Newsbytes, 4/16

Editors: Raymond D. Aller, MD, and Hal Weiner

Finding, fixing, and foiling shadow IT problems

The unsanctioned use of mobile devices and cloud-based software in the workplace, often referred to as shadow IT, is a pervasive problem. Yet, through education and enforcement of policies, it's a problem that can be minimized.

Not all risks related to employees sharing data via devices and applications that have not been approved by enterprise IT departments are obvious. For the health care industry, for instance, regulations such as the Health Insurance Portability and Accountability Act, which is intended to protect patient privacy, intensify the shadow IT problem. Furthermore, shadow IT produces information silos at a time when medical data need to be integrated into electronic health record systems, points out John Donohue, associate chief information officer for Philadelphia-based Penn Medicine.

A number of cybersecurity firms have attempted to measure both shadow IT and shadow data, the latter defined as any sensitive information shared in cloud apps without the consent and control of corporate information technology security teams. A 2014 report from CipherCloud stated that 86 percent of cloud applications used in Fortune 1000 companies are unsanctioned. And a fourth quarter 2015 shadow data report from Elastica, based on analysis of 63 million enterprise documents within cloud applications, noted that 10 percent of documents shared broadly via unsanctioned apps contain sensitive data.

For the most part, the problems created by shadow IT and shadow data are not the result of employee malice, wanton recklessness, or a penchant for slacking off, according to cybersecurity industry reports. On the contrary, most employees use personal devices and unsanctioned apps in the workplace to be more productive and because they perceive the formal IT-approval process to be too cumbersome.

Consequently, improving IT departments' understanding of and responsiveness to employee needs can go a long way toward mitigating shadow IT, as can educating employees about the dangers associated with unsanctioned applications, says Donohue. It also behooves organizations to implement robust policies and controls, he emphasizes, adding that policies that reward compliant employees by granting them network access work better than attempts to ban the use of personal devices or to penalize scofflaws with disciplinary action.

A year ago, Penn Medicine implemented a "bring your own device," or BYOD, policy, which allows employees to use their own smartphones, tablets, and laptops on the job as long as they install a security layer, provided by Penn Medicine, on their devices. "The security tool allows us to encrypt the data, enforce passwords, and wipe the device clean if necessary," Donohue says. Penn Medicine employees who download the tool on their personal devices can access the network server, while those who don't cannot.

Health care enterprises should also have standards that spell out which applications have been approved, Donohue says. “Organizations need to be prescriptive and state, for example, that, ‘If you’re file sharing, here is the tool that is sponsored by corporate IT,’” he says. Through employee orientations, Web pages, periodic emails, and other channels, organizations can continually educate staff members on why they need to limit themselves to the sanctioned apps.

To get the buy-in of employees and more easily measure results, phase in shadow IT policies gradually, advises Ulysses Balis, MD, professor and director of pathology informatics for the University of Michigan Health System, Ann Arbor, which has also made great strides in addressing shadow IT. At UMHS, “a number of policies that have been under careful development are being rolled out in thoughtful succession—not all at once because too much change too quickly can be overwhelming,” he says. Each phase of the rollout has a voluntary period followed by mandatory implementation.

At first, the health system established a BYOD policy that operated on the honor system. “The guidelines stated that if you bring your own device to work, you’re expected to have a current version of anti-virus software on it,” Dr. Balis explains. “We published a list of suggested vendors, but nothing was locked down.”

In addition, UMHS initially had rules against logging on to the network with a machine suspected of having malware. “But who really knows if a machine has a virus?” Dr. Balis says. The more sophisticated viruses stealthily invade computers, leaving users unaware that their machines have been compromised. Indeed, one common type of virus, referred to as keyloggers, covertly tracks computer users’ keystrokes to intercept user names, passwords, and other confidential information.

Because UMHS’ honor system lacked sufficient teeth to thwart these threats, the health system decided to implement more stringent measures incrementally. “We needed a more proactive approach to protecting the network,” Dr. Balis says. “The reality is that a single compromised device, once it’s plugged into our network from the inside, can do a substantial amount of damage.”

So during a roughly two-year transition period, the health system began to require all machines that connect to the network to be reviewed and approved by the IT department as having the appropriate level of anti-malware protection. In addition, UMHS started installing enterprise mobility management software on employees’ personal devices. “Only then would a set of keys for the wireless network be granted, allowing the device to be authenticated as a trusted machine,” Dr. Balis says. Individuals who comply can access the central network with their devices; those who don’t are restricted to the guest network so they can’t use server resources.

Although staff response to this phase of the rollout has been mostly positive, the next step will likely generate some pushback, Dr. Balis expects. To leverage HIPAA safe harbor provisions that minimize the likelihood of a data breach, UMHS is instituting a series of measures to encrypt data on all machines. The most stringent would disable the USB port of any machine not following the protocol.

“When you go from a voluntary period of using these technologies to forcing people to use them, there will probably be some grumbling,” he says. “I imagine that some people will be upset because we’re going to potentially take away their ability to use their thumb drives.”

While tough policies may generate pushback from employees, they are more essential than ever. Aaron Higbee, cofounder of the cybersecurity firm PhishMe, cites Hollywood Presbyterian Medical Center, in Los Angeles, as just one recent example of the need for vigilance. The medical center paid $17,000 in bitcoin to hackers who shut down the hospital’s computer system using ransomware, in February. “Hollywood Presbyterian couldn’t do any billing or access a lot of patients’ medical records,” he says. “Ultimately, the hospital decided to pay the ransom in order to get its business operations back as soon as possible.”

Nevertheless, shadow IT has a silver lining, says Willy Leichter, CipherCloud’s global security director: It has led to the adoption of innovative but secure applications that are good for the business of medicine and patient care.

—Carolyn Schierhorn

[hr]

HHS website highlights interoperability projects

The Office of the National Coordinator for Health IT has launched the Interoperability Proving Ground, an open community platform for sharing information about interoperability projects taking place nationwide.

Users of the IPG platform can share basic information about their interoperability projects, such as title, description, and a hyperlink to the project's website, as well as tag the project with any standards or keywords that may be associated with it. These data are used to populate the IPG home page so users can easily filter and search the interoperability project database or view interoperability projects nationwide on an interactive map, said Steven Posnack, ONC's director of the Office of Standards and Technology, in a Health IT Buzz blog post.

The ONC has included many of its interoperability projects on the site and will include those of other federal agencies.

"No matter how big or how small, every interoperability project you add to the IPG will make a difference and enrich the IPG's potential for the entire health IT community," Posnack posted. "The IPG is your chance to showcase your interoperability work nationwide, connect with peers tackling interoperability issues, and make visible progress toward a future where we are all part of a learning health system."

[hr]

BBCS offers discount to Blood Centers of America

Blood Bank Computer Systems has entered a partnership with Blood Centers of America that supports BCA's standardization initiative. Under the arrangement, blood centers that are members of BCA can receive a group purchasing discount for BBCS' ABO Suite blood bank management system.

"We have a significant number of members already using BBCS and many members that are in the process of evaluating moving to a new BECS [blood establishment computer software] system," says Bill Block, CEO of Blood Centers of America. "BCA members that decide to move to BBCS in the future will be rewarded for standardizing, and this, in turn, will benefit the total number of members using BBCS."

***Blood Bank Computer Systems**, 888-738-2227*

[hr]

Ambry Genetics debuts free human genomes database

Ambry Genetics has launched AmbryShare, which the company touts as the largest free, disease-specific public database of sequenced human genomes.

The site, www.ambryshare.com, has already posted anonymized, aggregated, allele-frequency data from 10,000 human genomes focused on hereditary breast and ovarian cancers. In addition to using samples from patients who consented to having their data shared for medical research, the company secured approval from an independent research board to conduct research exome sequencing on those samples.
The company will "sequence genomes and release the data for all of its consented and de-identified patient samples, potentially contributing data from almost 200,000 genomes annually based on projections from its current sample volumes and profoundly impacting the collective understanding of the genetics behind all human diseases," according to a statement from Ambry.

“Clinicians who have patients who require genetic testing and who want to support our efforts should consider sending us their patient samples for testing,” Charles Dunlop, founder and CEO of Ambry, told CAP TODAY. “Your patients get the answers they need for their own care, and if they consent to sharing that data anonymously, then they will help us all advance medical care to improve the lives of future generations.” Dunlop also encourages clinicians to draw pedigrees and track family health history data through Ambry’s free Progeny Cloud service.

The platform for the AmbryShare database is tailored to bioinformatics professionals, but Ambry plans to expand it to include information targeted at clinicians and, eventually, the general public. “Ultimately, the AmbryShare database will be compatible with third-party registries and other open-source databases,” the company reported.
[hr]

Omnyx launches digital pathology software

Omnyx LLC, a joint venture of GE Healthcare and UPMC, has introduced Dynamyx next-generation digital pathology software.
Through its relationship with Visiopharm, dating back to 2013, Omnyx has integrated Visiopharm’s clinically validated breast panel analysis algorithms for HER2, estrogen receptor, progesterone receptor, and Ki67 into its open platform Dynamyx software. Dynamyx is available for research use only in the United States.
The algorithms “give pathologists additional insights when evaluating certain breast tissue, helping to standardize data and produce concise and consistent results,” according to a statement from Omnyx.
The Dynamyx software is also integrated with the Objective Imaging Desktop Scanner from Objective Imaging, which allows Omnyx customers to connect remote networks of pathologists for collaborative purposes.
Dynamyx provides advanced image and tissue navigation via Omnyx’s TissueSync and TissueDirect algorithms. TissueSync reduces manual steps by automatically aligning an identified area across multiple stains, while TissueDirect reduces pan and zoom time while quickly navigating to tissue sections.

***Omnyx LLC**, 412-894-2100*

[hr]

Dr. Aller is director of informatics and clinical professor in the Department of Pathology, University of Southern California, Los Angeles. He can be reached at raller@usc.edu. Hal Weiner is president of Weiner Consulting Services, LLC, Eugene, Ore. He can be reached at hal@weinerconsulting.com.