THE 2021 PRIVATE EQUITY GUIDE TO CYBERSECURITY:

NEW RISKS, RESPONSIBILITIES, AND REMEDIATION STRATEGIES

Performance Improvement Partners
an ERIE STREET company

For years, Private Equity firms and their portfolio companies have sensed the danger of cybercrime lurking under the surface. Yet, there remains a wide range of risk tolerance, often determined by those who have suffered significant loss after experiencing a breach, and those who have yet to deal with the experience. In the new reality of cybersecurity in 2020, cyber criminals are getting more sophisticated than ever.

The top tactics of today's cyber criminals include ransomware attacks and compromised credentials, leading to financial fraud as victims send hackers their hard-earned cash. In the end, **not only is precious working capital jeopardized, but Private Equity firms run the risk of their portfolio companies being shut down** for sustained periods – if not entirely.

The insights in this guide are designed to help Private Equity firms understand the critical risks and associated costs of a cyber incident, and **how to take action and stay secure** when navigating the technical and increasingly human-centered world of cybersecurity.

Private Equity Firms Face a New Normal in Managing Cyber Risks.

Given the staggering costs of a cyber incident, as well as the increased risks in 2020, research proves **one data breach is all it takes to derail an investment thesis** – and the threat is more real than ever. As detailed by the latest research, cyber investments deliver higher returns than expected.

Page 2

Tactics Taken by Cyber Criminals are Evolving Faster than Ever.

In light of COVID-19 and a remote workforce, the tactics criminals take are evolving faster than ever. **With the average middle-market firm facing up to 10,000 attacks per day,** initiating safety measures to thwart an attack before it becomes a breach is imperative.

Pages 3 - 4

From Big Brands to Government Agencies, No Company is Safe.

The Private Equity industry is hesitant to disclose breaches, **fearing the loss of investors and portfolio revenue due to negative publicity.** Despite the under-reporting, as proven by recent attacks on publicly traded companies, government agencies, and Fortune 500 companies, no organization of any size is immune.

Page 5

The Responsibility for Cyber Protection is a C-Suite and Board Matter.

Given the impact a cyber breach can have on the bottom line, there is no doubt cybersecurity is an issue that goes beyond the IT department. As backed by many cyber experts, **the responsibility for protection, as well as the reality of the repercussions, falls on the shoulders of all leadership,** including the CEO and Board of Directors.

Pages 6 - 7

Taking a Strategic Approach to Portfolio Protection.

Forward-thinking Private Equity professionals are securing their investments with the same strategic thinking utilized in portfolio planning and acquisitions. In addition to assessing existing cyber investments, such as cyber liability insurance, many PE firms are taking a portfolio-wide approach. Those who do **reap the benefits of increased efficiency and potential cost-savings,** as well as visibility into the security health of their portfolio.

Page 8

Mounting a Defense Requires Multiple Layers and Company-Wide Vigilance.

Knowing that prevention is vastly cheaper than remediation post-incident, firms are finding protection in two key areas. The first, technology, provides a minimum base-level of security. Yet, it is important to note: **People hold a place of power in guarding company data,** recognizing threats that computers alone cannot.

Pages 9 - 11

PRIVATE EQUITY FIRMS FACE A NEW NORMAL IN MANAGING CYBER RISKS

When a portfolio company falls victim to a breach, the Private Equity owner faces both direct and intangible costs. In addition to the impact on earnings, **money spent on post-incident mitigation has a negative impact on funds allocated to grow the business.** The effects are long-lasting: According to IBM, one-third of data breach costs are incurred more than a year after it occurs.

While cyber crime was already on the rise prior to COVID-19, a remote workforce, **combined with a pandemic that preys on fears and emotions on both a personal and professional level,** has opened endless doors for cyber criminals to pilfer company credentials and gain access to business systems. Pandemic-themed attacks are expected to remain a threat as long as the virus looms.

The Increased Risk of Cyber Crime

- 68% of business leaders believe **cyber risks to their companies are increasing.** (Source: World Economic Forum)
- **92% of U.S. businesses** have seen increased cyber attacks in the past 12 months. (Source: Carbon Black)
- 49% of businesses **expect to experience a data breach or cybersecurity incident** due to a remote workforce. (Source: Barracuda)
- The 2019 odds of experiencing a data breach within two years was 29.6% - **a 31% increase** compared to 2014. (Source: IBM)
- The **FBI has reported a 300% increase in cybercrime** since the outbreak of COVID-19. (Source: The Hill)

The Long-Term Costs Associated with a Data Breach

- Globally, the average cost of a data breach is $3.86 million. Within the United States, **the average cost increases to $8.64 million per breach.** (Source: IBM)
- 22% of the costs associated with a data breach occurred the second year after the incident, with another 11% of costs occurring over **two years after the breach.** (Source:IBM)
- The average **cost of a ransomware attack** on a business is **$133,000.** (Source: Malwarebytes)
- **87% of consumers will take their business elsewhere** if they don't trust the company is responsibly handling their data. (Source: PwC)
- In 2020, the average **cost of lost business** following a data breach is **$1.52 million.** (Source: IBM)

Cyber Threats Specific to the Financial Industry

- **52% of all cyber attacks** in March 2020 were finance-related. (Source: VMware)
- The average cost of a 2020 data breach for the financial industry is $5.85 million – **almost double the average.** (Source: IBM)
- Financial service firms were hit by cyberattacks **300 times more than other sectors.** (Boston Consulting Group)

The Financial Benefits of Planning for Prevention

- Companies with an incident response team and extensive testing of response plans **save an average of $2 million.** (Source: IBM)
- Working with a managed security services provider results in **cost mitigation of $78,054.** (Source: IBM)

Learn more about the costs of a data breach, and get the latest research and cybersecurity insights by bookmarking the Top Cybersecurity Statistics, updated regularly.

TACTICS TAKEN BY CYBER CRIMINALS ARE EVOLVING FASTER THAN EVER

Ninety-four percent of cyberattacks begin with social engineering schemes. Instead of attacking software, **social engineering manipulates individuals into freely handing over confidential and personal information,** such as usernames, passwords, and other company data. The sharing of this information opens the door for exploits to occur, putting employees and customers, as well as the company itself, at risk. These social engineering crimes are most often executed through phishing attacks, stealing login credentials, and domain squatting.

Ransomware attacks are also on the rise, up 365% between Q2 2018 and Q2 2019. Companies in the finance industry are perceived to have deep pockets, making them a target for the increasingly steep ransom fees. Even when paid, **there is no guarantee stolen data will be recovered.** Given the financial focus and high-value information held by the Private Equity industry, firms and their portfolio companies are subject to any of the following attacks.

TYPE OF ATTACK	DESCRIPTION
Phishing	Cyber criminals who execute phishing scams use email and deceptive websites to misrepresent themselves, appearing as a trusted organization. With 1 trillion phishing emails sent annually, this "spray and pray" approach remains effective. COVID-19 has resulted in a sharp 600% increase in this type of attack, as bad actors prey on needs and emotions related to the pandemic.
Spear phishing	Like phishing, spear phishing is the fraudulent practice of sending emails that look like they are from a trusted person or business, instructing the individual to do something they shouldn't. Unlike phishing, spear phishing is a highly targeted attack sent to specific individuals.
Whaling	Whaling attacks are highly targeted, highly customized, and can be very convincing. Following the same principles as spear phishing, these attacks use information gathered from social media platforms, business networking sites, background checks, publicly available records databases, and other sources. While spear phishing targets specific individuals, whaling takes it to the next level, focusing on the highest-ranking individuals within a company.
Vishing	Vishing is a form of voice solicitation, in which the perpetrators make phone calls and leave voicemails, falsely representing themselves as trusted companies. Victims of these calls are lured into handing over personal information, such as credit card numbers.
Domain squatting	Domain squatting occurs when a cyber criminal creates a domain name that is very similar to that of an existing business, then inserts themselves into digital conversations to hijack systems. In the age of COVID-19, employees must remain vigilant when seeking resources related to the pandemic and the government initiatives surrounding it.
Malware	Malware is malicious software that was created with the intent to cause harm, such as damaging systems and stealing data. Viruses and spyware are the two most common examples.
Ransomware	Ransomware is a specific type of malware that, when enabled, locks the victim's computer, device, or data, demanding a ransom fee to regain access. Even when ransom fees are paid, businesses are often left unable to recover all of the stolen data.
Network scans	When used ethically, a network scan helps uncover vulnerabilities that put a system at risk, with the goal of improving the network's security by finding and patching them. Unethical scans, which can lead to cyber incidents, are also used to find and exploit network vulnerabilities. In this case, a network scan is similar to a burglar looking to gain entry through an open door or window.

THE PATH FROM CYBER ATTACK TO CYBER BREACH

Cyber attacks against Private Equity firms occur on a daily basis. Whether or not those attacks turn into data breaches depends on the decisions made by employees after the attack occurs.

The Likelihood of Cyber Crimes Affecting the Average Middle-Market Private Equity Firm

TYPE OF EVENT		RATE OF OCCURRENCE
An attack occurs any time a cyber criminal attempts **to gain unauthorized access to a system, or alter, destroy, disable or steal your data.** The two most common types of attacks are network scans and phishing attacks.	**Attack**	Network scans occur up to 10,000 times per day, while phishing scams happen up to 50 times per day per employee. In a 500-employee firm, this has potential to reach a total of **25,000 phishing attacks per day.**
A cyber incident occurs with any violation of security policies, or any **event that threatens the security of your system or data.** Common examples include users clicking on a phishing link, providing login credentials to a third party, when malware is activated on a network, or suspicious emails – falsely claiming to come from the company – are sent.	**Incident**	The average firm suffers a minimum of **2-to-3 cyber incidents each month.**
Once an attack reaches exploit level, the cyber criminal has officially gained the ability to access the system. **They are now able to harvest the data of the company, employees, and clients.**	**Exploit**	The average firm experiences at least **1 exploit per year**, unless MFA is enabled on both remote access and email.
A breach occurs when the attacker logs into the company system and steals data. From there, **further escalation may include holding that data for a ransom or publishing it on the dark web,** where other cyber criminals can buy personal information.	**Breach**	It is predicted that an average of **1 in 4 middle market firms will fall victim to a cyber breach this year.**

FROM BIG BRANDS TO GOVERNMENT AGENCIES, NO ORGANIZATION IS SAFE

With a slew of highly publicized attacks and breaches, there is no doubting the reality of cyber crime in 2020. Big brands often make for the best headlines, proving enterprise companies and government agencies are far from immune.

Yet, with nearly half (43%) of cyber attacks targeted against SMBs, **Private Equity firms must require accountability across all portfolio companies.** Criminals strike against companies of every size, big and small, executing attacks on a mass scale. Due to this, hackers are not aware of the company's size until the attack is well underway – only then getting involved on a direct level.

ORGANIZATION	DATE OF ATTACK	THE ATTACK
World Health Organization (WHO)	**March 2020**	In an attempt to steal passwords of WHO agency staff, criminals built a fake site designed to portray the organization's internal email system.
Italian Social Security System	**April 2020**	Criminals attacked the Italian social security website and forced it to shut down when citizens began claims for their coronavirus payout. At the time of attack, the site was receiving 100 applications per second.
Three British Private Equity Firms	**April 2020**	In this phishing attack, three unnamed PE firms were tricked into wiring $1.3 million to cyber criminals. The Florentine Banker, a criminal hacker who targets senior executives and those in charge of money transactions, had access to the firms' systems and were monitoring its executives for months before the crime took place.
Microsoft	**May 2020**	Up to 50,000 Microsoft Teams users were targeted in two attacks. In one, employees were baited via email into sharing login credentials through a fake Microsoft Office login page. The second was a phishing scam specifically targeted at corporate executives.
DocuSign	**May 2020**	Up to 60,000 DocuSign users were sent a phishing email containing a link to a "COVID-19" document. After several redirects, a page mimicking DocuSign's login page appeared, which was designed to steal user credentials.
Magellan Health	**May 2020**	Criminals exfiltrated data from Magellan Health, a Fortune 500 Company, by impersonating a Magellan client in a social engineering phishing scheme. The data accessed included personal employee information, such as names, contact details, and W-2 or 1099 data, including Social Security numbers.
Avon UK	**May 2020**	A June cyber attack caused Avon to shut down its UK website for over a week. While not disclosed, experts believe ransomware is the most likely explanation: Victims of ransom attacks face a stigma in paying ransom fees, and fear disclosure will lead to future attacks.
Twitter	**July 2020**	Over 100 Twitter users were compromised, with 45 high profile accounts used to promote a cybersecurity scam which resulted in hackers receiving $120,000 worth of Bitcoin from 518 transactions. Attackers targeted Twitter employees "with access to internal systems and tools."

THE RESPONSIBILITY FOR CYBER PROTECTION IS A C-SUITE AND BOARD MATTER

Private Equity professionals are familiar with the high-stakes decision making required in the industry. Yet, when making decisions around cybersecurity, some fail to look past the short-term results of preserving cash flow.

Today's senior executives must recognize **they are only one bad day away from a cyber attack with potential to not only derail their career, but their entire business.**

Insights and predictions from these leading experts demonstrate why cybersecurity is a business risk that requires the highest level of support at the executive and board level.

The need for CFOs to invest in cyber:

"Far too often, organizations implement measures to prevent cyberattacks in response to a data breach. **A meticulous CFO can save the company the embarrassment and financial impact of a major breach** by taking proactive steps in anticipation of targeted attacks... organizations of all sizes are so dependent upon technology and cyberspace to transact business that c**ybersecurity is now one of those critical areas** requiring continued investment."

- Steve Durbin, Managing Director, Information Security Forum, via SmartBrief

Private Equity is a target for cyber crime:

"The private equity community as a whole is very concerned... The major banks have invested an extraordinary amount of money in hardware, software, and training. The private equity firms have not."

- Gregory Garrett, Head of Cybersecurity at BDO Digital, via Bloomberg Businessweek

Cyber is an issue for board members and senior leadership:

"This is a vulnerable time for the country, and it's certainly a time when bad actors will attempt to compromise or hack into your corporate systems. **Vigilance by Directors is extremely important during this unprecedented time."**

- Joan Conley, Senior Vice President and Corporate Secretary at Nasdaq, via Nasdaq

Cyber attacks are a matter of if, not when, for every company:

"At this crucial time, one successful data breach could be the final straw for many businesses, which are already facing an uphill battle against COVID-19. And, in the current threat landscape, **it's no longer a matter of 'if' a company's security will be tested by cyber criminals, it's a matter of 'when.'"**

- Fleming Shim Chief Technology Offer at Barracuda, via Barracuda

Companies need to prepare for a cyber pandemic:

"COVID-19 is not the only risk with the ability to quickly and exponentially disrupt the way we live. The crisis shows that the world is far more prone to disturbance by pandemics, cyberattacks or environmental tipping points than history indicates. Our 'new normal' isn't COVID-19 itself – it's COVID-like incidents. And **a cyber pandemic is probably as inevitable as a future disease pandemic. The time to start thinking about the response is – as always – yesterday."**

- Nicholas Davis and Algirde Pipikaite, World Economic Forum

A STRATEGIC APPROACH TO CYBERSECURITY

Sponsors grow earnings by executing a well-planned, strategic approach. Utilizing this thinking when implementing cybersecurity measures does more than protect portfolios: It ensures Private Equity firms will maximize the value of their investment and mitigate risk.

Understanding the Risks of Cyber Insurance

In reviewing an insurance policy, it is standard practice to identify gaps in coverage before purchase. When it comes to cyber liability insurance, the technical nature makes gaps tricky to discover. Many times, **they are not recognized until it is too late,** after the incident has already occurred.

Keeping up with the evolution of cyber crime is challenging for many insurance companies. If the method of attack didn't exist when a policy was purchased, it's unlikely to be covered should an attack occur. In addition, underwriters who create the policies don't always have in-depth technical knowledge on cyber crime.

Cyber liability insurance overall is still in its early stage. Similar to employee practice liability at its initial offering, there is a wide range in what is actually covered. **Add-on cyber policies are often "feel-good insurance" – a business feels good having it, until a claim is made, and they discover what is (or isn't) covered.**

It is imperative to understand the nuances in how an insurance policy is written. As Bert Wells and Jeff Kiburtz share in Risk Management Magazine: "A broad definition alone does not guarantee that coverage will be available for every incident affecting IT assets within that definition. **Rather, insurers may deploy a number of other provisions to limit coverage scope.** Accordingly, cyber policies must be read as a whole, with attention to how one part may affect another."

Prudent investors seek the guidance of a cyber expert to review their coverage and gauge the level of protection. In addition, policies can't be blindly renewed. Rather, they should be carefully reviewed every other year– at a minimum– to ensure protection amidst the rapidly evolving nature of cyber crime.

Setting Portfolio Wide Minimum Cybersecurity Standards

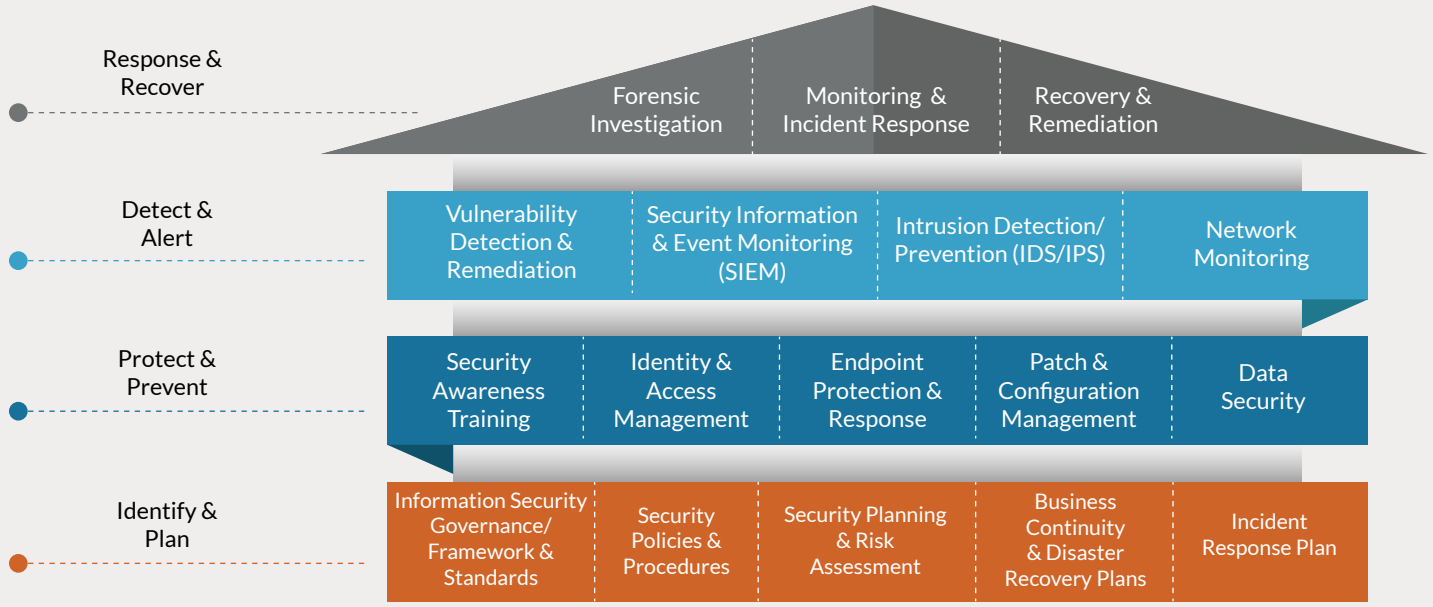
A portfolio-wide approach to cybersecurity enables firms to identify the common threats across their portfolio. This secures an action plan that aligns with the risk tolerance profile of the Private Equity firm, rather than individual CEOs or CIOs.

When establishing the policies and procedures involved with the action plan, investors are able to maximize efficiency regarding both time and spend. **Firms can develop an established minimum for all portfolio companies,** and should one fall short, have an immediate plan to remediate. Additional benefits include increased negotiating power and a comprehensive approach when working with one trusted provider.

PORTFOLIO PROTECTION REQUIRES A MULTI-LAYERED APPROACH

The best way to protect investments is by utilizing a multi-layered, holistic approach. Best-in-class security measures follow the Defense in Depth (DiD) approach, which is made up of four layers.

The Defense in Depth Approach to Cybersecurity



Identify and Plan

Similar to any business roadmap, **the foundation of the DiD approach is built through proper planning.** A key component of this includes creating cybersecurity policies and procedures for all company employees. Another building block requires assessing the company's current state of cybersecurity and identifying any gaps in protection. Developing an incident response plan with action items following an attack is also essential: According to IBM, **companies with an incident response team and extensive testing of response plans save over ~$2 million** compared to those with no response team or testing.

Proper set-up of these policies and procedures guides the development of a functional plan for business continuity, disaster recovery, and incident response.

Protect and Prevent

Elements of the DiD's second level, Protect and Prevent, include standard security measures, such as identity and access management and endpoint protection. Though often overlooked, **employee education is another vital element.** Vigilance by all personnel, in partnership with employee awareness training, **prevents a multitude of issues that could impact cash flow.** Other employee preventative measures include ensuring workstations are secure, as well as requiring the use of VPNs, multi-factor authentication, and anti-virus software.

Detect and Alert

While following cybersecurity best practices does mitigate risk, **there is no immunity when it comes to cyber attacks** - criminals are continually evolving their methods. **Cybersecurity is not "set and forget."** Regular system monitoring is required to build security momentum, detect attacks, and recognize vulnerabilities. Vulnerability scans should be conducted quarterly at a minimum, if not monthly.

Respond and Recover

Should a breach occur, the ability to respond quickly is essential. As stated by the Federal Trade Commission, **"The only thing worse than a data breach is multiple data breaches."**

Following a breach, some of the most urgent action items include securing systems, fixing vulnerabilities, and searching for exposed company data on the internet. Other activities may include sourcing cybersecurity professionals to negotiate with hackers to minimize losses, consulting legal counsel, and informing customers affected by the breach.

BUILDING A HUMAN FIREWALL

No business can succeed without a solid foundation to stand on when challenges arise. The same is true of the Defense in Depth approach to cybersecurity, particularly when it comes to the bottom two layers: Identify and Plan, then Protect and Prevent.

Without this basis, when incidents reach the top two levels – detecting and responding to incidents – companies will face too many issues to properly mitigate losses when a breach occurs.

It is estimated that 90% of data breaches are the result of human error, meaning training and **empowering all employees, at every level, is critical in building a secure cyber foundation** at each portfolio company.

90% of data breaches are the result of human error.

For Example: Every employee may have access to a VPN, but how certain are portfolio company CIOs that those VPNs are regularly being used?

Establishing the required use of cybersecurity technology, such as multi-factor authentication (MFA) and single sign-on (SSO) software, helps to mitigate the risk of human error.

Yet, even with these tools, one employee falling for one phishing email is all it takes to devastate a business.

Don't underestimate the importance of people in protecting your portfolio.

In the words of famous cryptographer Bruce Schneier, Fellow at the Berkman Center for Internet & Society at Harvard Law School, and a Program Fellow at the New America Foundation's Open Technology Institute, "Only amateurs attack machines; professionals target people."

Only amateurs attack machines; professionals target people.

– Bruce Schneier

PLANNING FOR PROTECTION

Due to the complicated nature of cybersecurity, there are a myriad of actions to take in the name of protection. **True protection requires a holistic view:** A strong cybersecurity foundation requires proper planning to build a shield first and foremost. Then, the protective and preventative measures that involve both technology and people reinforce the defense. Getting expert support enables companies to identify existing incidents before they escalate into breaches. By recognizing current vulnerabilities, the immediate action items needed to secure investments are made clear.

Increase Understanding with a Complimentary Private Equity Cybersecurity Workshop

Private Equity Firms are getting custom support for the cybersecurity needs of their firm and their portfolio in this complimentary cybersecurity workshop. **Uniquely tailored to help Private Equity firms mitigate risk** and maximize IT security posture, attendees walk away with:

- The most up-to-date cybersecurity **trends and tactics affecting investments,** including reg flags that can't be ignored.
- How the current risks relate to their portfolio, and **vulnerabilities distinct to the firm's investments.**
- The **baseline procedures** every portfolio company employee must follow to minimize threats.

A simple one-minute sign-up is the first step to securing investments before a breach occurs: Reserve a complimentary workshop now.

Train Employees on Cybersecurity Awareness

Building a human firewall around company data requires employee education and training. With **Employee Cybersecurity Awareness Training**, firms are building portfolios with employees empowered to make the daily decisions that protect investments. Awareness training provides personalized support in helping employees understand policies and procedures created specifically for each company. In addition to knowing how to spot often overlooked threats, employees learn the consequences negligent actions can have, and the role they play in protecting their company and co-workers. To ensure vigilance, **Simulated Cybersecurity Attacks** put employees to the test: Simulations ensure staff not only recognize an attack, but also take the proper action once threats are spotted.

Assess Cybersecurity Risk and Vulnerability

Investors are identifying immediate risks and determining the most cost-effective way to mitigate potential loss through cybersecurity assessments. A **Security Risk Assessment** identifies gaps in cyber governance, while a **Cybersecurity Vulnerability Assessment** gives an understanding of existing errors and weaknesses.

By conducting a vulnerability analysis of existing infrastructure, Performance Improvement Partners identifies the key short-term activities necessary for protection. Examples include verification that no security incidents are already in place, and identifying, then securing, any current exposure points which may result in security incidents.

Protect Your Investments Now

Secure your investments with guidance from the Performance Improvement Partners team of cybersecurity experts. Contact us today for boutique, pragmatic solutions tailored to suit the needs of your firm while driving portfolio value.

203-220-9556 performance@pip-llc.com pip-llc.com

Performance Improvement Partners, an Erie Street Company, is America's leading technology solutions company dealing exclusively within the private equity industry. Headquartered in Shelton, CT, with an infrastructure office in Stamford, CT, PIP offers a number of specialized practices geared to client needs and represents over 230 of America's most respected private equity firms, and has completed thousands of portfolio company engagements across B2B and consumer categories. For more information, please visit pip-llc.com.

ERIE STREET

A strategic and operational growth partner, Erie Street is a Chicago-based, independent advisory firm leveraging its operational heritage and entrepreneurial spirit to work with founders and management teams to achieve next-level growth. The firm brings corporate advisory, operational excellence, and go-to-market strategies to highly disrupted and changing business environments to mitigate risk, realize potential, and deliver exceptional value. Erie Street is led by Founder, Chairman and CEO Terry Graunke, a proven leader in the marketing services and digital communications industry. For more information, please visit eriestreet.com.

The insights on the implications of cybersecurity for Private Equity firms has been published by the following organizations:

- IBM: 2020 Cost of a Data Breach Report
- World Economic Forum: Why 2020 is a Turning Point for Cybersecurity
- VMWare: 2020 Cybersecurity Outlook Report
- Barracuda: Surge in Security Concerns Due to Remote Working During COVID-19 Crisis
- The Hill: FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic
- Malwarebytes: 2020 State of Malware Report
- PwC: How Consumers See Cybersecurity Privacy Risks and What to Do About it
- Deloitte: Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts
- Boston Consulting Group: For Wealth Managers, off Year Sparks Opportunity to Reignite Growth
- ESI Thought Lab: Benchmarking Cybersecurity Performance 2020
- CSO Online: More Targeted, Sophisticated and Costly: Why Ransomware Might be Your Biggest Threat
- CNBC: Cyberattacks Cost Small Companies $200,000, Putting Many out of Business
- Cyber Security Intelligence: 90% of Breaches are Caused by Human Error
- IBM: 2019 Cost of a Data Breach Report