Managing E-Discovery Providers In Times Of Crisis

By **Shannon Capone Kirk**

Shannon Capone Kirk

The current COVID-19 pandemic has led law firms and clients to reevaluate their crisis preparedness. Transitioning to remote work has become an area of key focus as law firms and their clients are forced to address employee and vendor workplace safety concerns, business continuity, information management, cybersecurity, and government advisories that — at times — have evolved dramatically during the course of a single business day.

In addition, providers face increased risks of ransomware attacks. As such, it is fair to say, there have been extraordinary efforts around security in the last month.

With respect to the use of e-discovery hosting and managed review providers, this atmosphere has necessitated rapid decision-making that contrasts with the often lengthy process of setting up and vetting such arrangements. Under normal circumstances, retention of e-discovery providers involves considerable time and several layers of approval.

In other words, practicalities during the current world health emergency have proven that law firms must have the acuity to make smart, but quick, game-time decisions. We should make sure that falling to the level of our training actually helps us rise to the level of our expectations.

In dealing with our current pandemic, it became clear, or more universally accepted, that some portion of the legal profession would be transitioning to a telecommuting model over a short period of time. However, telecommuting presents particular challenges for e-discovery providers, and managed review in particular.

To wit, it was almost always the case that, up until this pandemic, managed review centers did not provide contract attorneys with encrypted laptops for remote work, or, in large part, allow remote work at all. Certainly there are exceptions, but those are in the minority.

So what have we learned over the last few weeks? What decisions did we need to make? What compromises, or risks, did we have to mitigate and accept? And what should be expected from the e-discovery providers for crisis planning going forward?

Above all, we needed to mobilize quickly. We had to address both the need to ensure contract attorneys were in safe environments and practicing social distancing, as well as the need to ensure secure computing and confidential review space requirements. Toward this end, we held numerous calls and exchanges with clients, hosting vendors and managed review facilities.

All of this required a significant amount of coordination and confirmations, especially around information security, in order to provisionally approve a transition to remote review. Above all, we handled each vendor and matter separately, as there are nuances important to each case; levels of risk that are palatable in some cases do not transfer to all.

After provisional approval and our understanding of the remote security at each provider, each matter required informed client consent. Ultimately, only the client can judge the balance of risks. To obtain informed client consent, it was important to understand each aspect of a provider's remote work security requirements, and, importantly, what questions to ask and factors to pressure-test.

One example of a question that practitioners might want to ask themselves is this: Do I know if my remote contract attorneys are using personal computers or provider-supplied laptops, and has my client been so informed?

In this exercise, we found most vendors provided swift, detailed, appropriate, and, some, above par responses and protocols. A few did not. No names will be used herein or elsewhere. Rather, in viewing what we've learned across a selection of providers, we recommend considering the below practices going forward.

We also recommend considering whether these should be required in future provider contracts, even in the absence of an epidemic or pandemic.

In other words, if two providers' responses to a request for proposal are, for all intents and purposes, equal in terms of price, quality, tools and project management, perhaps consider whether one deciding factor is whether a provider has a good crisis management plan in place, one that they are willing to back up by adding express language into the terms of service and whether they have demonstrated that their actual resilience withstood the test of our times.

Protocols That Should Be Considered for Future Crises

1. E-discovery providers should have a plan in place to continue to monitor contract attorneys' productivity, engagement, consistency across reviewers, and group and individual performance. In addressing remote work for coronavirus needs, at least a couple providers noted their virtual rooms or classrooms, which should, in effect, provide an environment for the same guidance, oversight, feedback and tracking that would otherwise be had in a managed review facility.

2. Review and virtual meetings must be conducted in a way that maintains privilege. Providers must forbid contract attorneys from working anywhere within their residence where others, including family members, could overhear team meetings.

They must also make sure to position their computer screen(s) to prevent others, including any family members, from seeing displayed content. One provider we spoke with described extensive interviewing and background checks, requiring applicants to supply photographic proof of a separate home office.

3. The provider, if offering remote reviews in the event of crises, should be prepared to equip reviewers with secure, company-owned and -managed laptops. These laptops should have encrypted hard drives, up-to-date anti-malware software, and endpoint detection and response software, and be configured to allow for secure access to the hosted review platform through a virtual desktop environment by way of multifactor authentication.

The provider should also require secure remote access that prevents network traffic from being "split-tunneled."[1] Saving to a removable media must be disabled. Several providers we spoke with already offered to provide secure laptops with these features, rather than allowing reviewers to use personal computers. We viewed these providers favorably and appreciated their partnership in safeguarding client data.

4. Remote access to review platforms should be configured to prevent connections from devices that do not have up-to-date anti-virus software or current operating system and software security patches.

5. The process for provisioning remote access should be vetted with someone knowledgeable about information security. Over the course of conversations with several providers, we learned that we obtained the most accurate security information when speaking directly with the person or persons in charge of the providers' information security.

In some instances, the information security person's answers conflicted with a sales or project management lead. Providers should have qualified information security professionals on staff or a managed security service.

6. The provider's ability to log and audit remote access session information, including source IP address, username and authentication status, should be explored.

It can be expected that some reviewers might not have an ideal location in their home to telecommute and choose to conduct review in a public setting. To mitigate this risk from a technological perspective, providers should log all authentication events, including source IP addresses and usernames, and store in a centralized log-monitoring platform, such as a security information event management platform. Logging on source IP and some form of auditing of same should be explored where it is likely not possible to restrict source IP logins, given the nature of dynamic IP access.

An additional security measure would be to explore requiring reviewers to access the review database through Citrix or another virtual desktop. This setup prevents access for anyone not connecting through the virtual desktop client.

7. We noted that when a separate managed review provider and hosting provider were engaged for the same matter, it was necessary to bridge the security personnel at both providers and ensure a clear understanding of who was responsible for multifactor authentication and IP address white-listing, logging and monitoring. In short, if there was a breach, would we face two providers pointing to the other?

8. During the recovery phase and return to a traditional on-site model, managed review providers should confirm that no handwritten notes or papers remain in the personal possession of contract attorneys. Any such document should be disposed of using a cross-cut shredder. If a remote reviewer does not own a cross-cut shredder, they should be instructed and required to place printed material in a locked drawer, cabinet or safe until they return to the managed review facility and cross-cut shred it.

As a best practice, reviewers should not be permitted to remove physical binders from review facilities; instead, consider using only PDF binders and password-protected review manuals. If physical documents must be provided to reviewers, such materials should be promptly returned to the provider, which should maintain a log of all such materials to ensure their proper return.

9. The ability to print, download, take screenshots, copy and paste, save data to removable media (USB memory stick or optical media), access cloud-based file storage or collaboration sites, or otherwise capture and store information from the review environment should be disabled, along with blocking access to personal email.

10. Providers should have a plan in place to account for wellness and team building to

provide opportunities for hourly workers to alleviate stress. Above all, those providers that do not value their people will not be able to protect clients as well as those who invest in the health and well-being of reviewers.

11. Although no technology exists to keep reviewers from taking photos of computer screens with personal cameras or phones, providers should consider updating their confidentiality agreements to cover such possibilities, to the extent they do not already, and provide specific written remote-work guidelines to their reviewers.

Additional Protocols We Would Like to See in the Future

1. If it is necessary for the review to be conducted remotely, the provider should ensure that reviewers have access to dual monitors.

2. Providers should consider restricting remote access to the review database after defined review hours. Review quality falls significantly when reviewers are exhausted, and remote work can become a trap of being always at work.

3. Providers should consider providing additional training to reviewers and/or increase staffing of IT personnel to ensure a smooth transition to remote review.

4. Over the course of a week or two, as the industry advanced further into telecommuting, most providers did agree to provide company-issued laptops upon request. The standard should be that they are provided when requested, unless a robust container or controlled virtual machine is dropped onto physical computers.

Shannon Capone Kirk is counsel at Ropes & Gray LLP.

Ropes & Gray senior e-discovery attorneys Emily Cobb and Martha Harrison, e-discovery attorneys Chris Sun and Tina Soumela, senior manager of legal technology services Winston Burt, director of legal technology and IP paralegal services Barbara Gueth, and senior director of information security Scott Ashton contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Split-tunneling refers to a configuration where VPN software allows the VPN-related traffic to flow through the VPN, but other traffic to bypass the VPN connection, which frustrates the ability of the corporate security infrastructure to monitor traffic.