Mighty Guides

Sponsored by BlueVoyant

7 Experts on Evaluating and Managing Cyber Risk for Investors

How to assess and mitigate the cyber risk component of business risk for investments

INTRODUCTION

A successful cyberattack can severely damage a business in many ways. It can cripple business operations. It can steal intellectual property or valuable data. It can completely devalue a business brand. Such damage can be so severe that the business fails as a result.

Most investors are not technologists or cybersecurity experts. They typically focus on financial risks and return on investment, not the cyber risks associated with investment opportunities. So, how do venture capitalists and financiers consider cyber risk when they put their money on the line and seek to increase the value of their investments?

With the generous support of BlueVoyant, we asked seven different investment professionals the following question:

What role does cyber risk play when you weigh a potential investment, and how do you evaluate the level of cyber risk?

We spoke to investors with varying business backgrounds and investments in different industry segments. These conversations provided fascinating insights into how they balance cyber and other business risks, the business factors that affect cyber risk, and their need to see cyber risk in business terms.

I expect that anyone involved in cybersecurity or who has a management role in growing a business will find these investors' perspectives on cyber risk enlightening.

All the best,
David Rogelberg
Editor

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

FOREWORD

BlueVoyant is an expert-driven cybersecurity company that was founded to offer cybersecurity services to businesses of all sizes to defend themselves and their business ecosystems from cyber attack and respond in real-time 24/7/365.

From my time at Morgan Stanley, I knew that the Portfolio Companies of Private Equity Firms are often targeted by Cyber Attackers - for Ransomware, Data Theft, Financial Fraud, and/or Business Interruption. Once a Criminal Cyber Attack Group finds a vulnerable Portfolio Company or two - they may well attack the rest of the portfolio.

Many Private Equity Sponsors now make cyber diligence a part of their investment process, but post-investment it is challenging to monitor ongoing cyber defenses - unfortunately, criminal groups are doing so, waiting for the next new vulnerability.

To provide the required on-going monitoring and defense, BlueVoyant has combined its external cyber compromise and vulnerability detection and scoring, with the services of experts in our Risk Operations Center - this allows us to continuously assess cyber risk, curate out false positives, deliver specific remediation recommendations, and monitor remediation. While you could staff up for this, we can do it for you effectively and cost efficiently.

In this eBook, you'll hear from a range of experts with a common need to secure their investments and portfolios. Their experience provides valuable insight on the best practices to follow to effectively mitigate cyber risk.

Jim Rosenthal
CEO, BlueVoyant

BlueVoyant®

BlueVoyant is an expert-driven cybersecurity services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers, and advanced threats.

Led by CEO, Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials, BlueVoyant is headquartered in New York City and maintains offices in Maryland, Tel Aviv, San Fancisco, London, and Latin America.

"When there's a cybercrime against a financial institution, the brand erosion can be far more damaging than it would be for other kinds of companies."

Sasha Grutman,
Partner
Middlemarch Partners

Sasha Grutman is a co-founder of Middlemarch Partners, a merchant bank that focuses on advising and investing in fast-growing financial and business services companies. Prior to Middlemarch, Sasha made private equity investments for TH Lee Putnam Ventures, Citigroup, and Goldman Sachs. He began his career at Boston Consulting Group.

Cyber Risk Is Critical in Financial Services Investments

In serving as a merchant banker for ventures that focus on financial and business services, Sasha Grutman, partner at Middlemarch Partners, has two levels of involvement when evaluating cyber risk. He explains, "Like an investment banker, I am an intermediary. I help people raise capital for technology-enabled financial services and business services companies that use technology to either disrupt an industry or enhance service delivery in an industry. As merchant bankers, we also co-invest alongside lead investors in some of the deals that we bank."

In his investment banker role, Grutman works with companies to raise capital, guiding them through the process of presenting themselves to potential investors. This work includes helping them shape their cybersecurity story in a way that satisfies investors. Potential investors may and often do choose to hire a third party to perform their own security assessment. As a co-investor, however, Grutman becomes more directly involved in cybersecurity assessment, working to understand the strengths and weaknesses of a company's security practice and, if necessary, bringing in a third party for a deeper look.

It's an important part of due diligence, especially in the financial services sector. The big areas of cyber risk for financial services companies are loss of intellectual property, theft of money, and brand damage—a critical issue. Grutman notes, "In financial services, most of your brand is tied to how effectively you deliver a service and how safe it is to work with you. When there's a cybercrime against a financial institution, the brand erosion can be far more damaging than it would be for other kinds of companies." For example, if somebody were to hack into a product company and steal its customer list, that may be annoying to customers, but it would not rise to the level of changing the fundamentals of the business. However, if sensitive information about the financial dealings of a bank's customers leaked out, customers would quickly stop doing business with that bank.

"When we look at a company, one of the first questions we ask is whether anybody is responsible for technology security," says Grutman. "The responsible party is typically a C-level IT person or a dedicated cybersecurity expert. That's the first sign that the company is taking cyber risk seriously." That person then guides investors through the company's security practices. Investors want to understand the company's security strategy and policies, its infrastructure, the tools the company has in place, and what the company is doing programmatically to ensure compliance with a security plan and ongoing enhancements to that plan. "Cybersecurity is fundamentally cyber warfare," says Grutman. "It is an unending series of escalations. These are institutionalized attempts to destroy value in other people's property. You have to be ready for it."

Grutman cites an example that shows how important a strong cybersecurity stance can be in a financial services company. He was involved in an investment in a United Kingdom–based consumer lending company that was penetrated after the company had made an investment, and a significant amount of data was stolen. The Financial

When we look at a company, one of the first questions we ask is whether anybody is responsible for technology security. . . . That's the first sign that the company is taking cyber risk seriously.

Conduct Authority in England investigated and suspended the company's authority to make loans until it had addressed its cybersecurity breaches. Further, the company had to make restitution on the grounds that the confidentiality of sensitive information about consumers' financial circumstances had been compromised in the attack. In this case, investors had suffered significant damage to their investment. "You have to assess the readiness of an investment like this to weather such storms," Grutman emphasizes. "If you do make that assessment and take steps to put a security infrastructure in place, and then you are successfully attacked anyway, regulators treat you differently than if you had no plan whatsoever. If you look like you're asleep at the switch, regulators are going to throw the book at you."

Depending on the nature of the business and the size of the investment, an investor may bring in an expert to assess the target company and determine whether its technology is sufficiently secure. "These investors will engage with an outside party, whether it's Accenture, RSM, IronNet Cybersecurity, or another firm, to assess this company's readiness to defend against cybercrime," Grutman says. "That firm will provide a cyber risk report, with scores showing what's there and what's missing. The report will discuss key changes the company needs to make." The cyber risk report with recommendations becomes the basis for addressing cyber risk after the investment has been made.

Once the investment takes place, the investor can guide business strategy, including strengthening security. "In the private equity world, investors are on the boards of these companies," Grutman says. "They're going to share that security assessment report with management. They're going to say, we want to see you address these things because we want you to get a 10 of 10 on those things. That's part of what's going to drive each quarterly meeting." That ongoing effort to meet those goals

BlueVoyant's Hot Tip

Most investors typically focus on financial risks and return when evaluating an investment opportunity or managing their portfolio, not cyber risks. So, how do venture capitalists and financiers consider cyber risk when they put their money on the line and want to protect their investments from any damaging cyber attacks?

becomes somebody's responsibility in the organization. At quarterly board meetings, that person will report on what's being done, provide evidence showing where the company stands, and make requests for additional spending if needed.

When evaluating an investment opportunity, the first considerations are always the business fundamentals of the product, market engagement, and business design. If you cannot manage those controllable elements in a way that makes the business profitable, then the investment should not go forward. But, Grutman emphasizes, "Cyber risk comes right after those core operating elements, because if somebody penetrates your systems, steals your data, and exposes your brand as unsafe, you may never be able to recover. Cybercrime is an exogenous factor. If you are not prepared for it, it can devastate your business." ■

Sasha Grutman,
Partner,
Middlemarch Partners

Key Points

1. Depending on the size of the investment, an investor will bring in a security expert to look critically at the target company. That consultant will come back with a cyber risk report and recommendations for addressing gaps in security.

2. When evaluating an investment opportunity, the first considerations are always the business fundamentals of the product, market engagement, and business design. Cyber risk comes right after those fundamentals because it is an exogenous factor that can devastate a good business.

CONCLUSION

When investing in a company, it's critical to assess the level of cybersecurity in place to fully understand the associated risks and prioritize remediation activities accordingly. Unfortunately, most security teams often struggle with what is most important to look for.

This risk becomes compounded once that company is brought into a portfolio. Poor cybersecurity can result in direct financial losses, regulatory fines, and reputational damage.

Ensure you have a process in place and an experienced team of experts to fully assess and evaluate the cyber risks. As Chris Kim, one of the experts said: "The result of failing to meet the business hurdle and getting breached is the same. It's basically a business killer."

For more information on how BlueVoyant can help mitigate cyber risk within your investments and portfolio, visit

www.bluevoyant.com

For more information on sponsoring a Mighty Guide or sharing your insights in a Mighty Guide visit

www.mightyguides.com

BlueVoyant

Mighty Guides