CHECKLIST

Private Equity Cyber Risk

Cybersecurity plays a pivotal role in extracting and protecting equity in investments. In a recent survey, only 36% of firms felt that they had adequate time and resources to assess the cyber risk of an investment property, and not surprisingly, 65% of those firms expressed buyer's remorse due to cybersecurity issues.[1]

Cyber risks have demonstrated the ability to impact deal value and execution. The most obvious incidents include:

- Potash Corp. of Saskatchewan Inc. defending a $40-billion hostile takeover attempt from Australian mining giant BHP Billiton Ltd. Hackers infiltrated several Bay Street law firms representing both companies, leading to public exposure of the deal. The Canadian Federal government blocked the takeover in the wake of negative public opinion.[2]
- Marriott hotel chain was fined 18.4M GBP in the wake of the 2016 massive data breach of Starwood Hotels.[3]
- The $4B purchase of Yahoo by Verizon was discounted $350M after the massive Yahoo hack of customer data.[4]

Even perceived risk, foreign ownership or bipartisan ideological association can impact deal value. For example, TikTok was the focus of US government interest given its foreign ownership by China.

Portfolio Companies Are Easy Targets

Cybersecurity breaches and threats are pervasive concerns for any entity storing valuable data or managing large sums of money. Private investment funds are no exception. Attackers recognize that portfolio companies are growth-focused and are often secured with lean, less mature cyber operations. Private equity firms also have detailed disclosure requirements to abide by, making it easy for attackers to find these valuable targets.

Sophisticated attackers perform complex reconnaissance on private equity firms and their portfolio companies in order to obtain stolen/hijacked/poorly secured firm documents and harvest key employee credentials. They understand operational details, the names of key employees, and once they are embedded, they can hijack relationships, intercept emails, and even initiate wire transfers to steal millions of dollars.

Breaches can and will impact deal execution, deal value, integration, and put reputations and future deals at risk. In fact, the public nature of private equity work paints a target on both the buyer and seller.

[1] https://techcrunch.com/2020/09/10/its-time-to-better-identify-the-cost-of-cybersecurity-risks-in-ma-deals/
[2] https://financialpost.com/technology/chinese-hackers-went-after-aborted-potash-deal-report
[3] https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/?sh=2422b92ae4b0
[4] https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html#:~:text=Verizon%20will%20pay%20%244.48%20billion,that%20were%20disclosed%20last%20year

Where Every PE Should Start: The 30/60/90-Day Cyber Risk Checklist

CIOs at private equity firms are hampered by limited visibility into and the inconsistency of the overall security operations across their portfolio companies. eSentire has put together a comprehensive Private Equity Cyber Risk Checklist to narrow your focus on what is most important to consider as you look to mature your firm's overall cyber ecosystem. At a minimum, private equity leaders should conduct the following assessments and require standardization across their portfolio companies:

30-Day Cyber Risk Requirements

- Enforce proper (NIST 800-53B) password policies
- Deploy and enforce multi-factor authentication (MFA)
- Use a Virtual Private Network (VPN) to secure remote connections
- Disable administrative privileges for employees who do not require it
- Update and patch corporate systems and employee devices Conduct employee security awareness training including phishing campaigns
- Test back-up systems and services to ensure recovery of critical systems
- Inventory privileged, confidential or protected information (financial, PII, PCI, PHI, etc)
- Collect records of any material security events, policy violations, incidents, or data breaches
- Collect documented insurance policies related to cybersecurity

60-Day Cyber Risk Requirements

- Map protected data to Federal regulations (HIPAA, GLBA), state privacy and breach disclosure, privacy regulations (GDPR, CCPA), and industry-specific regulations
- Review supplier contracts for security requirements, notification guidelines, and indemnification clauses
- Conduct a risk assessment
- Conduct a penetration test and document all vulnerabilitiesDocument and inventory (including versions and patch levels) operating systems, file structure and network mapping, endpoints (MAC address and OS), cloud infrastructure, and list of users, groups with privileges and access rights
- Deploy Mobile device management (MDM), endpoint prevention or next-generation antivirus (NGAV) and endpoint detection and response (EDR)

90-Day Cyber Risk Requirements

- Document a corporate risk profile and complete a prioritized risk registry based on findings from the risk and vulnerability assessments
- Review and approve updated security programs and plans with appointed and qualified security leader (CISO/CSO) based on gap analysis of plans and vulnerability assessments
- Establish a regular cadence of annual penetration testing, review of risk assessments, and completion of risk registry action items
- Execute cyber insurance policy with specific coverage for business email compromise (BEC), ransomware (including extortion payments), and recovery costs
- Deploy continuous monitoring for unauthorized access including security monitoring and logging, proactive threat response, and incident response capabilities
- Access and document application testing, update procedures and verification policies
- Document policies to assess supply chain risk, vendor evaluations, and contracting requirements including service descriptions, division of duties, security event notification requirements, and indemnification in the event of security incident
- Run an incident response (IR) simulation (fire drill), assess response performance, and update IR program as required
- Document and implement a program to sanitize and destroy media containing confidential or proprietary information

How eSentire Can Help

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1500+ customers, across 80+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes. While many companies focus on detection, we recognize that there is no end to cyber risk. Preventative technologies will be bypassed and defenses will fail. That's why eSentire prioritizes Response. Our MDR is really MDR^3 - Response, Remediation and Results.

We proudly protect over 100 Private Equity firms and their portfolio companies. We would welcome the opportunity to outline how we can help defend your firm, and develop a custom security offering for your entire portfolio to subscribe to across our Managed Risk, Managed Detection and Response, and Incident Response services.

Reach out to learn more.

Get Started

If you're experiencing a security incident or breach contact us  **1-866-579-2200**

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.