# Dealing with Sensitive Data

By Mark Bednarz, CPA, CFE, CISA, Partner

Over the past few years, many organizations have found themselves in a position where they have to defend their reputation due to the unauthorized release of sensitive data. The exposure may also have adverse financial and regulatory consequences.

Private equity firms fall into this group because they may collect, analyze, transmit and store data. As a result, those firms that do not focus on data quality and protection run the risk of exposure and possible erosion of investor confidence. In addition, those firms are taking chances if they do not have in place an incident response mechanism to react to security breaches. How a firm responds to such situations is often as important as the event itself — especially to regulators and investors looking over their shoulder.

The data that private equity firms collect, whether from operations, investments, or investors, makes them attractive targets for hackers as well as disgruntled employees who might have insider access. Consider, for example, an Information Technology employee who is dissatisfied with his/her level of compensation and learns that there is a lucrative market for such data. The potential payoff provides the motivation.

## Managing a Cyber Attack

In the event of a cyber attack, a private equity firm may find itself dealing with a number of issues, including:

- Regulatory matters, where fines are imposed due to exposing or improperly collecting personal data.
- Operational exposures, related to failure to effectively manage data and apply proper security controls.
- Investment concerns, due to not properly safeguarding sensitive data and intellectual property.
- Third-party issues, where an outsourced provider may not properly safeguard data and the private equity firm is held responsible for doing business with such a supplier.
- Technology challenges, where data is collected via social media, Internet of Things (IoT) and mobile sources and then is released due to data leakage.
- Reputational risks, due to improper disclosure of personal information or trade secrets.

These risk factors can be mitigated with strong governance and internal controls. For instance, data leakage can be prevented, in part, if software is in place that can detect the intentional or inadvertent sharing of attachments containing sensitive data with outside parties before it is transmitted.

## Establishing a Privacy Program

Delivering stakeholder value requires a defined privacy governance and management program. Privacy is the right of individuals to determine if, when, how and to what extent data about themselves may be collected, stored, transmitted, used and shared with others. In return, this commitment can help the firm build competitive advantage and investor loyalty.

Prior to establishing such a program, the firm should identify the business needs and any "pain points" as well as obtain the commitment and buy-in of relevant stakeholders. The outcome of this exercise will be the identification of business objectives, which can include ensuring portfolio companies comply with regulations, producing accurate and quality information, and preventing data breaches resulting in loss of investor information or trade secrets. By protecting the privacy of individuals, firms retain employees and clients by establishing a culture of integrity and trust.

Management should establish integrated privacy governance policies across the firm and extend these practices to their portfolio companies by identifying processes, information types, behaviors and cultures, services, applications and the context within which the information is used. In order for the initiative to be successful, management must foster a privacy-positive culture.

Creating a strong tone at the top will help influence employees to follow established protocol and reduce the likelihood of a privacy breach. The individuals associated with the information should be proactive in identifying and mitigating risks. Management will assume responsibility for monitoring compliance and would be best served if they made it a point to "inspect what they expect" on a scheduled basis.

## Privacy Risk Profile

Business and technology are constantly evolving and such changes affect a private equity firm's risk profile in the case of privacy concerns. Management should be attuned to:

- New regulations or contractual requirements
- Significant changes in technology (e.g., outsourcing via the cloud, support and use of mobile devices)
- Actions of their portfolio companies and recent acquisitions, in the event that they capture sensitive information

To foster a risk-based approach, management will be best served by engaging representatives of IT, Internal Audit, Legal and Operations to identify tools for recognizing and monitoring risks and detecting incidents. When it comes to privacy and technology, one cannot assume that the laws cover new technologies because there is often a lag between introduction of the latest technology and legal precedent.

## Contact us

For information as to how we can help your company deal with the collection and storage of sensitive data, please contact Mark Bednarz, CPA, CFE, CISA, Partner at mbednarz@pkfod.com or 646.449.6376, or any member of the PKF O'Connor Davies' team.

### About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 28th on Accounting Today's 2017 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by Accounting Today. In 2017, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by Vault.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in 440 locations, in 150 countries around the world.