THE IMPACT OF CYBER-SECURITY ON FUND ADMINISTRATORS

KULJEET KAUR, OF OPUS, DEFINES WHY CYBER-SECURITY IS IMPORTANT FOR FUND ADMINISTRATORS, AND WHAT OPUS'S APPROACH IS IN MITIGATING THE RISK OF CYBER-ATTACKS

Dr Kuljeet Kaur is IT system administrator and security officer for Opus Fund Services and is based in the firm's Brentwood, California offices. Dr Kaur has spent the last few years obtaining her PhD in computer applications and information technology (identity authentication) and spent time formalising a data program within her previous employment. Prior to joining Opus in February 2017, she served as director and head of product & development cell and head of the computer applications division at TechNivarana.

Cyber-security has become one of the most important considerations for companies operating within the global financial system. The increasing number of data breaches and cyber-attacks have led many to question what the financial service industry is doing to address the important topic of cyber-security.

At particular risk are fund administrators who maintain sensitive information such as the names, addresses and social security numbers of hundreds, if not thousands of high-net-worth individuals. Add to this client trading data and you can begin to see why a data breach could be devastating not only for the security of the client and its investors, but the reputation of the administrator.

Data is increasingly being stored in the cloud, and the associated risks are attracting the attention of clients, their investors, and regulators. Just a single data breach could result in a class action lawsuit, jeopardising the future for all parties.

With increased global scrutiny, what should you know to ensure that your fund administrator is not exposing you to unnecessary risks?

ENFORCEMENT ACTIONS BY REGULATORS

In the wake of the recent WannaCry ransomware attack, the Securities and Exchange Commission (SEC) is warning managers that many are failing to perform steps that have been deemed critical in protecting against cyber-security attacks. The SEC conducted 75 examinations of SEC-regulated entities, aimed at assessing cyber-security preparedness, including the firm's ability to protect client information. Those examinations have resulted in substantial enforcement actions.

In September 2015, the SEC settled with R.T. Jones's Capital Equities Management, Inc. after charges were filed that the investment adviser had failed to establish the required cyber-security policies and procedures. This was in connection with a breach that compromised the personally identifiable information of approximately 100,000 individuals, including thousands of the firm's clients.

In June 2016, the SEC announced that Morgan Stanley Smith Barney LLC has agreed to pay a $1m penalty to settle charges relating to an alleged failure to adopt written policies and procedures reasonably designed to protect customer data. As a result, from 2011 to 2014, a then-employee impermissibly accessed and transferred data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.

LESSONS LEARNED

Cyber-security is now becoming the top priority for investors as well as fund administrators, evidenced through increased client awareness of cyber-security importance and continuous regulators' cyber-security initiatives. Hedge funds are now taking time to evaluate and analyse a fund administrator's level of preparedness for cyber-attacks.

Fund administrators now need to demonstrate their cyber-security capability and level of preparedness. This includes emphasising the need to define, track and prioritise all critical assets, monitor threats and vulnerabilities, manage and mitigate risks. Policies and procedures for business continuity and disaster management need to be documented.

THE OPUS APPROACH

Strong cyber culture: Opus ensures an internal culture of security by conforming to the best practices and internationally adopted frameworks for IT and cyber-security risk management. Opus has taken this commitment to the next step by hiring a dedicated cyber-security officer to lead our global initiatives.

Cyber Security Committee (CSC): Comprised of senior Opus team members and IT security personnel, the CSC has direct reporting and accountability to board level. The CSC is responsible for IT governance and compliance of security standards with sector specific regulatory bodies. The CSC is also responsible for periodical review of vendor management, access rights and controls, data handling and loss prevention, and storage processes.

Strategic plan: Opus has taken the initiative to develop a

company-wide strategic security plan addressing important areas such as:

- Security incident management, response, and recovery
- Data handling and loss prevention
- Third-party due diligence
- Threats and vulnerabilities management
- Risk management programme and strategy
- Training and education of staff
- Best practices and framework for IT and cyber-security.

Encrypted software: Opus ensures that data of clients and investors being accessed is always encrypted for protection against threats and vulnerabilities. Opus uses the latest encryption methods and technologies for data in use, SSL (Secure Sockets Layer), VPN (Virtual Private Network), secure data connections, networking technology that segregates traffic based on rules and data routing techniques to secure data in transit or motion. Cryptographic algorithms are implemented on the database and physical storage of databases to secure the data at rest.

ATE training: Opus has a mandatory ATE (Awareness, Training, and Education) programme to provide employees with information on IT security best practices, common threat types and the firm's policies and procedures regarding the appropriate use of applications, systems, services and networks.

Real-time monitoring: Opus uses third-party security tools to accurately assess and identify any security weaknesses in our networks, applications, industrial systems and networked software thus reducing their vulnerability to attack and data loss. Any security weaknesses and vulnerabilities that would give hackers an opportunity to do damage are identified.

> "WE STAY ON TOP OF ORGANISATIONAL WEAKNESSES BY EXAMINING OUR BUSINESS ENVIRONMENT THE WAY A HACKER WOULD"

External penetration testing: We stay on top of organisational weaknesses by examining our business environment the way a hacker would: through manual security penetration testing, aka "ethical hacking". Certified penetration testers use up-to-date hacking methodologies to identify vulnerabilities, minimise risk, and help protect our organisation against the most current hacking trends.

Annual cyber-security capability maturity assessments: Opus has engaged a leading financial services firm to provide an annual assessment of our framework for identifying, protecting, detecting, responding and recovering from a cyber-security incident in compliance with the National Institute of Standards and Technology.

CONCLUSION

As a key service provider for any hedge fund, fund administrators carry a significant responsibility to be vigilant regarding cyber-security. A cyber breach would result in irreparable operational and reputational harm not only for the administrator, but their clients and investors.

As a fund manager, you should make it a point to fully understand what initiatives your fund administrator has in place to address these serious risks. Be wary of those administrators that appear to delegate all responsibility. Having a 'strategy' that relies solely on software vendors, is insufficient to protect against the many cyber-security risks that exist.

Ultimately, the approach to address cyber risks has no middle ground. You either implement processes to protect your company and clients, or you leave yourself open to the risk of a potentially massive data breach. It is becoming increasingly important that your service providers should be able to demonstrate a strong culture of cyber-security to protect you and your investors. ■