In the Cybersecurity Hot Seat: How Law Firms are Optimizing Security While Reducing Cost and Risk

Your Highest Priority is also Your Greatest Challenge

Data breaches are not just dramatic headlines in the *Wall Street Journal* and *New York Times*—they are events that increasingly are affecting companies and individuals across the globe. Take, for example, Russian hackers that collected more than 1.2 billion Internet credentials from over 400,000 different websites; or, the "Backoff" malware used in the Target breach that infected the point-of-sale systems of more than 1,000 other retailers; or, the security bug, Heartbleed, which may have caused a hospital system breach affecting 4.5 million individuals.

It's not a matter of if, but when a data breach strikes. These threats are on the rise, and regulators and law enforcement are stepping up their efforts to ensure that organizations are managing personal data responsibly. It is no secret that law firms increasingly are considered a potential weak link in their corporate clients' cybersecurity programs, making security the highest priority—and also the greatest challenge—for law firms both large and small as they shore up on the number of compliance checklists, systems and security procedures.

This perfect storm of risk is especially critical for law firms handling of their clients' e-discovery data, since managing personally identifiable information (PII), trade secret and other sensitive data requires reasonable security safeguards to protect the confidentiality, integrity and availability of personal information.

Clients are increasingly conducting audits of law firms' information security risks as part of their due diligence. The security of a firm is measured, among other things, by data breach response, incident management, change control, firewall monitoring, disaster recovery, business continuity planning, use of encryption, access controls and physical security. While following a risk management methodology such as ISO 27005 and performing SSAE 16 attestation engagements helps focus technology spending and allocation of effort on risks of greatest potential impact to business performance, it may not be sufficient for many firms and their clients. More stringent data privacy requirements, such as becoming ISO 27001, may be necessary.

While there is no silver bullet for every law firm—as reasonable controls for a 1,500-lawyer firm with a large IT budget and department differ considerably from reasonable controls for a 50-lawyer firm with fewer resources—firms must justify that their rationale for their security program is adequate for their organization and, in particular, their clients' e-discovery data.

There is a perfect storm brewing: the volume, variety and severity of cyber threats, combined with rapidly evolving technology, an ever-increasing data footprint and costs to secure data are increasingly leading law firms to evaluate which businesses beyond practicing law they want to be in—and at what cost and risk to both the firm and their clients.

Understanding the Types of Security Risks

There are four general categories of risks law firms need to be aware of as it relates to information security: people, process, technology and data. It is often easiest to focus on the data security aspect—for example, requiring that employees have strong passwords and change passwords regularly, protecting laptops with whole disk encryption, encrypting backup media (a huge source of data leaks), thumb drives, and wireless networks and devices, and controlling access to applications by the employee's function or role. At the physical level, it is easy, at a minimum, to keep servers in a locked rack or room. And as it relates to employees, law firms are increasingly developing incident response and social media policies, and educating employees on those policies.

However, what happens if there is a service-impacting event? How quickly can data be brought back online? How is malicious code detected and prevented? How are networks managed and controlled in order to be protected from threats? How is security maintained for the systems and applications using the network, including information in transit? How are applications and networks tested on an ongoing basis to assess vulnerability?

Ensuring the highest levels of security across all categories of risks requires expertise and infrastructure investments that many firms are not prepared for.

Data Security as a Service

Law firms are moving to managed services as an e-discovery delivery model. They can: provide end-to-end services to their clients leveraging state-of-the-art technology without investing in hardware, software and resources to maintain technology and scale projects; offer budget predictability; and standardize

processes across all cases (which can ensure better results). Managed services is also an attractive model from a security standpoint.

Unlike law firms, managed service providers are in the business of information security. However, not all providers have the same level of expertise, investment and resources to address the major categories of security risk, so it's critical that law firms have their arms around best practices information security requirements before outsourcing key aspects of security to their managed service provider.

Best Practices Information Security Standards

The following are critical questions law firms should ask managed service providers to assess the robustness of their information security programs:

1. Is the managed service provider ISO 27001 certified? What other certifications does the provider conform to and/or have that are relevant to your industry?

ISO 27001 is a security certification standard set forth by the International Organization for Standardization (ISO). Developed to provide a model for establishing, implementing, operating, monitoring and maintaining an information security management system, it is widely recognized as the highest security standard in the industry for examining the efficacy of an organization's overall security posture. The ISO does more than just publish the standards; it also actively researches, creates and normalizes the standards with respect to best practices and the current threat landscape, updating and reissuing them periodically.

A managed service provider that is ISO 27001 certified provides independent evidence that industry best practices are being followed, offering peace of mind to clients that it has successfully implemented a strong information security management system. ISO 27001 also represents that a service organization has been through an in-depth audit of its control activities, demonstrating that it has adequate controls and safeguards in place for managing law firms' and their clients' data (i.e., hosting, processing, etc.).

It is important to note that SSAE 16, a replacement to SAS 70, the previous standard for Reporting on Controls at a Service Organization in the U.S., is not a security standard and it does not provide assurance of an organization's overall information security system. Unlike ISO 27001, SSAE attestation does not demonstrate security, continuity or privacy compliance standards.

Other types of certifications to look for include U.S.-EU Safe Harbor certification, which is a streamlined process for U.S.

Security Checklist

1. **ISO 27001 and Other Certifications**
   - Is the provider ISO 27001 certified?
   - What other standards are met, such as U.S.-EU Safe Harbor certification, HIPAA and certifications relevant to specific industries?
   - Who is conducting the audits to ensure this compliance and how often to they occur?

2. **Application and Information System Access**
   - Are passwords stored and authenticated using industry standard mechanisms?
   - Does the application employ two-factor authentication?
   - Does the application utilize at least 256-bit encryption?

3. **Data Encryption**
   - How is data protected during transmission and at rest?
   - Does encryption exceed standards for cloud-based security?

4. **Audits and Chain-of-Custody**
   - What processes are in place for end-to-end audit and documented chain-of custody for all data and actions?
   - Are all provider actions tracked and logged?
   - Can you access historical information about each document that is processed, loaded, exported or deleted?

5. **Data Center Intrusion Detection and Monitoring**
   - How is network, service and application activity monitored?

6. **Physical Data Center Security**
   - Is there 24/365 physical security and monitoring?
   - Is zoned keycard and biometric scanning access required?
   - Are all access events logged and securely maintained?

7. **Disaster Recovery, Business Continuity and Incident Response Plan and Processes**
   - Does infrastructure redundancy include at least two copies of all databases, servers and storage, as well as fault-tolerant application server clusters?
   - Is there a secondary data center with real-time back-up and equivalent processing power to the main site?
   - Are these processes and mechanisms regularly tested and audited?
   - Will the provider show you documentation of its incident response plan and validate that it is operational and routinely refined?

8. **Employee Screening, Training and Experience**
   - Do employees receive background checks and sign non-disclosure agreements?
   - How are documented security polices and procedures communicated to employees?
   - What security training programs are in place?
   - What is the level of expertise of the information security team?
   - What is the response time for any third-party breach remediation providers being retained?

organizations to comply with the European Union directive on the protection of personal data; HIPPA compliance; and financial services consumer protection requirements, such as PCI-DSS, if appropriate to your industry—all which ensure the highest levels of privacy and data protection.

Above and beyond industry certifications, ethical hacks, application vulnerability and network penetration tests should be conducted annually by independent, qualified third parties to ensure that information systems comply with security implementation standards.

2. How do law firm and client end users and the provider's employees access data?

All data should be stored and accessed only in secured areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

At the application level, authorization, authentication and user permissions processes check and confirm that you are approved to access your data and never see data you should not be viewing. Passwords should be stored and authenticated by industry standard authentication mechanisms to verify that the media stream or message received by the acquiring party is the one that was sent. Platforms should also offer two-factor authentication, which decreases the possibility that the requestor is presenting false evidence of its identity. IP address restriction that is determined by a least-privileges access model and is strictly limited based on job requirements provides further security.

At the organizational level, access control policies should be established, documented and reviewed based on an employee's business and security requirements for access. Changes to information processing facilities, software and systems should conform to a documented robust change control process.

3. How is data protected during transmission and at rest?

While managed service providers might conduct some work on-site, it is likely that client data will be transmitted between your firm and the provider's data center. Your provider should utilize at least 256-bit AES encryption to protect data during transmission—a protocol that exceeds standards for cloud-based security. Documents should also be encrypted with highly secure protocols (like 256-bit AES) that render them unreadable without the proper credentials.

All confidential information should be encrypted when in transit over external networks, and when stored at rest. Security features, service levels and management requirements of all network services should be identified and included in network and network equipment services agreements.

Finally, access to operating systems and confidential information should be controlled by a secure log-on procedure using unique, individually-identifiable credentials.

4. What processes for audits and chain-of-custody are in place?

Your provider should offer end-to-end audit capabilities and create a documented chain of custody for all data and actions (such as user logins, document views, coding edits, updates, print outs, etc.). These logs should be archived daily at an off-site facility. For data processing, all actions taken by the provider should be tracked, logged and driven by internal checklists, both automated and human, to ensure rigorous quality control. This creates an accurate and comprehensive chain of custody that provides historical information about each document processed and loaded into the review platform. You also should receive certification of all data exports and deletions.

5. What intrusion detection and monitoring services are in place?

All network, service and application activity should be monitored in real-time, 24/365. Designated staff should be alerted immediately of any suspicious activity, and track, escalate and report on system issues. Proactive system alerts, such as server temperature monitoring, redundant power distribution alerts and redundant storage path alerts, also assist in identifying potential failures. To verify uninterrupted operation of the platform and its related internal services, storage, servers and databases, both proactive and reactive alert systems should be used. To protect against malicious code, detection, prevention, recovery controls and appropriate user awareness procedures should be implemented. Finally, networks should be adequately managed and controlled. This ensures that they are protected from threats, and that security is maintained for the systems and applications using the network, including information in transit.

6. What physical security mechanisms are in place at the data center?

The data center should employ extensive physical security processes, including 24/365 staffing and monitoring, augmented by professional security guards. Robust mechanisms include camera systems to monitor all entrance and exit points, zoned keycard access with segregated security levels for essential staff in high-sensitivity areas and biometric scanning to identify approved personnel. The keycard system should log all employee access to the facility.

There should also be physical protection against environmental damage from fire, flood, excessive heat, cold, humidity, power loss and equipment failure.

7. What are the provider's redundancy, disaster recovery and business continuity capabilities? How robust is its incident response plan and process?

In order to quickly restore vital business functions in the event of a disaster, a provider should have extensive disaster recovery and business continuity plans in place—ones that are regularly tested and audited for full site failover capabilities to validate that service redundancy features remain current and available. Infrastructure redundancy best practices include at least two database tiers, two storage tiers and fault-tolerant application server clusters. Multiple internet service provider connections should be configured to provide failover capabilities. For offline backups, consider whether your provider offers live "hot" duplication and/or high-performance tape library devices, each dedicated to a single client case or matter, in a secure environment. This can facilitate rapid export and restore capabilities while meeting data segregation requirements.

Your provider should be able to show you a detailed, documented disaster recovery and business continuity plan that ensures an organized, timely response to causes of service disruption. It is equally important that the provider has a detailed incident response plan and can demonstrate that it is operational and updated regularly—as opposed to a generic document that fails to guide specific actions in the event of an incident. This plan should include a continually updated catalog of known risks and threats, a quick response guide for common scenarios and processes for making high-impact decisions, such as isolating an entire network segment. Furthermore, this plan should be integrated across departments to facilitate coordination, sharing of critical information and best practices. The service provider should be performing regular "war games" to stress test and refine this response plan.

Finally, in the event of a cybersecurity threat or attack, it is important to know how your managed service provider will communicate with you about how it has addressed the threat to protect your and your clients' data.

8. How are the provider's employees screened and trained? Does the information security team have demonstrated expertise and experience across all risk areas?

The "people" part of the security paradigm is often the most overlooked, but controls around people cannot be ignored. All employees should have pre-employment background checks (including drug testing) and signed non-disclosure agreements, especially if they will have access to confidential or privileged information. Documented security policies and procedures, approved by management, should be published and communicated to all employees and relevant external parties. On an ongoing basis, employees should be trained on the rules for the acceptable use of information and assets associated with information processing facilities, confidential data and social media, to name a few. All employees of the organization and, where relevant, contractors and third-party users, should receive appropriate information security awareness training and regular updates in organizational policies and procedures, as relevant for their job function. Duties and areas of responsibility also should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's IT and information assets by a single individual. In the case of a breach, there should be a formal disciplinary process, and, in the case of a separation, access to information should be immediately removed. Finally, confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and explicitly acknowledged by all employees with access to confidential information.

A service provider's information security team should also be evaluated to ensure that personnel have demonstrated expertise (i.e., relevant professional experience and certification). A service provider should also be able to illustrate that it is adequately staffed with veteran personnel—particularly with regard to security operations, network security and those who have been identified as critical to incident response. If the service provider partners with a third-party breach remediation provider, firms should make the same personnel inquiries and ask about any delays in response time that may result.

The Future of Law Firm Data Security

Due to the sensitive nature of client data, especially in an e-discovery context, law firms must be able to demonstrate a comprehensive, best-practices-based security and incident response program to their clients. As firms discover the cost and complexity of securing their environments, they are increasingly looking at managed services as a viable alternative to building, implementing and maintaining a program in-house—in essence relying on security-as-a-service for parts, if not all, of their e-discovery data security burdens. This not only delivers cost savings and efficiencies for law firms, but it also provides access to world-class security, threat detection and incident response capabilities by providers with a core focus on the security of their clients' data.

Xerox Litigation Services, the electronic discovery division of Xerox Corporation, is the trusted partner of corporations and law firms worldwide. We offer a suite of flexible, full-service capabilities to support litigation, investigations, regulatory compliance and other matters, delivering end-to-end services, industry-leading technology and consulting expertise to simplify your e-discovery processes. With operations across the globe, Xerox Litigation Services offers the options and scalability clients need to handle e-discovery challenges of all sizes and complexity.

For more information on Xerox Litigation Services, visit www.xerox-xls.com, call 877.273.3887 or email info@xls.xerox.com.