

# Cybersecurity: The New PE Firm Team Sport

## WRITTEN BY

James Koenig | Brent T. Hoard | Privacy + Security Advisors

## CONTACTS

Alexander “Alec” F. Watson | Bruce K. Fenton | Matthew M. Greenberg

---

*This [article](#) was originally published in the [ACG Middle Market DealMaker Magazine](#) | Spring 2024 issue on May 6, 2024 and is republished here with permission.*

Historically, many private equity firms have let their portfolio companies independently manage cybersecurity. Given the increase in data and cyber risks, sophistication of threat actors, and impact and cost of breaches, leading PE firms are taking a new collaborative approach.

While portfolio companies are still able to operate independently, PE firms and their deal teams are increasingly using periodic “rapid maturity assessments” to efficiently identify needs, remediate against company and portfolio risk, and drive consistent reporting and solutions across the portfolio.

If the idea of evaluating, monitoring, and enhancing portfolio company cybersecurity programs at a portfolio level seems infeasible, think again. Here are four steps you can take to implement a collaborative approach for your portfolio:

**1. Determine a common framework to assess maturity and risk across the portfolio.** While portfolio companies may use a variety of major information security frameworks (e.g., most commonly ISO, NIST and CIS-18), determine a preferred framework around which to organize the portfolio’s assessment and reporting. Crosswalks can readily tie together key controls and enable cohesive reporting and clear objectives regardless of a portfolio company’s chosen framework.

**2. Identify current-state maturity, individual portfolio company risks, and common vulnerabilities and needs across the portfolio.** The assessment consists of three types of fieldwork: surveys, interviews and document review (e.g., program documentation, assessment reports and in-flight initiatives). Assessments are repeated periodically/annually. Innovative organizations use the assessment results to maintain an enterprise risk register, develop a road map to prioritize and track remediation activities, and benchmark key program maturity controls at the company and portfolio levels.

**3. Develop a cross-portfolio maturation plan.** By conducting assessments across the portfolio, PE firms can identify and prioritize key areas for improvement. For example, the PE firm may wish to use a consistent incident response plan across the portfolio companies or identify common breach service providers (e.g., forensics, legal, threat negotiation) that are readily available and understand the entire portfolio. This approach enables the

portfolio to leverage economies of scale and purchasing power to secure preferential pricing for scalable security solutions for the portfolio companies (e.g., IAM, threat intelligence or endpoint detection and response).

**4. Track improvements over time.** Benchmarking facilitates efficient and systematic evaluation of controls and improvements for the entire portfolio and individual portfolio companies over time, enabling better informed investments and strategic decision-making for the organization (and to better prepare a company for sale). Subsequent assessments are even less disruptive, focusing on change during the interim period.

While information security was once viewed as table stakes and a cost of doing business, cyber preparedness and exposure to ransomware and data leaks are impacting PE deal diligence and valuations. It is also far less expensive to have security “baked in” from the beginning than to spend post breach. With some key tools and minimal investment, PE firms are increasingly assessing, measuring, and addressing both unique and common vulnerabilities across their portfolios. In this new information economy and cyber risk environment, if you can’t measure it, you can’t manage it!

---

*Jean Pawluk, Senior Security Advisor, also contributed to this article.*

## **RELATED INDUSTRIES + PRACTICES**

- [Data + Privacy](#)
- [Privacy + Cyber](#)
- [Private Equity](#)