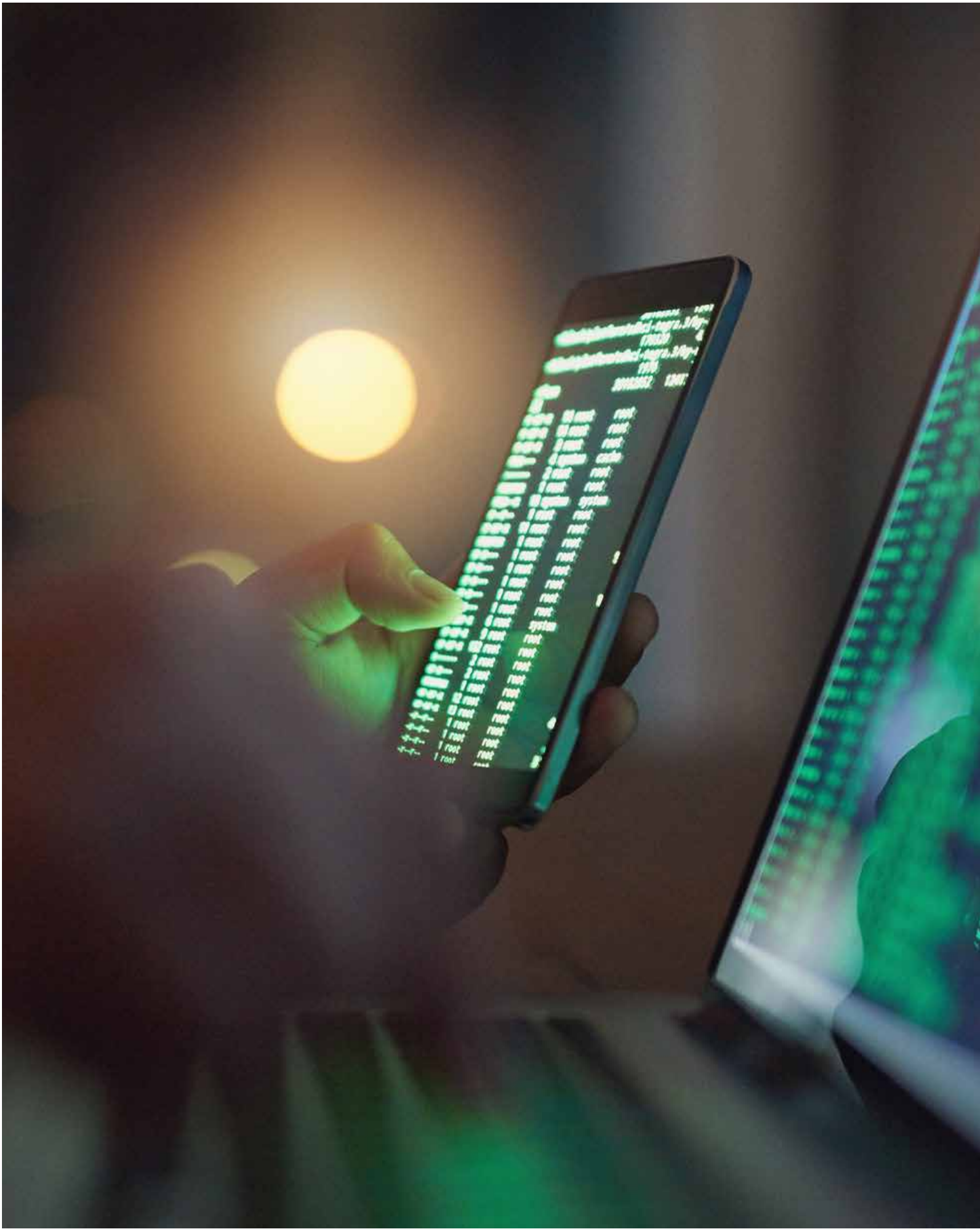
WHITE & CASE

Cybersecurity: At the crossroads of risk

Does private equity have the appropriate cybersecurity safeguards in its own operations and at the portfolio level?



Private equity in pole position

Cybersecurity is a rising threat to revenue and reputation. But as **Ian Bagshaw and Steve Chabinsky of global law firm White & Case** find, it also offers a new opportunity for the private equity industry for those able to master the risks

Cyberattacks have become one of the biggest threats not only to business but to society at large. Cybercriminals, hacktivists and nation states are capable of deploying malicious code to bring down everything from corporates to critical infrastructure in an instant.

As attacks grow more pervasive and sophisticated, investors have come to recognize the urgent need to ensure that assets are well protected and that cyber risk is managed effectively. This was thrown into sharp relief when the disclosure of two data breaches reportedly led to a US$350 million discount on Yahoo's US$4.8 billion asking price when the Internet firm was acquired by Verizon last year.

In private equity, the loss or gain of value is what determines a firm's success, and so understanding cyber risk has never been more important. This industry is also uniquely positioned because cybersecurity presents both a threat and an opportunity.

The very largest private capital firms are responsible for the management

of hundreds of billions of dollars across a range of asset classes and store sensitive client data and communications. If they were so unfortunate as to be the target of an attack, it could deter limited partners from making future commitments.

Arguably, of even more pressing concern is the defensibility of portfolio companies. Cyberattacks can ruin a business's reputation, cost it clients, customers and suppliers, and ultimately result in lost revenues and earnings.

A survey by Coller Capital found that private equity firms' limited partners are already thinking about this, with 55 percent of investors saying they will require their general partners to undertake cybersecurity risk assessments for their management companies, and 45 percent requiring the same assessments at the portfolio level.

Encouragingly, we are seeing private equity firms and other acquirers increasingly prioritize cybersecurity in due diligence processes, particularly where it intersects with data privacy issues. For instance, data porting, such as the transfer of credit card details from one company to another in retail M&A situations, is being thought about more judiciously than ever before.

Private equity funds are taking a risk-based approach and understand that boilerplate approaches to cyber risk are ineffective. Certain sectors—including healthcare, infrastructure, and transport and logistics—not only face greater disruption if they are attacked in ways that extend well beyond data loss, including the potential loss of business continuity and even the loss of life, but are exposed to higher reputational and value downside if they fall victim to breaches.

We understand that due diligence must go beyond law and regulations. Since often the only legal requirement is to have reasonable security under a risk management framework, the real diligence is in understanding the ways in which an individual company is exposed to cybersecurity risk in a practical, commercial, real-world sense.

Diligent acquirers price risk into their acquisitions. Just as private equity firms must understand the cyber risk profile of investment targets when they evaluate deals, they can also use hands-on management to improve cybersecurity governance at their investee companies, making them more saleable prior to exit. As the services of cybersecurity firms have become indispensable, we also see that private equity is taking a keen interest in this niche of the technology sector, its recurring revenue models and growth potential, representing a compelling source of investment returns.

As corporations and governments focus ever more attention on the scale of the cyber threat and their vulnerability, private equity is at once assessing its own exposure while spinning this threat into an opportunity.

"In private equity, the loss or gain of value is what determines a firm's success, and so understanding cyber risk has never been more important.

Cybersecurity startups offer investment opportunity

Sean Cunningham, a managing director at ForgePoint Capital, examines the growing investment interest in cybersecurity, from services to software products

> **“The consumerization of security is another area of opportunity for investors.**

Cybersecurity is no longer an afterthought. In the past it was considered a vertical market, but today it's needed across all business sectors, not just the technology industry. It has become a fundamental component of a company's infrastructure and therefore a mandatory investment for corporate enterprises, small and midsize businesses, as well as consumers.

There are really two drivers behind this growth: hackers with financial motivations and state-sponsored attackers. Couple that with the fact that every release of technology introduces vulnerabilities, whether it's a new application, or different modalities such as cloud security or bitcoin. There's no silver bullet; these security issues are not going to be solved easily and, consequently, we are having no issues finding good investments.

That said, there is a high volume of security companies out there. There's substantial duplication and a lot of private equity and institutional money funding these companies. In the last three years, we have seen an increase in private equity firms investing in later stages because they needed that shiny object in their portfolio to show limited partners before raising their next fund. This has created an environment that companies are raising larger rounds at higher valuations. If you look at the statistics, about 70 percent of all security exits are less than US$150 million. One of the biggest mistakes made by investors in cybersecurity is failing to understand the endgame of a company. It really is a specialist investment segment.

An area that we find interesting is the DevOps/SecurityOps space. ForgePoint Capital invested in a RASP (runtime application self-protection) company called Prevoty; Its software product enables developers to reduce time to market. The problem for many corporations is that they have hundreds of outward-facing applications that are ripe for hacking. When DevOps teams release or update an application, there are often unidentified bugs and security holes that are found after the application is pushed out live. Prevoty injects code into the DevOps cycle that looks for any potential vulnerabilities, allowing businesses to release their product faster because the security operations folks are comfortable that the threat will automatically be neutralized in case of an attack in production.

Artificial intelligence (AI) is also seeing growing interest in the cybersecurity space. This is a fundamental technology that we see underlying many security products,

such as malware inspections. One of our companies, Reversing Labs, uses AI to understand not just if a piece of code is good or bad but to proactively determine how hackers are developing the malware. When they see the remnants of a previous hack, they understand the methodology hackers are using, which helps identify incoming attacks, as opposed to anti-virus companies, which just look at specific malware signatures. The automation of security—the proactive analysis—is going to make AI critically important.

The consumerization of security is another area of opportunity for investors. If you look at the legacy-dominant security companies, the amount of their revenue coming from the consumer sector is phenomenal, with little innovation. Consumers are purchasing more sophisticated security software. Standard anti-virus packages are now commodity products. There is an opportunity to fund companies that build products that have traditionally been targeted at enterprises, now slimming them down for the consumer market. Physical security (home security systems), digital content protection, mobile security and Internet of Things (IoT) systems are in the market. The average home in the United States now has more than 25 devices with connectivity features, and it's very difficult to manage security on a case-by-case basis because these devices often don't talk to one another. The challenge is tying together all of these IoT technologies, as opposed to each device having its own security solution.

ForgePoint Capital has invested in Appthority, which scans applications on smartphones—all of which have been cleared by Google and the Apple stores—and tells you whether they are leaking data back to hackers, or if they are activating cameras and microphones. Appthority is an example of an application that is popular for family protection. This category, coupled with parental controls (digital health) and identity protection/breach remediation, will continue to be a high-adoption area with the continued growth of personal devices.

> **"Cybersecurity is now an extremely hot sector, so it's critical to understand the trajectory of technology.**

We continue to see huge potential in cybersecurity. However, it's now an extremely hot sector, so it's critical to understand the trajectory of technology and the security required to protect it, as well as how startups are implementing for these issues and what their endgame is. This will be the key to making successful returns.

Sean Cunningham is a managing director at ForgePoint Capital, a specialist cybersecurity venture capital fund. He spent 15 years at Intel Capital and has been cited as one of the top cybersecurity investors by market analyst firm CB Insights.

Due diligence: Cybersecurity at the portfolio level

Shawn Henry, president of CrowdStrike Services and the chief security officer of CrowdStrike, Inc., outlines the importance of strong cybersecurity governance at all points in the investment chain

> “It is now more important than ever for diligence processes to include a company’s cybersecurity awareness, processes and defenses.

No one would buy a property without first inspecting it—conducting a full survey before investing hundreds of thousands of dollars. The same is true in the private equity market. Financial due diligence is an established and expected component of every buyout transaction to provide assurance that the business has been accurately valued, is robust and is a viable investment.

It is now more important than ever for diligence processes to include a company’s cybersecurity awareness, processes and defenses over its information systems, products and services. Everything companies do today in support of their business is connected to their networks or their critical vendor’s networks, and the continuous data flow between them. Digital assets—from intellectual property to corporate strategies and customer data—are stored on networks persistently targeted by a broad spectrum of adversaries. Every desktop, laptop, smartphone, server and router is a potential entry point for a hacker, and there can be hundreds of thousands of endpoints in a single organization.

Many have already begun to take the issue of cyber protection seriously, and we often engage with law firms who understand that cybersecurity is a necessary part of the due diligence process. Some investors, however, still fail to recognize the scope of risk until they face a personal liability or suffer a loss. Private equity funds may not see their portfolio companies as likely targets for cyber attacks or may carry false confidence in the systems in place to defend network environments. These misconceptions can, in some cases, inflict irreparable damage to the company’s industry reputation, customer trust, and the overall value of the business.

Our philosophy is that you will never prevent every ingress into your organization’s environment. Rather, you need to identify and detect anomalous behavior quickly to mitigate the consequences of an attack before it becomes a breach. We often see adversaries that have breached networks for days, even months, undetected. In some cases, the company may not have even been the intended target but cyber tools and exploits can wreak havoc by proliferating across networks, spreading from organization to organization. In many investigations, we see the supply chain as the entry point for a breach, and this is becoming more and more frequent.

This is why cyber due diligence must be thorough—encompassing technology, processes and people. It should evaluate both the organization’s information security function and its leadership, which sets the tone for

cybersecurity governance. It should ask: Is the information system architecture effectively structured? Are the risks well understood, and are they reviewed on a constant basis to keep pace with the sophistication of threat actors and their tradecraft? Are the right measures in place to detect breaches, and what is the average response time? What are the policies and processes for connecting with third-party vendors, and does the organization assess the nature and degree of connectivity in the supply chain as a risk vector? There is a vast range of questions to answer in assessing the maturity level of an organization and how it benchmarks against its competitors and established industry standards.

Companies that lack formal cybersecurity risk management processes may be quick to say they haven't had a breach and have no material vulnerabilities. This is often because the company lacks the necessary insight into its potential areas of vulnerability and knowledge of the current cyber threatscape. Once we review them, we often find they either didn't have the capacity to find problems that riddled their networks, or they didn't see a benefit in looking for them, figuring then that they would need to disclose what they found. Ironically, the better companies tend to be those that disclose recent vulnerabilities but have them categorized by severity with a plan in place to address them.

The introduction of the General Data Protection Regulation (GDPR) in Europe this year is a major step toward the harmonization of personal data security, and is forcing businesses to improve their cybersecurity standards and technology defenses. All companies that hold EU citizens' data, no matter where in the world they are headquartered, fall within the scope of the law and risk paying punitive fines for major breaches. Under the GDPR's "security

principle," companies are obliged to adopt measures that are appropriate to the risks presented by the nature of their data processing. This includes evaluating how "state of the art" the technology is that is used to protect data and whether it is fit for purpose, a critical part of any valid due diligence process.

Of course, compliance in and of itself is not a security solution. It helps to build a foundation but does not keep up with the velocity of the threat. Substantive regulatory fines notwithstanding, security breaches can have a huge impact on a company's reputation and bottom line, and consequently its shareholders' return on investment. To protect revenue and preserve—indeed to enhance—the value of their portfolios, private equity firms must ensure that the companies in which they seek to invest apply best practice in managing cybersecurity risk and data protection threats.

Cyber M&A risk assessments are now, therefore, essential to avoid significant unforeseen investments to bring an organization's security controls up to an acceptable level. They also give investors peace of mind that companies are equipped to respond to and mitigate the impact of inevitable attacks. Performing a cybersecurity risk assessment within the context of an M&A transaction requires a unique combination of targeted timing and comprehensive analysis activities. Ideally, organizations would gain visibility into the cyber health of the company they want to acquire prior to a transaction. Where this isn't possible, the review should occur before introducing anything from one environment into the other. Tactically, it's recommended that you gain an understanding of the target organization's cyber health from two perspectives. First, assess whether there are any existing compromises or evidence of poor hygiene resulting from malware, policy violations or suspicious activities. Second, assess the cybersecurity capabilities of the organization to understand the relative maturity of the people, processes and technologies in place.

Organizations that take these prudent steps will identify problems sooner, help to mitigate the consequences of malicious activity and minimize risk. Organizations that fail to take due diligence prior to every buyout transaction are, ultimately, exposing themselves to great risk and failing in their fiduciary duty.

Shawn Henry is the president of CrowdStrike Services, the chief security officer of CrowdStrike, Inc., and a retired executive assistant director of the FBI.

WHITE & CASE

Ian Bagshaw
Partner, London
T +44 20 7532 1575
E ian.bagshaw@whitecase.com

Oliver Brahmst
Partner, New York
T +1 212 819 8219
E obrahmst@whitecase.com

Steven Chabinsky
Partner, Washington, DC
T +1 202 626 3587
E steven.chabinsky@whitecase.com

Christopher Kelly
Partner, Hong Kong
T +852 2822 8740
E christopher.kelly@whitecase.com

whitecase.com