E-MAIL

NARA Develops E-mail Retention Schedule

With the 2016 year-end deadline for managing all records electronically on the horizon, the National Archives and Records Administration (NARA) is preparing new rules and guidelines to help U.S. federal agencies meet the requirements of the 2011 presidential directive on management of government records.

NARA is putting the finishing touches on a retention schedule for retaining e-mail as part of implementing its Capstone program. The schedule is to designate as "permanent" the records of certain senior officials – such as all heads of department, deputies to senior officials, staff assistants, and chief executive officers – for transfer to the National Archives after declassification or 15 years, whichever is longer.

Federal agencies are not required to adopt Capstone, but they do have to meet the deadline set by the presidential directive, and their plans must be approved by NARA.

"Capstone dispenses with content analysis," said NARA General Counsel Gary Stern during a forum with agencies and other stakeholders in May. "It's a crude, simplistic approach. It may not be great, but it's better than the existing approach."

In a recent *FCW* article, Paul Wester, chief records officer for the U.S. government, said, "Our archivists who deal with the permanent records, some of them are a little frustrated with this approach because they know that they're going to be getting these large volumes, which still will contain lots of not very substantive records within them."

As the article pointed out, e-mail management has become a charged issue given the publicity around former Secretary of State Hillary Clinton using a personal e-mail server for State Department business. Just as her staff had to cull through tens of thousands of e-mails to separate the official from the non-official, so will others subject to Capstone – with the exception of those mentioned above whose records are deemed permanent by default. This can be a manual, automated, or hybrid process.

Although there is software that analyzes e-mail content, selects relevant e-mail, and deletes the chaff, it is not used much in government yet, pointed out Adam Mazmanian, a senior staff writer who covers Congress, health IT, and government-wide IT policy.

E-DISCOVERY

Proposed Federal Rules Advance

The Supreme Court of the United States has given the proposed changes to the U.S. Federal Rules of Civil Procedure (FRCP) its blessings. Now the rules await Congressional approval, which, if everything goes according to plan, will have the rules going into effect December 1, 2015.

Amendments to Rule 37(e) specifically address electronic discovery. In brief, the revisions provide a unified standard for the courts to use in situations where electronically stored information (ESI) is not properly preserved.

If ESI that should have been preserved for a legal hold is lost because the party didn't take the appropriate steps, and it can't be easily reproduced, it's up to the court to determine a remedy that is "no greater than necessary to cure the prejudice." Only if the court decides the offending party destroyed the ESI intentionally can it choose to issue an adverse inference, jury instruction, or dismissal.

The other FRCP amendments focus on the importance of cooperation, proportionality, and reasonableness in discovery. Part of the goal is to minimize delays and control the mushrooming costs of producing documents during discovery.

MOBILE

Is Your Mobile Policy Ready for Wearables?

The next big trend in mobile computing is wearables, such as a Fitbit, the Apple watch, and Google Glass. We're clearly still in the early-adopter phase, but consider how quickly smartphones changed the way people do business.

Like most new technologies, wearables bring both exciting opportunities and serious challenges. While they can put the data within a short glance of the wearer, they can also present privacy and data security concerns.

"Employers would have to address those [concerns] head on, and be prepared to answer an array of questions—for starters, what data will be tracked? How will the data get stored? Who in the organization will have access to it? How will the information be used," warned Alberto Torres, chief executive officer of Atheer Labs, in a recent guest article in *ReadWrite*.

This is likely to be true for all wearables. Torres pointed out that the medical sector, which has been an early adopter of many technologies (including tablets), has shown great interest in such gadgets as Glass. For example, Glass puts critical medical information in the literal view of doctors as they treat their patients, but it raises privacy concerns. During a patient visit, what information can/should doctors capture? Have patients given their permission to be recorded? How are files stored or shared and with whom?

Torres noted that these types of concerns are not insurmountable and may well be outweighed by the benefits of using the technology.

E-DISCOVERY

Survey Identifies Top E-Discovery Challenges

In-house legal and IT professionals involved in electronic discovery who were recently asked what their biggest e-discovery challenge is named the following:

- Locating potentially responsive data (36%)
- Controlling the amount of data sent for outside review and managing multiple e-discovery projects at once (14% each)
- Defensibly deleting data that was on legal hold (13%)

The survey, which was conducted by Exterro, offered the following four tips for addressing these challenges.

1. Implement an information governance program that enables you to know where the data is.
2. Integrate with commonly collected data sources for streamlined data collection.
3. Leverage new e-discovery technology that enables legal teams to rapidly identify and locate the most important documents before collection.
4. Develop repeatable, predictable processes between the identification, collection, processing, and analysis stages.

INFO SECURITY

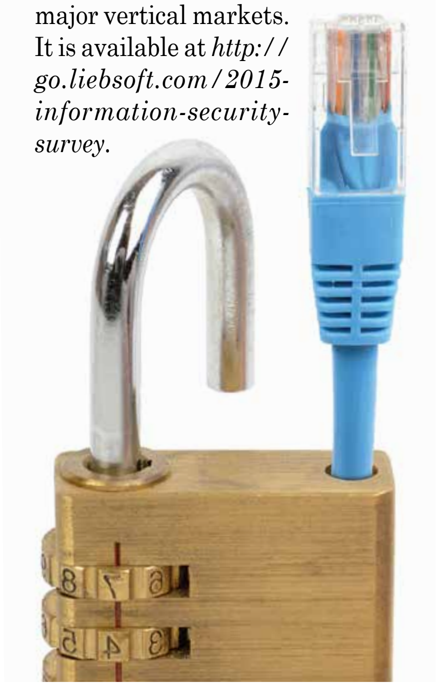
Compliance ≠ Security

The majority – 61%, to be precise – of IT professionals surveyed in April at the 2015 RSA Conference said their organizations had implemented an IT security product simply to satisfy a compliance requirement, which actually put the organization's data at greater risk.

This is one of several factors that prompted 71% of the respondents to fear for their organization's data security. The other major contributors were:

- IT security products not being used to their full potential (cited by 70% of respondents)
- The difficulty of finding skilled IT security personnel (reported by 85%)
- Cyber attacks evolving too quickly for IT pros to keep pace (76%)

Lieberman Software's annual *Information Security Survey* was conducted during the 2015 RSA Conference because its attendees include IT security professionals from all regions of the world and all major vertical markets. It is available at *http://go.liebsoft.com/2015-information-security-survey*.



PRIVACY

U.S., French Patriot Acts Meet Different Ends

In early May, as U.S. lawmakers were preparing to narrow the scope of the USA Patriot Act in light of opposition to the National Security Agency (NSA) surveillance made public in recent years, French lawmakers were passing their own legislation to expand state surveillance.

France's National Assembly passed legislation that grants the state sweeping surveillance rights, despite loud opposition from civil rights groups, which have reportedly dubbed it the French Patriot Act. It is one of several government reforms introduced following the terrorist attacks in Paris in January.

According to news channel France 24, the country is still on high alert and has received repeated threats from jihadist groups, including the Islamic State (IS) group in the Syria-Iraq region. It is also struggling "to keep up with the hundreds of French citizens who travel to and from battlefields in Iraq and Syria to wage jihad, often lured over the Internet," reported the *New York Times.*

The new law would give French intelligence services the right to gather potentially unlimited electronic data on such suspected terrorists. It would allow them to tap cellphones, read e-mails, and force Internet providers to allow government access to their subscribers' communications. In other words, it would allow them to collect bulk information and analyze metadata in much the same way the NSA did – the very thing U.S. lawmakers were seeking to limit.

The intelligence services could also request permission to hide microphones in a room or on objects, such as on cars or in computers, or to place antennas to capture telephone conversations or mechanisms that capture text messages, the *New York Times* said. Both French citizens and foreigners could be tapped. Civil rights groups fear such access could easily and quickly extend to others the state deems a threat. The senate is expected to pass the law prior to its summer recess.

Meanwhile, in Washington, D.C., lawmakers allowed a portion of the USA Patriot Act to expire in early June and then passed the U.S. Freedom Act, which leaves it to phone companies, rather than the federal government, to gather and store metadata – the numbers called and the time and length of calls – but not content.

U.S. officials will be able to access the data only after securing a warrant from a special court. According to an article in the *Christian Science Monitor*, a panel of civil liberty advocates will argue for privacy at the special court. The government has until the end of the year to make the transition.

RISK MANAGEMENT

NIST Releases Draft on Privacy Risk Management

iDENTiFY
ASSESS
ANALYZE
RiSK MANAGEMENT
REDUCE
CONTROL
TRANSFER

The U.S. National Institute of Standards and Technology (NIST) recently released for public comment the draft "Privacy Risk Management for Federal Information Systems," which, among other things, establishes a common vocabulary and a risk model for assessing privacy risk in information systems.

"Risk management methods provide systematic ways to identify and address risk and have proven effective in areas such as cybersecurity, safety and finance," says Naomi Lefkovitz, senior privacy policy advisor at NIST. "We see a great deal of potential for these methods to help agencies design and manage federal information systems that minimize risks to privacy."

Lefkovitz told *LegalTech News* that the impetus for the framework stemmed from a need to deal with the challenges of protecting personal data.

"The first trigger was internal, we're working on research concerning Big Data, smart grid, cybersecurity, and Internet of Things, and one thing they all have in common is there are implications for privacy. We had a need to think about how to consider privacy implications of these technologies in a consistent and repeatable, and measurable way," Lefkovitz said. "We are the measurement agency after all."

The framework focuses on best practices for the internal production and processing of private information. It leaves guidelines for dealing with cyber attacks and information recovery to cybersecurity research.

The comment period for the draft, which was available at *http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf,* was to close on July 13, 2015.

E-DISCOVERY

Courts Continue to Endorse Predictive Coding

Technology-assisted review (TAR), also known as predictive coding, continues to gain the support of federal courts. Magistrate Judge Andrew J. Peck of the U.S. District Court for the Southern District of New York, one of the first judges to endorse TAR, recently proclaimed that the right to use TAR for high-volume electronically stored information (ESI) cases is "now black letter law," reported Bond Schoeneck & King PLLC. Peck's statement was part of his discussion in *Rio Tinto PLC v Vale S.A., et al.*

The court's growing acceptance of TAR is expected to affect all producing parties in future cases, regardless of whether they would prefer to use traditional keyword searching instead of predictive coding. "As more courts tout the precision of TAR, requesting parties are ever more likely to demand that producing parties use this sophisticated technology to ensure that the maximum number of responsive documents are being unearthed," predicted Bond Schoeneck & King.

In large-volume ESI cases in which TAR would be appropriate, it may be wise to use the technology from the start and develop a protocol to ensure the selected technology is both defensible and transparent, the attorneys advised. It would maximize cost-savings and minimize the likelihood of expensive discovery disputes.

90/70

The percentage of large and small-to-midsize UK businesses, respectively, that has suffered an information security breach.

Source: ***Information Security Breaches Survey 2015, PwC***

CYBERSECURITY

Cost of UK Cybersecurity Breaches Doubles

The average cost of the worst single security breach experienced by UK businesses of all sizes has risen sharply over the last year, according to the Information Security Breaches Survey 2015 commissioned by the UK's Department for Business, Innovation and Skills (BIS). Breach costs include elements such as business disruption, lost sales, recovery of assets, and fines and compensation.

Costs have more than doubled for larger businesses (more than 500 employees), ranging from £1.46 million to £314 million (about $2.2 million to $4.7 million, U.S.) as compared to £600,000 to £1.15 million ($900,000 to $1.7 million) the prior year. Smaller businesses didn't fare much better as the average cost climbed to £75,000 to £311,000 ($112,500 to $466,500) from £65,000 to £115,000 ($97,500 to $172,500) in 2014.

The type of attacks didn't show such dramatic change. The majority of them (60%) came from external threats for larger businesses, 38% for smaller businesses. That compares to 55% and 33% in the 2014 report.

When asked specifically about the cause of the worst breach experienced, 50% were the result of inadvertent human error, up from 31% in 2014. That's even though 72% of large businesses and 63% of smaller businesses provide ongoing security awareness training for their employees.

To assist businesses in their efforts to secure their data, the UK government has issued "10 Steps to Cyber Security" advice sheets. They offer guidance in a variety of areas, including information management, security management, network security, and user education and awareness.

ELECTRONIC RECORDS

NARA Creating Registry for Controlled, Unclassified Information

The National Archives and Records Administration (NARA) is nearing completion of rules for managing the extensive volumes of controlled, unclassified information (CUI) the U.S. government generates. Reflecting input from agencies, the new rules establish 23 categories and 82 subcategories of CUI in a registry, with links to the statutory or regulatory basis for keeping the information under wraps, reported *FCW*.

Comments on the rules were due to NARA by July 7. The final rules are expected before the end of this year, at which time a three- to four-year phased implementation will begin. The greatest change for agencies is that they will need to mark CUI documents prior to dissemination rather than after. NARA is developing a marking handbook with input from agencies.

CYBERSECURITY

India Wants to Become Cybersecurity Hub

In March, India Prime Minister Narendra Modi called on his country's IT industry and youth to help address the global cybersecurity challenge. Three months later, the industry's lobby group Nasscom announced it was heeding the call and had formed the Nasscom Cyber Security Task Force with its goal to make India the hub of cybersecurity research, training, and products, reported the *Economic Times*. It will present a comprehensive cybersecurity plan within the next year.

"This task force will study the Indian cyber security ecosystem to identify issues and challenges and develop an action plan to address the priority issues," said BVR Mohan Reddy, chairman of Nasscom. "It will also identify possible intervention opportunities for the Indian IT industry in global cyber security space and bring together stakeholders from across the board to develop cutting-edge technologies and address the global market requirements."

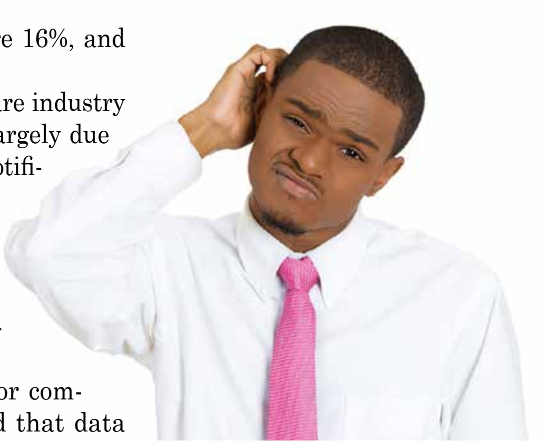
The task force will include four working groups focused on industry development, policy enablement, technology development, and skill development, the *Economic Times* article stated. Their recommendations will be the foundation for the country's cybersecurity plan.

In the meantime, the National Cyber Security Policy of India strives to create a half-million skilled cybersecurity workers in India by 2018. The number of cybersecurity professionals is increasing, but quality is the major concern.

"The challenge is finding that ultra-specialized group of people [in cyber security]," said the task force chair, Rajendra Pawar. This challenge exists not only nationally, but globally.

CYBERSECURITY

Survey Cites Human Error as Biggest Cause of Data Breaches



External cybersecurity breaches get the headlines, but evidence points to human error as a greater cybersecurity threat for organizations of all sizes.

A data security incident response report released in May by BakerHostetler revealed that in the 200-plus cases its firm advised on in 2014, human error was the top cause of data security incidents. Employee negligence was responsible 36% of the time, while theft by outsiders was 22%, theft by insiders 16%, malware 16%, and phishing attacks 14%.

While the healthcare industry was affected most – largely due to strict data breach notification laws healthcare providers must follow – no industry is immune from threats to its sensitive information.

"It is important for companies to understand that data security is not just an issue for retailers, financial firms and hospitals. Incidents do not only occur at businesses that have payment card data or protected health information. Privacy and data security issues are firmly entrenched as a significant public and regulatory concern and a risk that executive leadership and boards of directors must confront," stated the report's authors.

Other findings noted in the report include:

- Not all security lapses involved the theft or hacking of electronic records; 21% involved paper records.
- 58% of the incidents required notification of affected individuals, based on state breach notification laws.
- Credit monitoring was offered in 67% of the incidents.
- In 75 incidents where notification letters were mailed, only five of the companies faced litigation by potentially affected individuals.
- For incidents involving stolen payment card data, PCI Data Security Standards fines for non-compliance ranged from $5,000 to $50,000 per matter. Initial demands for operating expense and fraud assessments ranged from $3 to $25 per card involved.

"Our analysis shows that best-in-class cyber risk management starts with awareness that breaches cannot be prevented entirely, so emphasis is increasingly on defense-in-depth, segmentation, rapid detection and containment, coupled with ongoing effort to monitor threat intelligence and adapt to changing risks," the authors advised.

RECORDS AND INFORMATION MANAGEMENT

AU National Archives Issues RIM 'Capability Matrix'

Because managing an organization's records and information is each employee's responsibility, the National Archives of Australia developed a "capability matrix" that outlines the skills and knowledge each one needs to enable an organization to transition to fully electronic information management and ensure its information assets remain accessible and usable over time.

"Rapid advances in technology, the growing volume of information, and the increasing complexity of the online environment all mean that Australian government Agencies face significant challenges in managing their business information," stated Director-General of National Archives David Fricker when announcing the matrix, as reported by *PS News*.

The matrix addresses the capabilities for all staff, for information communication technologies specialists, and for records and information management specialists and is designed to be used in conjunction with the Australian Public Service Commission Integrated Leadership System, which has a stronger focus on behaviors.

E-DISCOVERY

The Challenges of Cross-Border Discovery

Global organizations are increasingly finding themselves in a difficult position in their attempts to address cross-border discovery.

If they comply with U.S. data preservation obligations, they could violate the rights of employees, customers, or other individuals under EU and other countries' international data protection laws. But, if they abide by individual countries' data protection laws, they risk potentially devastating spoliation sanctions in U.S. courts, explained e-discovery experts Jeane Thomas and Brad Davis in a recent *Corporate Counsel* article.

Bridging that gap is challenging, if not impossible. Thomas and Davis offered some practical steps counsel could take before and after litigation to minimize the conflict.

- **Retain records only as long as required by law or business necessity.** This will limit the volume of personal data that may be subject to preservation requirements.
- **Institute a litigation-readiness program.**
- **Educate foreign business units with the concept and requirements of U.S. discovery.**
- **Foster transparency.** "Advise employees through policies and specific notices that the company may be required to preserve and collect work-related email and other data containing personal information in the event of U.S. litigation or an investigation."
- **Ask for consent.** It may not be considered sufficient under foreign law, but explaining to affected employees why you need access to their data and what you intend to do with it and asking for their written consent "demonstrates respect for foreign data protection laws and the employee's individual rights."
- **Preserve data in place.** Avoid "imaging, harvesting, relocating or otherwise altering the data," particularly before you know what's needed.
- **Tailor legal holds, particularly for non-U.S. custodians.** Instead of issuing a company-wide legal hold, ask the necessary custodians to preserve data related to a particular transaction, activity, or issue.
- **Address foreign data-preservation issues with opposing counsel.** Discuss ways to limit the scope of non-U.S. data preservation obligations by narrowing discovery requests and focusing on available U.S. sources first.
- **Ask the court for a stipulation or court order.** This should address "limitations and requirements for the preservation and production of non-U.S. personal data, including restrictions on use and dissemination of the data and providing confidentiality and security protections."
- **Release preservation measures as early as possible.** Once you know non-U.S. data is no longer subject to U.S. preservation obligations, return it to normal data management practices.

CYBERSECURITY

Employee Cybersecurity Training Tips

Hackers prey on the most vulnerable links in your company's security – your employees. That's why they use *phishing* e-mails, malware-laden messages that appear harmless to the untrained employee's eye. It's imperative for organizations to train their employees in the best cybersecurity practices. Entrust, an identity-based security solution provider, suggested the following basic practices for all employees:

Avoid any e-mail that asks for username/password information – even if it's on their personal device. Connecting an infected personal device to the company network can infect other devices on the network. No legitimate service or website will ask users to transmit sensitive account-related data over e-mail. Make it clear that employees should enter sensitive data only on sites that have been administratively vetted or after consulting with IT.

Have open discussions about cybersecurity around the office. The most important step in getting people to be proactive about an issue is to promote awareness about it. Just setting aside five to 10 minutes at a company-wide meeting to discuss emerging threats and to share safe computing tips from the IT team can make a huge difference.

CLOUD

The Top Trends Driving Cloud Use

There are many ways to leverage the cloud. Some can make you a hero, others can be disastrous. To understand both scenarios, it helps to look at how others are using the cloud. According to a recent *Cloud Computing Magazine* article by Mike Chase, J.D., executive vice president and chief technology officer for the cloud service provider dinCloud, some of the top trends are:

- Virtual offices for disaster recovery – Companies intent on staying in business no matter what are leveraging the cloud to relieve concerns about the effects of such emergencies as environmental disasters, global terrorism, criminal activity (internal and external), and shifting legal/political landscapes. Setting up virtual offices with servers, desktops, file shares, and everything synced to the cloud can make business continuity easier.
- Desktop as a service – The cloud can offer so much more than the typical enterprise desktop. There are fewer licensing headaches and the cloud may have functionality that is not even available at the enterprise level.
- Regulatory relief – "Cloud has become the best way to meet new regulatory challenges because regulatory requirements around physical facilities hosting sensitive customer data can be a real drain on time/money/resources," stated Chase. "Security guards, cameras, logs, man-traps, cages, availability, become a real headache."
  - Security – Cloud-based security can be licensed monthly and is scalable. There also is a huge marketplace of cloud-based tools from which to choose. Leveraging the cloud can provide a depth of security not possible at the enterprise level.
  - Mobile – The cloud makes it easy to tie servers, desktops, and cloud storage to an existing Microsoft Active Directory, keeping full policies and permissions intact across most, if not all, mobile devices.

EHRs

Overcoming Health Information Blocking

The ability to share medical records electronically is a critical element in creating an effective healthcare system. So, why isn't it happening? According to a recent *New York Times* article, too often it's because that transfer is being blocked by the developers of the technology or "greedy medical centers that refuse to send records to rival providers."

The Office of the National Coordinator for Health Information Technology (ONC) recently presented a report to the U.S. Congress about the issue and provided criteria for identifying it and distinguishing it from other barriers to inoperability. ONC stated that it's difficult to assess the full extent of the problem, especially because of contractual restrictions imposed by software developers on their clients.

According to the report, ONC is already taking steps to target, deter, and remedy information blocking, including strengthening in-the-field surveillance of health IT certified by ONC. Many of the requirements for certification are aimed at enabling information-sharing between systems. Tightening standards is another step being taken.

"One of the most effective ways to reduce information blocking is to promote transparency in the health IT marketplace," the ONC told Congress. "Providing customers with more reliable and complete information about health IT products and services would make developers more responsive to customer demands and help ameliorate market distortions that enable developers to engage in certain opportunistic and other behavior that raises serious information blocking concerns."

The office also noted that congressional action may be needed to address some issues that are beyond the reach of current federal law and programs.

E-MAIL

E-Mail Overload Has Predictable Results

Knowledge workers today are dealing with e-mail overload, a perception that they send, receive, and process more e-mails than they can handle, find, or process on a daily basis. Interestingly, on average, those who receive 100 or more e-mails each day can respond to only about 5% of them, according to a report on a recent study of 2 million users exchanging 16 billion e-mails over several months, "Evolution of Conversations in the Age of Email Overload."

In short, the researchers found that "as users receive more email messages in a day, they reply to a smaller fraction of them, using shorter replies," and they often reply faster.

Some of the key findings of the research, as summarized in a blog post by the Information Governance Initiative (IGI), were:

- People generally reply quickly to e-mails, most often within an hour of receiving a message.
- Younger users reply faster to messages than their older peers, and they send shorter responses.
- Women are slightly more affected by e-mail overload than men, but the difference is negligible.
- E-mailing behavior is predictable; the research team was able to forecast the time and length of a reply, as well as when a conversation between two people will end with high accuracy.

"These findings could be used in designing better email clients that help people deal with email overload," Farshad Kooti, a Ph.D. student at the University of Southern California who conducted the research with four colleagues, told IGI.

The full report can be accessed at *http://arxiv.org/pdf/w1504.00704v1.pdf*. **END**