PEI Alternative Insight

pfm

private funds management

Cybersecurity in private equity

How prepared is the industry?

A research report

January 2016

Sponsored by

esentire®

eSentire Inc.
sales@esentire.com
In North America: 1-866-579-2200
In the UK: 0800 044 3242

Dan Gunner
Director of Research & Analytics
Tel: +44 20 7566 5423
dan.g@peimedia.com

Helen Lewer
Managing Editor
Tel: +44 20 7566 5478
helen.l@peimedia.com

Ashwin Rattan
Commissioning Manager
Tel: +44 7566 4272
ashwin.r@peimedia.com

Julie Foster
Production & Design Editor

Contents

Preface 3

Survey highlights 5

Survey analysis 6

1. **Profile of respondents** 7

2. **Perceived threat level** 8

3. **Awareness of sources and types of risk** 10
   Portfolio company risk 10
   Third-party and data-sharing risk 12
   Internal risk 12

4. **Preparedness for an attack** 15
   Investor indifference 16

5. **Responsibility for cybersecurity** 18

6. **Conclusion** 20

About eSentire 21

About PEI 22

Preface

By eSentire Inc.

Research reveals cybersecurity gaps in private equity firms

Cyber crime has skyrocketed in recent years and several corporate giants have endured catastrophic breach events. Cyber attacks targeting behemoths like Target, Home Depot and Talk Talk have triggered a contagion effect that impacts organisations spanning all industries, regardless of scope, scale or boundary.

Many small and mid-sized financial firms (wrongly) consider themselves too small to be of interest to cyber criminals and choose to ignore the threat, leaving them open to attack. Private equity firms are particularly vulnerable as most operate with small cybersecurity budgets and limited IT staff. However, news headlines throughout 2015 have emphasised the real risk that *all* firms face. It is not surprising, therefore, that the whole financial industry is coming under increased pressure from governing authorities to do something concrete about it.

Regulatory associations – among them the US Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE), the Financial Industry Regulatory Authority (FINRA) and the UK's Financial Conduct Authority (FCA) – have already delivered detailed reports exposing how unprepared and ill equipped firms currently are to defend against threats. In these reports, the authorities have also set out their expectations on the benchmarks, measures and procedures that firms need to implement in order to identify, prevent and respond to possible future attacks. As regulatory associations work to fully define and outline these expectations, it is essential that firms gain an understanding of governance analysis to better prepare themselves for the continuous programme and posture evaluation and audits that lie ahead to demonstrate their efficacy.

As a leading cybersecurity advisor in the financial industry, eSentire Inc is aligned with the regulatory associations driving change and remains committed to delivering essential programmes to help firms in the sector stay ahead of governance requirements.

In addition to identifying noticeable trends, the purpose of this survey is to assess the cybersecurity hygiene and protocols used by private equity firms. What it reveals is that while most are concerned about cybersecurity and regulatory compliance, a large majority of those surveyed are unprepared for an audit or an attack. Broadly, three main vulnerabilities are exposed:

1. The absence of current cybersecurity programmes.
2. Unmonitored and unsecure devices.
3. Lack of the requisite expertise among staff to develop effective cybersecurity protocols.

eSentire and private funds management (pfm) are pleased to present the full results of our first *Cybersecurity in Private Equity* research report. We hope you enjoy reading it and find the responses insightful and thought-provoking on an issue that will no doubt present the industry with one of its biggest challenges in the years ahead.

Kind regards,

Eldon Sprickerhoff
Founder & Chief Security Strategist, eSentire Inc.

Survey highlights

Three quarters of survey respondents feel that cybersecurity is a relatively high risk to their business operations. On a scale of one to five (five being the highest), almost 45 percent believe the threat is at the highest level.

More than 53 percent of respondents confirm their business has already experienced a cyber attack.

More than 50 percent of respondents are of the opinion that regulatory compliance is of the highest importance to their businesses' cybersecurity management.

Just over half of respondents believe that responsibility for cybersecurity falls to their Chief Financial Officer (CFO). Almost a quarter of respondents feel it is the responsibility of their Chief Operating Officer (COO). Only 4 percent think the burden falls on their Chief Technology Officer (CTO).

The biggest perceived cybersecurity threats among respondents are: SSL encrypted threats; infected mobile devices; and brute force attacks.

Encouragingly, 46 percent of respondents recognise that having a robust cybersecurity programme can be a competitive advantage for their business.

It is a concern that 42 percent of respondents are still not tracking data movement within their IT infrastructure.

Only 23 percent of respondents say they have a fully operational SEC-compliant cybersecurity programme.

Almost half (48 percent) of the businesses surveyed allow their employees to use personal devices (mobile phones, laptops etc.) for work-related tasks.

Worryingly, over 56 percent of respondents do not issue any cybersecurity guidelines to staff around the use of different device types (mobile phones, laptops etc).

Survey analysis

Cybersecurity threats – whether from highly organised criminal groups or lone hackers operating from their bedrooms – are increasing on an almost daily basis. Private equity firms are every bit as vulnerable as other types of business, but to what extent do fund managers and other professionals working in the sector recognise this themselves? Are they taking the threat seriously? Do they even perceive cyber crime as a major threat to their business? And what are they doing to manage and mitigate the risk of attack? This survey attempts to answer these questions and assess the industry's preparedness for future attacks.

The regulators' view

The main financial regulatory authorities worldwide are certainly taking the threat to private equity firms seriously. In June 2015, the US Securities and Exchange Commission (SEC) made it clear that the industry needs to protect itself against cyber attacks. Further, in April this year, the SEC and FINRA (Financial Industry Regulatory Authority) published a 'Guidance Update' that will form the basis for the SEC's future scrutiny of the industry's performance in this regard.[1] Although aimed at US-based firms, the basic principles and recommendations in the Update are applicable to entities anywhere in the world. For example, it provides a general outline for dealing with the issues and examples of specific types of risk, such as identity theft and fraud, that can potentially disrupt funds' services and their ability to process shareholder transactions.

Particularly noteworthy are the three specific areas of action that the Guidance Update expects private equity firms to take to minimise cyber risks:

1. Conduct regular assessments of data collected, processed and stored, threat and vulnerability assessments of technology used, as well as assessments of controls and processes in place, impact assessments and, finally, assessments of governance structures in place for the management of associated risks.
2. Develop strategies to prevent, detect and respond to cybersecurity threats.
3. Write formal firm-wide policies and procedures setting out how these strategies are to be implemented and how the fund's officers and employees are to be trained accordingly.

While it is impossible to completely guard against all future attacks, regulators are clearly now of the opinion that those private equity firms that plan, design and implement clear cybersecurity policies and procedures will find it easier to mitigate attacks and the impact of them on clients and others with whom they do business.

We now turn our attention to the survey results. Do the respondents share regulators' sense of urgency with regard to cybersecurity?

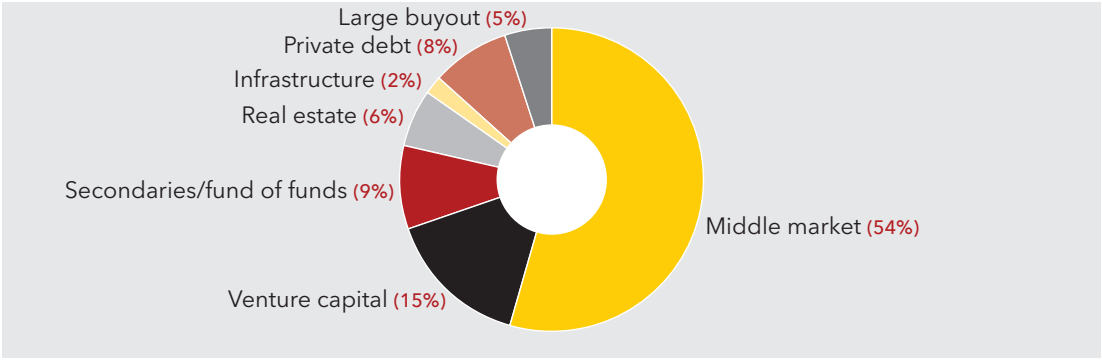
[1] IM Guidance Update, April 2015, No. 2015-02.

1. Profile of respondents

A total of 91 private equity firms responded to the survey questions. The data is rounded up or down throughout the survey.

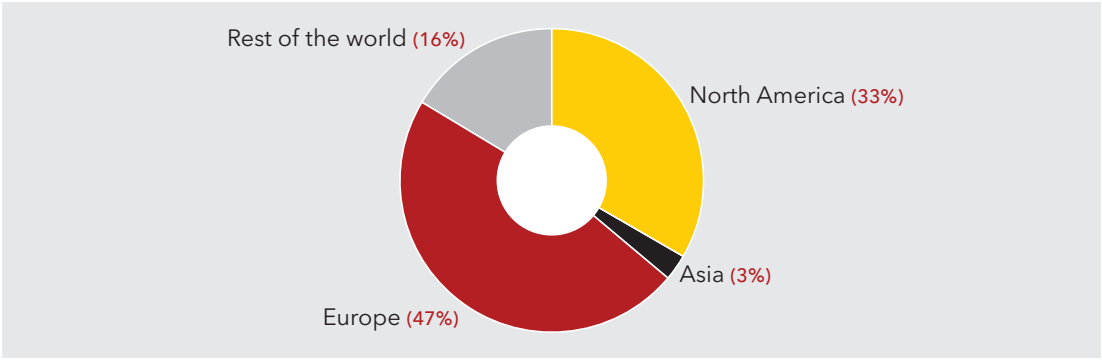
The majority (54 percent) describe themselves as middle market while the second largest group of respondents are venture capitalists (15 percent). Only 5 percent of survey respondents are large buyout firms. See Figure 1 for a full breakdown of the types of funds that participated in the survey.

Figure 1: **What type of fund do you work for?**



Nearly half (47 percent) of the survey respondents are headquartered in Europe. One-third have their HQ in North America. Only 3 percent are Asia-based. See Figure 2 for a full breakdown.

Figure 2: **Where are you headquartered?**



2. Perceived threat level

The survey results clearly show that respondents are fully aware of and appreciate the seriousness of the risk of a cyber attack to their business. In fact, 54 percent have already been subject to an attack (see Figure 3) and the majority (61 percent) are expecting an attack in the next 12 months (see Figure 4).

Figure 3: **Have you ever been under cyber attack?**

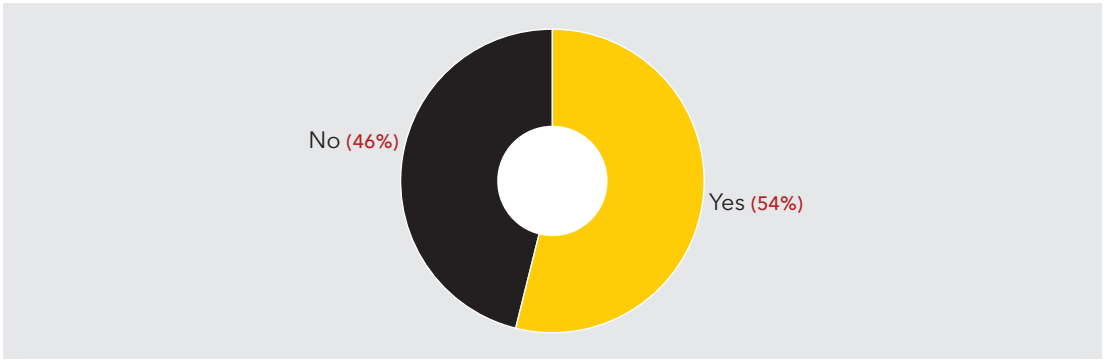
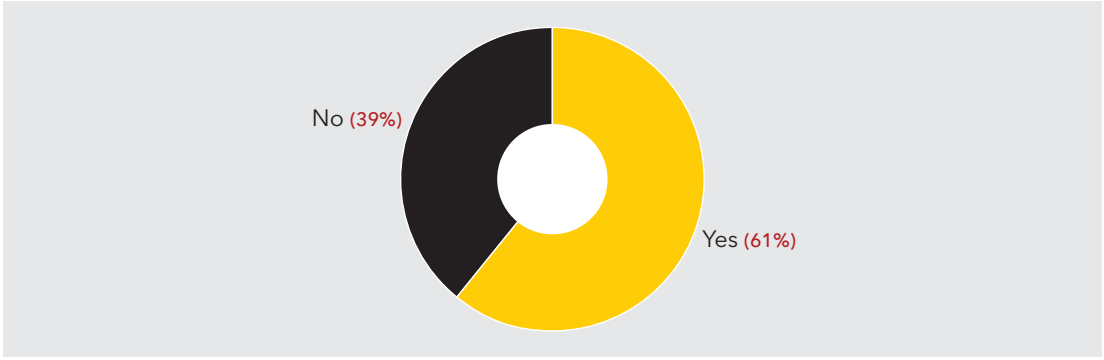
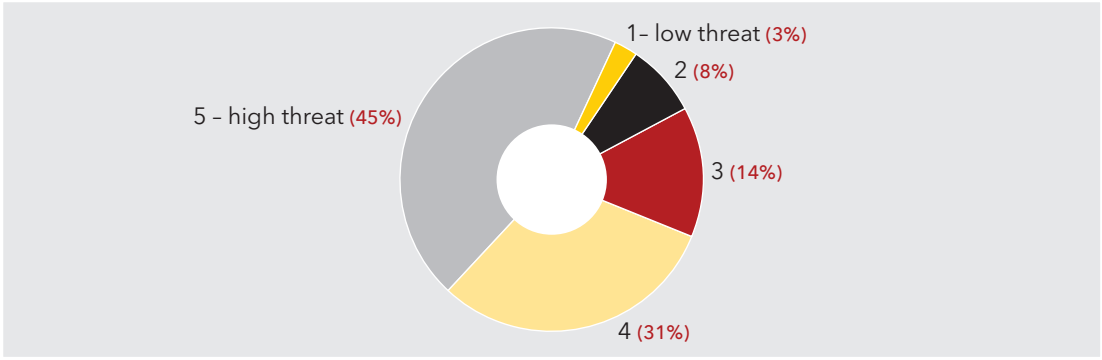


Figure 4: **Do you expect to come under cyber attack in the next 12 months?**



Cybersecurity is viewed by most respondents to be a critical threat to business operations. Asked to rate the threat level on a scale of one to five (five being the highest), just over three quarters believe the threat is high (see Figure 5).

Figure 5: On a scale of one to five, how critical a threat do you think cybersecurity is to your business operations?



As Figures 6 and 7 illustrate, respondents do not believe, however, that private equity is more of a target for cyber attacks than other areas of the financial sector, other business types or government.

Figure 6: Do you believe that private equity is more or less of a target than other parts of financial services?

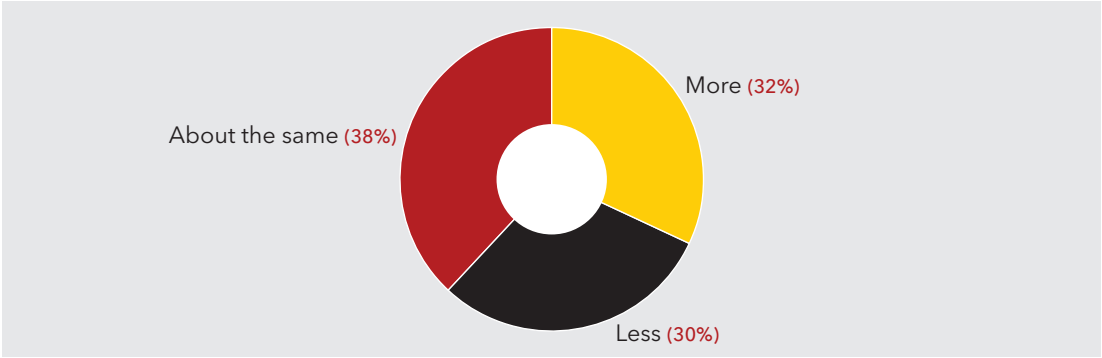
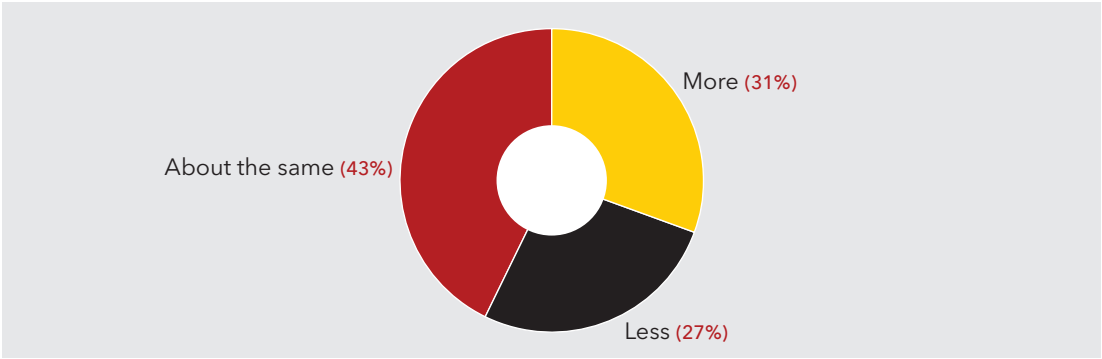


Figure 7: Do you believe that private equity is more or less of a target than other parts of business/government?



3. Awareness of sources and types of risk

When asked to identify the most likely source of a cyber attack on their business, respondents seemed uncertain. The majority selected the 'Other' option, but it is unclear which sources would, in their opinion, fall into this category. Criminal organisations and hackers are not perceived as a major threat. Instead, competitors, ex-employees and external business partners rank higher (see Figure 8).

Respondents were also asked to rank the five types of threats that are of most concern to them. The results are shown in Figure 9. Brute force attacks, SSL encryption-related threats and attacks from infected mobile devices are perceived as the biggest threat. Vulnerability risk is ranked fourth. The lack of vulnerability testing cited in Figure 21 on page 15 could therefore be viewed as a point of concern when it comes to maintaining a robust cybersecurity posture.

Figure 8: Rank the organisations and individuals most likely to pose a cyber threat to your organisation

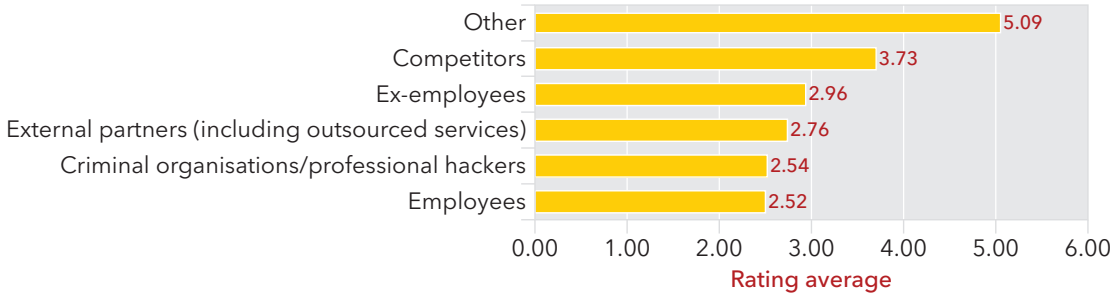
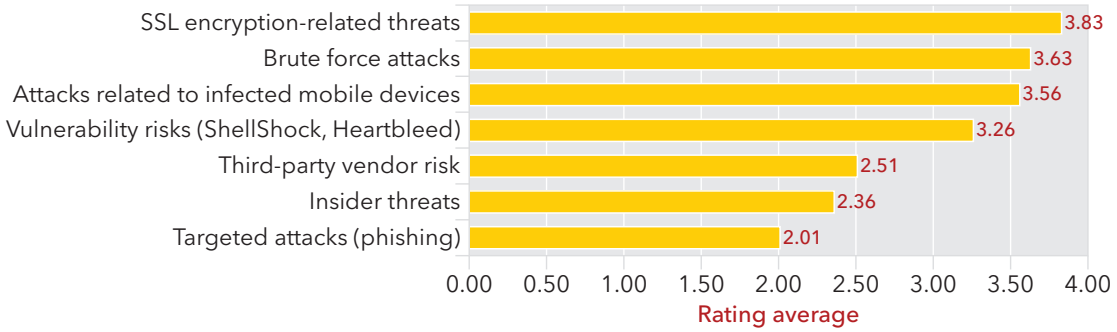


Figure 9: Rank the 5 biggest threats you perceive within cybersecurity



Portfolio company risk

Although portfolio companies should have the freedom to operate in their own style, it is nevertheless important that private equity firms maintain oversight of them to ensure cyber-related

risks via this relationship are effectively managed and mitigated. Yet a whopping 89 percent of firms participating in our survey do not have a standardised cybersecurity programme in place for their portfolio companies (see Figure 10). Further, 76 percent are not conducting a cybersecurity assessment as part of their due diligence when acquiring portfolio companies (see Figure 11) and almost 83 percent have no standard processes for systems integration following a mergers and acquisition (see Figure 12).

Figure 10: Do you have a standardised cybersecurity programme in place for all of your portfolio companies?

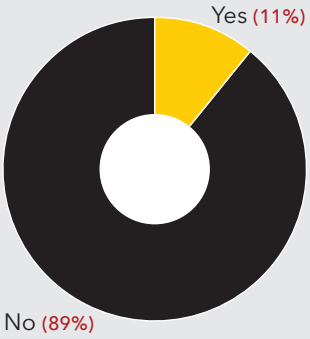


Figure 11: Is cybersecurity assessment part of the due diligence programme in acquiring portfolio companies?

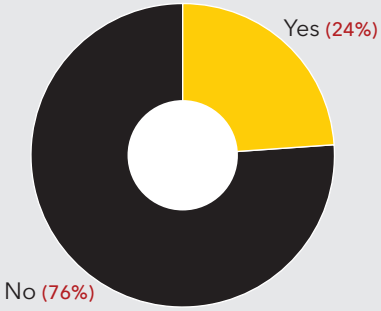
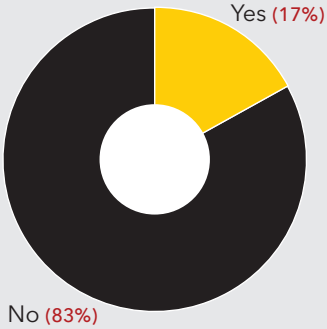


Figure 12: Do you have standard processes in place for systems integration following M&A?



Third-party and data-sharing risk

As well as their relationship with portfolio companies and LPs, private equity firms have a wide range of third parties with which they do business, including outside vendors, placement agents, law firms, accountants and tax advisors. And there have been some recent examples of breaches via these connections, resulting in the theft of personal and financial information.

Sensitive data is shared with all of these parties. This is unavoidable. So we were naturally curious to find out how secure the practices, systems and technology platforms being used by respondents for sharing data are. The answers make rather grim reading: 84 percent do not have customised processes for handling sensitive data from high value IP sectors such as healthcare (see Figure 13). However, it is encouraging that many of the survey participants are proactively tracking data movement within their IT infrastructure (see Figure 14).

Figure 13: Do you have customised processes for handling data from sensitive and high-value IP sectors, including software, medical devices and healthcare?

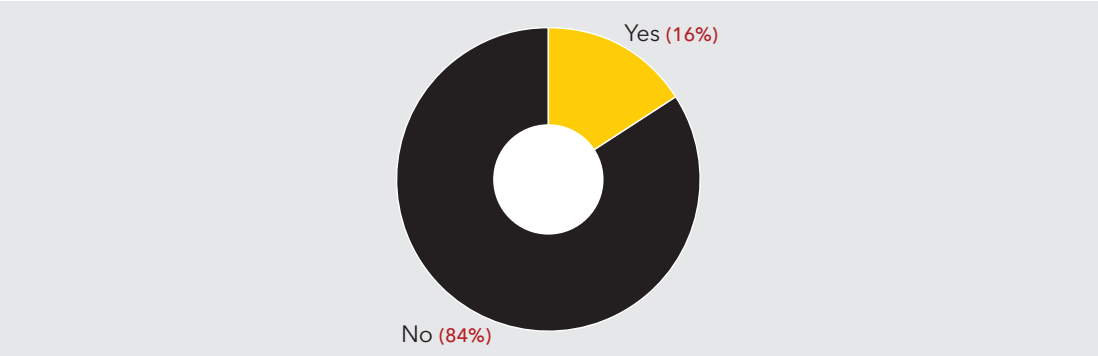
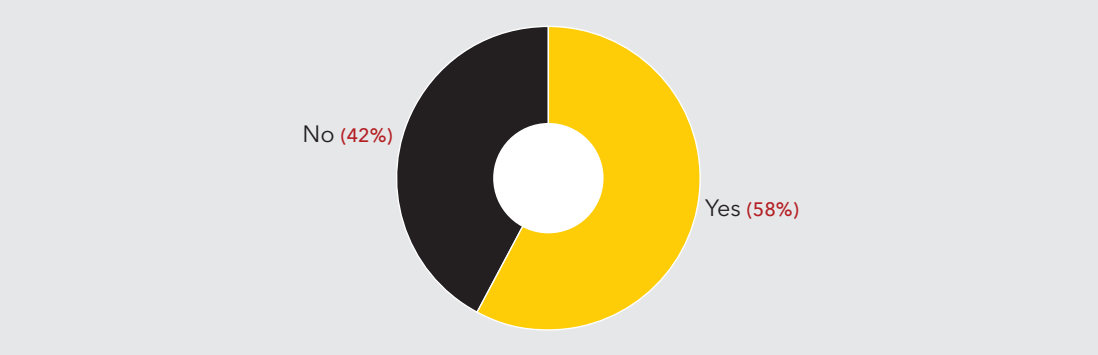


Figure 14: Does your firm track data movement within your IT infrastructure?



Cybersecurity should form a fundamental part of the due diligence and selection of third parties. Agreements between funds and third parties should contain explicit mention of cybersecurity issues with clear steps outlined for mitigating risk as well as set out the compensation that will be owed in the event of a breach. Indemnification provisions should also form a part of the agreement.

Internal risk

Of course, the risk of a cyber attack does not necessarily emanate from external relationships and sources. Private equity firms must also look at security within the organisation. Employees (and former employees) are an obvious potential risk, especially if they have (or had) access to corporate data. Just

some of the things that could create a breach include leaving an unencrypted laptop or memory stick containing personal or corporate information in a public place and careless use of an IT device used for both personal and business purposes.

However, firms may be underestimating or even ignoring the risk from internal sources. Figure 15 shows, for example, that survey participants could do better at identifying employees who are most vulnerable to a cyber attack. Figure 16 illustrates very cleary that respondents believe it is more critical to carry out information audits on sensitive customer data (56 percent) than sensitive employee data (only 23 percent).

Figure 15: As cybersecurity attacks get ever more personal, have you identified your most vulnerable employees by:

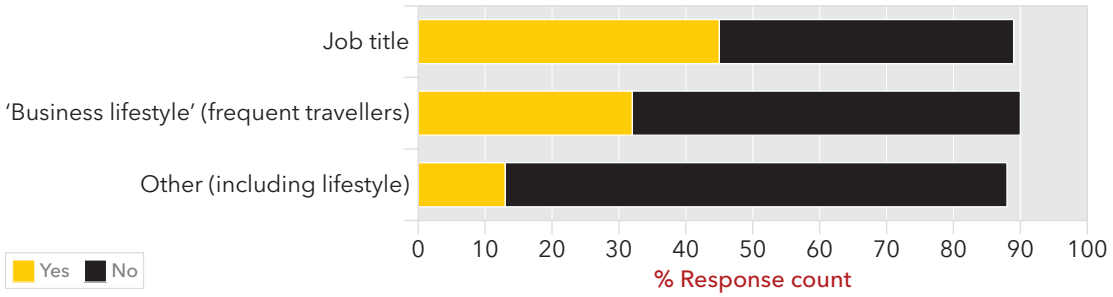
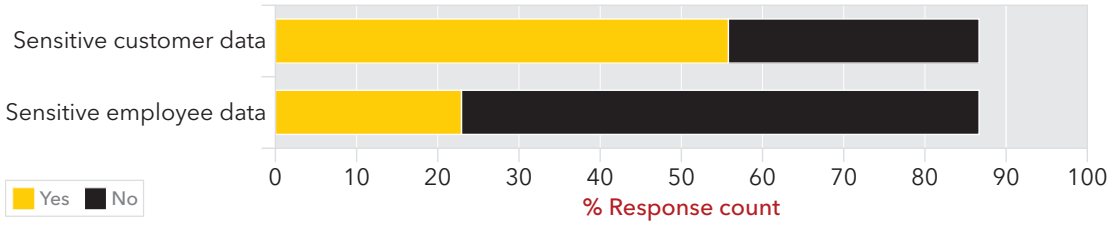


Figure 16: Do you carry out information audits on the following?



While just under half of respondents allow staff to carry out work on their personal mobiles and computers (see Figure 17), a similar percentage do not issue guidelines on the use of such devices (see Figure 18). Further, as shown in Figure 19, 74 percent do not issue employees with work-only digital devices.

Figure 17: Do you permit staff to carry out work on personal devices?

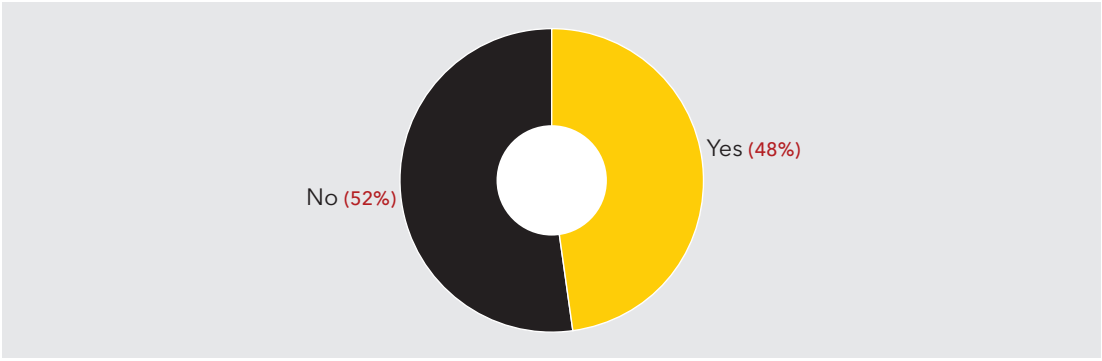


Figure 18: **Do you issue guidelines to staff on the use of different types of device (home PC, work PC, laptop and mobile device)?**

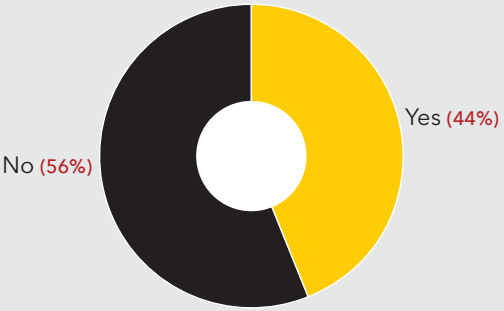
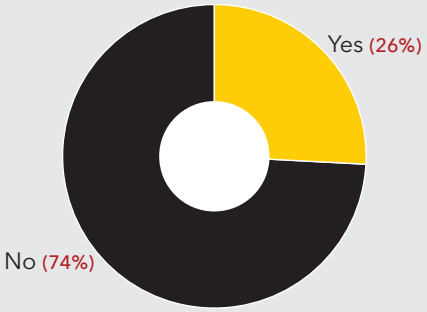


Figure 19: **Do you issue work-only digital devices?**



4. Preparedness for an attack

One of the central goals of this survey is to gauge how prepared respondents are for a future cyber attack. Again, the results indicate strongly that more progress is required.

A significant majority of respondents (66 percent) thus far have only a partially implemented cybersecurity programme. Only 23 percent have a fully operational programme that is compliant with SEC guidelines (see Figure 20). The latter result is somewhat surprising given that in Figure 21, 53 percent cite regulatory compliance on cybersecurity as most important to their firm. It must surely be a concern, however, that only a small percentage of firms rate awareness training, and continuous monitoring and reporting to be less important.

Figure 20: How would you describe the operational status of your cybersecurity programme?

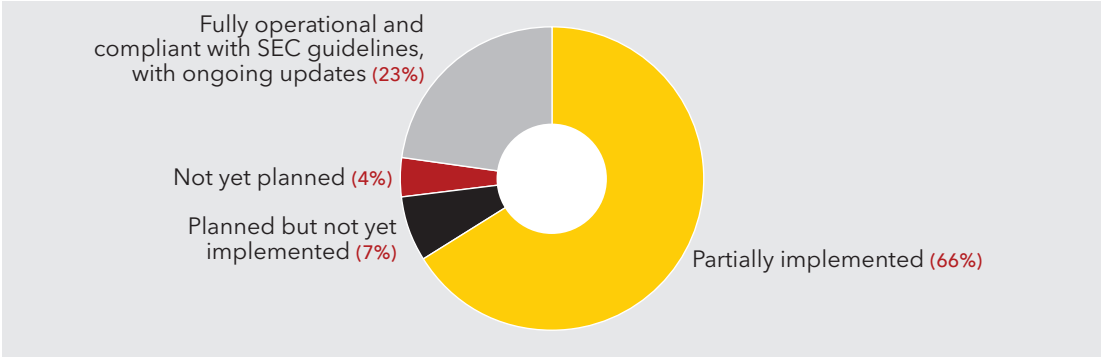
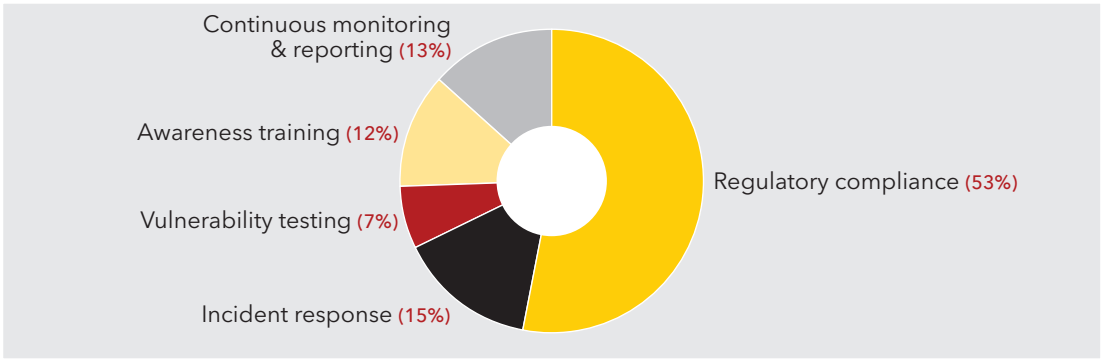


Figure 21: Which component part of cybersecurity is the most important to your firm?



It is clear that even among respondents with operational cybersecurity programmes, it is a relatively recent addition to the business – 43 percent have had it in place for between one and two years and only 23 percent for more than two years (see Figure 22). And generally speaking, these programmes are not expected to be a permanent fix, with one-third of respondents replying that they expect

obsolescence within one year and a further 49 percent expecting a lifetime of no more than two years (see Figure 23).

Figure 22: How long have you had your cybersecurity programme in place?

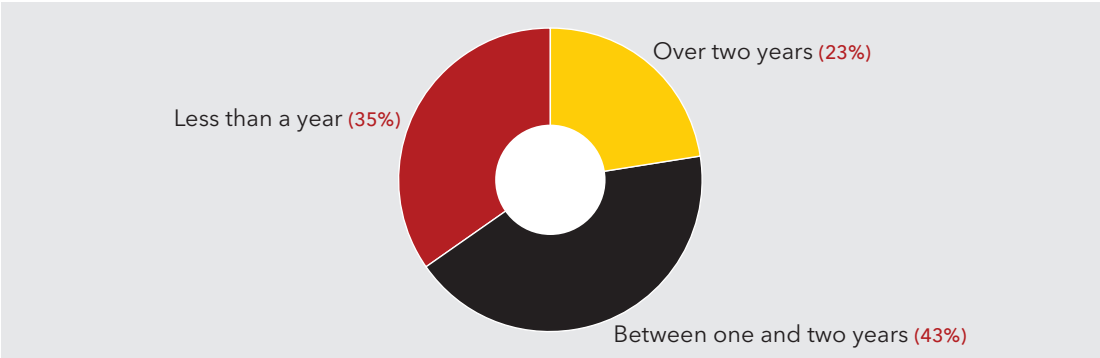


Figure 23: How long do you expect your cybersecurity programme to be fit for purpose?

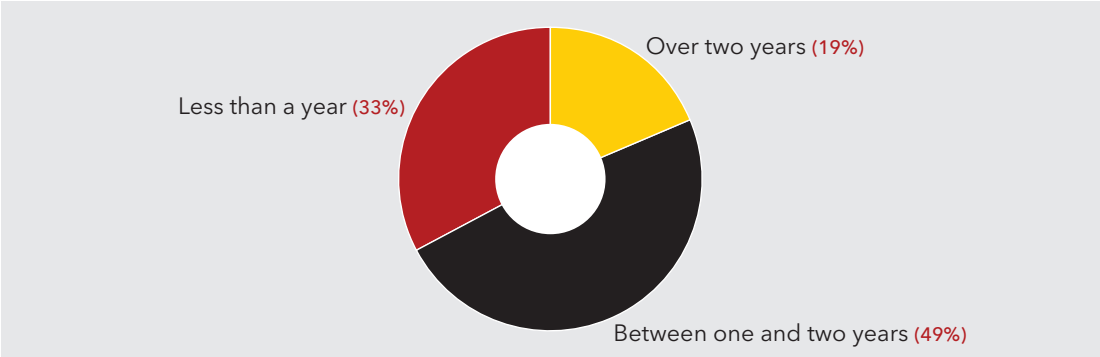
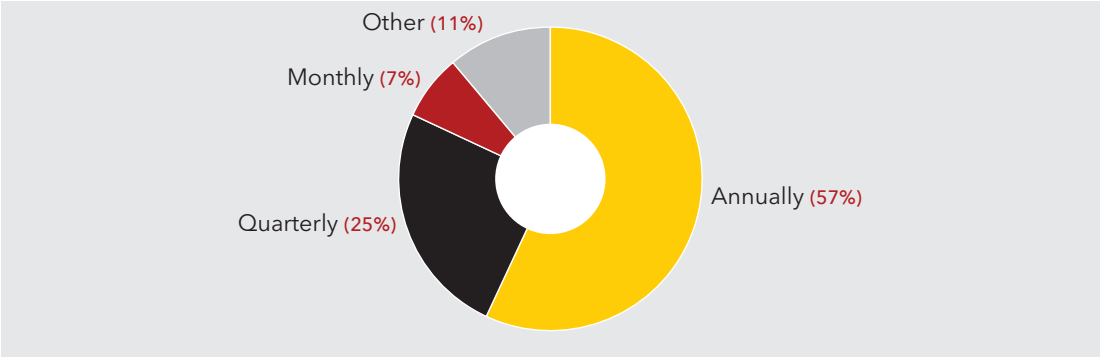


Figure 24 also suggests that respondent firms are not reviewing their cybersecurity processes with sufficient regularity – only 7 percent review on a monthly basis and the majority (57 percent) do so annually.

Figure 24: How often do you review your cybersecurity processes?



Investor indifference

One reason why firms' have not been proactive in implementing fully operational cybersecurity programmes may be the seeming indifference of investors on the matter. Just over half of funds

surveyed say that their LPs comment only occasionally on their cyber readiness, 20 percent say their LPs never mention it at all and just 27 percent of respondents say that all their LPs enquire about it (see Figure 25). This is perhaps why 54 percent do not believe that having a robust cybersecurity programme will give them a strategic or competitive advantage in the marketplace over the next two years (see Figure 26).

Figure 25: **How important is your cyber readiness to existing LPs?**

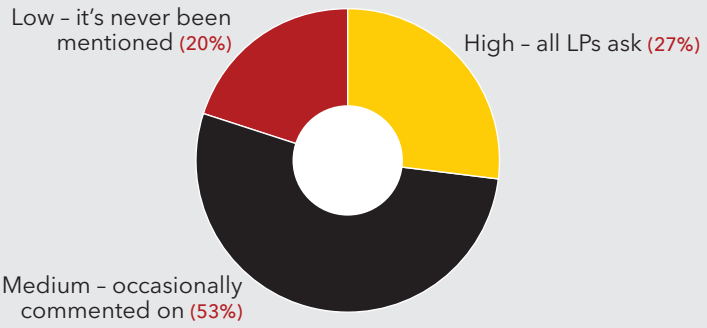
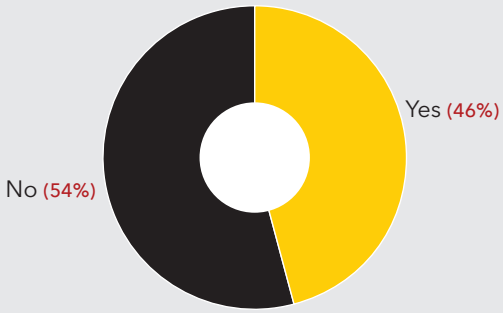
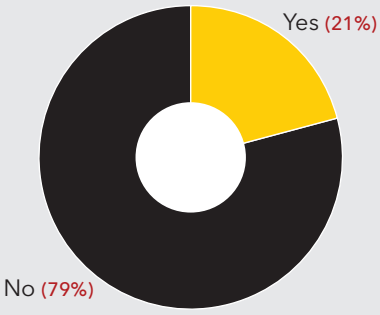


Figure 26: **Could you see robust cybersecurity becoming a competitive advantage for your firm in the next two years?**



Despite the range of risks facing the industry and the evident lack of preparedness of respondents, it is somewhat concerning that almost 79 percent do not possess cybersecurity insurance (see Figure 27).

Figure 27: **Do you have cybersecurity insurance?**



5. Responsibility for cybersecurity

The need for dedicated technology management at the C-level does not seem to be a prime concern. Almost no firms (96 percent) surveyed have appointed a dedicated Chief Technical Officer (CTO) with the requisite skills to take the lead on cybersecurity. Further, 85 percent have no plans to recruit a CTO in the next 12 months (see Figures 28 and 29). Rather respondent firms are drawing on other executives in the business to take responsibility for cybersecurity. In particular, as shown in Figure 30, the burden appears to fall most often on the Chief Financial Officer (CFO) followed some way behind by the Chief Operating Officer (COO). This is concerning as Figure 31 indicates that these experts are somewhat lacking in the deep and expert knowledge needed to monitor and manage cybersecurity issues; only 12 percent think their C-level executives are informed to a high level.

Figure 28: **Does your firm have a CTO?**

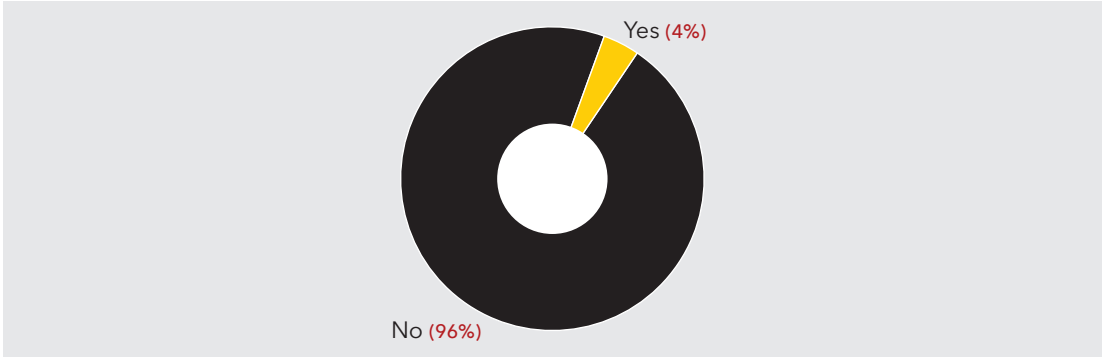


Figure 29: **If your firm does not have a CTO, do you have plans to recruit one within the next 12 months?**

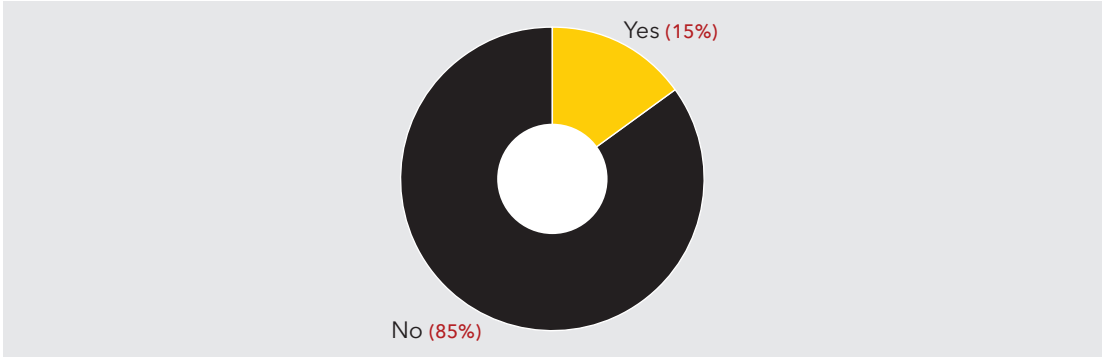


Figure 30: **Who in your organisation (job role) has responsibility for cybersecurity?**

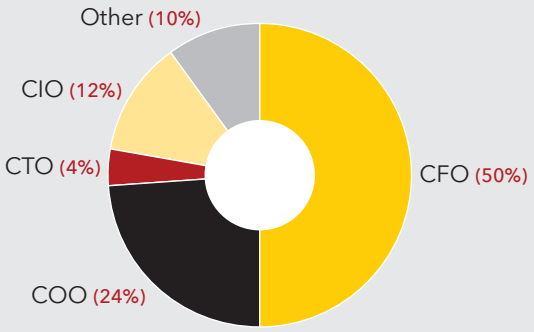
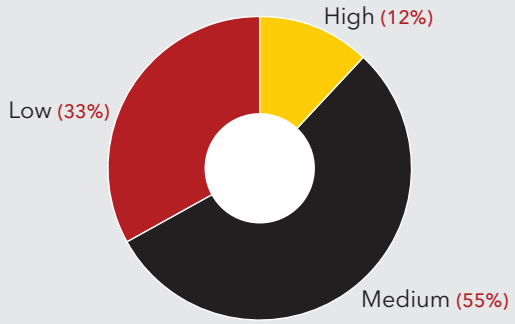


Figure 31: **How would you describe the level of knowledge of cybersecurity issues among middle and C-level staff at your firm?**



6. Conclusion

This survey suggests that the private equity industry has some way to go before it can confidently claim to have a watertight grip on cybersecurity issues. While our participant firms certainly seem to be aware that threats exist to their business, many are failing to make the transition to implementing practical and meaningful cybersecurity processes and programmes. While it is impossible for any business to completely prevent cyber attacks, it is better to be safe in the knowledge that you have done everything needed to prepare for the eventuality. In that respect, the private equity sector could do better.

About eSentire

At eSentire, our Active Threat Protection™ platform is designed to serve organisations with high-value targets and a low tolerance for risk. We recognise that organisations are challenged to manage unique industry drivers, and complex regulatory and legal requirements. We have combined people, process and technology to deliver a premium white glove service that is continually evolving to defend against today's advanced cyber threats, while taking the complexity of industry requirements into consideration. eSentire provides mid-sized enterprises with advanced cybersecurity capabilities. Our state-of-the-art security operations centre delivers Active Threat Protection to our clients on a more economical and efficient basis than what can be achieved in-house.

With global security operations centers (SOCs), our security analysts continuously monitor client networks, detecting, remediating and communicating threats in real-time, 24/7/365. Today we protect more than $2.5 trillion USD AuM. We are the award-winning, trusted choice for security decision makers in small to mid-size enterprise.

About PEI

pfm is published by PEI, the leading financial information group focused exclusively on alternative asset finance and investment. We specialise in covering the private equity, private debt, real estate and infrastructure industries globally and are increasingly active in other, emerging alternative investment fields and practices too. The company has over 120 staff based in three offices – London, New York and Hong Kong.

We started in London in November 2001 when a team of managers at financial media group Euromoney Institutional Investor PLC, with the backing of US-based investors, bought out a group of assets that centred on *www.PrivateEquityInternational.com*. In 2001 we launched our first magazine: *Private Equity International*. A year later, we opened our New York office and launched two more titles: *Private Funds Management* and *PERE*. In 2009 we launched *Infrastructure Investor* and in 2013, *Private Debt Investor*. In 2014 we acquired *Real Estate Capital* and launched the *Specialist Investment Networks*.

PEI specialises in connecting practitioners active in our chosen asset classes with value-added market information and analysis via our print and digital publications and with each other via marquee industry events. We help to define and convene these industries. We now publish six magazines, host ten news websites, manage a very extensive set of databases dedicated to alternative assets, run 55 annual conferences globally and publish a library of more than 40 books.

The world's largest investors in, and fund managers of, alternative assets are among our many thousands of clients and we have customers based in nearly 100 different countries.

Since we started our aim has been to deliver timely and relevant products and services to alternative asset professionals wherever they are based in the world. Our full-service regional offices in Hong Kong, London and New York mean that our connections with local markets are both broad and deep.

PEI Alternative Insight
pfm
private funds management

Published in January 2016 by
PEI
6th Floor
140 London Wall
London EC2Y 5DN
United Kingdom

Telephone: +44 (0)20 7566 5444

ISBN 978-1-908783-98-1

LONDON
140 London Wall, 6th Floor
London EC2Y 5DN
United Kingdom
Tel: +44 20 7566 5444

NEW YORK
16 West 46th Street, 4th Floor
New York NY 10036-4503
United States
Tel: +1 212 633 1919

HONG KONG
14/F, Onfem Tower
29 Wyndham Street
Central, Hong Kong
Tel: +852 2153 3240