

Data Security

What Hedge Fund Managers Need to Know About Information and Data Security

By Edward Stroz and Steven Garfinkel, *Stroz Friedberg*

While hedge fund executives are experts at identifying and managing the risks relating to their financial assets and portfolios, they generally do not have the time or expertise to focus on the security of their people and intellectual property (IP) assets. However, all organizations – especially financial institutions – must be prepared for the inherent risks and responsibilities associated with doing business in an online world through a sound digital risk management strategy.

The appropriate approach to digital risk management varies from firm to firm based on unique business models and requirements. However, all hedge fund managers should take a risk-based approach to security and ensure that the approach is aligned with the way executives manage other business issues. While physical security and information security present different challenges, they are strongly related, are part of internal controls and should be managed using an integrated strategy.

This article outlines the most critical aspects involved in implementing a digital risk management program for hedge fund managers.

Protect and Defend Intellectual Property through Both Cyber and Physical Security

Most IP is held in digital form, making it easy to steal or alter, and is extremely difficult to protect. IP is targeted by competitors, both foreign and domestic, as well as through state-sponsored organizations; and the methods of theft range

from hacking and electronic transmission by insiders, to an information dump onto a flash drive that is walked out the front door.

Cyber breaches create problems that extend beyond the financial value of lost IP. For example, a breach can subject a hedge fund manager to significant legal and public relations consequences. The fallout from a breach can include the loss of personally identifiable information, which raises issues such as notification requirements, hefty penalties, mitigation expenses and regulatory scrutiny.

The immediate response to a data breach requires a skilled digital forensic analysis that not only determines what was stolen, but does so in a manner that ensures the evidence is preserved in a legally defensible manner. Evidence should be collected by trained professionals who are prepared to testify about their findings in possible litigation. Furthermore, should a decision be made to bring in law enforcement, proper data collection and preservation can be essential in determining whether or not an investigation is pursued.

As part of a risk-based approach to safeguarding IP, firms should consider an ongoing program that integrates both network and physical security. First, a total security audit should be conducted that examines the spectrum of significant information loss attack vectors in terms of their likelihood, vulnerability and impact. This will assist in focusing the assessment and is critical to addressing the most relevant security hazards.

A competent IT department can provide many of the safeguards required to provide adequate solutions for network security, including monitoring the transmission of information and control of access to data. With respect to the threat of information loss, an organization must scrutinize these controls and how they affect the cycle of information creation, transmission, retention and disposal. Experience and historical references are key to developing both practical and effective remedies, especially in high-risk venues.

It is also important to recognize the practical limits of security provisions in a business environment, especially in an environment like a hedge fund management company, where portfolio managers, analysts and others need access to data immediately at their fingertips. The overarching goal is to provide a set of reasonable and culturally appropriate recommendations on security controls that balance the need for information access with the need to protect the information. Overall, the controls should not adversely impact the business and be flexible enough to accommodate changing conditions.

Assessing risk effectively yields a snapshot in time. But risk is rarely static, and risk mitigation must be periodically evaluated at a rate determined by local conditions. As technology evolves, risk profiles change. For instance, the transformation to a cloud-based network presents a new set of challenges for securing data.

Former Employees who are “Bad Leavers”

It is a fact of corporate life that employees, officers and directors are not wedded to a single firm for life. In the majority of cases, departing employees will leave on good terms and not “burn bridges,” but unfortunately, this is not always the case – hence the term “Bad Leaver.”

Bad Leavers could steal from companies on the way out the door or vandalize property, but the most egregious cases involve the theft of IP. Specifically, categories of IP that may be stolen include proprietary trading software code, pharmaceutical formulas, marketing strategies, customer lists and merger and acquisition deal information.

The trick about IP theft is that what is stolen is almost always copied, not taken away. This means that the proof of theft cannot be established the same way as with physical property, where the victim is deprived of the stolen property. IP theft investigation requires a more sophisticated approach. The common element in all Bad Leaver cases is that no matter what type of IP has been compromised, the Bad Leaver leaves behind digital footprints. Digital expertise is required to forensically analyze data to determine what was stolen, the extent of the damage and the involvement of co-conspirators. In addition to the expertise in finding the data, the ability to gather the data in a legally defensible manner is crucial.

We have been involved in multiple cases where the seeds of a conspiracy involving employees leaving a firm to start a competing entity have been located during an analysis of employee laptops and mobile devices. Employees are aware that their firm has the right to monitor their e-mail usage, yet Bad Leavers will still use company owned computers and PDAs to access Internet based e-mail and other systems to communicate.

Corporate policy can mitigate the damage from Bad Leavers by defining proprietary IP in solid non-compete and employment agreements and defending that property through sound policies and practices and technology.

One of the most important benefits of conducting a robust investigation of Bad Leaver situations is that it sends a message regarding the seriousness with which an entity will protect its IP. It also serves as a deterrent to others who may harbor thoughts of engaging in similar conduct in the future.

Due Diligence – With Whom Are You Really Dealing?

Due diligence in this context is in fact a form of investigation, and should be conducted by people with expertise in that area. We know from direct experience that due diligence could have uncovered clues in some of the largest frauds in history including the Madoff Ponzi scheme, the Bayou fraud and the Martin Frankel cases.

Both the Madoff and Bayou cases contain stunning examples of failures in due diligence. In neither case was any effort made to verify the verifier or receive a reliable answer to the question: “Who is auditing your financial statements?” This lack of due diligence, or superficial due diligence, is one of the reasons why investors were victimized in both schemes.

Bernard Madoff Investment Securities LLC was purportedly a multi-billion dollar business audited by David Friehling, a one-man accounting firm in a suburban strip mall 40 miles from New York City. Friehling had no other clients unrelated to Madoff. A visit to his offices would have raised serious questions as to the capacity of Friehling’s firm to conduct an audit of a client the size of Madoff, but no on-site visits were ever made by investors.

In the Bayou case, Bayou founder Samuel Israel III ran a \$400 million hedge fund management company. The Bayou funds reported consistent positive returns for eight consecutive years. Mr. Israel claimed his funds were more transparent

than others because he reported financial statements that were fully audited by a CPA firm. One investor actually did conduct due diligence on the funds’ CPA firm, Richmond-Fairfield Associates, CPA. A single investigative step was taken by running a Dun and Bradstreet check. D&B produces good information, but the information is submitted by the subject company and not verified. In this instance, Richmond-Fairfield reported its offices at a midtown Manhattan address. That address was in itself of interest because the FBI knew this address to be the same as a business that provides virtual office services and quickly determined that the accounting firm was created by Bayou’s own CFO.

Performing comprehensive due diligence on a potential business partner, investor or investment is not only a “good business practice” – it can also be a regulatory, know your customer requirement. It is a relatively small upfront cost that can obviate involvement in future civil litigation trying to recover assets, or worse – becoming a witness or defendant in a criminal or regulatory action.

The same level of due diligence applied to making a decision regarding an investment in financial assets should be made in employment decisions. Too often, resume fraud is allowed to occur because of a cursory background investigation. Although financial institutions are required to fingerprint and conduct criminal history checks on employees, individuals with a checkered past can appear in the workplace as temporary employees and consultants.

Forensic Accounting: Leave Due Diligence to the Experts

When a due diligence exercise requires the verification of assets and fraud risk associated with an acquisition, experienced professionals in the forensic accounting practice

have a unique skill set combining traditional accounting and law enforcement in order to investigate and recognize fraud. Unlike a traditional financial audit, which seeks to offer an opinion on compliance with specified accounting standards, the work of forensic accountants is a mission whose focus is defined by the client. For a hedge fund manager, this can entail an investigation verifying the existence of assets; examining the potential for fraud in a financial process; and examining the books and records of a prospective investment partner.

A key part of almost any forensic accounting project for financial due diligence requires the examination of voluminous data sets from multiple sources. As audit trails and evidence have become almost exclusively digital, proper data analytics requires blending information technology know-how with prior experience in detecting fraud.

Internal Investigations

Firms are coming under an increased burden to conduct internal investigations at the earliest inkling of internal misconduct. Regulatory and law enforcement scrutiny has been ratcheted up by the SEC with the passage of Dodd-Frank, by the Department of Justice with FCPA investigations, and in the UK with the scheduled implementation of the Bribery Act. Acts by rogue employees, employee mistakes, compliance gaffes and unfounded customer or competitor complaints can lead to a criminal or regulatory investigation.

A basic tenet of all these various types of investigations is that they require an analysis of electronic data. Digital evidence often yields the truth because so much of what we do leaves a digital trail, and internal investigations require a deep understanding of this digital evidence.

Implementation of systems for the early identification of problems via controls such as the monitoring of internal communications and a whistleblower programs are critical. Conducting an investigation at the earliest sign of a problem bears significant weight by prosecutors and regulators when considering possible sanctions. Having an independent party who is familiar with a firm's operations and that is ready to assist counsel in internal investigations can provide a tremendous advantage when conducting an efficient investigation. Additionally, the independent expert can assist with shepherding the case through the reporting process.

The Time is Now for Digital Risk Management

As we have seen in past cases, a single person has the ability to take down an entire firm in today's digital era. A proactive digital risk management program can help guard against some of the dangers brought on by the possession of vital digital information, prevent digital information theft, and help put into place due diligence protocols for major business decisions, such as investing and hiring. Given the inherent value of hedge fund managers' data and information, many managers are developing and implementing a digital risk management plan that best meets their unique business needs.

Edward Stroz is Co-President of Stroz Friedberg, a digital risk management and investigations firm. Mr. Stroz has supervised forensic assignments for federal prosecutors, defense attorneys, and civil litigants, and has conducted network security audits for major public and private entities. As a Federal Bureau of Investigation (FBI) Special Agent, Mr. Stroz was responsible for the formation of the FBI's Computer Crime Squad in New York City, where he supervised investigations involving computer intrusions, denial of service attacks, illegal Internet wiretapping, fraud, money laundering, and violations of intellectual

property rights, including trade secrets. Earlier in his FBI career, Mr. Stroz successfully investigated major financial crimes, including approximately two dozen bank frauds in west Texas; bank fraud and money laundering committed by the CEO of Arochem Corporation stemming from a \$196 million oil-trading scheme; kickback schemes in the stock market through an undercover stock brokerage firm; and a \$1.1 billion fraud scheme at Daiwa Bank in New York.

Steven N. Garfinkel is Vice President of Stroz Friedberg's Business Intelligence & Investigations Division, where his responsibilities include internal investigations, forensic accounting, due diligence, monitoring and special master assignments. Prior to joining Stroz Friedberg, Mr. Garfinkel was a Federal Bureau of Investigation Special Agent for 21 years. His entire career at the FBI was devoted to investigating white collar crime in the New York branch office, starting in 1989 as an

agent for the Wire and Bank Fraud Squads. In 1996, Mr. Garfinkel became a founding member of the FBI's Computer Crime Squad in New York City. While there, he directed one of the first international computer hacking investigations in the Vladimir Levin/Citibank case, resulting in the successful prosecution of individuals in multiple international jurisdictions. In 2002, Mr. Garfinkel was appointed the Supervisor of all fraud and public corruption cases in the White Plains, New York Resident Agency. In that capacity he lead the investigation of financial crimes and public corruption cases, effectively resolving high-profile, high-dollar cases, such as the Bayou Hedge Fund fraud and the Andrew Kissel mortgage fraud scheme, plus numerous cases involving bribery of public officials. Mr. Garfinkel was most recently assigned to the Asset Forfeiture Squad, where he directed the FBI's investigation into the recovery of assets in the Bernard Madoff Ponzi scheme.