Vendor management – how to protect your data

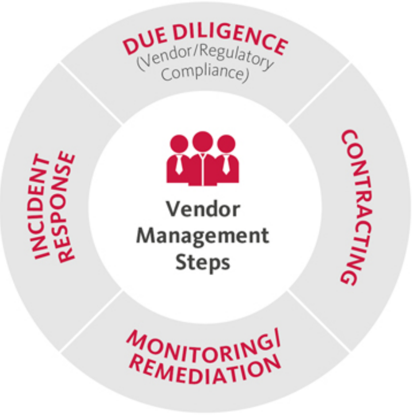
MAY 17, 2017 1 MIN READ

Related Expertise

- Commercial Technology Transactions
- Cybersecurity and Security Incident Response
- Privacy and Data Management
- Professional Services

Authors: Michael Fekete, Wendy Gross, Evan Thomas

Giving vendors access to your systems and data can be critical to your organization's success but can also create significant risks. Managing these risks effectively requires a combination of due diligence, monitoring, contractual protections and incident response. The below infographic provides a checklist to ensure you have your bases covered.



Case Studies

A credit reporting provider processed credit applications on behalf of a major mobile phone carrier.

Attackers gained access to the service provider's databases and obtained records for 15 million of the carrier's customers.

Some data was encrypted but there were concerns the encryption may have been compromised.

Attackers gained access to a major retailer's corporate network via a vendor.

Using a phishing attack, the attackers installed malware on the vendor's computers to capture login credentials for the retailer's internal network.

The malware was well known and could have been detected by widely available security software. As of October 2015, the retailer had recorded $290 million in expenses, including $116 million for class action settlements.

Various major retailers outsourced online photo printing services to a vendor.

Attackers gained access to the vendor's systems and deployed malware designed to capture personal and credit card information from customers.

As of early 2016, class action litigation was ongoing in the U.S. and Canada and the owner of the service provider had incurred incremental expenses of $18 million related to the incident.

Checklist – Do your agreements address:

- ☑ your organization's control of the data stored or processed with the vendor, including how it is used, how it is accessed, and how long it will be retained?
- ☑ the return, transfer or destruction of your organization's data?
- ☑ disclosure of personal information and other dates to law enforcement?
- ☑ notice to a customer of a legal obligation to disclose personal information (unless legally prohibited from doing so)?
- ☑ the use of subcontractors which may involve access to or transfers of data?
- ☑ use of your organization's data for the vendor's own purposes?
- ☑ consent before using personal information for marketing or advertising purposes?
- ☑ disclosure of countries where personal information may be stored or processed?
- ☑ notice to your organization of data breaches and disclosure of information needed by your organization to meet notice obligations?
- ☑ the timeframe for providing notice of data breaches?
- ☑ recording the type, timing and consequences of data breaches?
- ☑ disclosure of information about the vendor's processes and procedures used to protect personal information and other data?
- ☑ parameters for restricted access and use of data?
- ☑ logical segregation of data from the data of the vendor's other customers?
- ☑ restriction of access to data to those who need it to do their job?
- ☑ logging of access to data in protected audit trails?
- ☑ appropriate authentication/access controls (e.g. multi-factor authentication)?
- ☑ use of encryption to protect data in transit and/or data at rest?
- ☑ procedures to ensure business continuity and prevent data loss in the event of an outage?
- ☑ compliance with internationally recognized security standards (e.g., ISO 27001, 27002 and 27018), including confirmation of compliance by an independent third-party auditor?
- ☑ allocation of costs of investigation and remediation of data breaches?
- ☑ allocation of risk of claims by third parties?
- ☑ appropriate insurance coverage?
- ☑ other audit rights for verifying compliance?
- ☑ remedies for non-compliance, such as injunctive relief?

Add this infographic to your website

Download infographic

Add this infographic to your website using the following HTML

```
<a
href='https://develop.osler.com/en/resources/governance/2017/vendor-management-how-to-protect-your-data' rel='nofollow'><img
src='https://develop.osler.com/osler/media/Osler/infographics/privacy-data-management/vendor-management-how-to-protect-your-data.jpg' width='780'></a><br/><a
```