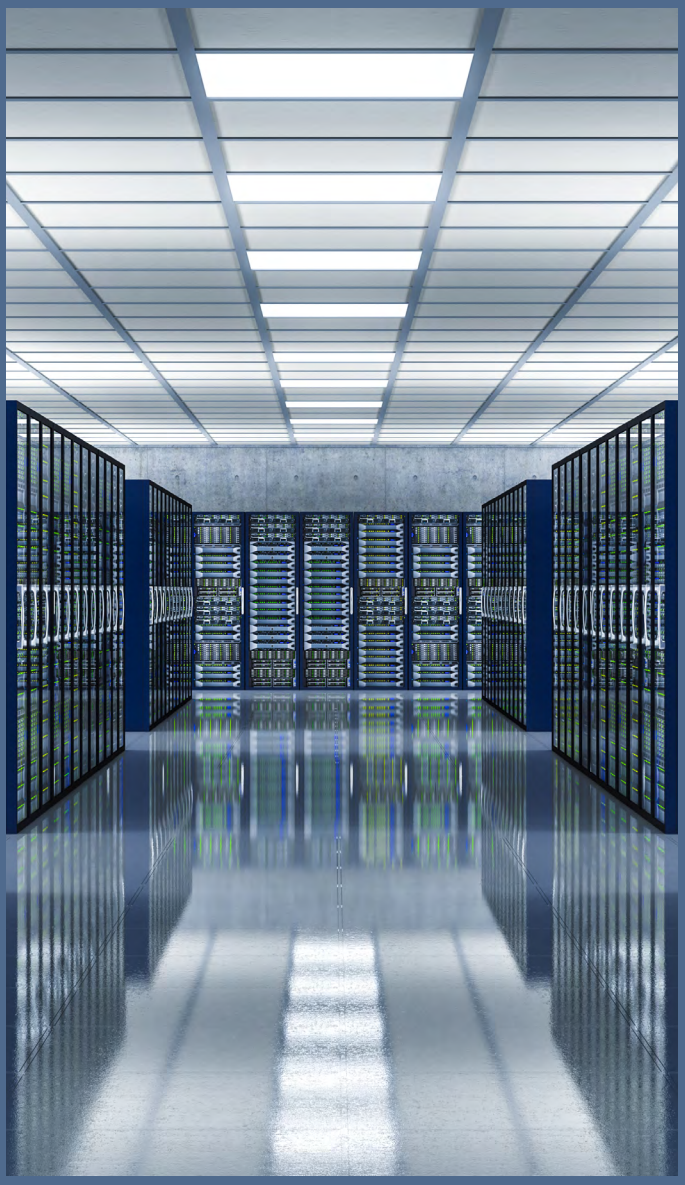

JS|HELD

PERSPECTIVES

Safeguarding Cloud-Based Data & Mitigating the Cyber Risks Associated with a Remote Workforce

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Efficiency, scalability, speed, increased cost savings, and advanced security for highly sensitive data remain in high demand by users of eDiscovery services. To meet that demand, cloud technology promised several of those benefits.

However, the advanced security of the data depends on how an eDiscovery service provider implements, maintains, and manages sensitive client information.

This issue has become more significant as the majority of the workforce is dispersed and often working from unsecured home environments has therefore driven an increased usage of cloud services. That greater cloud usage has opened the door to riskier data storage scenarios that might not be fully apparent to those users of eDiscovery services. Furthermore, the firms providing these services may not be knowledgeable about all of the risks inherent to their activities and processes.
Because the industry has moved toward commoditization over customization, the workforce within some eDiscovery providers consists largely of junior staff who should follow strict protocols and procedures while in the office. While these activities may have been proven and vetted in the office environment to meet minimum security standards, the majority of employees are not likely to be mindful of the security risks inherent to working at home.

This paper examines the inherent risks surrounding the protection of client electronic data on cloud-based platforms that have arisen with the proliferation of the at-home work setting. It also explains why it's important for users of eDiscovery services to scrutinize the technical capabilities, practices, and experience of the professionals that will be handing their data to ensure proper precautions are in place.

THE CLOUD: A SOLUTION THAT INTRODUCES ADDITIONAL RISKS

Many eDiscovery providers have recently migrated hosted client data from private data centers to public or private cloud environments. As hosted data volumes increased, so did the complexities involved in scaling the physical resources required to maintain private hosting environments in a way that met the speed, efficiency, redundancy, and security requirements of clients. Consequently, eDiscovery providers began reexamining the risks and costs associated with their hosted portfolios and many of them turned to the cloud as a solution. But this also introduced other issues as well that may not have been fully reconciled to date and may have been exacerbated by the pandemic.

Security

It is not uncommon for an organization's most sensitive data to be found on eDiscovery platforms. That data often includes privileged communications, business strategy decisions, trade secret information, potentially embarrassing personal communications, and other confidential communications from its employees, leadership, and legal counsel. Cloud hosting services that are run by eDiscovery providers have a range of security capabilities that are often unexamined by the eDiscovery user.

Due to the increasing sophistication of state and non-state cyber hackers, there is continued and mounting risk of infiltration by hostile actors. This was illustrated in the 2020 SolarWinds attack on the U.S. government. In that scenario, a trusted technology service firm tasked with maintaining the computing environment within several of the world's most secure data centers provided the doorway for hackers to access the country's most sensitive data.

Then there are the inherent risks with at-home working environments that have increased due to the COVID-19 pandemic. With the advancement and continued adoption of IOT (Internet of Things) devices and the expansion of high bandwidth Internet services for residential consumers, there exists multiple pathways for trusted home-based Wi-Fi connected services in the form of "smart devices" (smart speakers, thermostats, alarm systems, TVs, etc.) to become compromised in an environment that isn't usually monitored for malicious network activity. This is compounded when employees of eDiscovery providers lack experience or knowledge around network security risks.

Reliability

Cloud services offer the promise of unparalleled reliability with limited downtime for the document review operations of eDiscovery users. Although there may be regularly scheduled maintenance windows, emergency outages do happen occasionally. Consider Google's outage in December of 2020. Disaster-related outages to users of eDiscovery services hosted in the cloud can have severe impacts on a client's ability to meet court-mandated and other production timelines.

Data Protection and Privacy Concerns

Cloud hosting solutions can and often do provide data storage local to regional jurisdictions that require personally identifiable information (PII) redaction and identification before extraditing that information to another country (such as the United States). This offers the promise of eDiscovery providers having locally available data storage in the region requiring the privacy regulations.

However, given the multitude of regions throughout the globe with data privacy regulations, a user of eDiscovery services should not assume that their data is be hosted in accordance with local regulations. In general, users of eDiscovery services should confirm with their providers where the physical servers are located that will be housing the protected data.

Additionally, with the majority of the staff of eDiscovery providers working from home due to the pandemic, it may be important to ask how a mindful approach to global data privacy regulations is being addressed.

Global Context

Cybercrime is projected to have cost the global economy nearly $1 trillion in 2020. Furthermore, hacking and infiltrations into government and business entities is increasingly viewed as the best way for adverse nations and other bad actors to have the greatest impact on their targets. This is all intensified by the global pandemic, when at-home working environments and increased use of social engineering in generally insecure environments present added risks to the security of data under management.

HOW TO ENSURE YOUR DATA IS SECURE

What are some of the ways that users of cloud-based eDiscovery services can verify that their data is being safeguarded?

Cloud Security

One important step to take is to ask if the cloud-based eDiscovery solution has been certified to various security standards. While this isn't a guarantee that your data is not exposed, it does present some level of comfort that security protocols are tested on a regular basis by an impartial third party. Some certifications that are relevant here include: SOC2 Type 2, ISO 27001, ISO 27017, ISO 27018, as well as certifications that indicate the hosting provider is mindful of data privacy regulations and HIPPA requirements.

It's important to differentiate certifications that are attributed to the cloud operator as opposed to the data hosting service provider. For example, AWS, Google, and Microsoft Azure have a number of sophisticated data security certifications associated with their up-stream operation of the cloud environment.

However, it's important to note that an eDiscovery platform running within that cloud environment employs its own security protocols to allow reviewers to access documents and as a result does not inherit all of the security controls that exist on the base layer cloud offering. Make sure you know what security protocols and certifications your application of choice can directly lay claim to.

Work From Home Security Considerations

This presents additional considerations. Many eDiscovery providers will point to employee handbooks and corporate policy documents as an initial answer, but in this unprecedented time, it is unlikely that those guidelines anticipated a scenario where the majority of the workforce was working from disparate outside and nonsecure locations.

Depending upon the technical environment available at the eDiscovery provider, measures can be taken to come

close to the network restrictions in place in the office. No solution will be 100 percent risk free , but there are best practices that can be implemented to mitigate major risks. For example, the provider can take a centralized security approach through the use of a VPN (virtual private network) connection to the office environment that restricts access to non-essential networks and prevents employees from using non-work issued computers.

It's also crucial to be aware of the different levels of security restrictions appropriate for employees focused on different aspects of the eDiscovery process. For instance, someone performing document review likely requires less access to sensitive client data than the project manager in charge of organizing the review. It's necessary to understand what at-home procedures your provider is using and how that affects the safety and exposure of your data.

CONCLUSION

Notwithstanding the issues that have arisen, cloud-based eDiscovery solutions provide users numerous advantages in tackling the unprecedented challenges being faced in the post-COVID world. At the same time, it's equally important for users to know and understand what protection providers are enacting to safeguard their data. Cloud storage solutions address issues faced by aging technical infrastructure, can greatly bolster cybersecurity and provide eDiscovery providers the flexibility to operate in a global setting. The added risks posed by work from home environments due to the pandemic mean that buyers of these services should closely monitor the whereabouts, protection, and technical environments employed by the firms working with their sensitive data.

ACKNOWLEDGMENTS

We would like to thank Stephen O'Malley for providing insight and expertise that greatly assisted this research.

Stephen O'Malley is a Senior Managing Director and serves as the practice leader for J.S. Held's Digital Investigations & Discovery practice within Global Investigations. He has engaged on some of the largest multinational investigations and has provided expert testimony in the areas of analysis and restoration of electronic data, electronic discovery best practices, and testing of related computer software. He is an expert eDiscovery practitioner and data analyst. Stephen has significant experience in major fraud and corruption investigations including FCPA, Ponzi schemes, DOJ and SEC investigations; in multijurisdictional litigations; in provision of evidence for litigation support; and in advanced data analysis.

Contact Stephen O'Malley at somalley@jsheld.com or +1 718 510 5617