Private equity

The rising cost of cyberattacks

accenture

About the authors

Paolo Dal Cin

Senior Managing Director, Accenture Security Lead

Paolo oversees the full spectrum of security services across the globe and is a member of Accenture's Global Management Committee. He brings over 20 years of deep experience to C-Level leadership across the largest organizations in the world. Paolo is a prolific author and is frequently invited to speak in the security community. He is based in Milan.

Ramnath Venkataraman

Senior Managing Director, CTO and Managed Services Lead, Private Equity

Ramnath has extensive experience working with clients in multiple industries across strategy, consulting, technology transformation and talent transformation. He has also successfully steered large-scale execution of technology programs that drive cost optimization whilst modernizing the technology landscape for clients. Ramnath is based in New Jersey.

Brian Crandall

Senior Managing Director, Private Equity

Brian focuses on helping private equity firms leverage digital and technology to unlock new growth and improve profits at each stage of the investment life cycle. Most recently, he was Senior Vice President at Platinum Equity, where as an operating partner he drove value creation across the flagship fund investments. Brian resides in San Francisco.

Bleuzenn Pech de Pluvinel

Managing Director, Private Equity Lead, Europe

Bleuzenn is specialized in large deals with a strong cross-border dimension, focusing on the whole deal lifecycle, from the strategic agenda including sourcing to long-term transformation and turnaround. She has demonstrated her ability to drive strategic value-based projects and deals and to deliver on operational topics on a long-term basis. Bleuzenn is based in Paris.

Martin Metz

Managing Director, Accenture Security

Martin is adamant about improving the security posture of private equity firms and their portfolio companies at scale. He brings experience in strategizing, implementing, and running security 24/7 across large portfolios of investments. He started in security 15 years ago and authored multiple security books and frameworks. Martin enjoys the sun of Phoenix.

Key takeaway

PE acquired assets possess a higher risk of cyber attack

01.

Attractive targets

Non-state actors are targeting the private equity industry explicitly.

68%

of our clients see an uptick in cyber incidents during the month of a deal closure, in some instances more than double the incident volume.

02.

Low maturity

Many portfolio companies lack the cyber maturity required to monitor, protect and respond to incidents.

$1M+

average ransom paid for mid-sized companies in addition to potential downstream impacts such as rising insurance costs or loss of customer trust.

03.

High probability

There are things investors can do better in the diligence process today.

1 in 2

attacks breach security at businesses that have not been cyber remediated.

04.

New models

Models are emerging to reduce exposure and deliver cybersecurity capabilities across the portfolio.

65%

reduction in costs per successful attack for firms prioritizing cybersecurity capabilities.

In the summer of 2019, an airplane parts manufacturer was in the process of getting acquired when its IT department received worrisome calls from areas of the business. What seemed to be a contained event spread quickly. Soon the company found itself held hostage; its servers locked by a ransomware group. The inevitable demand for payment arrived. Manufacturing sites in four countries ground to a halt. Hundreds of employees were out of work.

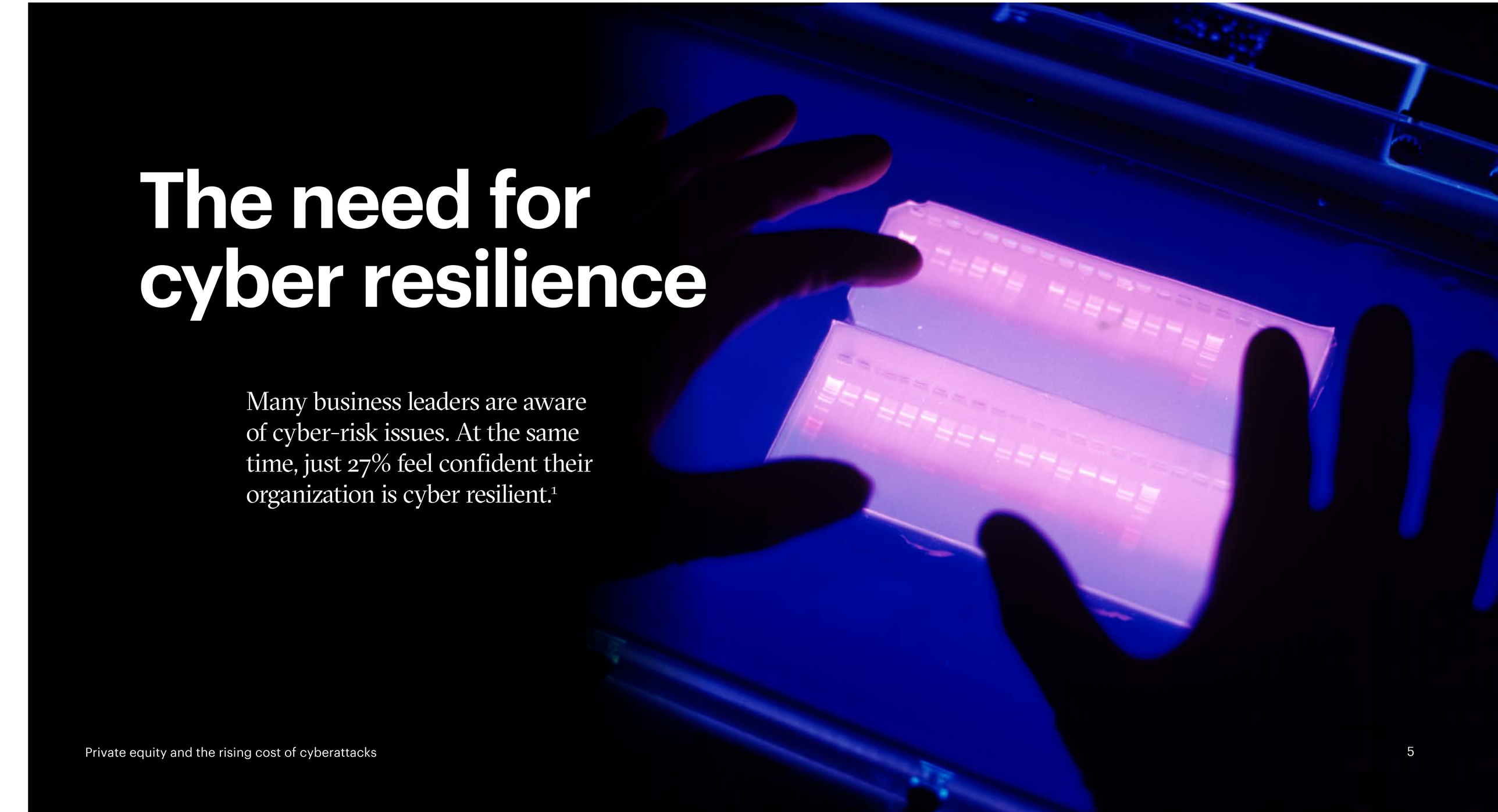
$150 million was lost,
the acquisition delayed by a year

Still, it got worse. The incident threw the asking price back by US$150 million and the full takeover was delayed to more than a year after the event.

What's interesting: The ransomware group's attack started by breaching the acquirer's network. From there, they burrowed into the IT system of the manufacturer. The attackers knew exactly what they were doing...

The need for cyber resilience

Many business leaders are aware of cyber-risk issues. At the same time, just 27% feel confident their organization is cyber resilient.[1]



Cyberattacks. They are attempts to steal, expose, or outright destroy information through unauthorized access to IT systems. And they are on the rise in every business sector.

In 2021 alone, the average number of incidents per company rose an alarming 31%.[2] Geopolitical instability, rapidly maturing and emerging technologies, and a lack of available talent compound the issue.[3]

Our Global Disruption Index shows that levels of disruption increased by 200% in the past five years, compared to only 4% from 2011 to 2016.[4] Cyber attackers are exploiting these rapid changes and companies need to adapt or face significant risk.

Companies face a 31% year-over-year increase in cyber incidents

The impact has hit in the boardroom. According to Accenture analysis of quarterly reports for 500 companies, there's a spike in legal, economic, and internal discussions around cybersecurity consequences.[5]

What are the nuances of cyberattacks for Private Equity (PE) firms and their portfolio companies?

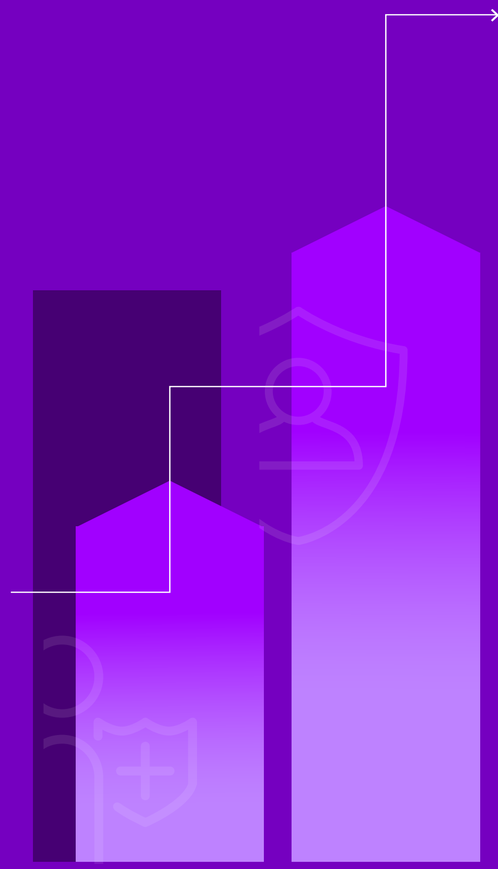
To uncover this, we analyzed open-source intelligence, searched dark web forums and marketplaces, and examined proprietary data for information on breaches.

Where deals are happening non-state actors see opportunity, targeting companies traded in the open market:

Announce to close:

68%

of clients see an uptick in cyber incidents during the month of a deal closure.



Post close:

Within the clients that see an uptick, the increase in incidents can spike as high as

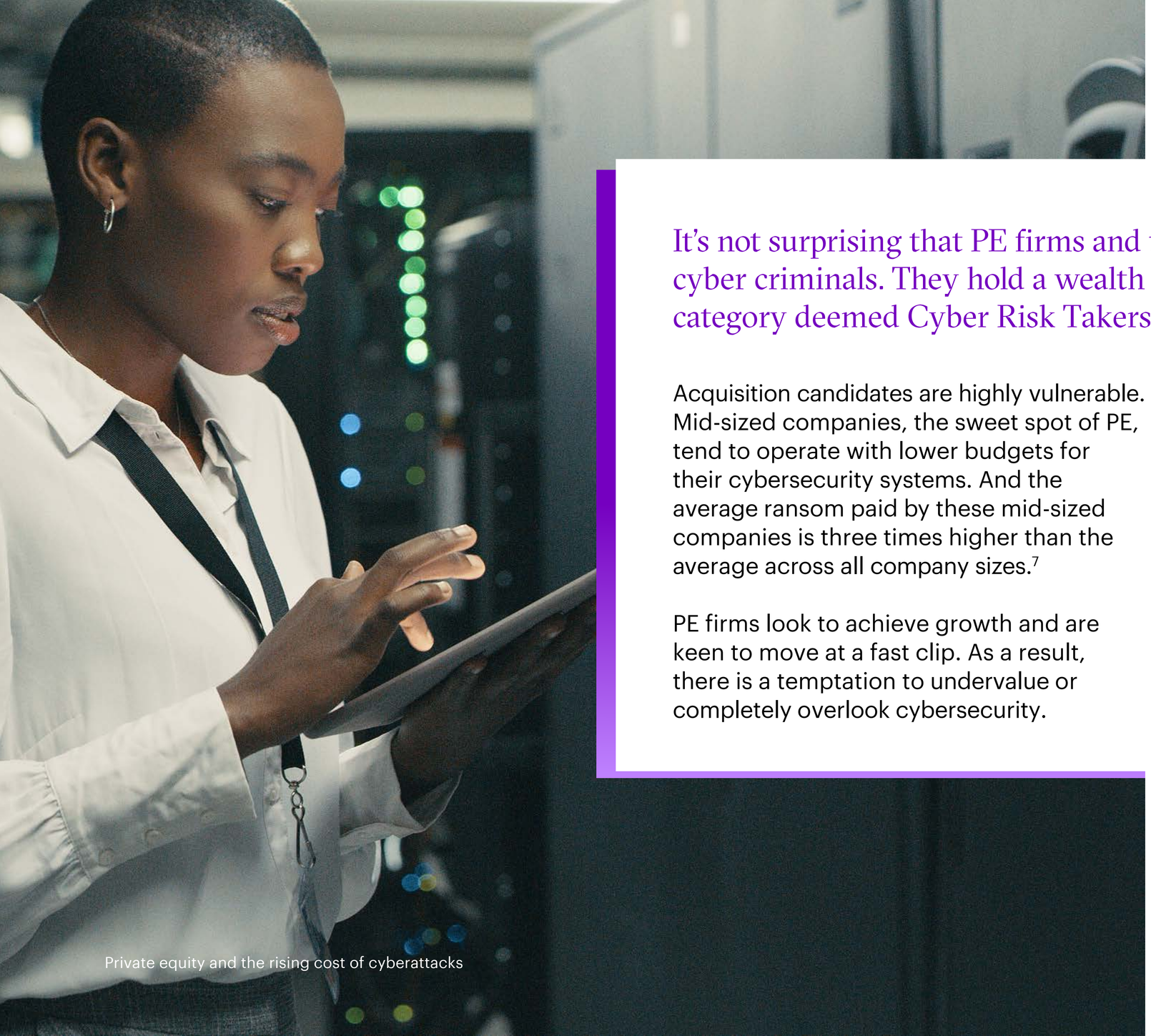
116%

The month after deal closure sees even higher incident numbers, suggesting that the acquired company—and the acquirer—face a period of increased cyber risk after a deal is struck.[6]

For frequent acquirers, like PE firms, addressing such risks proactively is a must.

Why private equity firms are prime targets

The announcement of a deal and the appeal of ready cash can attract cyber attackers the same way an open purse attracts pickpockets.



It's not surprising that PE firms and their portfolio companies are alluring to cyber criminals. They hold a wealth of sensitive information, may fall into a category deemed Cyber Risk Takers and are known to have capital on hand.

Acquisition candidates are highly vulnerable. Mid-sized companies, the sweet spot of PE, tend to operate with lower budgets for their cybersecurity systems. And the average ransom paid by these mid-sized companies is three times higher than the average across all company sizes.[7]

PE firms look to achieve growth and are keen to move at a fast clip. As a result, there is a temptation to undervalue or completely overlook cybersecurity.

This means most of these portfolio companies may fall into a category deemed "Cyber Risk Takers" in our research (see Figure 1). Their performance is among the poorest when it comes to security breaches and the share of attacks resulting in significant damage to the business (see Figure 2). By increasing their performance to Cyber Champion levels, Cyber Risk Takers could reduce costs per successful attack by 65%.[8]

Cyber Champions sustain 65% lower costs per successful attack

Figure 1: In our experience, PE firms and their portfolios companies tend to have lower cyber resilience and prioritize growth, which may put them in the area of Cyber Risk Takers.

Source: Accenture, The state of cybersecurity resilience 2021.

Figure 2: Easy moves and small investments can make a big difference in exposure—financial, operational and reputational. Cyber Champions stop more attacks and face less disruption.

	Cyber Risk Takers	Cyber Champions
Stop more attacks Number of attacks that breach security	1 in 2	1 in 6
Find breaches faster % breaches found in <1 day	11%	55%
Fix breaches faster % fixed in 15 days or less	30%	100%
Reduce breach impact % breaches with no impact	23%	72%

Source: Accenture, The state of cybersecurity resilience 2021.

For mid-sized companies, the average ransom paid is well over US$1 million.[9] Nearly half of these companies lack cyber insurance.[10] For those that do, insurance costs will likely go up after a claim.

With this price tag comes an array of consequences:

The reputations of both the portfolio company and the PE firm are at risk.

The acquired portfolio company's value creation can be sandbagged, not to mention the value of the overall holding enterprise.

To add insult to injury, once paid, threat actors could come back, targeting the PE firm itself or infiltrating other portfolio companies.

Recent examples of cyberattacks in private equity.

Hacking-for-hire threat group BellTroX targeted a PE firm's healthcare portfolio company, among many other organizations. The resulting data breach exposed the personal information of **60,000 patients and employees**.

Two PE firms learned of a data breach affecting their joint iOS and Android application that included **425 gigabytes of 500,000 legal and financial documents**. The threat actors reportedly accessed the data from an unsecured Amazon data storage bucket.

A threat actor in an underground forum sought to target a Canadian venture capital firm's customer relationship management software. The actor intended to obtain data on backers and portfolio companies, suggesting a **supply chain-motivated targeting against PE and venture capital entities**.[11]

Value through vigilance

There is a way for PE firms to mitigate the risk of cyberattacks—painlessly and without sacrificing speed.

Based on the experience serving 3,100 clients worldwide, we recommend five steps that can be taken to improve a portfolio company's cybersecurity capabilities before deals are inked. This helps firms prepare for the expected spike in incidents and build cyber resilience as part of a strong digital core.

01. Rethink the cyber model

Building internal capacity is neither fast nor necessarily useful. Instead, have someone else do the blocking and tackling.

- Create a 24/7 managed Security Operations Center service, forward your logs to a platform, and provide access to endpoint protection tools.
- Establish an incident response retainer with strong Service Level Agreements. In the event of a breach, every minute counts and help must arrive quickly to limit the impact.

02. Improve how you approach due diligence

Rather than conducting no security due diligence—or spending too much time—PEs can limit their due diligence efforts to a week, to then double down on high-impact areas that present themselves as remediation opportunities before deal announcement. Remediation is key, not interviews and one-time scans, of which the results can well be expected to reveal glaring gaps.

- Use an automated engine, limit the number of questions, and tie them back to inherent risk: What is actually needed? And what's a distraction?
- Track the progress against target maturity, leveraging the due diligence solution for a continuous improvement journey instead of one-time activity.

03.
Provide basic security hygiene

There are often quick wins that don't require significant interventions, yet raise the bar quickly when it comes to increasing the resilience of the portfolio company. For example:

- Set up multi-factor-authentication and protocols to help validate emails and reduce phishing and other potential threats.
- Communicate the increased danger of phishing and smishing attacks to employees that criminals could time with the M&A process. You could also run a phishing campaign into an existing O365 license.
- Add a subscription for the existing firewall, like URL filtering on your Palo Alto, to prevent users from clicking on a malicious website.

04.
Reduce your blast radius

Not everybody should have access to everything. A quick review followed by one-time remediation prevents overly open access.

- Take away "all-access". Fine-grained permission sets can be developed later. Cut the data sets into coarse chunks to limit the impact of a data breach.
- Reduce the number of domain admins to just those that need it.

05.
Ensure incident response readiness

Prepare for the worst with a tested plan to respond to an incident. The damage of an attack can oftentimes multiply because of misguided communication and uncoordinated action.

- Create an Incident Response Plan to establish the who, when and what surrounding an incident.
- Run a quick simulation with the leadership to put the plan in action and get everybody prepared for the worst-case scenario.

The PE firm can act as an agent of change and develop IT foundations that are secure by design, by providing structural cyber resilience guidance and solutions as part of the playbook.

As technologies continue to advance, cyber resilience is an ongoing journey. By setting up a dashboard, PE leaders have a consolidated view of cyber resilience across the portfolio at their fingertips.

Not all PE companies have a desire to take such a proactive approach. We are seeing three types of approaches with varying degrees of involvement, as outlined in Figure 3.

The low-touch security approach for PE firms is limited to covering security during due diligence, whereas PE firms with a high-touch security approach define and strongly recommend common security standards and establish a community of practice for information sharing across the portfolio.

Figure 3: We see PE firms apply three types of approaches with varying degrees of involvement.

		- PE firm involvement -		
Element	**Description**	**Low**	**Medium**	**High**
High-level security due diligence	Addresses security during the due diligence.	✓	✓	✓
Product security due diligence	Addresses the security of the main products (e.g., software-as-a-service solutions or applications) with a dedicated technical review.		✓	✓
Cyber financials	Supports the Portfolio Company with high-level financial advice as it pertains to cyber, such as salary-bands for internal staff or cyber insurance design.		✓	✓
Annual review	Runs a regular (often annual) review cycle for security to portfolio companies during the hold period.		✓	✓
Portfolio-wide standard / recommendations	Establishes standard of security measures to be expected across the portfolio, e.g., 24/7 security operations center, incident response retainer, or strong endpoint protection mechanisms.			✓
Portfolio-wide dashboard	Establishes dashboard to track security baseline and progress across its portfolio.			✓
Regular security-focused interaction with portfolio company IT or security teams	Regular sync up between an operations team representative and the security team of the portfolio company to align on security program needs, progress, and maturity.			✓
Community of practice	Establishes info sharing community among Chief Information Security Officers (CISOs) and security teams of the portfolio with dedicated workshops, webinars, or conferences.			✓

Client interview

Dror Karidi

Managing Director,
Portfolio Transformation Team,
Oaktree Capital Management

How important is cybersecurity in your decision-making process for an investment?

Cybersecurity is one of the key pillars to consider in all investment due diligence. In most cases, cybersecurity issues uncovered in the due diligence process can be improved during ownership.

When working with portfolio companies, we use a playbook developed with a dedicated partner and perform in-depth security reviews at each company, investing time and resources to identify target cybersecurity maturities commensurate with each organization's risk profile and its ability to sustainably operate under new guidelines. Part of our due diligence at the outset is determining the target operating model, what technologies the company uses, and the investment needed to achieve the desired outcome.

How well is cybersecurity represented in the board discussions for your portfolio companies?

Over the past two years, many firms have increased their focus on cybersecurity, developing coherent and consistent governance models that can be applied uniformly across the portfolio.

While the definition of cybersecurity is not always consistent at the board level, we create consistency at the strategy level and leverage shared knowledge to inform our decision making. Portfolio companies often have an appointed board member responsible for the organization's cybersecurity program. I expect to see cybersecurity receive more attention in the boardroom going forward in both the private and public sectors.

What should be the role of a private equity owner when it comes to enforcing security across a portfolio?

Our role is to give practical guidance to management and make fast operational improvements on opportunities that can create more resilience in a business. Asset managers often have the benefit of working across many portfolio companies, so may have developed best-in-class standards for cybersecurity and have expertise across various risk and size profiles.

Cybersecurity should be considered at every part of the investment cycle; this starts with due diligence, followed by fast remediation post-investment, continued engagement and strong governance at the board level.

Historically, many companies had small or nonexistent cybersecurity budgets, and the execution of a comprehensive security strategy in that environment was highly challenging. Today, companies have significantly more resources to tackle this risk, including leveraging experts and partners to create processes, problem solve, and support management teams.

Client interview

The good news

Cyber threats have raised the stakes for PE firms and their portfolio companies. Beyond any immediate costs, the reputations of everyone involved hang in the balance. That's the bad news.

The good news? Interventions can be catalyzed quickly and painlessly. And can be done before deals are closed—to prepare for a surge in cyberattacks, manage the risk and ensure speed to value.

Looking to improve cyber resilience for your portfolio while reducing your cybersecurity insurance expense?

Accenture ranks #1 in cybersecurity service providers, employing more than 16,000 professionals globally.

Contact us about how to mitigate risks and increase security with ease and at speed.

References

1. World Economic Forum, Global Cybersecurity Outlook, 2023.
2. Accenture, The state of cybersecurity resilience 2021.
3. World Economic Forum, Global Cybersecurity Outlook, 2023.
4. Accenture, Total Enterprise Reinvention, 2023.
5. Accenture Research analysis of 1,548 Securities Exchange Commission 10-K quarterly reports across 500 companies during 2017-2020.
6. Accenture, Private equity cyber threat intelligence research, 2022.
7. Coveware, Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021, February 3, 2022.
8. Accenture, The state of cybersecurity resilience 2021.
9. Coveware, Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021, February 3, 2022.
10. World Economic Forum, Global Cybersecurity Outlook, 2023. Of the companies surveyed between 251-1,000 employees, 46% indicated they currently do not have a cyber insurance policy.
11. Accenture, Private equity cyber threat intelligence research, 2022.

Contributors

Carl Baumgarten
Senior Manager, Security

Ben Socher
Manager, Private Equity

Jack Yule
Manager, Security

Join the conversation

www.linkedin.com/company/accenture
@Accenture

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 738,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

Visit us at www.accenture.com

About Accenture Strategy

Accenture Strategy works with boards, CEOs and C-suite executives to create 360° value for all stakeholders by defining and answering their most strategic business questions—including growth, profitability, technology-driven transformation, mergers and acquisitions (M&A), operating models and sustainability—with insights from AI and data science, combined with deep industry and function expertise.

Visit us at www.accenture.com/strategy

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.

Visit us at www.accenture.com/security

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity. For more information.

Visit us at www.accenture.com/research