Data security

Make sure your 'big data' headline isn't about a big data breach

by Brandon Sedloff

For far too long, headline-grabbing data-privacy breaches at Equifax, Anthem and Target Corp. reinforced a false notion that data security crimes are an epidemic confined to the largest and most visible companies. As brand-name firms hardened themselves to attack, investment managers presuming to "fly under the radar" of cybercriminals failed to bolster their defenses. Today, they're paying the price. Real estate investment managers have a target on their backs. They house valuable libraries of personally identifiable information (e.g., bank account, Social Security and tax ID numbers), and sit at the center of millions of dollars in daily transactions. Hackers seeking to exploit weak links in an increasingly connected financial ecosystem are targeting these firms with an escalating level of sophistication and aggression.

In first quarter 2018 alone, we have heard several firsthand accounts of successful cyberattacks targeting real estate investment firms. Consider these real-life examples:

- A capital call notice delivered unsecurely to the investor was intercepted by a hacker who changed the bank wiring instructions.
- A senior executive lacking proper data-security training responded to a phishing attack requesting the transfer of client funds.
- A malware attack exploiting a delayed software-patch implementation held a real estate manager's servers hostage in exchange for ransom.

In pursuing the transformative promise of "big data," artificial intelligence and machine learning, real estate managers have often diverted IT resources from the far-less-sexy imperative of organizing and securing data. Several managers still struggle to even locate their sensitive investor data from within a complex web of Excel spreadsheets, physical documents and legacy software systems that each house pieces of information. Multiple surveys of investment managers reveal data security as a top concern. Still, many have yet to address it.

Investors are losing patience. One of a manager's most important duties as a fiduciary is to safeguard not only investors' capital, but also their sensitive data. Improper data handling can be a disqualifying offense for even the best-performing and most established managers. In a 2018 CFA Institute survey of 829 institutional investors, data and confidentiality breaches leapfrogged to the No. 1 reason investors cited as grounds for leaving an investment manager — a greater concern than underperformance or fee increases. For their part, pension consultants are placing particular focus on codifying procedures for underwriting data practices as part of their manager due diligence.

Regulators, too, are paying close attention, increasingly emphasizing manager accountability to data security. It's no longer enough to produce a generic set of data-security policies and procedures; regulators expect those policies to be appropriately tailored, implemented and followed. In its recent round of cybersecurity "sweeps" of 75 registered investment advisers and broker-dealers, the Securities and Exchange Commission found that, although most firms now maintain cybersecurity policies, "firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices." In addition, certain firms were behind on basic system maintenance, such as installing the latest software patches, leaving them unable to properly protect clients' sensitive records.

Improper data handling can be a disqualifying offense for even the best-performing and most established managers.

Brandon Sedloff
Juniper Square

When it comes to securing your data, there is no margin for error. Consider the following safeguards to help limit your risk.

Make data security the responsibility of all employees. It's all too common for managers to assume data security starts and ends with the IT department. Company leaders often underestimate how much of their risk lies within their own organization. Hackers aim to exploit a lack of "cyber-cleverness" or mere carelessness among a firm's own employees. To protect your data, ensure all employees attend regular cybersecurity trainings that focus on real-world threats, such as how to detect and prevent phishing or malware attacks. As an added precaution, consider hiring outside consultants to simulate phishing attacks as part of ensuring employee readiness.

Bring IT to the management table. Gone are the days when your IT team was mainly an on-call resource to fix your BlackBerry. IT professionals should be integrated into all aspects of your organization, and technology should be a consideration in every organizational decision. For firms big enough to have a chief technology officer or chief information officer, ensure they have a seat at the business table to help guide your core operations.

Consolidate and integrate your data sources. Securing your data starts by consolidating it from disparate sources. The spreadsheets managers commonly rely on for data storage were never designed to be a system of record. They're not equipped to handle complex workflow processes, access restrictions, or simultaneous input by multiple users. Overreliance on spreadsheets within an organization creates data silos that lead to redundant and often conflicting records. As a result, managers often lack a single "system of truth" where all information can be stored and easily found. Augmenting the problem, managers commonly use spreadsheets as the glue to patch together multiple software systems, introducing excess opportunities for the kinds of fat-fingering that instantly compromises data integrity. Multiple studies reveal nearly 90 percent of spreadsheets contain errors caused by manual inputs. Instead of relying on spreadsheets as glue, invest in integrating your various software systems together. If your software vendor refuses to integrate with another, find a new one. Modern software vendors understand the importance of data integrity and want their systems to integrate with the rest of the systems in your operation. Your data security depends on it.

Implement controls on data permissioning. After consolidating your data, implement a role-based permissioning model for both staff members and outside investors, ensuring confidential information is restricted to the select few who need it to do their jobs. Don't fall into the trap of presuming confidential information is limited to a handful of documents, such as Schedule K-1s. Permission-based access should be scoped to all confidential investor data, such as bank account information, correspondence and transaction details. Assign an internal data administrator to control and track who has access to all confidential investor information at any one time.

Use strong passwords, and ensure your confidential data is encrypted. In the United States, a laptop is stolen once every 53 seconds. It's far easier to walk off with an unsecured laptop than to hack a database. Don't let the one abandoned laptop in the airport lounge take down your entire organization! It's imperative the hard drives of all employee computers are encrypted and all systems, including employee computers, are protected by strong passwords. Likewise, when transmitting confidential data, default to using password-protected portals.

Choose purpose-built software. Software development has come a long way since the legacy real estate systems designed in the 1990s and 2000s. The past decade's rapidly falling software-development costs have made it financially feasible for skilled engineers to design high-quality solutions purpose-built for evolving data needs. From a security standpoint, newer software solutions benefit from advances in cloud computing. Compared with on-premise solutions that host data on managers' internal servers, cloud-based data hosting can offer a level of security infrastructure that would be cost prohibitive for most firms to replicate internally. Rather than attempting to force legacy systems to perform functions they were never intended for, managers are best off complementing legacy systems with the right mix of modern, out-of-the-box solutions.

Complete thorough due diligence on your software providers. To ensure your software providers are appropriately safeguarding your data, ask them for full transparency about how their data is stored and secured, and also verify providers have passed extensive third-party security and data-privacy audits — including service organization control 2 (SOC 2), third-party penetration testing and GDPR compliance. Inquire whether software vendors own the major components of their own solutions. Vendors that outsource core pieces of functionality to third parties have less control over their products and are more limited in driving software enhancements.

Although firms should make data-security basics an operational imperative, it's not important for real estate managers to understand data security's every nuance. Rely on the expertise of thoroughly vetted partners to help implement best practices. The most effective software providers will not only have bulletproof data-security practices, but also possess the real estate industry expertise to help you implement those practices most productively. ❖

Brandon Sedloff is a managing director and the vice president of sales at investment management software company **Juniper Square.**