Published on *The National Law Review* https://natlawreview.com

Tips for Vacation Rental, Property Mgmt. Businesses Facing Vendor Cybersecurity Risk

Article By:

Joseph J. Lazzarotti

No organization can eliminate data breach risks altogether, regardless of industry, size, or even if the organization has taken significant steps to safeguard their systems and train employees to avoid phishing attacks. Perhaps the most significant reason these risks remain: third-party service providers or vendors.

For most businesses, particularly small to medium-sized businesses, service providers play a critical role helping to manage and grow their customers' businesses.

Consider vacation rental and property management businesses. Whether operating an active website, maintaining online reservation and property management platforms, or recruiting and managing a growing workforce, these businesses wind up collecting, processing, and storing large amounts of personal information.

With a national occupancy rate of approximately 56%, a vacation rental company with 100 units for weekly rental might expect to collect personal information from about 5,000 individuals annually (25 weeks rented X2 persons per rental X100 properties). My crude math leaves out website visitors, cancellations, employees (and their family members), and other factors. After three years in business, the company might easily be storing personal information of up to 15-20,000 individuals in their systems.

There are lots of good resources online helping to protect VR businesses from online scams, including those that could lead to a data breach. "Vacation Rental Scams: 20 Red Flags for Spotting Hoax Guests" and "How to Protect Your Vacation Rental from Phishing Attacks" by Lodgify are good examples.

But what happens when the VR business' guest and/or employee data is breached while in the possession of a vendor?

Last year, as reported on the Maine Attorney General's Office website, Resort Data Processing (RDP) experienced a data breach affecting over 60,000 individuals caused by a "SQL injection vulnerability which allowed an unauthorized third party to redirect payment card information from in-process transactions on our RDP's clients' on-premises Internet Reservation Module ("IRM")

server.” Affected individuals likely included consumers who stayed at properties owned by RDP’s business customers. At least, that is what one plaintiffs law firm advertised about the incident.

Addressing this risk can be daunting, especially for small businesses that may feel as though they have insufficient bargaining power to influence contract terms with their vendors. But there are several strategies these organizations might consider to strengthen their position and minimize compliance and litigation risks.

- Identify all third parties that collect, access, or maintain personal information on behalf of the business.
- Investigate what personal information they access, collect, and maintain and assess how to minimize that information.
- Make cybersecurity a part of the procurement process. Don’t be afraid ask pointed questions and seek evidence of the vendor’s privacy and cybersecurity policies and procedures. This should be part of value proposition the vendor brings to the table.
- Review service agreements to see what changes might be possible to protect the company.
- A vendor still may have a breach, so plan for it. Remember, the affected data may be owned by the business and not the vendor, making the business responsible for notification and related obligations. The business may be able to assign those obligations to the vendor, but it likely will be the business’ responsibility to ensure the incident response steps taken by the vendor are compliant.

Experienced and effective counsel can be instrumental here, both with negotiating stronger terms in service agreements and improving preparedness in the event of a data breach.

National Law Review, Volume XIV, Number 337