VC & PE: AI Threats Are No Longer Emerging Risks. They Are a Portfolio Cybersecurity Issue Now.

I think a lot of investors, operating partners, and portfolio leadership teams are still looking at AI through the wrong lens.

Most of the conversation is still centered around productivity, automation, faster workflows, and competitive advantage.

That matters.

But from where I sit, AI is also becoming one of the most important **cybersecurity and risk management issues** for VC and PE-backed companies.

Not in theory. Right now.

The reason is simple: AI is changing both sides of the cyber equation. It is helping businesses move faster, but it is also helping attackers move faster, target more precisely, and operate with a level of scale and personalization that many portfolio companies are not prepared for.

For VC and PE firms, this is not just a technology trend. It is a **portfolio risk issue**.

Why this matters more in VC and PE

In private equity and venture capital, the cybersecurity conversation is different from a typical enterprise environment.

You are not just protecting one company.

You are often dealing with a portfolio of businesses at different stages of maturity, different industries, different tech stacks, and very different leadership capabilities. Some have formal security teams. Some have a lean IT function. Some are still building basic governance. Some are growing faster than their controls can keep up.

Now add AI into that mix.

That means:

- more employees using public AI tools without clear guardrails
- more companies embedding AI into products before security catches up
- more exposure of sensitive IP, customer data, board material, and deal information

- more sophisticated phishing and impersonation attacks against executives, finance teams, and privileged users
- more pressure on already-stretched leadership teams to move fast without introducing avoidable risk

For PE and VC, the challenge is not only whether one company is exposed.

The challenge is whether the **same pattern of weakness exists across multiple portfolio companies at once**.

That is where this becomes an operating model issue, not just a technical one.

The AI threats I believe matter most for VC and PE-backed companies

1. AI-powered phishing is becoming much more convincing

This is one of the most immediate risks.

AI can help attackers create highly personalized phishing emails, fake personas, and realistic business communications. Instead of broad, poorly written phishing attempts, threat actors can now generate messages that look relevant, polished, and believable.

That matters even more in VC and PE environments because attackers know exactly where to focus:

- CFOs
- Controllers
- executive assistants
- deal teams
- founders
- portfolio CEOs
- legal teams
- privileged IT administrators

When the attacker understands the company, the transaction context, or the investor relationship, the email becomes much harder to spot.

And when deepfake voice or video is added to the mix, the risk moves beyond inbox security and into business trust.

2. Sensitive data leakage through AI use is a real portfolio problem

This is one of the biggest issues I see developing quietly.

Employees are using AI tools to summarize contracts, draft communications, review code, analyze documents, or speed up routine work. On the surface, that sounds harmless.

But what gets entered into those tools?

Internal strategy. Product roadmaps. Customer data. Source code. Financials. M&A discussions. Legal analysis. Board content. Pricing models. Intellectual property.

For venture-backed and PE-backed companies, that can be devastating.

In high-growth environments, teams move fast. The problem is that AI use often grows faster than governance. So what begins as productivity can quickly become an unmanaged data exposure issue.

3. AI is helping attackers move from broad attacks to tailored attacks

This is the strategic shift that I think leadership teams need to understand.

A lot of traditional cybersecurity programs were built around known attack patterns. Known malware. Known signatures. Known tactics. Known indicators.

AI is changing that.

Attackers can now use AI to conduct reconnaissance faster, analyze environments more efficiently, identify likely vulnerabilities, and tailor attacks to a specific company or even a specific individual.

That means attacks are becoming less “one of many” and more “one of one.”

And that is a serious issue for portfolio companies, because tailored attacks are much harder to stop with baseline controls alone.

4. AI can increase the quality of post-compromise activity

Once attackers gain access, AI can help them work smarter.

It can support password guessing based on context, summarize data, identify the most sensitive files, classify documents, and help determine what is most valuable to steal.

For PE and VC-backed companies, this is especially dangerous because the data is often disproportionately valuable:

- IP
- product designs

- semiconductor or engineering data
- investor communications
- customer contracts
- M&A information
- legal and regulatory material
- financial reporting
- employee and payroll data

This is not just about more theft. It is about **more targeted theft**.

Where I think many firms get this wrong

The mistake is assuming AI risk belongs only to the product team, the CIO, or the security team.

It does not.

In a VC or PE environment, AI risk touches:

- portfolio operations
- legal
- compliance
- finance
- product
- technology
- investor reporting
- third-party risk
- incident response
- board oversight

In other words, this is a governance topic.

And I would go one step further: firms that manage cybersecurity centrally across the portfolio should now start looking at AI risk the same way they look at identity, cloud, ransomware readiness, and third-party exposure.

Because over time, AI will sit across all of them.

What VC and PE firms should be doing now

This does not require panic. It requires discipline.

1. Establish a portfolio-wide AI usage baseline

At minimum, firms should know:

- which portfolio companies are using AI tools
- whether employees are using public AI platforms
- whether AI is embedded into products or services
- what sensitive data may be exposed
- whether any guardrails, policies, or approvals exist

You cannot manage what you cannot see.

2. Put clear guardrails around sensitive data

Every portfolio company does not need the same model, but every company does need clarity around what data should never be entered into AI tools without approval.

That includes:

- customer data
- regulated information
- legal material
- source code
- board content
- financial forecasts
- M&A and investor information
- proprietary product or engineering data

This is one of the fastest ways to reduce unnecessary exposure.

3. Treat identity as a frontline AI control

If AI is making phishing, impersonation, and credential theft more effective, then identity controls become even more important.

That means stronger authentication, privileged access controls, joiner-mover-leaver discipline, access reviews, and monitoring for abnormal account activity.

For PE and VC-backed companies, identity maturity is often one of the highest-return investments because it reduces risk across many attack paths at once.

4. Review AI-enabled products and workflows like security-sensitive systems

If a portfolio company is embedding AI into its product, support operations, internal workflows, or decision-making, that should trigger a security review.

The key questions are straightforward:

- What inputs influence the model?
- What data is exposed?

- What actions can the system trigger?
- How are outputs validated?
- What happens if the model is manipulated or wrong?

This is where a lot of organizations move too quickly.

5. Improve detection and response for abnormal behavior

If attacks are becoming more tailored, firms cannot rely only on known indicators and static detections.

Portfolio companies need better ability to identify unusual behavior across users, endpoints, cloud platforms, SaaS, and data movement. That does not mean every company needs a massive SOC. But it does mean they need enough visibility to spot deviations before they become material incidents.

6. Include AI risk in portfolio governance and board discussions

This is the big one.

AI should now show up in:

- cyber risk reviews
- portfolio assessments
- due diligence questions
- operating partner discussions
- board updates
- legal and compliance conversations
- incident response planning

The goal is not to create noise. The goal is to make sure AI risk is being managed intentionally rather than accidentally.

My view: this will become a separator between mature firms and reactive firms

The firms that do this well will not necessarily be the ones with the biggest budgets.

They will be the ones that create repeatable discipline across the portfolio.

The ones that ask the right questions early.

The ones that put guardrails around data before there is a problem.

The ones that understand AI is not only a business accelerator, but also an attack accelerator.

And the ones that realize cybersecurity in VC and PE is no longer just about whether a company has antivirus, MFA, or a policy set.

It is about whether the firm can recognize emerging risk patterns early and operationalize controls across multiple portfolio companies before those issues become incidents.

Final thought

AI is not just another technology wave for VC and PE to monitor.

It is now part of the cyber risk landscape that can affect valuation, resilience, investor confidence, regulatory exposure, and operational stability across the portfolio.

The firms that get ahead of this now will be in a much stronger position to protect their portfolio companies, guide leadership teams, and reduce avoidable risk as AI adoption continues to accelerate.

The firms that wait may find that AI did not just change productivity.

It changed the threat model.

What are you seeing across VC and PE-backed companies right now: more AI productivity upside, or more unmanaged AI risk?