privateequitywire



Cybersecurity

IN FOCUS 2021

CYBER STRATEGY
Planning a building block of infrastructure

PE MANAGER LANDSCAPE
Cybersecurity critical to remain competitive

ONGOING MAINTENANCE
Regular reviews to keep cyber plan relevant

Featuring Drawbridge | Eze Castle Integration | RFA

EzeCastle
INTEGRATION

Leading global provider of managed IT services and technology solutions

Our expert team will deliver a highly secure, managed IT solution designed around your business needs.

- Complete Digital Services
- Complete Managed Cloud Solutions
- Complete Cybersecurity Protection
- Premier Outsourced IT

To find out more, call +44 (0) 207 071 6802
or visit www.eci.com

LONDON | BOSTON | CHICAGO | DALLAS | HONG KONG | INDIA | LOS ANGELES | MINNEAPOLIS
NEW YORK | PHILADELPHIA | PHILIPPINES | PORTUGAL | SAN FRANCISCO | SINGAPORE | STAMFORD





INSIDE THIS ISSUE...

04 BUILDING A CULTURE OF SECURITY
By A. Paris

06 ROBUST CYBERSECURITY CRITICAL TO REMAINING COMPETITIVE
Interview with George Ralph, RFA

08 BEST LAID PLANS TO NOT GO ASTRAY
Interview with Jamie Smith, Eze Castle Integration

11 ONGOING MAINTENANCE VITAL FOR SUCCESSFUL CYBERSECURITY
Interview with Jason Elmer, Drawbridge

13 DIRECTORY





privateequitywire

Published by: Private Equity Wire, 8 St James's Square, London SW1Y 4JU, UK
www.privateequitywire.co.uk

©Copyright 2021 Global Fund Media Ltd. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher.

Investment Warning: The information provided in this publication should not form the sole basis of any investment decision. No investment decision should be made in relation to any of the information provided other than on the advice of a professional financial advisor. Past performance is no guarantee of future results. The value and income derived from investments can go down as well as up.



Building a culture of security

By A. Paris

General partners (GPs) have a raft of technology solutions to choose from when looking to make sure their cybersecurity infrastructure is robust. Deploying state-of-the-art technology which meets the needs of the organisation and provides the security necessary is vital for GPs to continue operating, both from a regulatory point of view and also to ensure they continue to attract capital.

However, systems alone are not enough. A large part of cybersecurity relies on all the firm's staff – from the C-suite to regular employees. Their understanding, vigilance and willingness to highlight any issues they may encounter in the course of their working day can make or break a PE firm's cybersecurity strategy. In view of this, organisational culture plays a huge role in ensuring GPs are securing their data and that of their portfolio companies.

A study of 50 major data breaches carried out by Boston Consulting Group (BCG) found that only 28 percent were caused by inadequate security technology. "In the vast majority of cases – 72 percent – the breach was the result of an organisational failure, a process failure, or employee negligence," the consultancy outlines.

In a research paper for the Harvard Business Review, Keri Pearlson, Brett Thorson, Stuart Madnick and Michael Coden explain the importance of testing and making sure that even the C-suite are familiar with all the necessary protocols.

"To make sure they are aligned and aware of company plans during a cyber attack, they [C-suite executives] need to practice ahead of time and build muscle memory in how to respond. Simulated scenarios help organisations to validate their plans and prepare company leaders," the authors write.

Jamie Smith, Eze Castle Integration's Director of International Technology, stresses the importance of tabletop testing: "Incident response isn't accidental, it's something you test and it's perspective you gain when you do carry out these tests and gauge how quickly you react. The more you test your response, the better you'll get at responding. Also, these tests need to have a certain level of granularity to cater for different types of cyber attack; having a different playbook for each one is really important."

RFA outlines the benefits of phish testing and security awareness training: "Training significantly reduces your chances of a breach or an attack. Knowledge is always power. Educating your employees and developing a

security-conscious culture is essential and typically not a priority for firms, but it should be," says RFA global managing director, George Ralph.

Jason Elmer, CEO and founder at Drawbridge advises: "Driving cybersecurity within the firm must come from the top down, and ownership remains within the firm. Should a GP choose to hire a cybersecurity specialist in-house, it is critical that this person be educated enough on the importance and impact of cybersecurity to drive enforcement. That can come from careful work with a cybersecurity firm and does not necessarily require prior skills or expertise."

As the incidence of cyber attacks continues to rise and the likelihood of falling victim to one is high, GPs need to make sure to foster a culture in which employees feel comfortable coming forward with any concerns. A culture of blame in this regard is severely disruptive. So, although cybersecurity is everyone's responsibility, to some degree, it is up to the GP management to empower its employees to speak up. Smith details: "It's important for people to know what to look for and know when to raise their hand and highlight any issues. It is really important that the culture within the firm is one of togetherness and everyone pulling the same rope, rather than finger wagging at someone who has forwarded something suspicious or clicked on a phishing email."

Organisations should strive for adherence (active participation) rather than compliance – rapidly emerging threats require employees who are engaged and willing to step up. Organisational leadership has a key role in developing effective and workable security – by helping security specialists to fit security into the business, breaking down silos and leveraging other organisational capabilities (safety, HR, communications) – but not least by setting the tone and leading by example.

Security issues across the deal lifecycle

A guide published by the British Private Equity and Venture Capital Association (BVCA) together with PwC highlights the key principles GPs should consider in relation to cybersecurity.

"Private equity fund managers should care about cybersecurity risk in a deal context because it can either cost or generate money depending on how it is treated. The frequency of cyber attacks and the complexity of the threat are increasing, and the downside risk that comes with poor handling of the issue can be significant and manifest in a variety of ways," the guide warns.

There are differing cybersecurity considerations within each phase of the deal lifecycle. When conducting due diligence, GPs need to identify risk exposures and factor any remediation into their negotiations as appropriate. In the onboarding phase, GPs need to help the portfolio company achieve a baseline level of security maturity which is at least in line with its industry peers.



> *"PE executives are beginning to understand that if something were to happen, they would be at risk of financial, investment and brand damage."*
>
> **Paul Harragan, EY-Parthenon**

During the value creation stage, firms should initiate enhanced programmes to maximise security capability and establish this as a business differentiator. Validating that the organisation has not suffered an unknown breach is then an essential step GPs must take when preparing for a sale.

The BVCA guide advises: "More money is not always the answer. Many companies underspend on security, but many others spend too much or poorly. Optimise security and make sure your portfolio companies are not carrying unnecessary fat."

According to Paul Harragan, EY-Parthenon Director, Strategy and Transactions, Ernst & Young, PE firms are beginning to change their behaviours in relation to cybersecurity diligence, though they were historically lax in this area: "PE executives are beginning to understand that if something were to happen, they would be at risk of financial, investment and brand damage.

"This is due to an increased awareness of threats to their portfolio companies and their own operations.... Prominent data breaches have shown the scale of the potential impact on the value of a compromised portfolio company." In addition, he argues the pandemic also contributed by widening the landscape and leaving investment managers exposed as a result of the change in operating models most had to implement. ■



Robust cybersecurity critical to remaining competitive

Interview with George Ralph

Cybersecurity is connected to every single part of a business. Having the right solution and working with experienced partners is critical. Private equity firms understand that having a robust set up in this regard is necessary to remain competitive. Those willing to learn and evolve faster are reaping the rewards in terms of harnessing the value of secure cloud-based business IT architecture.

"I would always recommend reaching out and getting the expertise you need to get the right advice and build from the ground up," outlines George Ralph, Global Managing Director at RFA. "The right solution will be scalable for your firm. This is the beauty of cloud-based tech, firms can build an IT architecture for now and the future."

"We often hear that PE firms have been slow on the uptake in relation to new tech in the past. I think that has changed. It is basic business sense that if you don't keep up with your competitors in terms of your technology estate and capabilities, you simply won't win the business," he says.

When putting a cybersecurity framework in place there are many moving parts and Ralph strongly advises that PE managers work with a technology partner who has experience and access to the entire market. PE firms at the start of their cybersecurity journey would begin by carrying out a risk assessment. They would then consider their cybersecurity solution from two perspectives: what is optimal for them as a business and what will also support them best when working with vendors, regulators and investors.

Ralph also points out that cyber is an



important part of a PE firm's ESG policy: "We are seeing questions around cybersecurity in ESG due diligence questionnaires. These include questions around competence and training, monitoring and reporting, risk, change management, third party vendor management and reparations in case of attack. Your cybersecurity set up is so closely linked to your data management that you have to be able to evidence you understand how your deal flow works and that you have a 360 degree view of all the moving parts."

Costing a breach

When it comes to considering the impact of a breach, Ralph believes it isn't possible to put a cost on a cyber breach: "It depends on whether the breach was directly attributed to the PE firm or a third party vendor. Also, what is breached, what is lost, affected, or stolen as well as the resolution, also make a difference to the repercussions of such an event."

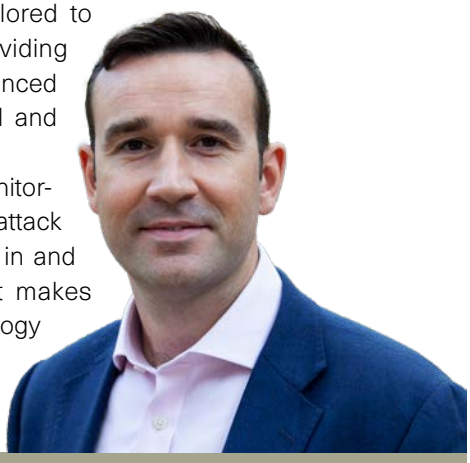
However, he acknowledges that reputational damage can be hard to come back from, therefore it follows that putting the right security measures in place to mitigate risk rather than manage attacks is the best approach. However, attacks do happen. "I would strongly suggest that a manager has a plan in place in the event of a cyber attack. How do they intend to communicate the event internally and externally? What is their plan for alternative communication channels should their main channels have been breached?" Ralph comments.

The outsourcing question

The decision whether to outsource the cybersecurity function or hire an in-house professional largely depends on the size of the PE firm in question. Ralph says: "Very few firms would require a full time CTO to support their business IT requirements. Firms who embark on a comprehensive digital transformation journey, using digitisation to automate operational processes would also have little need for additional in house expertise. The idea of digitisation is to take day to day tasks away from individuals allowing them more time to focus on their main business functions."

Services like RFA's Managed Detection & Response (MDR) is designed to support PE firms with an entire end to end cybersecurity solution. From 24/7/365 monitoring for internal and external anomalies to full reporting and support via engineers in its Security Operations Centre, the platform enables firms to outsource their solution. In terms of public cloud security, RFA has been at the forefront of cloud development since 2014. MDR uses AI and machine learning to spot anomalies across a firms technology estate, alerting you to any potential risks or forms of attack. MDR is also compliance tailored to regulatory requirements, providing hundreds of clients with enhanced data and applications control and reporting to reduce risk.

"I would also say that monitoring for cyber prevention and attack is a 24-hour programme, day in and day out, 365 days a year. It makes sense to work with a technology partner that can provide this," he highlights. ■



George Ralph
Global Managing Director & CRO, RFA

As Global Managing Director and CRO of RFA, George Ralph is a technology and business leader with a proven track record of strategic alignment, process improvement and guidance. Having been both a COO and a CTO of his own technology firms over a nineteen-year period, he looks to provide transparent guidance to every business he serves and the people he leads. George has extensive delivery and technical experience in cloud and data architecture, large-scale migrations utilising leading technology brands and IaaS offerings. An Assessor for the British Computer Society (The institute of IT) and a Certified IT professional, George is keen to ensure that the RFA gives its clients the highest levels of service.



Best laid plans to not go astray

Interview with Jamie Smith

Planning ahead must form a building block of certainty for private equity firms looking to bolster their cybersecurity infrastructure. An attack or a potential breach is bound to take place, given the current market conditions and being well-prepared is the bedrock of their defence and response to such an event.

"The more effort you put into your planning, the better the outcome will be when an attack happens," comments Jamie Smith, Eze Castle Integration's Director of International Technology, "It's no longer about if it happens, but when. I think every company will either have a bump in the road or a full on data leak at some point. It's the reality of cyber today given there is a lot of bounty to be had in financial markets and the interest by bad actors is huge."

Smith believes that a large part of a successful cyber programme is made up of tabletop testing: "Incident response isn't accidental, it's something you test and it's perspective you gain when you do carry out these tests and gauge how quickly you react. The more you test your response, the better you'll get at responding. Also, these tests need to have a certain level of granularity to cater for different types of cyber attack; having a different playbook for each one is really important."

Planning an instant response to a cyber attack or a potential attack is critical to general partners (GPs) looking to strengthen their cybersecurity. "If you don't have the skills to do it in house, you can engage with third parties and find the right people specialised in this area and have them on a retainer to call in when you need them," notes Smith.

Assessing the risk

Of late, private equity firms have been becoming more prescriptive in how their portfolio companies approach cybersecurity. "A PE firm

builds a portfolio of different companies across different industries and sectors. There is often no baseline for the factors which might go into a cyber profile," Smith outlines, "Therefore GPs are being stricter with how they expect their portfolio companies to manage their cyber risks and the infrastructure or processes they need to have in place."

Although it may be hard to quantify, the cost of a breach is undoubtedly significant. Smith highlights: "To try to estimate the impact a breach can have on company valuations, the public markets can serve as a good proxy. Some metrics found a public company stock can drop as much as 11 percent in value following a cyber breach. In addition, such an event plays on people's minds for a long time so the company is likely to experience a prolonged dip and a slow recovery. Portfolio companies could follow a similar trajectory if they are victims of a cyber attack."

In addition to the valuation hit, the repercussions of the reputational damage caused by a cyber attack could be immense.

"The market cycle is a lot shorter now so a data breach at a company will be instantly in the news and spread on social media. This heightens the impact of such an event which makes damage control a lot more challenging," Smith underscores.

In the context of the current market, where limited partners (LPs) have a lot more choice, this resonates even more.

"Since there are many investment opportunities bred by the market volatility, LPs are driven to invest in firms with proven track records and reputation plays a crucial role in that. In times of volatility, they want to put their money where they feel it's safe," says Smith.

A cyber attack can have a huge impact on a firm's reputation and as a result, he believes the PE industry will see a lot more effort going into the due diligence process, with GPs carrying out full cyber assessments of a portfolio company before they invest in it.

Trusted partners

"The penetration of cybersecurity programmes has increased in the past year. The shift to cloud-centric solutions has meant GPs began to re-certify and reclassify their cyber risks and how they're securing their firm. This has led to significant interest and uptake of security programmes," Smith observes.

He warns against considering cybersecurity as a tick-box exercise: "Cybersecurity isn't something you can pick up and hold. There is a plethora of different things which play into it. The key to success here is strategy. It's no good going out and buying products if you don't understand how they can work together."

Smith stresses the importance of cohesion: "You can buy a long list of products but without a strategy to pull them all together you could still fall victim to the biggest cyber breach ever."

Working with an outsourced provider to assist with this can prove highly beneficial, especially for GPs still on the growth path. However, Smith says its crucial for firms like ECI to have a GP employee act as a cybersecurity sponsor: "This is the best relationship for us as we can work with that individual to identify the help they need and the gaps we can seek to fill. That internal sponsor can build trusted partnerships with experts and service providers to bolster the GP's cybersecurity framework to outsource any elements they cannot fulfil directly themselves."

These internal experts can also ensure the GP adheres to the strategy it set out for itself and is not overcome by the raft of cybersecurity products and solutions being brought to market. Smith highlights: "There are some great cyber products available at the moment, but GPs need to consider what they really need. This is where the relationship between the GP and the service provider comes into focus; we've worked with our clients to make sure that the business risk they're exposed to warrants the additional span of security, so justifying any additional solutions is a huge part of our role as trusted partners to the industry." ■



Jamie Smith
Director, International Technology, Eze Castle Integration

Jamie Smith is Director of International Technology at Eze Castle Integration. Jamie has over 15 years of IT experience specific to the hedge fund and alternative investment sector. Jamie served as head of technology for a financial-focused managed service provider where he helped drive the company's growth and expansion from three to 70 employees. His experience also includes a six-year tenure on the technology team at global hedge fund and alternative asset manager, Och-Ziff Capital Management Group. With vast experience in technology bespoke to the alternative investment management space, Jamie is able to help Eze Castle Integration's clients continue to leverage IT to achieve their strategic goals. Jamie attended University of Hertfordshire, where he studied Computing and Business. He also holds several industry specific certifications for technologies such as Microsoft, VMware, Citrix and Cisco.

DRAWBRIDGE

DrawbridgeConnect-R™ for PRIVATE EQUITY

Vulnerability management is an ongoing, comprehensive program that will analyze the vulnerabilities of an organization's network in a continuous manner.

Cybersecurity breaches are occurring in the Private Equity space, which has resulted in **increased regulatory and investor scrutiny for managers**. LPs want to have confidence that their assets and information are safe with the managers they invest in.

- At the GP level, it is important to have ongoing maintenance and oversight in order to protect the Firm, its assets, and its confidential information.
- At the Portfolio Company level, it is important to regularly test the environment and remediate vulnerabilities.

The DrawbridgeConnect-R™ user interface allows PE Firms transparency and insight into their cybersecurity vulnerability management program by having access to data and reporting **both at the GP and Portfolio Company Level.** The UI also consists of executive summary level reporting to be evidenced to LP's. This will show progress of the

The DrawbridgeConnect-R™ platform provides the following:

Drawbridge provides vulnerability scanning on the Firm's internal and external network, and Portfolio Company internal and external networks, on an ongoing basis and aggregates data highlighting, but not limited to, the following:

- Missing Patches
- Operating System Vulnerabilities
- End-of-Life Detection
- Software Vulnerabilities
- Configuration Mistakes
- Weak Passwords / Default Credentials
- Remote Code Execution
- SSL/TLS Vulnerabilities
- SSH Vulnerabilities

The Managed Service Component:

Drawbridge provides ongoing solution maintenance and upkeep, remediation guidance, and advisory to the client in order to help the client operate as an institutional cybersecurity program would.

Drawbridge works directly with Firm IT, Portfolio Company IT or any of the Managed Service Providers on any items related to remediation and validation to ensure reporting, advisory, and action items are clear and actionable.

©2019 Drawbridge Partners, LLC, All Rights Reserved.

Ongoing maintenance vital for successful cybersecurity

Interview with Jason Elmer



Cybersecurity cannot be a one-time implementation exercise. It requires ongoing management, review and maintenance. And although there has been significant growth in private equity (PE) managers adopting cybersecurity software and solutions, there is still considerable progress to be made.

"It is clear we're still working within an industry that is learning about its own cyber needs and goals," points out Jason Elmer, CEO and founder at Drawbridge, "We're still in an education phase, which is some way from an industry-wide standard or optimal level."

This is despite the firm having witnessed significant growth of its services in the PE space over the course of 2020.

Elmer stresses the importance of reflecting changes in the way people work within any cyber policies: "Policies need to be practical in their implementation. There is no point writing policies which are either unenforceable or unachievable by staff and systems.

"It is critical for firms to work through a baseline of policies early, and to do this while selecting and building their technology platforms. It can be unpleasant to be forced to re-evaluate the implementation of a platform because it doesn't meet the expectations set out while drafting policies. Something as simple as a new password policy can be difficult to implement once everyone has already set their expectations."

Early consideration of cybersecurity also matters for portfolio companies. Elmer advises: "It's critical that cyber be addressed early and comprehensively for any portfolio company. The fund should set the standard within its business and for its portfolio. Cybersecurity always needs to be driven from the top down, so the manager is seen as the driving force."

PE managers increasingly need to handle news media outlets which are keenly aware of the impact cyber attacks can have. In addition, they need to cope with the rise in regulations around disclosure of such events.

"The consequences of a successful cyber attack are more transparent than ever. A PE firm's reputation can be damaged quickly. It's not unusual to see PR firms being involved in the recovery from a cyber attack, alongside technical and cybersecurity firms. This obviously adds to the cost of said recovery," Elmer outlines.

Another cost concern is return on investment (ROI). This can be approached in a few different methods for private equity. Elmer explains: "Traditionally, we would calculate the Annual Loss Expectancy (ALE) of particular threats if mitigation methods are not in place. In comparing ALE to the cost of mitigations, we're able to drive a comparison of ROI for various technologies.

"However, ALE is hard to quantify when PE is involved since some of the losses are not straight outages to commerce but centre on reputation and opportunities in the marketplace. In these instances, relying on studies such as the CISA "Cost of a Cyber Incident" (October 26, 2020) can help align business sector and size to known incidents and create an average value of loss, per PE firm or portfolio company."

He underscores that across a PE firm and its portfolio companies, often a combination of the two is applied, with ALE being computed on disruptions to commerce and average losses on service industries. ■

Jason Elmer
Founder & CEO, Drawbridge

Jason Elmer has more than 20 years of experience within the financial services space, specifically in providing fintech solutions to the banking community, hedge funds, and private equity managers. Jason has worked closely with clients across a variety of areas of their businesses, including establishing cybersecurity and operations infrastructures; completing risk assessments; selecting appropriate service providers; performing vendor due diligence reviews; and preparing for and dealing with regulatory examinations and operational due diligence reviews.



Award-winning IT partner to the global private equity sector

World-class technology services for private equity

- MANAGED CYBERSECURITY AND COMPLIANCE
- CLOUD SERVICES
- WORKSPACE AND COLLABORATION SOLUTIONS
- 24/7/365 IT SERVICES AND SUPPORT
- MANAGED DATA SERVICES
- DUE DILIGENCE SUPPORT
- BUSINESS CONTINUITY PRACTICE

Whether you're operating locally, nationally, or internationally, RFA is your global technology partner

www.rfa.com
gralph@rfa.com

RFA The Trusted Technology Partner

9 global locations
US | EU | APAC

DRAWBRIDGE

Drawbridge is a premier provider of cybersecurity software and solutions and a trusted partner to more than 400 funds in the alternative investment industry. Our technology platform empowers firms to build customised cyber programs that proactively manage vulnerabilities, simplify risk management and grow with their business. Our clients benefit from a centrally managed security programme, improved risk profile, compliance with regulatory body requirements, and with raising institutional capital.

www.drawbridgepartnersllc.com

Contact: Jason Elmer | info@drawbridgeco.com | +1 203 569 6400

EZE CASTLE INTEGRATION

Eze Castle Integration is a trusted technology partner to the private equity sector, globally.

With over two decades of experience and 800 clients around the globe, we deliver complete cloud solutions, premier IT services, cybersecurity protections and digital transformation solutions encased in award-winning client service and around the clock IT support.

www.eci.com

Contact: Amisha Shah | ashah@eci.com | +44 (0)20 7071 6833

RFA

RFA is a unique IT, financial cloud and cybersecurity provider to the financial services and alternative investment sectors, redefining the future of technology support and managed services. Through R&D, DevOps, automation and machine-learning enabled tools, RFA provides clients with customised and automated workflows, data management services, operational risk management and strategic technology advice and guidance. RFA has been serving its alternative investment client base for over 30 years and now works with over 800 clients across 9 global locations.

Our 24/7 managed Network Operations Centre monitors and protects clients' data and systems using the latest AI and machine learning capabilities, giving clients peace of mind. Fully integrating with all public cloud providers, RFA's on demand, scalable SaaS model creates bespoke working solutions around infrastructure, collaboration, cybersecurity and business process solutions for clients worldwide.

www.rfa.com

Contact: sales@rfa.com | +44 (0)20 7093 5000

