The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2017
PHILADELPHIA, TUESDAY, JUNE 6, 2017 VOL 255 • NO. 108 An ALM Publication

CYBERSECURITY

Cloud Control: Data Security Hazards and How to Avoid Them

BY ABRAHAM J. REIN
Special to the Legal

Cloud computing, virtually nonexistent 15 years ago, is now verging on being the rule rather than the exception in the business world. According to the Gartner technology research firm, by 2019, more than 30 percent of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only, and by the year 2020, a corporate "no-cloud" policy will be as rare as a "no-internet" policy is today. It is more critical than ever that lawyers and their clients become familiar with the data security and compliance pitfalls potentially associated with cloud computing and acquire the knowledge and tools to avoid them.

CLOUD IS DIFFERENT

The National Institute for Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources ... that can be rapidly provisioned and released with minimal management effort or service provider interaction." In laypersons' terms, the cloud is a model of computing that utilizes shared computer processing and storage resources, usually provided by a third party, which are accessible via the internet on demand from anywhere; examples to many consumers include Dropbox, Gmail and Apple's iCloud. Convenience, ubiquity, and on-demand availability and scalability are built in to the very concept. While this is, generally speaking, a feature rather than a bug—and no doubt has contributed to the rise of the cloud as a standard approach to business computing—it carries with it certain risks that are new or heightened in the cloud age.

The most concerning of these dangers from a compliance and risk-mitigation perspective stem from the facts that: unsophisticated individuals,

ABRAHAM J. REIN *is co-chair of Post & Schell's information privacy and security practice group and a principal in its internal investigations and white collar defense practice group. A former web developer, his practice focuses on the intersection of technology and the law, advising clients on legal aspects of data security, social media compliance, e-discovery and constitutional rights in a digital era. Contact him at arein@postschell.com.*

> *It is more critical than ever that lawyers and their clients become familiar with the data security and compliance pitfalls potentially associated with cloud computing and acquire the knowledge and tools to avoid them.*

including employees and staff of a law firm or its client, can put data in the cloud completely unbeknownst to those in the organization with responsibility for managing information-related risk; and using a cloud services provider can create the temptation to let down one's guard, believing that the third-party provider is handling the "hard stuff," including data security and compliance.

Each of these issues, in its own way, can and has led to legal problems for companies entrusted with sensitive data. They point to certain high-level risk mitigation measures that companies should be considering with respect to the cloud.

Some cases in point:

• **Privilege waiver.**

Earlier this year, a federal magistrate judge in the Western District of Virginia heard arguments about a party's use of the cloud file-sharing service Box.com to transmit sensitive material to counsel. In that case, *Harleysville Insurance v. Holding Funeral Home* (W.D. Va. Feb. 9), Harleysville Insurance Co. sought a declaratory judgment that it did not owe a funeral home's fire loss claim, because the fire was intentionally set. An investigator with Harleysville set up an account on Box.com for sharing material related to the case. First, he used that account to transmit the surveillance video of the incident to the National Insurance Crime Bureau (NICB), a third-party organization that was helping the company look into potential insurance fraud. Then, some time later, the investigator used the same link to send the entire claims file to counsel. And some time after that, the funeral home subpoenaed NICB for its files relating to the case, and received as part of the production the email containing the link to the Box.com site. The funeral home's counsel followed the link and downloaded the ostensibly-privileged case file, which was not encrypted or password protected.

The magistrate, while disapproving of the funeral home's counsel's accessing and retention of the putatively privileged material, held that the unprotected use of Box.com resulted in a waiver of attorney-client privilege and the work product protection. The court said, "It is hard to imagine an act that would be more contrary to protecting the confidentiality of information than to post that information to the world wide web," and described the act as "the cyberworld equivalent of leaving the claims file on a bench in the public square and telling its counsel where they could find it," adding:

The technology involved in information sharing is rapidly evolving. Whether a company chooses to use a new technology is a decision within that company's control. If it chooses to use a new technology, however, it should be responsible for ensuring that its employees and agents understand how the technology works, and, more importantly, whether the technology allows unwanted access by others to its confidential information.

• **HIPAA violation.**

In the summer of 2016, the Oregon Health & Science University (OHSU) agreed to pay $2.7 million to settle with the Department of Health and Human Services (HHS) a HIPAA breach claim partly involving Google cloud services. Several residents and physicians-in-training had placed spreadsheets of patient information in Google's cloud, for the purpose of keeping one another up to date regarding admissions. Although the services were password protected, and although there was no evidence that the data had been accessed by anyone without a legitimate purpose, OHSU did not have the requisite business associate agreement with Google. The cloud usage was, therefore, a HIPAA breach, and triggered a $2.7 million settlement.

• **SEC enforcement.**

Investment adviser R.T. Jones used a cloud provider to host information about eligible participants in its client retirement plans. That information included social security numbers, dates of birth, and names, which Jones used to verify the eligibility of visitors to its website. The cloud provider did not provide encryption for the data it held; Jones, for its part, also did not encrypt the data before loading it into the cloud. Eventually, China-based hackers gained rights to copy the personal data of some 100,000 individuals. Although Jones's forensic consultant was not able to determine whether the hackers had actually extracted the data to which they had access, and there was no evidence that any of the victims

suffered any financial harm, Jones (appropriately) notified all potentially affected individuals, offering free credit monitoring; Jones also appointed an information security manager, implemented a new firewall and logging system, and retained a cybersecurity firm to provide real-time monitoring and reporting. The SEC, finding a violation of Regulation S-P, which requires registered investment advisers to adopt written policies and procedures that are reasonably designed to safeguard customer records and information, imposed a civil monetary penalty of $75,000.

• **FINRA examinations.**

In January, the Financial Industry Regulatory Authority (FINRA) issued its annual letter outlining its priorities for this year's compliance examinations. As it has for years, FINRA included cybersecurity among its priorities. This year, however, FINRA noted that, "in multiple instances," firms have failed to preserve certain records in a nonrewritable, nonerasable format commonly known as "write once read many" (WORM) format as required by Securities Exchange Act (SEA) Rule 17a-4(f). Importantly, the examination priorities letter goes on to specifically call out the use of third-party service providers to host such data: "This includes situations where vendor-provided email review and retention services"—generally cloud-based email platforms that advertise a compliant environment for archiving and otherwise following financial sector data requirements—"did not fulfill SEA Rule 17a-4(f) requirements." In December 2016, FINRA fined 12 firms a total of $14.4 million for failures to retain records in WORM format.

KEEPING YOUR HEAD IN THE CLOUD

As Harleysville Insurance Company and OHSU learned, a naive employee's well-meaning attempt to get something done can lead to data finding its way into the cloud that had no business there, with potentially disastrous results. The high-level lesson here is that companies stewarding sensitive data—and that is nearly every company today—should work to foster a culture of awareness around data security issues. This starts with training, which is key, but it does not end there. Perhaps the most important element of a culture of compliance is the tone at the top: companies should make efforts to demonstrate that the highest levels of the organization prioritize data privacy and security. Work to develop a sense of shared values that include safeguarding customers' and the company's sensitive information. Importantly, react when things go wrong, and do so visibly (one of OHSU's problems was that it was a repeat offender—over the years, multiple unencrypted OHSU laptops and thumb drives containing protected health information were lost or stolen, but OHSU did not react by encrypting its devices). Consider running data breach response drills and appointing a chief information security officer, and ensure appropriate funding and infrastructure are in place to sufficiently support data security efforts.

Another lesson, equally important but perhaps less intuitive, is that companies, including their data security and compliance functions, should strive to listen to their employees to enable them to do their jobs securely. In the OHSU case, the residents and physicians-in-training were trying to respond to a need for a shared data repository; perhaps, if management had been aware of that need and worked with staff on implementing a secure solution, the problem could have been avoided.

Finally, as demonstrated by the SEC and FINRA actions described above, companies should not assume that their cloud service provider will take care of everything. At bottom, this means that companies should have all of their key stakeholders—not just IT, but legal, compliance, risk management, representatives of the staff who will be using the systems, etc.—at the table from the beginning when negotiating a new cloud arrangement. Ensuring that all voices are heard from day one will go a long way toward mitigating risks before they become full-blown problems.

CONCLUSION

Companies cannot avoid the cloud, nor should they: the cloud represents convenience and cost savings in many situations. But this means that companies should come prepared to address the potential risks that poorly planned or poorly executed cloud usage can pose. As with all things compliance, there is no magic bullet, but fostering the right culture, and involving the right stakeholders in decision-making from the beginning, can help to avoid pitfalls. ●