Safeguarding Your Portfolio: A Private Equity CIO's Imperative for Cyber Risk Mitigation

By Mike Grabowski, Founder and CEO; Bryon Griffin, Dir of IT @MDRN Tech

The biggest risk to any business is not understanding how much risk it has, and cyber risks are growing for organizations – especially private equity firms – across the board. And for CIOs, the job isn't just to protect the firm, but to ensure your portfolio companies are prepared to face an ever-evolving landscape of cyber threats, too.

- According to **Sophos State of Ransomware** 2024, nearly *60% of companies were hit last year*, with the average **ransom demand being over $4.2 million**
- In September 2023, a **BlackCat attack** shut down the entire infrastructure – from check-in systems to slot machines – of the **Caesars and MGM hotel chains**, with Caesars paying a $15 million ransom and MGM restoring its infrastructure on its own in 9 days, which cost the company $100 million++
- A **mere 60% of organizations have cyber insurance**, and of those, a shocking **80% are underinsured.**

Because the financial, legal, and reputational consequences of cyberattacks can be catastrophic, it is essential to refine your approach to cyber risk mitigation, so you're prepared for the worst-case scenario in your firm, and your portfolio - ***because those risks do roll uphill.***

Here's how you create a comprehensive cyber risk management strategy.

1. Quantify cyber risk exposure across your portfolio

Quantifying cyber risk exposure across your portfolio demands a methodical approach. Start by **conducting thorough assessments of your firm**, and each portco's digital infrastructure, evaluating vulnerabilities in systems, networks, and data management practices. Identify potential entry points for cyber threats like malware and insider risks through penetration testing. Then, map out the company data flows and evaluate them through the lens of the relevant regulatory landscape to assess compliance risk and potential liabilities.

Next, contextualize your findings within the broader business. **Employ a quantitative risk assessment model** like FAIR (Factor Analysis of Information Risk) to **assign monetary values to identified risks** based on the potential risk reduction and return on investment. This data-driven approach enables prioritization of cybersecurity investments, aligning protection efforts with strategic objectives and risk tolerance thresholds – which ensures that cybersecurity efforts are calibrated to protect critical assets without stifling innovation or operational agility.

With these strategies, you can bolster cybersecurity across your portfolio, safeguard critical assets, and enhance overall operational resilience.

2. Implement robust monitoring of insider threats and third-party risks

Once you understand your cyber risk exposure, **establish comprehensive monitoring frameworks** that continuously assess user behavior within digital environments - leveraging advanced analytics and machine learning to detect anomalies indicative of insider threats. Then implement **stringent access controls and conduct regular audits** of privileged accounts to further mitigate these risks.

Best practice is also to thoroughly **vet and monitor third-party vendors and partners**, verifying their cybersecurity practices and compliance with industry standards. Implementing **continuous monitoring mechanisms** and real-time alerts for suspicious activities enables you to take proactive response measures and ensure swift mitigation of potential threats before they escalate. By integrating these practices, CIOs can strengthen cybersecurity postures across their portfolio, safeguard sensitive data and maintain trust among stakeholders and investors.

3. Foster a culture of cyber awareness among portfolio company leadership

Even with a strong, comprehensive plan, if cybersecurity isn't treated as a strategic priority at the highest levels of executive leadership, an organization will carry tremendous cyber risk. That's why f**ostering a culture of cyber awareness among portfolio company leadership is pivotal** for CIOs to enhance overall cybersecurity resilience.

You can create that culture by emphasizing the importance of executive buy-in and active participation in cybersecurity initiatives. Then **implement regular training programs tailored to the specific roles** and responsibilities of executives, focusing on emerging threats, best practices for data protection, and incident response protocols. Establish open communication channels for reporting potential security incidents and promote a proactive approach to cybersecurity risk management throughout the organization.

By establishing culture where cybersecurity is integrated into decision-making processes and viewed as a shared responsibility, CIOs empower portfolio company leadership to effectively mitigate risks and safeguard critical assets against evolving cyber threats.

4. Establish a continuous cycle of cyber risk assessment and management

Part of establishing a culture of cyber awareness includes the attitude that combating cyber threats is a never-ending battle, and that a **continuous cycle of risk assessment and management is required**. That means conducting regular and comprehensive cyber risk assessments using industry-standard frameworks - such as NIST Cybersecurity Framework or ISO 27001 – and implementing robust monitoring tools and technologies to continuously track and analyze cyber threats and vulnerabilities in real-time.

Assessments should evaluate **vulnerabilities, threats, and potential impacts on critical assets and operations**. Monitoring tools should utilize **threat intelligence feeds** and IT security personnel should collaborate with industry peers to stay ahead of emerging threats. **Developing and regularly updating incident response plans** is also critical, along with conducting tabletop exercises to test preparedness and refine response procedures.

By embedding this cycle into the organizational culture, CIOs can ensure that their cyber risk management remains agile and responsive to evolving threats, while ensuring business continuity and protecting valuable assets within their portfolio companies.

5. Leverage cyber insurance as a risk transfer mechanism

No matter how good your defenses and organizational preparation, organizations still carry significant risk, which is where cyber insurance can be used to mitigate potential financial losses stemming from cyber incidents.

To obtain the coverage you need, collaborating with insurance brokers to select policies that align with **each portco's specific risk tolerance thresholds and business continuity objectives** are just the beginning.

You want to ensure policies cover a broad range of potential cyber threats, including data breaches, business interruption, reputational damage, system restoration costs, and regulatory fines. Also, before buying a policy, **make sure you understand the nuances between first-party and third-party coverage, and scrutinize policy exclusions**, such as social engineering schemes and third-party risks.

Regular review of each policy is advised, so you can update coverage to adapt to evolving cyber threats and regulatory changes. Also, establish clear communication channels between IT teams, legal counsel, and insurance providers to streamline claims processes and ensure prompt response to incidents.

Being able to **point to the robust nature of your cyber approach**, continuous efforts to improve can also prove invaluable when negotiating premiums, and if you have **sufficient quantitive controls and monitoring in place**, you can also be fully armed (perhaps even more so than your carrier) to drive the conversation on where **your true premium** should land against your peers, and the financial services industry which is under continual attack.

Start the Conversation.

lovethemdrnteam@mdrntech.com