LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

OM OPERATIONS MANAGEMENT

Staying Safe in the Cloud

What should firm administrators know about security in an era when hackers are targeting their organizations?

A couple of years ago, Jobst Elster, Head of Content and Legal Market Strategy for InsideLegal, attended a legal technology conference during which the chief information officer of a law firm representing the online sharing service Dropbox acknowledged his firm didn't sanction attorneys' use of Dropbox for security reasons.

ED FINKEL
Freelance Writer and Editor

"You'd think you could make an exception for your own client," Elster says, but he also understands why the policy was put in place. "It's the consumerization of information technology," he said. "People are using it already for at-home use because most of them have free accounts. They're familiar with it, so they're wanting to use these same services for professional purposes."

Dropbox is but one of many such file-sharing services — provided by mega-companies like Microsoft and Google down to small startups — that have populated the online cloud in recent years, giving attorneys and other professionals the ability to share and store documents and data. But just because they can use those services doesn't mean they should — at least not without first carefully considering the security concerns involved.

CLOUD CONSIDERATIONS: THE PROS AND CONS, WHAT TO STORE, AND WHERE TO STORE IT

Entering the cloud presents a tricky calculus, but law firms — especially larger ones — should be considering their options, says Stewart A. Baker, Partner at Steptoe & Johnson in Washington, D.C., and a former Assistant Secretary for Policy at the U.S. Department of Homeland Security.

"On the one hand, there are new and uncharted vulnerabilities in cloud computing, and we're going to find out about them only when breaches occur," he says. "On the other hand, most law firms are not in the IT business and certainly aren't in the IT security business. You have to ask, 'Will I and my IT staff do a better job of protecting information with the resources we have than some company that can afford to put substantially more resources into protecting that data?' "

Law firms and other organizations are drawn to the cloud "to try to leverage the power of the scale of web services," says Stephen L. Surdu, Vice President of Professional Services for Mandiant. "For smaller organizations, it's an easier financial situation and personnel situation if they can outsource their IT functions. … With time, we've seen more and more outsourcing into the cloud. I don't think this is a pendulum shift, where it's going to swing back. It's really a trend where you can get quality while outsourcing. That doesn't mean it's secure."

"A law firm that is outside counsel to a major financial institution that can spend millions of dollars on net defense might not have the same resources to protect themselves, yet they are given the proprietary information from the company and entrusted to protect it as if it were their own."

AUSTIN P. BERGLAS
Assistant Special Agent, Federal Bureau of Investigation

That means firms and administrators need to think about what they're willing to put out in the cloud, says Ben Schorr, Chief Executive Officer of Roland, Schorr & Tower. "The firm's softball brochure, a draft copy of the firm's brochure, you probably don't care about locking that down," he says.

Firms should bifurcate their data into what does and does not need a high level of security, says Dan Pepper of Pepper Law Group LLC. "The high level might be, certainly, financial information, but also personal information regarding the client," he says. "That's the kind of information I would think twice about before storing in the cloud; you're better off keeping it behind a firewall in your own firm. But court filings, or other documents that might be public, or quasi-public, such that if they were disclosed or subject to a breach, you would have minimal or low damage – perhaps that's more appropriate for cloud storage."

Austin P. Berglas, Assistant Special Agent in charge of the cyber branch at the Federal Bureau of Investigation (FBI), says that a law firm's crown jewels, such as intellectual property information, should probably be walled off from anything external-facing, although at the same time, the firm needs to strike a balance. "You have to take ease of use in thought when you're trying to do that," he says. "A lot of lawyers are not in the office every day, and they need to access the information remotely."

"Just because you assemble documents in the cloud doesn't mean they have to be stored there."

JOHN SIMEK
Vice President, Sensei Enterprises Inc.

SCOPING OUT THE THREATS

Law firms need to realize that would-be hackers see them as valuable and efficient paths to sensitive client information, Berglas says. "They are often times considered a softer target," he says. "A law firm that is outside counsel to a major financial institution that can spend millions of dollars on net defense might not have the same resources to protect themselves, yet they are given the proprietary information from the company and entrusted to protect it as if it were their own." Once a law firm is identified as being involved in a deal, merger or acquisition – whether through the press or by other means – he says, it can expect to be attacked by a hacker.

The threats facing law firms in the cloud aren't that different from those they face on premise, although they're different in scope, Schorr says. Those include "losing the data entirely, losing access to the data temporarily at critical times, having the data compromised in some way in the hands of people who shouldn't have it," he says. "If the people coming after your data are state-sponsored actors from China or wherever, you're going to assume they have a significant budget. … On the other hand, opposing counsel from a small town, they're not going to send a team of ninjas to break into your office."

Legal administrators, information technology staff and firm partners need to be concerned about a few different categories of threats, says Surdu. Hostile nation-states might target law firms because

they're interested in either intellectual property litigation or mergers and acquisitions. In other cases, "If a hack-tivist gets a bee in his bonnet, sometimes [he'll] find vulnerable sites and create a reason why they have a problem — concoct a reason why they want to go after the organizations."

Law firm Kelley Drye & Warren LLP is concerned both about rival firms and foreign governments, says Judith Flournoy, Chief Information Officer for Kelley Drye in Los Angeles. "There are outside countries that are tremendously interested in what we are doing," she says. "It's not a question of, 'Have you been [breached]?' It's a question of, 'When were you, and how do you avoid getting breached again?' "

John Simek, Vice President of Sensei Enterprises Inc., notes that disgruntled employees can be a concern. "Maybe you're involved in a high-stakes litigation," he says. "[The opponents] approach one of the employees and say, 'I'll give you $10,000 if you get the data for this particular firm.' "

"Every firm is very mindful of the potential threat of being breached. We take our relationships with outside vendors very seriously; we do due diligence, understand what their security plans involve, what certifications they have."

JUDITH FLOURNOY
Chief Information Officer, Kelley Drye & Warren LLP

SELECTING A CLOUD PROVIDER

To test out the cloud, many law firms are piloting certain applications rather than taking an all-or-nothing approach, Elster says. "They use different services for different applications to see the [pros and cons] and see what maybe complements each other, so they have a diversity of [vendors]," he says.

Simek sees firms at all points along the spectrum. He suggests starting with a non-critical service and seeing how it goes. "If that's successful after several months, try something else, maybe document assembly," he says, adding, "Just because you assemble documents in the cloud doesn't mean they have to be stored there."

Kelley Drye is using Microsoft Office 365 for document management, after hosting such services internally, Flournoy says. "[It has] all the appropriate security certifications," she says. "Every firm is very mindful of the potential threat of being breached. We take our relationships with outside vendors very seriously; we do due diligence, understand what their security plans involve, what certifications they have."

Baker urges firms to negotiate what they can, realizing that vendors will have different priorities. "Law firms tend to want a lot of assurance in the form of liability. Cloud companies tend to want to provide standardized products with very limited assurances," he says. "If you can't get comfortable with the extent of liability that cloud providers tend to take on, then you're facing a difficult choice."

Firms need to investigate what level of security each vendor provides — and get it in writing, Surdu says. "There's a due diligence that any organization should do to make sure they articulate what

they're looking for — and have some mechanism, whether it's contractual or monitoring, to make sure they're getting what they want," he says.

Simek says firms and legal administrators need to read the terms of service for a potential provider to see what they're being promised. "It amazes me how many people just don't," he says. "They need to see what [are] the vendor's obligations, what [is it] going to do and how [is it] going to do [them]. The key components are the encryption and protection of data."

And what about court orders or subpoena requests — does the provider give up the data right away, or notify the firm and give it an option to file a motion to quash the subpoena? "For law firms, that's certainly one of the provisions they want to be sensitive to and look for," Simek says. "Encryption is your friend when it comes to protecting data, despite urban legends about the National Security Agency having a back door to everything."

Surdu agrees that law firms and administrators should ask whether their information will be encrypted and segmented appropriately from that of other organizations. "That commingling can be a problem," he says. Be concerned if a cloud provider says, "I don't have the ability to separate your traffic from other people's traffic."

Such arrangements might cost you, but "that's a tradeoff you have to go through," Surdu adds. "If you allow yourself to be thrown into the lowest common denominator because you didn't specify the requirements, you may get something that works for you, from a security standpoint, and you may not."

Firms also should ask where their data is being stored, and where the backup is, Schorr says. "Somebody might say, 'Our data center is in Ohio.' OK, fine," he says. "Where is your backup? 'Our backups are in Singapore.' This might be a problem." But many firms don't ask that question, he says. "Many times they can get cheap data storage in these offshore countries, but it puts them at risk or at [the] mercy of local governments."

Firms also need to find out what happens if you want to retrieve your documents and move them somewhere else. David Gracey, Founder and President of Network 1 Consulting, a technology outsourcer that works with law firms, says law firms should ask about the process or cost of extracting data onto a USB drive. "Unless you plan on having it there forever," he says, "someday you're going to have to move your documents. What's that going to look like and feel like?"

The bottom line? Deal with your vendors the same way your clients deal with you, Berglas says. "I'm entrusting that important information to them, and hopefully they'll treat it like it's their own," he says. "But you're one of many clients. They may not afford the same protections as you would with their own data. It's a business decision; something's going to have to give. You don't have enough storage space or money to build your own storage space inside your company — but you have to be concerned about the standards of these third parties."

"People are using these solutions without much guidance and without a lot of forethought. They don't think through the various risks when they throw a document up on Dropbox. Later on, somebody shares it with somebody else, and now you're in a world of hurt."

DAVID GRACEY
Founder and President, Network 1 Consulting

MANAGING FIRM LEADERS

To guard against these threats, legal administrators must lead other senior staff in developing a security awareness program, whether internally or with the help of an outside vendor, Flournoy says. "How do you get senior people to pay attention?" she says. "Citing a few facts, citing the FBI, citing what your rival firm down the street is doing."

Flournoy suggests tapping an attorney to be the point person for communicating risk management to the firm's partners. "For a law firm administrator, having that person in the same camp, standing shoulder to shoulder with [her], can be very effective," she says. "Messages carry much more weight if they come from the chairman, managing partner or general counsel. I have no reluctance whatsoever to leverage those resources."

Working with firm leaders on with cloud security compliance requires a delicate touch, Elster agrees, because senior partners are sometimes the worst offenders. "You know what you signed up for when you decided to work in a law firm," he says. "You know whose name is on the door. Bring-your-own-device policies started because a senior partner said, 'I use my iPad at home; I want to bring it to work.' It's part of a broader trend [toward those policies] that creates a lot of security concerns."

Senior attorneys and staff don't always follow policies — or pay attention to them in the first place, Gracey says. "A lot of times they bypass IT because IT is the 'Department of No,' " he says. "People are using these solutions without much guidance and without a lot of forethought. They don't think through the various risks when they throw a document up on Dropbox. Later on, somebody shares it with somebody else, and now you're in a world of hurt. Get an IT person involved in those decisions; [he's] going to ask a lot of questions that the lawyers and staff don't think about."

Setting up an information technology committee can help partners, legal administrators, IT directors and others come together in an open forum. "As the IT guy, my job is to say, 'no,' but also to listen and find out what your needs are and come up with a solution," Gracey says. "Most partners want to do the right thing. They're not rogue and doing it on their own."

To convince senior partners of the need to concern themselves with security, Elster suggests citing any concerns a client might have about how their documents are stored. "We won't be able to land this client if we don't have these security measures in place," he suggests. Some firms are hiring senior staff from agencies like the U.S. Securities and Exchange Commission, which "don't have a lot of baggage related to law firms," Elster added. "They can say, 'You hired me to do this; you need to comply.' "

Simek suggests making the business case — but being flexible about devices. "They all listen to money," he says. "If you can say, 'I can save money by doing such and such, and here's what the risks are,' they love it." But if you say, "We don't have to spend $8,000 on new software, we can use this service for half the cost, but you can't use your iPad to get it," senior partners are likely to balk. "Whatever solution you give them, their toys had better work, whether it makes sense or not."

Schorr suggests totaling all the costs on either side of the ledger when it comes to devices. "It's a lot cheaper to encrypt it than it is to write letters to all of your clients apologizing for losing all of their data," he says. "You don't want to be the guy who has to admit in court that he didn't do what he was supposed to do because he was too cheap or lazy. The expense is miniscule compared to the expense of losing that stuff."

ASSESSING YOUR FIRM'S NEEDS

Law firms can hire a third party to undertake a vulnerability assessment and identify potential threats, Surdu adds. "We have tools that allow us to look for the presence of current activity by attack groups, or past activity," he says. "There was a person in our environment, and there's how [he] got in — those things usually get people's attention."

A security audit can help firms ensure that they're meeting clients' expectations and that they're handling sensitive information appropriately, Pepper says. "I don't think, as a general rule, lawyers have met those expectations," he says. "We're looking to reduce costs, increase efficiencies, and move into the cloud or other technologies to streamline the business flow. What do we need to worry about?"

To learn more about vulnerability assessments and other best practices when it comes to implementing cybersecurity techniques, read Jonathan Adams article, "Cybersecurity: The New Frontier," in this month's issue of *Legal Management*.

ABOUT THE AUTHOR

Ed Finkel is a full-time freelance writer and editor who covers law, technology, medicine, education and youth, and other issues. His legal writing background includes work for the *ABA Journal, Student Lawyer* magazine, the *Illinois Bar Journal* and *Chicago Lawyer*.

Email
Website