I love the idea of taking what are these simple moments and elevating them and putting them on a platform for people to view so that we can have these shared experiences. It makes us all realize that we all kind of do the same things and we are similar as human beings."

PRIVACY

FTC Okays Modifications to TRUSTe's COPPA Safe Harbor Program

On its website, the Federal Trade Commission (FTC) announced approval of TRUSTe's proposed modifications to its safe harbor program under the Children's Online Privacy Protection Act (COPPA).

COPPA requires operators of commercial websites and online services targeted to children under the age of 13, or general audience websites and online services that knowingly collect personal information from children, to post comprehensive privacy policies on their sites; notify parents of their information practices; and get parental consent before collecting, using, or disclosing any personal information from children under 13.

COPPA includes a safe harbor provision that permits industry groups and others to seek FTC approval of self-regulatory guidelines that use "the same or greater protections for children" as those in COPPA. Organizations that take part in an FTC-approved safe harbor program will usually be subject to the review and disciplinary procedures provided in the guidelines in lieu of formal FTC investigation and law enforcement.

In a *Federal Register* notice, the FTC had sought comment on proposed changes to TRUSTe's safe harbor program, including adding a requirement that participants conduct an annual internal assessment of third parties' collection of personal information from children on their websites. The FTC received six comments on the notice and voted 2-0 to approve the modifications to TRUSTe's safe harbor program.

FOIA

Public-Private Partnership Seeks to Strengthen FOIA Process

FCW.com reports a group of private sector officials is working with agencies to develop recommendations for improving the Freedom of Information Act (FOIA) process.

This summer, the FOIA Advisory Committee established three subcommittees, each led by a government member and a non-government member, with each group focusing on a specific frustration with the FOIA process.

The Proactive Disclosure Subcommittee seeks to handle agencies' universal releases (such as cabinet secretaries' daily schedules) and establish a universal format for disclosing FOIA logs.

The Searches Subcommittee intends to make it easier to find documents and improve communication between requesters and agencies.

The Efficiency and Resources Subcommittee is identifying agency best practices and sharing them across government. While this subcommittee is still in the information-gathering process, the other two are developing recommendations in consultation with agencies and transparency experts.

The subcommittees are expected to submit their recommendations by October 19 and finalize them by December 15, in time for a January vote.

CYBERSECURITY

Cisco Report Cites a Resurgence in Traditional Cyber Attacks

Cyber attacks have dramatically evolved and increased in magnitude of late, and they show no signs of slowing, according to Cisco's "Midyear Cybersecurity Report," published on July 20 and covered by *ITWorldCanada.com.*

Traditional attacks such as spam, spyware, adware, and ransomware are returning in high numbers and often succeeding because they are easier to implement than before and can pose a significant risk, according to the report. "Spam volumes are significantly increasing, as adversaries turn to other tried-and-true methods, like email, to distribute malware and generate revenue," the report states.

Cisco research uncovered the fact that 20% of the 300 companies it studied had been infected with spyware or adware during a four-month period. Ransomware, considered an "as a service" attack, brought in more than $1 billion dollars in 2016, Cisco reports.

The study also notes the WannaCry and Nyetya ransomware attacks foreshadow destruction-of-service attacks that could eliminate organizations' backups and safety nets, leaving them with no means to recover.

"As recent incidents like WannaCry and Nyetya illustrate, our adversaries are becoming more and more creative in how they architect their attacks," says Steve Martino, chief information security officer at Cisco, in the report. "While the majority of organizations took steps to improve security following a breach, businesses across industries are in a constant race against the attackers. Security effectiveness starts with closing the obvious gaps and making security a business priority."

The report provides several pointers on better defending against such cyberattacks:

- Use an integrated defense; limit siloed investments.
- Engage executives early to make sure they have a real understanding of the risks, rewards, and budgetary constraints.
- Use role-based training for employees rather than a one-size-fits-all approach.
- Don't "set and forget" security controls and procedures.

Take Your Career to the Next Level

Master of Archives and Records Administration

Convenient, flexible,
100% online graduate program

Built on the competencies required to become a certified archivist and a certified records manager, the Master of Archives and Records Administration online degree program at San José State University uniquely combines archival science, records management, and information governance into one comprehensive master's degree.

In this flexible 100% online program, students study the entire information lifecycle and are readied for professional positions across a broad spectrum of fields. And through a partnership with the Institute of Certified Records Managers, they can apply MARA courses for credit toward the ICRM examinations.

WESTERN ASSOCIATION OF SCHOOLS AND COLLEGES
Accrediting Commission for Schools

"Being part of the San José State University program has helped me achieve my career goals by giving me the knowledge, skills and abilities to deliver on what I've been tasked to do."

Edward Sumcad, '18 MARA
Records and Archives Manager,
Los Angeles County

100% Online · Scholarships Available · Self-Paced Program

Now accepting applications for admission!

ischool.sjsu.edu/mara

SJSU SAN JOSÉ STATE UNIVERSITY

EHR

OCR Updates Data Breach Reporting Tool

According to the *Hunton Privacy Blog*, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) recently released an updated web tool – the HIPAA Breach Reporting Tool – that highlights the latest breaches of health data.

Entities covered by the Health Insurance Portability and Accountability Act (HIPAA) are required to notify OCR when they have a data breach. OCR uses the reporting tool to publish information it gets on data breaches that affect more than 500 individuals. The tool publishes the name of the reporting entity; the number of people affected by the breach; the type of breach (e.g., hacking, IT incident, theft, loss, unauthorized access or disclosure); and the location of the breached information (e.g., laptop, paper records, desktop computer).

The new features of the reporting tool include a functionality that highlights data breaches currently under investigation and reported within the last 24 months; an archive of older data breaches; improved navigation to additional data breach information; and tips for consumers.

PRIVACY

New Jersey Shopper Privacy Bill Signed into Law

New Jersey Governor Chris Christie signed legislation that limits a retailer's ability to collect and use personal information

ascertained from driver's licenses and other ID cards in an effort to crack down on data breaches and the sale of this information to marketers, *Law360.com* reports.

As specified in the Personal Information Privacy and Protection Act, retailers can scan customer identification cards only for certain purposes, such as to verify the authenticity of the card or a consumer's identity or age. The data they can collect from the scan is limited to name, address, date of birth, the state the card was issued from, and the ID card number. Retailers also must report any breaches of this stored data in accordance with the state's notification law. They are banned from sharing the information with marketers or other parties that are unknown to the customers.

Civil penalties of $2,500 are tendered for a first offense, and $5,000 for any subsequent infractions. Further, according to the bill's language, "any person aggrieved by a violation" can bring an action in Superior Court to recover damages.

The new law takes effect on October 1.

"Consumers should not have to worry about their personal information possibly ending up in the wrong hands every time they go shopping," Assembly Democrat Joseph Lagana, a sponsor, said in a statement. "Technological advances have made it harder to protect our privacy. This law will help ensure that businesses are only scanning driver's licenses under certain circumstances and that only certain information is stored."

Take Our Latest Two-Minute *IM* Poll

In the article "What Is Past Is Prologue: What History Reveals About the Future of RIM," David O. Stephens, CRM, FAI, writes about today's top RIM challenges. Please take a moment to identify which one is your program's greatest challenge at ***http://imm.exploreamra.org/InfoTechTools.***

Read the article on page 34 that prompted this survey.

July/August IM poll respondents (11) said their organizations use:

- Records schedule and research management tools (**70%**)
- Private cloud-based services to store, manage, or process information (**50%**)
- An electronic document or content management system (**50%**)

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

PRIVACY

EU Privacy Approval Would Ensure Data Transfers to Post-Brexit UK

Bloomberg BNA reports that UK lawmakers are seeking approval from the European Union that would allow easier data transfers after Brexit is effected; otherwise, British businesses will be at a "competitive disadvantage."

After it leaves the European Union in March 2019, the United Kingdom will be treated like other non-EU countries that wish to lawfully transfer data from EU member countries. Obtaining an official European Commission finding that the UK's privacy regime is adequate to protect the privacy of EU citizens' personal data is critical to maintain effective data transfers in a digital economy, according to a July report from the House of Lords EU Committee.

The report said three-quarters of data transfers made by UK companies are with EU countries. If the government cannot secure an adequacy decision, "it could present a non-tariff barrier to trade, particularly in services, putting companies operating out of the UK at a competitive disadvantage."

"Post Brexit, UK businesses who also operate in, or sell to, the EU, will have to comply with GDPR for that portion of their business…"

Ruth Boardman, of the London-based firm Bird & Bird, told *Bloomberg BNA* that the European Union's new General Data Protection Regulation (GDPR) complicates the post-Brexit privacy analysis. UK companies that do business in the European Union will have to comply with the union's new privacy regime when it takes effect next May, but Boardman doesn't believe the United Kingdom must rush to change its privacy laws to meet those obligations.

"Significant change will just add uncertainty and cost – and will damage attempts for the UK to secure an adequacy decision," she said.

The House of Lords panel told businesses to keep up their preparations for the GDPR, even if the government doesn't "pursue full regulatory equivalence in the form of an adequacy decision" with the European Union.

"Post Brexit, UK businesses who also operate in, or sell to, the EU, will have to comply with GDPR for that portion of their business," Boardman said.

INFO SECURITY

FTC Chooses Winner in Competition to Protect IoT Devices

The Federal Trade Commission (FTC) announced on its website that a mobile app built by a New Hampshire software developer won the top prize in the agency's competition seeking tools to help consumers protect the security of their Internet of things (IoT) devices.

With the help of five judges, the FTC awarded Steve Castle the $25,000 prize for his proposal for a mobile app called "IoT Watchdog." Castle said he entered the contest to distill his network security knowledge and experience into a tool that can help users see if their devices are out of date and their networks insecure.

The mobile app he proposed would help users manage the IoT devices in their homes and enable them to scan Wi-Fi and Bluetooth networks to identify and inventory connected devices. It would then flag devices with out-of-date software and other common vulnerabilities and provide instructions on how to update each device's software and fix other vulnerabilities.

The FTC also awarded an honorable mention to a team that proposed an alternative method of securing home networks from vulnerable IoT devices. The team, led by Silicon Valley-based engineers BJ Black and Michael Birmingham, was awarded $3,000 for its proposal to develop "Persistent Internal Network Containment" (PINC), a tool that uses virtual networks to isolate each device on a home network so consumers can easily monitor and manage their IoT devices.

CYBERSECURITY

HBO Hack Highlights the Need for Encryption and Data Governance

The widely reported August hacking of HBO's systems resulted in 1.5 terabytes of data stolen, including unaired episodes of some of its programs. The CEO of AlertSec has told *EsecurityPlanet.com* the incident serves as a reminder that hacking isn't limited to financial, health, and personal information.

"All information is vulnerable because some hackers are motivated by the thrill of it," Ebba Blitz said. "They steal because they can, not because the information always has any real long-term value. All data needs to be protected with encryption."

Jason Hart, CTO of Gemalto, told the online site that broadcasters face a unique threat. "Due to the

nature of the industry, hackers have the opportunity to access data as it is transmitted between multiple data centers, and so they require solutions to help encrypt their high value TV transmissions – without interfering with the audience's viewing experience," he wrote in an e-mail message to *EsecurityPlanet.com*. "HBO now joins a list of other Hollywood victims of crime such as Netflix and Sony."

Richard Stiennon, chief strategy officer at Blancco Technology Group, said the HBO incident is a good example of the need for data governance.

"Content producers and all the parties involved in shooting, editing, and post-production processing and distribution should be on high alert," he said. "They should immediately review their data governance policies and discover the weak links in protecting their content and shore up their defenses. An information governance policy should take into account where critical content resides at all times."

CYBERSECURITY

Organizations are Typically Liable for Vendor-Related Breaches

To date, errant steps taken by third-party vendors have caused many notorious data breaches. The Netflix, Target, and Verizon incidents, for example, are just a few that can be cited. Such failures to protect data can lead to bad press, operational headaches, hits to the bottom line, and a host of fines and lawsuits.

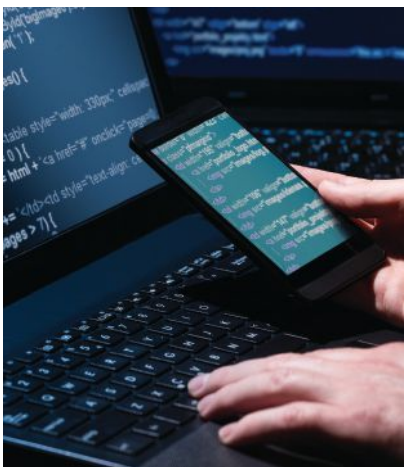
How liable are the vendors? A recent *LegalTechNews.com* article offers answers to the question. Depending on the situation, a breach of an organization's data by a third-party vendor could open a company up to legal and regulatory liabilities under many state, federal, and international laws. Jason Vanto, of the law firm Polsinelli, says that even though a cybersecurity incident happens outside an organization, the organization is still liable for it because it's the custodian of the data. Further, according to Vanto, there's an expectation for organizations "to retain vendors that can keep the data secure."

Legal liability can vary based on such factors as state notification laws and industry sector. Financial companies often face tougher action by local and federal regulators, empowered in part by the Gramm-Leach-Bliley Act of 1999 and the Federal Deposit Insurance Act of 2003. And the New York State Department of Financial Services' data security regulation even spells out the protections vendors must have.

Further, according to Vanto, organizations also must face contractual liabilities that stem from promises made in their privacy statements or customer contracts about the security of their data.

"There is really not too much you can do in terms of protecting yourself if your vendor breaks the law," Vanto says.

But you can limit your exposure to these liabilities and their consequences. An organization's legal liability is greatly limited if it and its vendors are found to have "reasonable cybersecurity protections" in place, as defined by commonly used industry best practices and governmental guidelines.



CYBERSECURITY

Common Flaws Make 55% of Corporate Networks Vulnerable

Infosecurity-magazine.com recently reported on a survey that suggests corporate information systems became more vulnerable last year, at the same time that user awareness about information security issues significantly decreased.

The security audit, sponsored by Positive Technologies, found that critical vulnerabilities were detected in 47% of investigated corporate systems in 2016. During these audits, experts simulated internal and external attacks. When acting as an external threat, the Positive Technologies testers gained full control over the corporate infrastructure 55% of the time. When simulating internal intrusions, they were successful on every system.

According to the audit, staff awareness of information security was very low in half of the systems in 2016, compared to a quarter of them in 2015. Further, wireless network security was also extremely weak in three-fourths of cases.

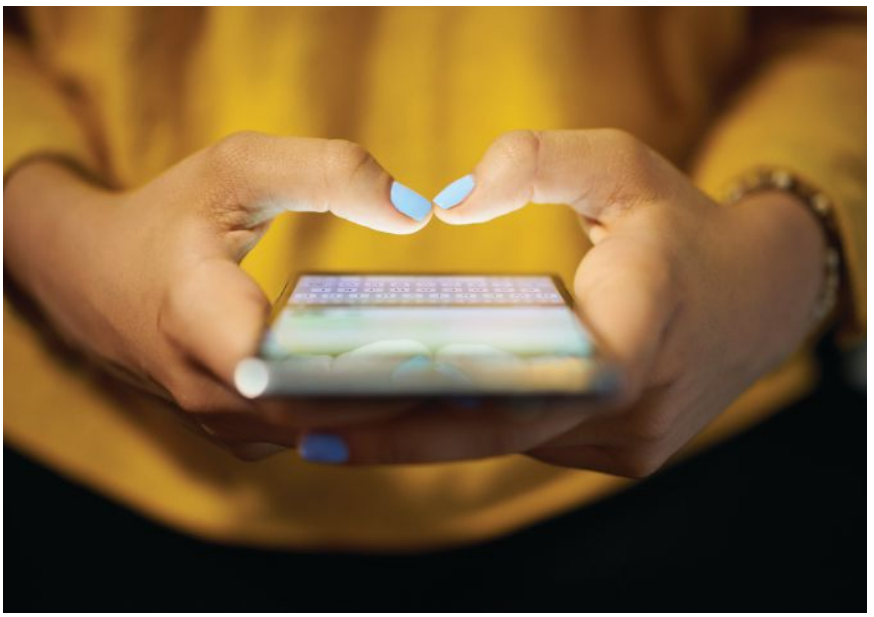
The audits found several common protection flaws, such as configuration errors (in 40% of the systems), errors in web application code (27%), and failure to install security updates (20%).

The initiative also found that bypassing a network perimeter often requires just two steps. Typical vulnerabilities are dictionary passwords, unencrypted data transfer protocols, vulnerable software versions, and publicly available interfaces for remote access.

Evgeny Gnedin, an executive with Positive Technologies, said companies could dramatically improve their security by applying basic rules: "Develop and enforce a strict password policy, minimize privileges of users and services, do not store sensitive information in cleartext, minimize the number of open network service interfaces on the network perimeter, regularly update software, and install operating system security updates."

E-DISCOVERY

National Law Review Gives Guidance on Using Ephemeral Communications Tools



The issue of using ephemeral communications tools in the workplace is a legally complicated one, particularly when it comes to legal holds and e-discovery. A recent article on the *National Law Review's* online site spells out the risks and provides guidance for maneuvering through the legal landmines.

Many organizations use instant messaging systems, and employees often send work-related texts and communicate over collaborative tools, some of which generate the automatic deletion of data.

Unless there is an "affirmative duty to preserve," organizations have no general obligation to save or store their communications, according to the authors, Adam C. Lenain and Wynter Lavier Deagle. Organizations can use technology to enable "effective, timely and consistent disposal of electronic information that no longer needs to be retained" within its information governance program.

The authors warn that organizations must retain and dispose of their data responsibly and within carefully crafted information governance policies that are designed with the help of legal counsel. The courts, say Lenain and Deagle, have "struggled to keep pace with the rapid changes in communications technology and the scope of a party's preservation obligations" regarding ephemeral communications.

The authors say a risk vs. reward approach should be used before an organization adopts any emerging technology in its workplace. In the article, Lenain and Deagle provide a deeper look at the advantages of using ephemeral communications tools, the duty to preserve electronically stored information, case law related to ephemeral data, and considerations for using such tools following a legal hold.

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 by booking your room and the conference hotel when you register.

Special Thanks to Our Sponsors:

Access Information Protected. docfinity IBM Iron Mountain MICRO FOCUS personify EDGRAVE 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, subject matter experts, and solution providers in a virtual exhibit hall. Part one provided the content instruction in an online virtual conference on August 29. 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 have taken part in the online virtual conference 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

You'll also have a chance to

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

New Zealand's Privacy Mark Could Provide 'Competitive Advantage'

Recently the Office of the Privacy Commissioner of New Zealand (OPCNZ) launched a survey on using a privacy trust mark system that it would administer. The trust mark would likely help consumers believe their personal information is safeguarded and would, in effect, lead them to choose privacy-friendly goods and services.

Christie Hall, a privacy law expert, told *DataGuidance.com* the proposal has merit and shows the ongoing effort by the OPCNZ to encourage good privacy management among

businesses. "Organizations would also benefit from consumers being able to make more informed choices. [H]aving a privacy enhancing reputation will allow them to connect with a greater number of consumers, and, consequently, they will see the competitive advantage in working towards achieving excellent privacy policies and standards," she said.

The concept of a privacy trust mark is not entirely a new one. It is used in many jurisdictions, allowing organizations to certify and be endorsed through various means. At the international level, the Asia-Pacific Economic Cooperation Privacy Framework, for instance, relies on trust mark certification processes, with certification awarded by regional accountability agents.

Allan Yeoman, partner at Buddle Findlay, said the move could be in response to what the OPCNZ describes as the country's weak privacy law: "The Privacy Tick might be an alternative way for organisations to be incentivised to take privacy seriously. If it becomes widely recognised and adopted, then it might become a necessity for companies operating in competitive sectors who want to be seen to have sound privacy practices."

PRIVACY

Study Suggests Consumers Will Forfeit Certain Privacy Rights if Given Discounts

Consumers are willing to toss out certain privacy rights if it means saving money, according to a recent report. Roughly half of U.S. broadband households are willing to share data and device control for discounts on electricity, says "The Value of Data – New Smart Home Business Models" report, conducted by research firm Parks Associates.

Across the categories, the results were essentially the same: 51% of smart thermostat owners, 50% of hot-water-heater owners, and 48% of owners of smart clothes dryers are willing to share data and control for electricity discounts, as reported on *InfoSecurity-Magazine.com.*

"The real value from the internet of things will be derived from the data collected by smart products," said Tom Kerber, a director at Parks Associates. "In general, IoT industries agree that the consumer owns the data from smart products and that smart home solution providers are the stewards of the data. Given this reality, it is essential for all IoT players to understand consumers' willingness to exchange data for services, their views on privacy and security, and the conditions under which they will grant access to their data."

The study also found that 40% to 50% of consumers will share data under some circumstance when presented with other incentives.

It is your life. It is your career. It is your certification.

CRM

In a business world of doing "more with less," your designation as a Certified Records Manager shows that you understand the many facets of the RIM profession.

In a business world that is rapidly changing, your designation as a Certified Records Manager shows you are up to date on the latest technology, the latest rules and regulations, and the techniques of the RIM profession.

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager (CRM) demonstrates that you have the experience and expertise to lead change and deploy best practices as they evolve in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 694-5362 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

INFO SECURITY

Spain: DPO Certification Intended to Offer Security and Reliability

As reported by *DataGuidance.com*, the Spanish data protection authority recently announced it had instituted a data protection officer (DPO) certification in alliance with the National Accreditation Entity (ENAC), as a response to the forthcoming General Data Protection Regulation (GDPR). Under the certification scheme, DPO certification will be granted by entities accredited by ENAC.

The certification scheme sets forth the competencies required for those who hold the position of DPO, and the criteria for assessing that the applicants embody them. When the evaluation process is favorable, the certification body will issue a declaration of compliance or a certificate. The tasks required under the scheme are to advise the data controller, data processor, and employees involved in data processing of their obligations under the GDPR; oversee the training of staff; advise on Data Protection Impact Assessments and monitor their implementation; and act as a point of contact for the supervisory authority.

INFO GOVERNANCE

CDOs Not Enough: Governance and Strategy are Needed

In a StateScoop podcast, several data professionals agree that as chief data officers (CDOs) increase in number in government, there must be a proportional increase in information governance. In the podcast, representatives from the public and private sectors say governance and strategy will drive the future of data analytics in state government.

State and local governments are beefing up their data and analytics practices. Arkansas recently announced the hire of its first CDO, and earlier this year New Jersey codified the position into law. As these transitions occur, decision makers need to look toward governance and strategy as next steps.

"The first thing [states] need to do is figure out an information governance policy," HPE's Lewis Carr says in the broadcast.

Elizabeth Rowe, New Jersey's CDO, had served in the role for two years before the law established the position. She says, "Right now we have a lot of individual agencies at various levels of maturity, but from an enterprise perspective, I think our overall analytics perspective is immature. But thanks to those recent developments, that will help with standardization of data and processes across the executive branch."

The podcast was one in a series that chronicles the top 10 priorities of state chief information officers.

ARCHIVE RECORDS MANAGEMENT
Made Simple

Managing and retaining public records may sound like a relatively simple process, but for government archiving agencies it can be quite a daunting task. Local and state government regulations vary but non-permanent public records typically must be kept available for anywhere from three to 50 years. In the past, Chester County Archives and Records Services (CCARS) of Pennsylvania would store many of these records on microfilm for both retention and employee access purposes. Although microfilm was the best option CCARS had available at the time, it also proved to be arduous and expensive to produce.

> **"We have cut the time it takes to convert a box of documents from a day to 90 minutes."**

CCARS instituted a system designed to manage these records electronically using document scanning technology. Unfortunately, the initial scanning system that was used proved to be very labor-intensive and inefficient. On average, the department was effectively scanning a year's worth of court records each year. Faced with this and a variety of other challenges, CCARS began a search for a better way to address their document retention needs.

In order to come up with a better solution, the records management team explored a variety of options. Initial research suggested that switching from microfilming to document scanning would be the ideal solution since scanning takes less time and it is much more cost-effective. Unfortunately, some of the initial feedback proved less than positive.

CCARS moved forward with scanning technology they were told would be able to address all of their needs. However, after just a few months of collecting production data, they realized this was not the case.

"It didn't take us long to figure out that the new scanning hardware couldn't support the volume of documents we were processing," said the Records Manager of Chester County Archives. "One box worth of documents would take an entire day to scan and store. To put that in perspective, one of our departments has a 15 year backlog of documents which means it would have taken us 15 years to put all of their information into a digital format. We also had issues preparing the documents for scanning, such as removing staples or adjusting for bindings, which made the entire process way too costly and time-consuming. We were very frustrated but knew that there were other technologies available that could address our needs."

With a clearer understanding of the requirements needed to tackle their issues, CCARS examined a number of options and realized that one vendor, OPEX® Corporation, could address CCARS's unique document conversion needs. Much to his delight, the Records Manager saw immediate improvement in how his organization functioned by working with OPEX.

- **Increased speed**: It used to take an entire day to convert a box of documents to a digital format. By switching to OPEX, that time was reduced to 90 minutes.

- **Improved workflow:** Requests for original hard-copy documents can take up to 24 hours to process. However, once a record has been scanned, any employee of Chester County with proper login credentials can now access records instantly.

- **Enhanced security:** CCARS now can rest easy knowing that all of the digitized and indexed documents are stored in a data center that is located at another site. In addition, if a paper-based document is damaged, it is very costly to repair. By having documents stored electronically, CCARS has direct access to a backup copy without having to incur the high cost of document restoration.

To learn more about managing your archive records with OPEX, visit www.opex.com.

OPEX® CORPORATION

INFO ACCESSIBILITY

India Governmental Agency Blocks Access to Wayback Machine

The Wire (India) reports that India has blocked access to the Internet Archive, a website that hosts the Wayback Machine, a tool that helps users get past censorship efforts when they wish to view archived or deleted web pages.

Users who tried reaching the service last month got an error message that said the URL had been blocked due to directions received from Department of Telecommunications, Government of India.

The Wire says that authoritarian countries often remove contentious online content, which results in the popularity and usefulness of the Wayback Machine, which has a 20-year archive of the world's publicly accessible web pages.

According to the article, such blocks have become commonplace over the last decade in India. High courts there, prompted by allegations of copyright infringement or of defamation, sometimes respond with broad orders to block content by disabling access for Indian users through an ISP. Further, the Department of Telecommunications has also previously issued orders to ISPs to block access to certain webpages.

The article concedes it does not know the reasoning behind the censorship and says access to a more secure, HTTPS version of the website appears to be unblocked.

E-DISCOVERY

Employee Self-Selection of E-mails Satisfies Discovery Obligations

The *National Law Review* reports that a federal court in an employment discrimination case has held that an employee's self-selection of e-mail messages for the purposes of discovery was appropriate.

In *Mirmina v. Genpact, LLC,* Civil Action No. 3:16-CV-00614 (D. Conn. July 27, 2017), the court denied the plaintiff's motion to compel discovery, finding the self-selection was appropriate under the circumstances, though the employee was involved in the litigation.

The plaintiff had sought to compel the defendant to conduct further searches for electronically stored information (ESI), expressing concern that the defendant could be withholding relevant documents from the initial discovery protocol.

In response, the defense argued that it issued a timely, detailed litigation hold to custodians of ESI,

instructed ESI custodians on the nature and parameters of the searches, explained the importance of a thorough search, and gave guidance when questions arose.

The court accepted the search process because of the close involvement of counsel and its sworn statement that all responsive messages had been disclosed. The court also said there was no supportive case law or evidence backing the plaintiff's allegations.

Attorney Brett M. Anders, principal with Jackson Lewis P.C., and author of the *National Law Review* article, says the ruling "provides some measure of protection to litigants who choose to rely on the custodians themselves to locate and retrieve relevant documents." He warns, though, that litigants who rely on self-selection must take appropriate precautions to see that a complete search is performed and that counsel provides close oversight.