BDO CYBERSECURITY SPOTLIGHT

Fall 2020 Report

SPECIAL FOCUS: PRIVATE EQUITY (PE) INDUSTRY

BDO DIGITAL

In this issue

Preface

BDO Digital is proud to introduce our second edition of our new quarterly publication entitled "Cybersecurity Spotlight." Each quarter BDO will research, write, and publish a new edition focused on a specific industry/business group. This second-edition is focused on cybersecurity services for the private equity (PE) industry. This edition focuses on boosting the resilience of private equity firms and their portfolio companies and rethinking their cyber security strategy.

At BDO, we have a robust PE industry team, which is dedicated to serving the needs of private equity firms and portfolio companies globally. Within BDO's PE practice are specialized teams providing a comprehensive suite of advisory services, tax, audit, valuation, mergers and acquisitions (M&A), and a vast array of BDO Digital services, including: information technology, digital transformation, data analytics, data privacy, and cybersecurity.

BDO has over 2,500 information technology and cybersecurity professionals available to support clients in both the public and private sectors worldwide. BDO cybersecurity advisory services teams are currently located in 35 countries on six continents and provides a comprehensive portfolio of advisory and managed security services to all industries.

In this issue, we focus on understanding the unique aspects of private equity firms, potential cyber-threat actors, typical cyber-threat vectors, different types of cyber-attacks, specific M&A cybersecurity challenges, and best practices before, during, and after a deal is done. We will also discuss how to successfully implement a threat-based cybersecurity program for PE firms in order to create a customized, resilient cyber defense. Each PE firm has unique business risk issues, regulatory compliance matters, budget, and schedule requirements to support the evolving needs of the shareholders and their portfolio companies.

This report is based upon BDO's extensive experience providing cybersecurity advisory and managed security services to PE firms worldwide. We hope you will find this report both interesting and valuable.

Respectfully,

RIC OPAL
Principal

The World We Live in – Rethinking Cybersecurity & Embedding Resilience

Globally there has been a sharp rise in cyber-attacks since the Chinese government disclosed the spread of COVID-19 within China and internationally. Especially, cyber-attacks focused on healthcare providers using spear-phishing and ransomware, cyber-attacks on ATMs and point of sales (POS) systems, impersonation attacks combined with business email compromise (BEC) targeting financial systems, supply-chain cyber-attacks focused on manufacturing operations and food distribution, and distributed denial of service (DDoS) cyber-attacks on the energy, hospitality, and travel industries.

With the spread of COVID-19 worldwide, every country has seen unprecedented demands for increased internet services, cloud-based services, and information technology (IT) support services occurring across nearly all industries. Globally employees and others are being asked or required to work remotely from their homes to reduce the spread of the virus and keep businesses running. As a result, nation-state and criminal cyber-attack groups are taking maximum advantage to target cyber vulnerabilities in selected industries, especially those most impacted by the current crisis.

As companies are now returning to work and adapting to the new normal there is a great demand for both public sector economic stimulus and private equity investments to facilitate a rapid growth of our national and global economy. The PE industry is being called upon to help rescue financially distressed companies.

In the world of private equity, it is vital for the buyer in the M&A process to ensure they fully understand: the value of the information assets they possess, the value of the digital assets they are looking to purchase, and the level of cyber threats and vulnerabilities facing the company they are considering acquiring. Further, the buyer must be able to determine the potential financial impact of both their company's cybersecurity preparedness and that of the company they are looking to purchase or lack thereof upon the deal price.

Likewise, it is imperative for the seller in the M&A process to take appropriate actions to reduce their organization's probability of a cyber data breach and the potential negative impacts post-breach, in order to optimize their sale price while ensuring a strong cyber defense. According to IBM Security's latest findings the average cost of a cyber data breach is now $8.2 million.

PE Firms are Target Rich Zones for Cyber-Attacks

It is important to know that PE firms come in all shapes, sizes, and level of services depending upon the unique requirements of their shareholders and their investment portfolio of companies. PE firms are considered by cyber-attack groups as target rich zones. Why? Simply said, because PE firms manage very large amounts of money, usually have minimal to modest cybersecurity, and it is not likely that PE firms will report actual cyber-attacks, in an effort to protect their firm's reputation and pending company acquisitions or mergers.

Most PE firms outsource their information technology (IT) services to either local small IT firms or large professional services companies. As a result, the level of cybersecurity expertise available to most PE firms tends to vary from very little and cheap to a lot but very expensive. Increasingly, cyber criminals have turned their focus on PE firms and their respective portfolio companies, as they see a significant opportunity to steal a great deal of valuable information and money while facing a minimal amount of cybersecurity measures to overcome.

Case Study – A Rock & A Hard Place

Situation: A sportswear distribution company owned by a NYC PE Firm is victim of a cyber ransomware attack in the Fall of 2019. The firm and their PE owners receive a demand for over $3 million in crypto-currency payment within 24 hours. The Russian cyber-criminal group threatens to destroy most of the sportswear distribution company operational data, valuable intellectual property, and release/sell compromised personal identifiable information of all of the company's employees and key members of the PE firm.

Resolution: The sportswear distribution company executives and their PE owners talked with their attorneys, insurance company partners, and consultants, and decided to negotiate the ransom demand and settle with the cyber-attackers for a 50% reduction in payment of $1.5 million. The company received a decryption key and was back working in two days after the attack. The insurance company agreed to reimburse the company for most of the cyber ransom payment per their cyber liability insurance policy requirements.

The Rise of Cyber Threat Actors Targeting PE Firms & Their Portfolio Companies

Unfortunately, PE firms are increasingly becoming victims of cyber-attacks from three distinct groups of cyber threat actors:

- **Nation-State Cyber-Attack Groups:** Most cyber-attacks originate from four (4) nations: China, Russia, Iran, and North Korea. The extent of cyber-attacks on PE firms from nation-states often depend upon the amount of wealth and profile of the major investors, including their political, industry, economic, social influence, and connections. Cyber-attacks are often focused on blackmail, espionage, or theft of valuable and/or sensitive information, contacts/connections, and financial assets. Often nation-states funded or sponsored criminal cyber-attack groups, are provided with resources, facilities, and/or hacking technologies and tools to perform the targeted cyber-attacks for an agreed fee.
- **Organized-Criminal Cyber-Attack Groups:** Typically, criminal cyber-attack groups are seeking to steal PE firms' wealthy owners' personal and sensitive information and then monetize the stolen information via transactions on the dark web, including:
  - Personal Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Payment Card Information (PCI)
  - Intellectual Property (IP)
- **Hacktavists Cyber-Attacks Groups:** Groups of hackers are formed based upon a shared political, economic, religious, or social agenda. Often these cyber-attack groups seek to negatively impact influential and wealthy family members seeking money or promotion of their issues/agenda on social media or national press coverage to advance their messages.

According to recent FBI reports, the three above stated cyber-attack groups are often working in a coordinated, sponsored, or integrated manner to facilitate larger and more complex national or multi-national cyber-attacks. Since, many PE owners manage property and other financial assets in numerous countries they are increasingly targeted by a combination of these cyber-attack groups.

CYBER DATA BREACH – 7 QUICK TIPS:

Immediate Actions:


Assess the situation and gather information


Implement the incident response plan with senior executives, legal, and IT


Contain the breach


Eradicate the malware


Communicate with all necessary parties


Notify authorities and law enforcement as needed


Recover data and restore operations

Growth of Email-Based Cyber-Attacks on PE Firms & Their Portfolio Companies

Based upon BDO research and extensive field-experience, most successful cyber-attacks on PE firms and their portfolio companies have used email as the preferred threat vector, including:

Socially-Engineered Spear-Phishing Cyber-Attacks
Designed to gather personal information, gain computer access, and control of sensitive PE firms' shareholder information

Business Email Compromise (BEC) & Impersonation Attacks
Aim to redirect financial payments, charitable contributions, or investments

Emails Containing Malicious Web Links or Attachments
Intended to launch malware or spyware on your computer or other devices to steal valuable information

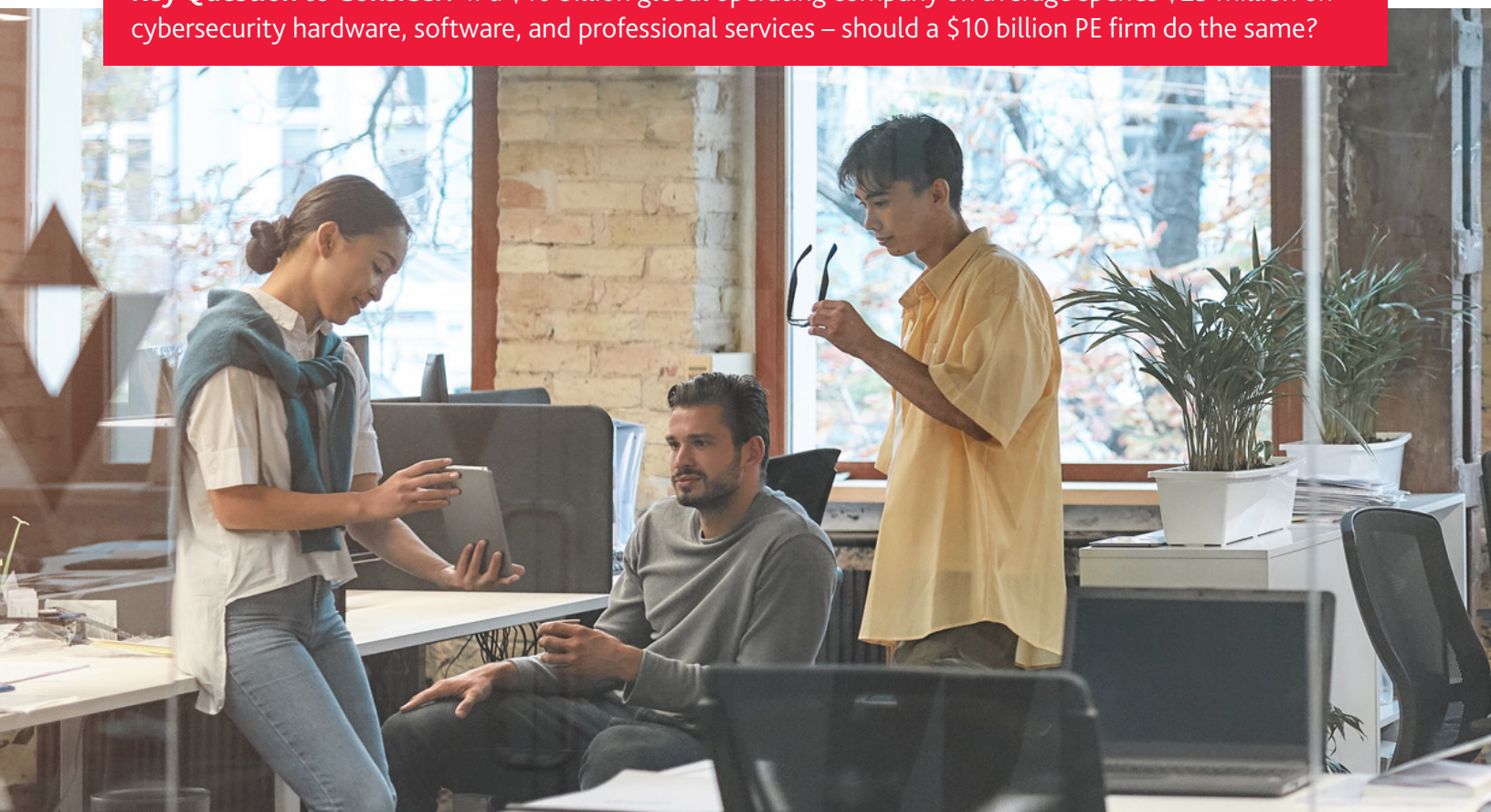
Ransomware Cyber-Attacks
Designed to encrypt information and extort payment via a demand for crypto-currency such as Bitcoins

PE Firm: Top 12 Cybersecurity Challenges

PE firms typically experience numerous cybersecurity challenges, including:

1. Minimal cybersecurity education and training of employees
2. Lack of information technology (IT), data privacy, and cybersecurity strategic plan
3. No dedicated Chief Information Security Officer (CISO) to lead cybersecurity strategic planning
4. Lack of a cyber incident response (IR) program, IR communications plan, and periodic IR testing
5. Inadequate cyber intrusion monitoring and detection system for the email, network, and all endpoints
6. Insufficient computer vulnerability scanning to identify malware
7. Lack of regular independent penetration testing of firewalls, anti-virus, and anti-malware software
8. Inadequate or non-existent business continuity plan (BCP) or back-up plan for the information systems
9. Failure to meet state or industry-specific data privacy and cybersecurity regulatory compliance requirements
10. Insufficient identity, credentials, and access management information security controls
11. Inadequate mobile phone communications security, especially for senior executives traveling internationally on either business or pleasure
12. Under investment in information technology, automation, and cybersecurity to enable business growth, ensure data integrity, and protect data privacy

Key Question to Consider: If a $10 billion global operating company on average spends $25 million on cybersecurity hardware, software, and professional services – should a $10 billion PE firm do the same?

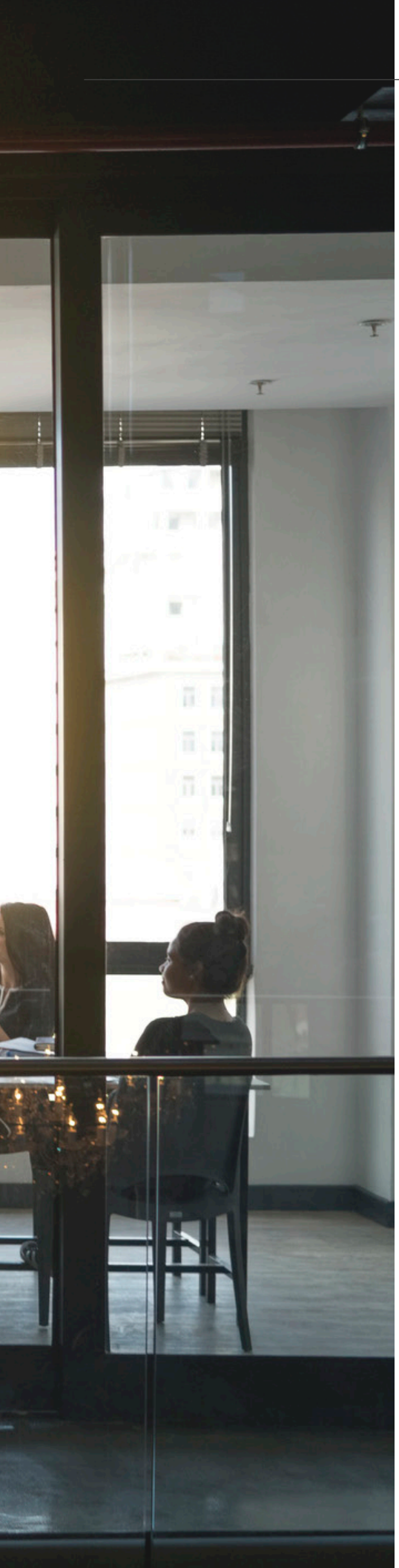


Implementing Threat-Based Cybersecurity for PE Firms

In the face of ever-expanding cyber threats and increasingly sophisticated cyber-attackers, PE firms should protect themselves and their portfolio of companies by implementing a threat-based cybersecurity program. Developing a threat-based cybersecurity program begins by conducting specific cyber diagnostic tests/assessments to gain an understanding of the actual cyber threats the organization is currently encountering. It is vital for the PE firms to know:

- Who are the cyber-threat actors attacking the PE firms and their portfolio companies?
- Which cyber-threat vectors are most commonly used?
- What types of cyber-attacks should the PE firms and their portfolio companies be prepared to defend against: tactics, techniques, and procedures (TTPs)?
- What are the PE firms and their portfolio companies' information system vulnerabilities to cyber-attacks?
- What are the PE firms and their portfolio companies' email system and network endpoints vulnerabilities to cyber-attacks?
- How susceptible are PE firms' employees to potential cyber-attacks?

Once the PE firms' executives and owners gain a clear understanding of the answers to the above stated questions, then it can begin to design a customized cyber defense program to protect the organization's data. With increased investment and adoption of new technologies (cloud computing, advanced data analytics, artificial intelligence [AI] powered devices, and more) threat-based cybersecurity can serve as an essential element of success for PR firms by providing real data privacy and information security.



PE - Cybersecurity Recommendations: Before, During & After the Deal

To reduce both the probability of a cyber-attacks or a significant data breach and mitigate the negative financial and reputational impacts, we offer the following cybersecurity recommendations for buyers and sellers engaged in the M&A process.

Before the Deal – Letter of Intent (LOI)

Buyers should engage an independent cybersecurity firm to take the following proactive actions regarding their acquisition target company:

- Conduct a dark web analysis for the company, key personnel, and selected supply chain partners
- Conduct a social media analysis on the company and key personnel
- Conduct an extensive internet search of the company and key personnel

All actions taken should be focused on identifying potential negative or damaging information, which could lead to cyber vulnerabilities including: ransom, malware penetration, ransomware attacks, spear-phishing attacks, business email compromise (BEC) attacks, and other cyber- attacks.

During the Deal (Due Diligence) – In 30 Days or Less

Buyers should engage an independent cybersecurity firm to conduct the following actions on the acquisition target company to assess their level of cybersecurity maturity and actual cyber defense in 30 days or less, including:

- Review the company's information security – policies, plans, and procedures, including: incident response plan, business continuity plan, and disaster recovery plan
- Evaluate the company's cybersecurity leadership, resources, and cyber education and training program
- Conduct company internal computer/mobile device vulnerability scanning
- Conduct company external penetration testing – to assess the strength and vulnerabilities of firewalls and network endpoints
- Assess the information technology infrastructure – people, processes, and technology
- Conduct a cyber liability insurance coverage adequacy assessment

After the Deal is Done (Post-Transaction)

Buyers should ensure the following top three actions are performed either internally or outsourced to a qualified managed security services provider (MSSP):

1. **Conduct advanced cyber diagnostic assessments, on a regular basis, including:**
   - Email cyber-attack assessments
   - Network and endpoint cyber-attack assessments
   - Computer and mobile devices vulnerability scanning assessments
   - Penetration testing
   - Spear-phishing campaigns
2. **Establish a rapid cyber-attack incident response plan** - Develop and periodically test an enterprise-wide, well-coordinated information system incident response plan to quickly identify, contain, eradicate, and recover from cyber-attacks.
3. **Implement 24 x 7 x 365 monitoring, detection & response (MDR)** – It is essential to continually monitor, detect, and respond to all cyber incidents including: email system, network, software applications, and all information system endpoints using advanced security information event management (SIEM) software, data visualization tools, automation, and artificial intelligence (AI) capabilities.

Cybersecurity Recommendations for Sellers Involved in the M&A Process

Sellers should ensure the following actions are taken before engaging in the M&A process, including:

- Cyber risk assessment
- Vulnerability assessment
- Penetration testing
- Cybersecurity education and training program
- Information security documented policies, plans, and procedures
- Multi-layer cyber defense with end-to-end software encryption and multi-factor authentication
- Continuous 24 x 7 x 365 cyber intrusion monitoring and detection
- Incident response plan and testing
- Business continuity plan and testing
- Disaster recovery plan and testing

Summary

The one area which many PE firms need additional expertise is cybersecurity. Increasingly, cyber-threat actors including: nation-state cyber-attack groups, organized criminal cyber-attacks groups, and hactivists are targeting PE firms which are considered by cyber-attackers as a "target-rich-zone." PE firms are rapidly realizing they can no longer fly-under the radar of hackers. Instead, PE firms need to enhance their digital transformation and data privacy via implementing a threat-based cybersecurity program.

BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

CYBER RISK ASSESSMENTS

- Risk assessments against multiple frameworks
- Cyber risk remediation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Network Operations Center (NOC)
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)
- Email & Network Attack Detection & Monitoring Services

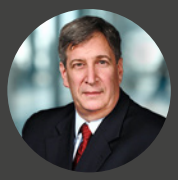
Cybersecurity Leadership Team

RIC OPAL
Principal
630-686-4302 / ropal@bdo.com

SCOTT HENDON
Managing Partner
Head of Global Private Equity
214-665-0750 / shendon@bdo.com

MICHAEL DOMBROWSKI
Managing Director
302-468-3774 / mdombrowski@bdo.com

TODD KINNEY
National Director
Business Development, Private Equity
212-885-7485 / tkinney@bdo.com



MICHAEL STIGLIANESE
Managing Director
212-817-1782 / mstiglianese@bdo.com

People who know Cybersecurity, know BDO Digital.