UNDERSTANDING VENDOR MANAGEMENT AND YOUR THIRD-PARTY RISKS

By Caroline Libarian & Travis Walker

Third parties that access your systems, infrastructure or data add an additional layer to your organization's risk profile and can ultimately be a source of compromise or significant operational impact. Failure to properly vet or manage these third parties can undermine an organization's security and data protection programs. It is critical that you have strategies and procedures in place to minimize the risks posed by your vendors, partners, and third-party service providers.

HIROC strongly recommends you take the following proactive steps to reduce the risk your vendors could pose, potentially leading to jeopardizing the confidentiality, integrity and availability of your systems and data:

- Develop a standardized questionnaire to be used with all potential vendors, thereby ensuring a consistent process of due diligence and consistency of information gathering to support an efficient comparison among vendors.

- Ensure the vendor's security practices are strong and meet acceptable information/cybersecurity standards (e.g., NIST, ISO 27001, SOC 2).

- Contractually obligate the vendor to maintain accepted information/cybersecurity standards throughout the term of the agreement and to engage in, at their expense, regularly scheduled penetration tests or vulnerability scans by a reputable firm and to produce the results of those tests. The frequency will depend on the extent to which the vendor accesses your organization's IT systems or holds/processes sensitive data but should generally be annually at minimum. This will help you assess your vendor's risk of compromise and commitment to its information security standards.

- Contractually limit the vendor's right to access the organization's IT systems and use its data to only the extent required to provide the negotiated services.

- Contractually require the vendor to notify you of all security breaches and privacy breaches within a specified time period (24 hours or shorter) from the occurrence date or when a breach is reasonably anticipated. The vendor should also be required to produce forensic findings relevant to the organization's systems and data or to facilitate the organization's own investigation into the incident.

- Ensure the vendor's incident response plans are inclusive and meet acceptable standards for healthcare organizations.

- Contractually require the vendor to comply with all applicable privacy legislation, regulations, or industry standards.

- Perform periodic reviews and assessments of a vendor's performance and compliance with agreed-upon security standards. This can take the form of on-site visits, disclosure of relevant security information by the vendor, or a third-party assessment or audit.

- Where feasible, periodically, or annually evaluate vendor agreements, to ensure they are appropriate and relevant, and that any inconsistencies in key contractual provisions across agreements with different vendors is identified and remedied. Consider developing and maintaining a vendor agreement database or register to facilitate this.

Cloud Service Providers

The widespread adoption of cloud computing services, between its various models (SaaS, PaaS and IaaS) and deployment options (public, private and hybrid), raises questions about the risks associated with those services and their variations. Those risks manifest in several ways, including data security, legal and regulatory compliance, data residency, and loss of control or accessibility as a result of service interruptions and downtime, among others.

HIROC encourages healthcare organizations to consult with IT and legal professionals to assess privacy and security risks implicit in the cloud services they are considering implementing or are already utilizing. The Canadian Centre for Cyber Security has issued several useful guidance documents for organizations and government departments on utilizing cloud computing in a secure manner. HIROC's Cyber Risk Management: A Guide for Healthcare Administrators and Risk Managers also offers advice.

Prior to engaging in services with a cloud provider, it is important that your organization have a defined due diligence process in place to evaluate prospective vendors' security standards and practices and fit with your organizational needs. The due diligence process should include: obtaining and consulting with references from potential vendors which align with your operations and are as similarly-situated and configured to your organization as possible, obtaining third-party attestations of the vendor's compliance with security standards (e.g., SOC 2/ ISO 27001; 270018/CSA STAR), and completing your own threat and risk assessment (TRA) and privacy impact assessment (PIA).

At minimum, here are some questions to ask a potential cloud services provider:

- **How would the cloud service provider detect, contain and remediate cyber breaches?**
- **How is the organization's data stored, transferred and processed?**
- **Is the data stored on servers outside of Canada and, if so, where?**
- **How will you be able to repatriate data if the cloud service provider goes out of business, is acquired, or is absorbed?**
- **If the cloud service provider is taken over by another provider, who has rights to the data? What are the terms and conditions?**
- **What protections (encryption, access controls, segmentation, etc.) are in place to protect the organization's information?**

- **What are the vendor's data retention and destruction processes?**
- **Are backups of the system or data conducted? If so, understand where the backups are stored, how often the backups are generated and destruction details.**
- **Does the service provider support single tenant architecture? If only multi- tenant architecture is supported, how will the organization's data be protected against unauthorized access, use and disclosure?**
- **What sort of data migration support will be provided if the healthcare organization wants to migrate to another cloud provider or internal system?**
- **What type of auditing and logging capabilities are in place and how can they be accessed by the healthcare organization?**
- **What cyber and privacy breach incident management protocols are in place? Understand the breach notification process and timeframe; healthcare organizations should be notified of breaches as soon as reasonably possible and furnished with adequate information to understand the impact to their data and assess their legal obligations.**

Healthcare organizations may wish to consider negotiating some or all of the following provisions into their cloud service agreements with vendors:

- Representations and warranties regarding the vendor's compliance with specified security standards (NIST, ISO 27001, CSA STAR) and data breach notifications laws and regulations.
- Approval rights over the use of subcontractors or to be notified of changes to the vendor's subcontractor list.
- Prompt notification of security and privacy breaches which have, or are reasonably likely to, impact the cloud service offering or the organization's data.
- Designated backup schedules and archiving at an off-site data storage facility physically removed from the vendor's operational data centres.
- Retention of all rights and authority to notify affected individuals and applicable regulatory authorities following a data or privacy breach on the vendor's systems.
- Return of the organization's data upon request or expiration or termination of the agreement, in an organization-friendly format.
- Compliance audit rights including provision of regularly scheduled, independent security assessments and access to logging information pertaining to access and use of the organization's data.

- Maintenance and testing throughout the term of the agreement of a business continuity and disaster recovery plan by the vendor.
- Geographic zones or jurisdictions for data centres where the organization's data can be stored and designation of exclusive ownership of the organization's data at all times, including in the event of a breach.

Finally, review service contracts and service level agreements (SLAs) to verify compliance with applicable regulations and the organization's privacy and security standards/practices.

One check is never enough – make it a habit to review SLAs regularly to monitor the service provider's compliance with commitments and requirements.

> ***"Despite the opportunities for improved operational efficiencies and services, and for reduced overhead overhead and other costs, cloud computing introduces its own privacy, security and compliance risks that must be addressed"***
>
> **INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO (2016)**

Select and Follow a Standard Cybersecurity Framework

As a healthcare organization, you can greatly minimize your cybersecurity exposure by staying on top of threat trends and security standards. If feasible, you should consider selecting and following a cyber/information security framework.

There are definite advantages to doing this – adopting an industry standard security framework ensures that guidelines are appropriately followed, and cyber risks are identified, tracked and managed in a systematic and standardized manner.

Available cybersecurity frameworks and resources:

- **Cyber Risk Management: A Guide for Healthcare Providers and Administrators**
- **Contracts - Data Sharing Agreements PHI to Third Parties**
- **International Organization for Standardization, ISO/IEC 27001 and ISO/IEC 27002 – Information Security Management Systems Standards**
- **The Centre for Internet Security (CIS), CIS Controls**
- **Public Safety Canada, Fundamentals of Cyber Security for Canada's Critical Infrastructure Community**

- **Canadian Centre for Cyber Security, IT Security Risk Management: A Lifecycle Approach (ITSG-33)**
- **National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Cybersecurity Framework**
- **Healthcare Information Trust Alliance (HITRUST), Common Security Framework (CSF)**
- **United States Computer Emergency Readiness Team (US-CERT), Cyber Resilience Review (CRR)**

Have questions? We're here for you!

Reach out to us at **inquiries@hiroc.com** with any questions.

Caroline Libarian is the Claims Associate at HIROC & Travis Walker is a Senior Associate at Norton Rose Fulbright Canada