INFO SECURITY

Consumers Don't Trust Healthcare IT Security, Benefits

Results from a recent survey could be troubling for the healthcare industry and providers of healthcare IT products and services.

As reported in a Jan. 9 article on the Health Data Management website, one national survey of 12,000 individuals, conducted last fall by market research firm Black Book, found that 70% of respondents distrust health technology. Further, 57% of consumers are skeptical of the overall benefits of health IT, such as electronic health records, patient portals, and mobile apps. The distrust and skepticism apparently stem from high-profile data breaches and a general perception of poor security.

"We saw that distrust number in particular with consumers and mental health records and pharmacies," said Doug Brown, managing partner at Black Book. "They feel that there's some kind of leakage of information, even if it's not cybersecurity-related."

More specifically, respondents overwhelmingly fear their prescription (90%), mental health (99%), and chronic conditions (81%) information is being shared with retailers, employers, and the government. Accordingly, the survey suggests that 89% of consumers in 2016 withheld health information during doctor visits. A clear majority of respondents (69%) also believe their primary care physician lacks the technology savvy to protect their personal information.

"High-level data breaches, and now ransomware, are becoming mainstream," said Brown. "Consumers may have had concerns before, but now it's constantly in the news, with millions of American impacted by breaches like Anthem."

GOVERNMENT RECORDS

White House Use of Encrypted Messaging May Violate Law

As reported in the *Wall Street Journal* and elsewhere, senior Trump administration aides are using encrypted messaging apps to communicate, which might violate federal recordkeeping laws.

The *Journal* reported that aides close to the president are using Signal, which encrypts data end to end. The app was reportedly used by some staff in the Obama administration as well.

The incentive to encrypt may have been boosted by the hacking of the Democratic National Committee. But by keeping such communications private, the administration may be violating the Presidential Records Act, which requires staff to keep records of conversations.

The article quotes Michael Morisy, founder of news site MuckRock: "If new agency appointees are using Signal or other disappearing message apps routinely for work, even if it's not classified, that's a serious lapse in records retention policy. Email retention is still a huge struggle, and I have a hard time believing that Signal messages are properly being archived."

Alex Howard, an executive with the Sunlight Foundation, says it's "a recipe for corruption" and a "willful effort not to be held accountable."

According to U.S. federal law, all records of government business must be preserved by the National Archives and Records Administration (NARA) within a few days of their creation. While a 2014 update to the law expanded the tools that federal employees can use, allowing a wider range of instant messaging and social media platforms for communication, it did not exempt them from being archived. Data generated on apps like Signal cannot be captured and therefore cannot be archived; any back-up efforts would have to be self-policed.

The White House did not respond to requests from the *Journal* on whether the new administration had set up data retention policies for its encrypted messaging.

PRIVACY

NYC Commission Wants to Collect Details on Uber, Lyft Trips

Since 2009, the New York City Taxi and Limousine Commission (TLC) has collected extensive trip data from NYC taxis, such as pick-up and drop-off data, distances, fares, payment types, and passenger counts. The data is published online as well. Now the TLC wants to do the same for ride-sharing companies, according to an article on *jdsupra.com*.

In January, the TLC proposed amendments to its driver-fatigue rules that would require ride-sharing companies also to provide more details on their trips, such as the date, time, and location of every drop-off. The TLC defends the amendment as a safety measure to ensure drivers are not working while fatigued and as a tool to help city officials investigate complaints about unsafe driving.

The TLC claims not to want the names, credit card numbers, or other personal data about passengers, and it pledges not to publish specific addresses online or make them available.

Uber says the amendment will result in serious privacy risks and would give the government "and anyone else who accesses the information a comprehensive, 360-degree view into the movements and habits of individual New Yorkers." If made public, the data could be mined to reveal intimate details about where someone lives, worships, shops, and more.

Uber has urged its NYC customers to protest the proposed rule by posting on social media with the hashtag #TLCDontTrackMe. The company has told the TLC it could provide general trip duration data to help monitor for driver fatigue. Currently, Uber provides an online portal that anonymizes trip data to help city planners evaluate transport systems and infrastructure; it doesn't believe the TLC needs the exact pick-up and drop-off locations.

Uber also states it doesn't trust the TLC to protect the information from data breaches and demands from other agencies that may want to use it for unauthorized purposes.

The fact that Uber is resisting the amendments might seem ironic to industry watchers. Uber itself has been criticized for collecting too many details and for allowing employees to access the users' accounts. Additionally, Uber once permitted its employees to use a tool called "God View" to monitor passengers' trips. The tool displayed aerial views of the Uber cars on the road and personal data about the passengers. Upon being investigated by the state attorney general, Uber replaced that tool with one that did not reveal personal data. The current application lets the company access a passenger's location data from the moment he requests a ride until five minutes after drop off.

.

E-DISCOVERY

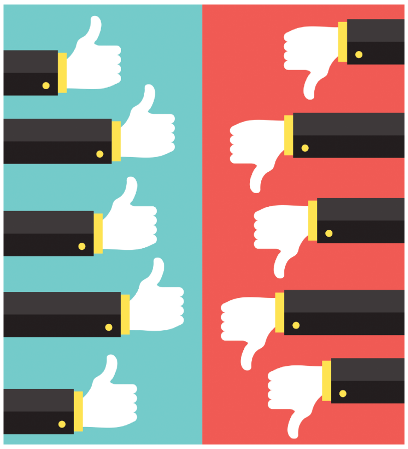
Australian Court Recognizes Value of Predictive Coding for E-discovery

As noted by KrollDiscovery on *ediscovery.com*, Australian courts for the first time recognized the advantages of using predictive coding for e-discovery purposes in a legal proceeding. The finding stems from *McConnell Dowell Constructors v. Santam*, a liability dispute in which the parties faced massive costs to review 1.4 million documents and couldn't agree on an e-discovery technique. The court designed a special "referee" to find an effective method that was also consistent with proportionality and compliant with Australia's Civil Procedure Act.

The court found that predictive coding "is far more sophisticated than a word search facility" and that traditional methods of discovery were inappropriate for such a case. Further, the court said its judgment was influenced by the success of predictive coding in Ireland, the United Kingdom, and the United States.

GOVERNMENT RECORDS

Views Clash on Whether Social Media Entries Are Records



When an outgoing administration of Montana's Office of Public Instruction's (OPI) left the premises, certain social media communications disappeared as well, according to a recent article on *Missoulian.com*.

The lost Twitter and Facebook accounts had been managed by former OPI Superintendent Denise Juneau and Communications Director Emilie Ritter Saunders. In an e-mail to reporters, Saunders wrote, "Once the term in office expires, the pages essentially expire." It is Saunders' view that social media is used to link constituents to public records, and its contents are not public records.

The state, however, has a different view. Montana's social media policy says that any communication to or from state personnel that uses social media is presumed to be a public record. Format, then, is not a factor; content is.

Montana lacks a centralized method for managing digital content as public records; each branch determines its own guidelines. The executive branch says that all digital records must be retained and destroyed according to the schedules in state law, but it doesn't specify how to do either.

Corey Stapleton, secretary of state, believes Montana's retention policies are outdated, and the lack of a clear policy and the lack of consistency among branches are limiting the public's ability to see how their government is run.

"We ought to have a discussion about meaningful retention of the right things," he told the *Missoulian*. "But it might be an uphill battle."

CYBERSECURITY

Parliament Committee Assails UK's Cybersecurity Defenses

The influential Public Accounts Committee (PAC) of British Parliament has issued a report that says the UK's approach to cybersecurity is "inconsistent, dysfunctional and chaotic," as reported by *zdnet.com.*

The indictment is contained in PAC's "Protecting information across government," and it seems especially relevant after Defence Secretary Michael Fallon's recent warning about persistent cyber attacks by Russia against the West.

In urging the government to establish a clear approach to protecting the nation from hackers and cyber-espionage, the report describes breaches at Tesco Bank, Northern Lincolnshire, and Goole NHS.

The report suggests the government has been too slow responding to the threats; it has been warned about such a national security risk since 2010. Over the years, the government has established initiatives and agencies but has not coordinated the "alphabet soup" of the 40 agencies and departments that are tasked to protect British cyberspace.

Meg Hiller, PAC chair, says the government must "raise its game." She says, "Its approach to handling personal data breaches has been chaotic and does not inspire confidence in its ability to take swift, coordinated and effective action in the face of higher-threat attacks."

The report also warns that a shortage of skills is compromising the fight as well, a weakness that continues to intensify matters because of the evolving capabilities of the hackers.

PAC recommends the Cabinet Office to develop a detailed plan for the National Cyber Security Centre by April, which will detail who it will support, what assistance it will provide, and how it will communicate with organizations that need its help.

ScanPro i9300

Bring your Blipped Microfilm into the Digital Age with the **ScanPro i9300**!

The ScanPro® i9300 microfilm scanner is the product you've been waiting for to bring your blipped film into the digital age. We know that original blipped film scanners are aging and limited in their capabilities. That's where the i9300 comes in!

Find your blip the first time

Utilizing patent pending technology, the ScanPro i9300 finds your blip the first time with fast and exceptionally accurate searching. It works with one, two, and three level simplex and duplex film and is ALWAYS as easy as 1-2-3.

1 load your film | 2 enter your search address | 3 click search

Automatic Scanning/Printing Included:

The i9300 automatically scans and prints a single image or a range of images of one-, two-, or three-level simplex and duplex film.

Optional IMS AUTO-Scan® Pro:

With the IMS AUTO-Scan Pro optional software, the i9300 will also automatically:

- Scan and print an entire roll of film
- Name the files using the document address
- Convert the files to text with OCR technology
- Collate them into multi-page PDFs grouped by batch, file, and page addresses

IMS AUTO-Scan Pro does all of this with unparalleled speed and accuracy.

The ScanPro i9300.

Precise. Powerful. Universal.

Universal microfilm scanner

Not only does the i9300 support blipped film, it also scans/prints your fiche, ultra-fiche, aperture cards, micro cards, and 35mm roll film microfilm, making it truly universal!

The ScanPro i9300 is the solution you've been waiting for. It is easy to use, reliable and backed by an unmatched 3-year warranty and a lifetime lamp warranty.

e-ImageData
microfilm scanners

www.e-imagedata.com • 800-251-2261

www.facebook.com/eimage.data • @eImageData

INFO SECURITY

China Pledges to Safeguard Info 'Using All Means'

A recent article published on *Bloomberg News* says that China vows to use all necessary means to protect its information security, even if it must dispatch the military.

"China will do its utmost to protect the information safety of the country and its citizens," said Zhao Zeliang, a top-ranking cybersecurity agent, who presented China's first National Cybersecurity Strategy Report.

In November, China adopted a sweeping cybersecurity law that requires web operators there to cooperate with police investigations and at times provide source code and encryption keys.

Further, any new technologies to be used by the government and major industries will face heightened scrutiny, according to Zhao.

Under President Xi Jinping's tenure, cybersecurity has been a priority, a stance intensified by the revelations about U.S. spying on other nations, and, more recently, by the suspicion that Russia was instrumental in hacking American election systems.

In a statement, James Zimmerman, chairman of the American Chamber of Commerce in China, said Beijing's direction is beginning to alarm foreign companies, and the new measures "create barriers to trade and innovation."

CYBERSECURITY

Lawmakers Unveil Cyber Recommendations for Trump Administration

As reported on *FCW.com*, a cybersecurity task force issued a report with recommendations for the Trump administration on combatting cyber crimes and terrorism. The January 5 report, "From Awareness to Action: A Cybersecurity Agenda for the 45th President," suggests the administration reorganize oversight authorities, elevate the role of the White House cybersecurity coordinator, and clarify the cyber defense roles of civilian and military agencies.

According to the report, the most contentious issue was how to best protect the nation's critical infrastructure. In November, Trump suggested the Department of Defense (DoD) would develop a "comprehensive plan to protect America's vital infrastructure from cyberattacks," an authority that's now under the Department of Homeland Security (DHS) jurisdiction.

Task force Co-Chair Rep. Michael McCaul (R-Texas) believes that giving the authority to DoD would be a serious mistake.

"I don't believe the American people want to militarize our cyber defenses," he said. "We have civilian police officers, civilian FBI agents … We don't have the military walking through the streets … I think the same principle applies to cyber, in terms of needing a civilian agency to defend the nation's critical infrastructure."

McCaul said the DHS will need an independent operational component to handle digital threats.

The report proposed establishing a Division of Data Protection within the Federal Trade Commission to strengthen consumer data security.

Co-Chair Sen. Sheldon Whitehouse (D-R.I.) also proposed using a roving or independent oversight authority "across a wide array of civilian agencies" that would "stress test their security, rather than simply check off a minimum security checklist."

He said the public must be promptly informed of all cyber incidents and the steps government is taking to mitigate such threats.

"One obstacle to transparency is the culture of overclassification that pervades the executive branch," he said, suggesting Trump should designate a specific "cybersecurity discloser" position within the White House charged with reporting to the public.

Whitehouse was uncertain which recommendations would require legislation.

CYBERSECURITY

Report Finds That Ransom Is Top Motivation for Cyber Attacks

As noted on *BetaNews.com*, a report from cyber security firm Radware, "Hackers & Companies Agree: Data Is Lucrative," reveals that 49% of businesses say they were targeted by cyber attacks in 2016. Of those affected organizations, 41% claim that ransom was the motivation; 27% cite insider threats; and 26% cite either political "hacktivism" or competitive gain as the motivation.

Additionally, 55% of responding organizations say the Internet of Things (IoT) makes detection and mitigation more difficult because of the expanded landscape for attack.

A Radware executive, Carl Herberger, says it's clear today that money is the top motivator in the threat landscape.

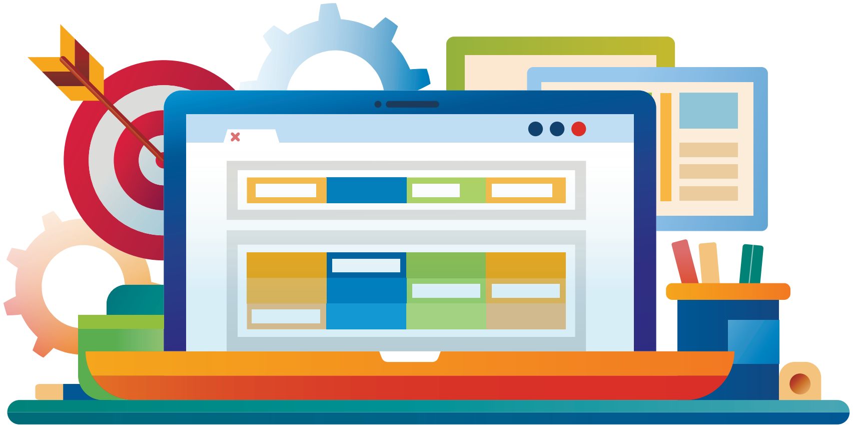
> "… security must be woven into the customer experience for a company to truly succeed"

Despite such threats, many organizations remain poorly prepared. The report suggests that 40% have no incident response plan in place, 70% lack cyber insurance, and only 7% have bitcoins on hand to make payments.

"Threat actors have a single focus, to develop the best tools possible to either disable an organization or steal its data," says Herberger. "Businesses focus on delivering the highest value to their customers. …security must be woven into the customer experience for a company to truly succeed. Without this change in thinking, organizations will remain vulnerable."

PRIVACY

Privacy v. Revenues: EU Proposes Limiting Web Tracking for Ads



On January 10, the executive arm of the European Union (EU) proposed rules to limit how companies track users in their efforts to deliver targeted ads. As reported in the *Wall Street Journal* and elsewhere, the proposed rules would require users to actively consent to the use of tracking cookies.

The European Commission said the rules would protect user privacy and enhance transparency on how an individual's data is used. According to the EU, such regulations would have wide support; the EU claims 80% of Europeans say it's important that such cookies are employed only with the user's permission.

"Transparency is important. People must know whether information stored in their devices is being accessed or whether their online behavior is tracked," the European Commission said in a press release.

If enacted, the rules would give users the right to allow or reject the tracking cookies when they are installing a browser. Users could change their choice at any time. Anyone who rejects the tracking would continue to see the online ads, but they likely would not be personalized.

Townsend Feehan, an executive with the Interactive Advertising Bureau Europe, claims the proposal would damage the advertising business model and provide no privacy benefits. Instead, Feehan believes the legislation would create a nuisance because companies would probably display pop-ups asking users to switch their settings in order to use their services. "People who thought cookie banners were annoying will be disappointed to hear that things won't get better," Feehan said.

The commission's proposal "is an improvement over what we have now but it is clearly not as good as a 'do not track' setting turned on by default," said Johannes Kleis of BEUC, the European Consumer Organization.

The commission says it hopes the rules are adopted by May 2018, when the EU's General Data Protection Regulation (GDPR) will enter into force.

FREEDOM OF INFORMATION

Indiana Universities Allowed to Delete Public Records

In Indiana, e-mails are considered to be public records by law, but universities are not subject to the retention rules that govern other public agencies. According to state law, public universities are not required to have a policy, as recently reported by *Ball State Daily.*

Ball State University, for example, does not have a policy to safeguard e-mail and other public records from being destroyed.

Joan Todd, university spokesperson, says Ball State doesn't have a records retention schedule, but the lack of one doesn't impact how records are kept. The university only has a policy that ensures personnel records, financial information, and travel and attendance records aren't destroyed.

"The university is well aware of the duty to preserve records when, in the regular course of doing business, it is necessary to preserve those records to complete university business or the university is lawfully obligated to do so, such as when records are the subject of litigation," Todd told *Ball State Daily.*

The issue was sparked when several Indiana news outlets sought copies of e-mails between Ball State's departing president and its trustees. The university said it had no such e-mails between the parties that included any of the proposed relevant keywords.

Gerry Lanosga, president of the Indiana Coalition for Open Government, doubted the university's response.

"That's pretty astonishing," Lanosga said. "I think that's rather unlikely."

The absence of any e-mail between the president, his board, and top advisors suggested the mail could have been deleted, said Lanosga.

According to state law, the school isn't required to have a policy. Universities self-police when it comes to records retention.

"It's not a very good situation from a transparency standpoint," said Jim Corridan, director of the Indiana Archives and Records Administration (IARA).

Universities can work with the IARA to develop a retention schedule if they please, Corridan said, but it's up to them.

"From my perspective, it would make most sense if public universities had a unified retention schedule so they all did things the same way," Corridan said. "If they provide citizens of Indiana access, it allows them to hold administrators accountable for their actions. But we're not quite there yet."

REGULATORY COMPLIANCE

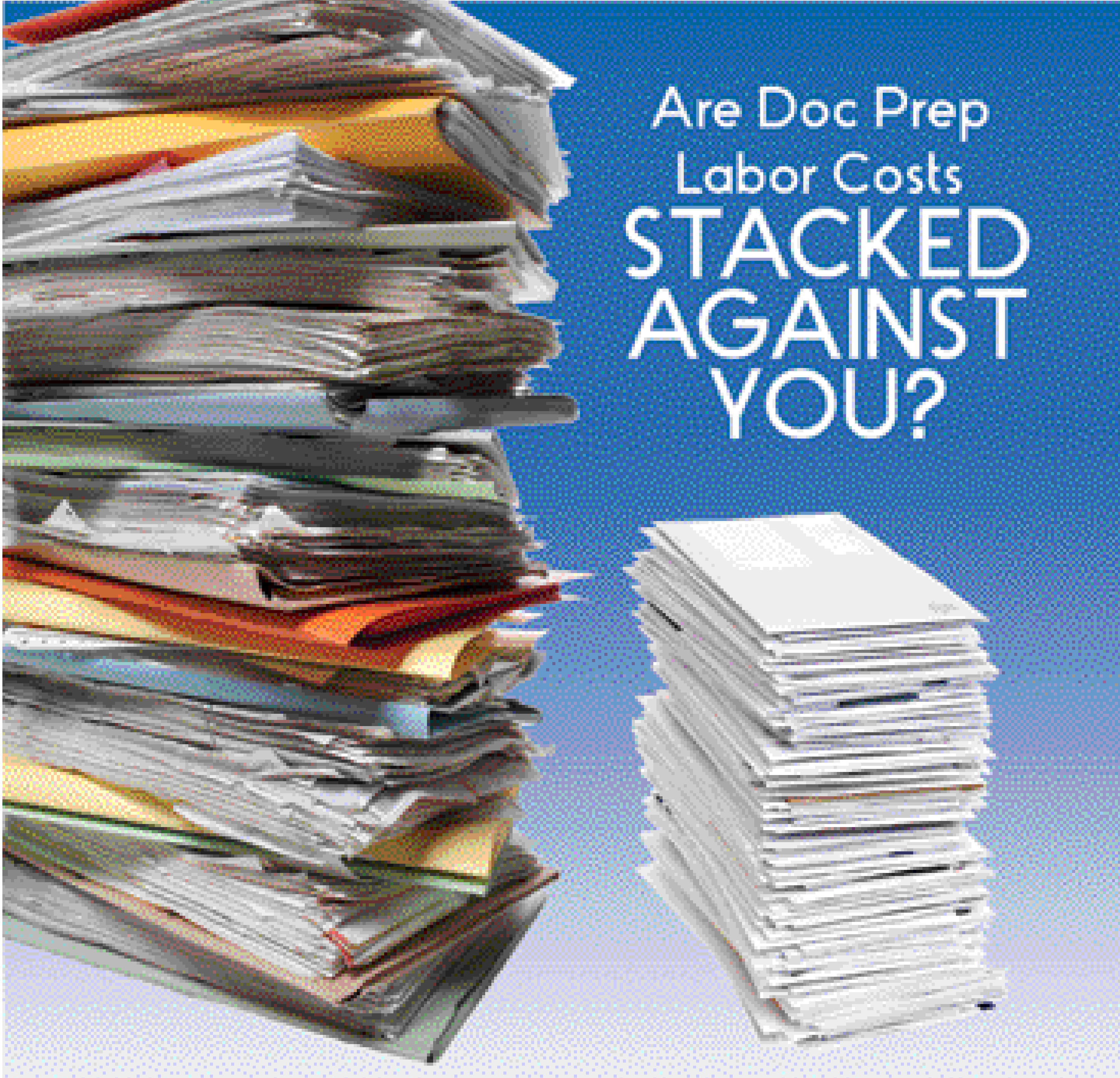
OSHA Reiterates: Employers Must Maintain Accurate Injury, Illness Records

In the final days of the Obama administration, the Occupational Safety & Health Administration (OSHA) issued a final rule that requires employers to make sure their illness and injury records are maintained appropriately, *JDSupra.com* reports. The rule went into effect on January 18.

OSHA says it intends to cite employers for any inaccuracies in the illness and injury logs for a period of six months after the required five-year retention period. The final rule also states an employer must maintain accurate records on an ongoing basis.

Industry groups may seek to block the new rules through litigation.

As OSHA transitions more to electronic recordkeeping and reporting, the agency should more easily identify employers who are under-reporting injuries. The cost of non-compliance could be much higher if OSHA can look for errors over five and one-half years.


Are Doc Prep
Labor Costs
STACKED
AGAINST
YOU?

PRIVACY

German Consumer Group Sues WhatsApp Over Data Policy

According to *Bloomberg*, Facebook's WhatsApp is under fire in a Berlin court for new privacy clauses that permit the messaging service to collect and transfer data between the platforms. The suit was filed by German consumer group VZBV, which insists that each consumer must be given the right to decide how his personal data is revealed and used.

"Our experts brought the misconduct to light. Now we'll meet in court," VZBV said. "Be it Facebook, Google, Amazon or now WhatsApp: we target violations."

European regulators also are concerned about the changes and are probing Facebook for possibly giving "incorrect or misleading information" about its plans to use customer data when it filed to acquire WhatsApp.

In a statement, WhatsApp said its privacy policy complies with the law and gives a clear explanation of how customers can determine the ways their data is used.

E-DISCOVERY

FRCP Amendments Dominated 2016 Federal E-Discovery Cases

According to a November Kroll report, "New Frontiers in E-Discovery," courts in 2016 sought to better educate attorneys on proportionality and on preservation processes in relation to the 2015 amendments to the Federal Rules of Civil Procedure (FRCP).

The report, summarized by *LegalTechNews.com,* reviewed 57 federal opinions on e-discovery in 2016 and found a 56% increase in cases addressing FRCP Rule 26, as compared to the previous year. Rule 26 concerns proportionality, the scope of discovery, and the production of discoverable items.

The report also found a 32% increase in the number of opinions that addressed Rule 37(e) on preservation and spoliation of ESI, and an 8% spike in opinions on procedural e-discovery issues, such as predictive coding.

Michele Lange of Kroll Ontrack said there were "certainly a number of cases where judges needed to educate parties on the new rules and instill the importance of the FRCP amendments."

Lange highlighted *Fulton v. Livingston Financial LLC* as a good example of the modified discovery landscape: "The defendant's attorney cited the pre-2015 FRCP amendments, claiming that he acted in 'good faith' because the new version of Rule 26 did not change the meaning of relevance."

The court disagreed, saying the old amendments were out of date.

"… it was reiterated that a responding party is best situated to decide how to search for and produce ESI responsive to a document request."

According to Lange, "Parties cannot purposely ignore or recklessly fail to address the new proportionality requirements of Rule 26(b)(1). Fulton proves that courts simply will no longer tolerate such outdated and out-of-touch legal advocacy."

Courts have also sought to finesse how Rule 37(e), concerning the preservation of ESI, is applied in discovery. Lange said this has always been a tricky area for e-discovery law, given that "what is considered 'proper preservation' is a blurry line, often dependent upon a myriad of case-specific facts, which makes it ripe for courts to intervene and clarify when disputes arise."

Lange expects this fine-tuning to continue in 2017.

While courts are offering instruction on preserving ESI, they are not mandating that parties employ predictive coding, based on what Lange refers to as "two key opinions." In those actions, *Hyles v. New York City* and *In re Viagra (Sildenafil Citrate) Products Liability Litigation*, the courts did not compel a party to use the new technology. Said Lange: "Instead, it was reiterated that a responding party is best situated to decide how to search for and produce ESI responsive to a document request."

GOVERNMENT RECORDS

Federal Agencies Can't Compete for Top Cybersecurity Analysts, Says FBI

An FBI official recently claimed that U.S. federal agencies have a shortage of cybersecurity analysts, which is contributing to the vulnerability of the nation's computer networks, according to a report on *LegalTechNews.com.*

At a public event in Manhattan, Agent Prashanth Mekala of the FBI's New York office said it takes unique skills to detect such "bad actors," and the government is failing to compete well with high tech companies in recruiting such experts.

"In the federal government, there's a shortage of skills of folks within cybersecurity space," Mekala said. "There is a growing third party in the private sector that we are also competing with."

Google and Microsoft, for example, hire many of the same cyber-savvy candidates that law enforcement agencies pursue. Mekala said the problem is affecting the National Security Agency (NSA), the CIA, the Department of Defense, and the FBI.

Professor Nasir Memon, New York University Tandon School of Engineering, asserted that an effective cybersecurity analyst must be trained in analyzing human behavior as well as the technology.

"Security is not just a technical problem," Memon said. "It's a business problem. It's a legal problem. It's a policy problem. It's a human behavior problem."

In 2014, according to the U.S. Bureau of Labor Statistics' Occupational Outlook Handbook, there were 83,000 information security analyst jobs, and employment was expected to grow 18% from 2014 to 2024, much faster than average. The median wage was $90,120 in May 2015.

In its 2017 budget request, the FBI requested $85.1 million to increase cyber-investigative capabilities.

Timothy Howard, cybercrime coordinator for the U.S. Attorney's Office for the Southern District of New York, said federal officials encourage private companies to promptly report any breaches because quick notice gives federal authorities insight into the latest methods used by cyber criminals.

REGULATORY COMPLIANCE

Future Looks Bright for 'Data Scientists' as Organizations Seek Ways to Leverage Big Data

As reported on *Information-Management.com,* the *Harvard Business Review* has said being a data scientist is "the sexiest job of the 21st century." Likewise, McKinsey & Company, a management consultant firm, has projected that in the United States alone some 1.5 million data scientists – that is, professionals who can analyze big data to make effective decisions – will be needed.

Leveraging big data can pay off. The article cites the 2016 McKinsey study "Big data: Getting a better read on performance" to show that investments in big data yield a multiple of 1.4 to 2.0 on the level of investment, increasing profits an average of 6%.

In related news, the annual Glassdoor report suggests that data scientist remains the top job in America, based on hiring demand, job satisfaction, and pay potential. Technology and data jobs dominated the rankings; 18 of the top 50 jobs are in the tech and data fields.

PRIVACY

RIM Can Help Organizations Seize GDRP Opportunities

A recent opinion piece found on *Information-Management.com* emphasizes the opportunities rather than the challenges that come with the May 2018 enactment of the EU's General Data Protection Regulation (GDPR), which will impact any entity that handles personally identifiable information (PII) of any EU citizen.

David Kemp, an information governance official at Hewlett Packard Enterprise, writes that there is great potential for those organizations that get ahead of the GDPR: "These benefits can include greater credibility with customers, increased operational efficiency, accelerated product development and protected brand reputation."

Kemp believes that records and information management plays a leading role in such proactive compliance. One UK insurer, for instance, in an effort to comply with the forthcoming PII statutes, drained its "data lake" and soon noted significant ROI from reduced storage costs.

In a second example, Kemp says a multi-national oil company has already incorporated the compulsory GDPR anonymization of data. In doing so, its mass migration of that data from on-premises storage to the cloud has heightened its credibility with cloud-managed information.

Kemp cautions that any reactions to the GDPR should be measured and should involve the executive team and key officials from legal, compliance, risk, IT, audit, and security. It is especially important to engage legal and compliance professionals, according to Kemp, because the GDPR has many detailed stipulations that can be confusing.

The author also writes that a risk assessment "is essential to identify the exposure detailed from non-compliance, as well as an assessment of the advantages."

CYBERSECURITY

NY Setting Precedent for Cyber Regulations in Financial Industry

Information-Management.com reports the state of New York is taking the lead in developing serious cybersecurity regulations, with the financial industry its first target.

Effective March 1, the New York State Department of Financial Services (DFS) will require banks, insurance companies, and other DFS-regulated entities to establish a cybersecurity program that's designed to protect consumers and ensure the safety of the state's financial services industry.

The regulations will require the affected institutions to have a valid cybersecurity program in place that describes what information the organization has, who has access to it, and what is necessary to control and secure that data and its systems.

More specifically, the program must assess internal and external risks; use defensive policies to prevent unauthorized access and use; and detect, respond, recover, and report on any events. It also defines requirements for multi-factor authentication, data retention, encryption, and training and incident response.

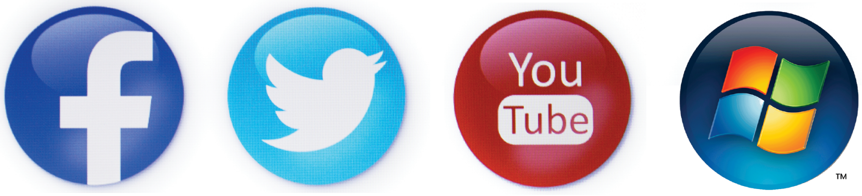
The DFS is calling for a chief information security officer (CISO) to be responsible for implementing the program and reporting to the governing board its progress and any cyber events that have occurred. The CISO must also ensure that third-party providers have equal controls and practices to ensure protection.

Bill Noonan, who wrote the article, believes these regulations are the first of many that will come to the individual states – regulations that will eventually reach beyond the financial industry.

ARMA
INTERNATIONAL®
INFO
GOV
INFORMATION GOVERNANCE
CONCEPTS | REQUIREMENTS | TECHNOLOGIES
SAFFADY
WILLIAM SAFFADY, PH.D.

CYBERSECURITY

Internet Titans Will Team to Detect Terrorist Content



As recently reported by *Bloomberg News,* four Internet giants are teaming to improve their efforts in removing terrorist-related content from their services. Facebook, Microsoft, Twitter, and YouTube have agreed to create a shared database of the most extreme terrorist images and videos they've removed. Facebook will host the database, which will store a unique digital fingerprint generated by a cryptographic algorithm (called a "hash") for each item.

Subsequently, all videos and photos that are uploaded to any of these four services will have its hash checked against the database. If there's a match to a hash that's already stored, the database will set in motion a process for the content's possible removal, according to a statement provided by Facebook.

Facebook asserts that because the database stores only the hash – and not the actual image or video – no personally identifiable information will be shared among companies.

Western governments have been pressuring the companies to do more to combat such content from terrorist and far-right organizations. The European Commission recently said that time is running out for these U.S. tech companies to prove they're serious about confronting hate speech. In fact, German officials have threatened to file criminal charges against Facebook for neglecting to curb such content from neo-Nazi affiliated groups.

CYBERSECURITY

SEC's Data Breach Probe of Yahoo Could Set Precedent

According to *LegalTechNews.com* and the *Wall Street Journal,* the Securities and Exchange Commission (SEC) is investigating whether Yahoo Inc. should have disclosed its data breaches to investors earlier. Any resulting penalties would be the agency's first ever for such a charge.

The SEC is checking whether Yahoo broke securities laws when it waited until 2016 to disclose the two breaches, which together compromised the data of more than a billion users. The incidents occurred in August 2013 and in late 2014.

Last September, U.S. Sen. Mark Warner (D-Va.) wrote to former SEC Chair Mary Jo White asking her to investigate.

Robert Cattanach of Dorsey & Whitney in Minneapolis, which represents companies in cybersecurity matters, said it can take weeks or months to gather enough information about a breach and the data that was compromised to disclose an incident accurately.

"I can promise you that there are so many different open questions when you are in the middle of one of these [data breaches], your head is just swimming," he said. "So the fact that [Yahoo] waited a while before [disclosing] is in many ways understandable, but from the SEC perspective: you don't get forever."

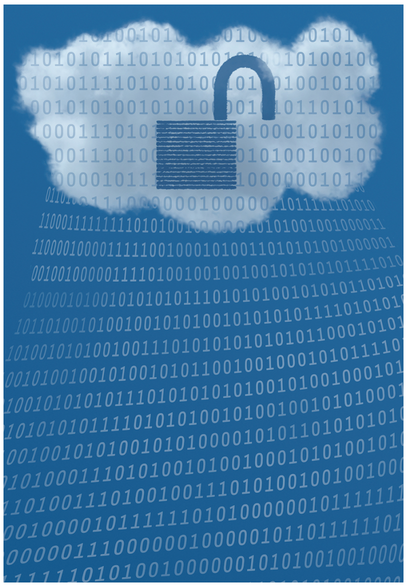
Craig Newman of Patterson Belknap Webb & Tyler in New York, which represents clients in financial and cybersecurity matters, said companies are in a tough spot because "they don't want to jeopardize law enforcement efforts, they don't want to jeopardize investigations, but at the same time, securities laws require them to be transparent with their own investors."

According to Newman, SEC guidance on disclosures provides no direction on how long companies should take. Most states have data breach laws that include a time frame, some giving companies 45 days to disclose.

Yahoo declined to comment on this particular SEC investigation. E

PRIVACY

OIG Finds Unprotected PII in Federal Cloud Computing System



In February, *HealthITSecurity.com* reported that the Office of Inspector General (OIG) discovered the General Services Administration (GSA) had unprotected personally identifiable (PII) information in its cloud computing system.

The OIG's report, "Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment," details how the GSA left PII unprotected in 2014. Such reports were not made public then because OIG worried they "presented information about then existing security vulnerabilities."

At least one data breach was found in the GSA cloud computing environment, containing "sensitive but unclassified building information" and PII, the report said.

"The sensitive information was accessible to GSA employees and contractors without a valid need to know such information," OIG wrote. "We determined that GSA was not proactive in securing sensitive data in its Google cloud computing environment and has not taken a comprehensive approach to correct the problem."

Approximately 900 individuals were affected by the incident. GSA sent breach notifications to nearly 600 of those individuals in August of 2014. But the OIG believed the notification downplayed its severity.

E-MAIL

E-mail Auto Delete Policies in Minnesota County Stir Debate

In Hennepin County, Minn., government transparency advocates are unsettled by policies adopted by local governments that allow them to auto-delete e-mail. Most worrying to the advocates is a 30-day e-mail retention policy adopted by the sheriff's office.

"If you've got stuff in there you really don't want the world to see then the best way to deal with that is to get rid of it," Don Gemberling of the Minnesota Coalition for Government Information told television news outlet KARE. "It's pretty easy here in Minnesota because of vague language in our statutes that regulates the retention of government information."

Sheriff Rich Stanek defended the policy, citing the updated schedule and policy will allow the county to be better data stewards while reducing storage expenses.

The sheriff said his employees will continue to comply with state rules requiring that certain messages, depending on content, be retained longer.

Gemberling claims such a process can be subjective because employees must manually move the e-mails into folders that are immune from the auto-deletion functions.

"Our law has language that essentially gives government a lot of discretion in deciding what information in an email is 'official' and that kind of discretion, handed over to the people who have the email, is just bad policy," he said.

Two state lawmakers plan to introduce legislation in 2017 requiring government agencies to retain e-mails for at least six months.

"We have 210 million emails in Hennepin County right now, and our employees get about six million emails a month, which is a lot of email," Judy Regenscheid, the county's operations director, told KARE.

She said giving employees a hard deadline will save money and create a more efficient work flow. "In 2013 it cost us about $1 million for email storage, and now that has climbed to $3 million for 2016." E