A WORD FROM DELOITTE

# Don't let cyber insecurity hurt your valuation

The new reality for companies seeking funding reads like a thriller: Ransomware gangs operate like professional corporations; hackers work around the clock; and amid the digital chaos, robust cybersecurity has become table stakes for startups pursuing venture capital (VC).

Though artificial intelligence (AI) remains a hot sector in VC, cybersecurity isn't too far behind. Cybersecurity unicorns outperformed many of their emerging tech peers in valuation growth in 2023,[1] according to PitchBook. The reason is clear: Cyber threats have become pervasive across all aspects of business life, from consumer applications to enterprise solutions. Companies with elevated security measures may find it advantageous for locking in funding, while those lacking comprehensive protection might face increased scrutiny from possible investors. It turns out that when hackers treat corporate networks like an all-you-can-breach buffet, investors tend to notice.

In this article, Deloitte's Heather Gates and Tiffany Kleemann detail how cybersecurity isn't just an IT concern—it's a fundamental business imperative that can make or break company valuations. Read on for important guidance and insights.

**Your next merger's big threat? A weak firewall.**

The tectonic plates of mergers & acquisitions (M&A) have shifted, and perhaps nothing illustrates the growing importance of cybersecurity more than the fact that it's becoming inextricably linked to a business's chances for success. "Based on business activity, the first three months of the fiscal year saw more cyber-related due diligence than the entire previous year combined," says Tiffany. This surge signals a fundamental shift in how acquirers evaluate their targets.

"Without a solid cyber plan in place, the value of your enterprise could be significantly diminished, especially if there is a cyberattack on the business," notes Heather. Five to 10 years ago, this wasn't even a consideration during exits, but now it's mandatory.

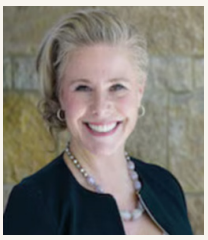
**The startup's security paradox**

For early-stage startups, this new reality can present a challenging paradox. Heather says, "While early-stage investors may not scrutinize cybersecurity during initial funding rounds, the moment a startup begins engaging with customers, security becomes paramount." The old Silicon Valley mantra of "move fast and break things" has evolved. Today, cybersecurity is foundational to risk management. That said, it is a matter of "when, not if" that enterprises will eventually experience a material cyber incident, so they should do all they can to build a cyber program that can operate through disruption, not just assume attacks can be prevented.

This evolution doesn't mean startups need enterprise-level security from day one. Instead, starting with essential controls and scaling security measures as the business grows is a suggested leading practice. Many young companies opt for outsourced security solutions, similar to how they might farm out accounting functions in their early days. The key is striking that delicate balance between "good enough for now" and "won't keep future investors up at night."

**Heather Gates**
*Audit & Assurance Private Growth Leader, Deloitte & Touche LLP*

*With more than 30 years of financial services experience, Heather serves as the national Private Growth Leader within Audit & Assurance.*



**Tiffany Kleemann**
*Emerging Growth Leader, Managing Director – Cyber & Strategic Risk, Deloitte & Touche LLP*

*Tiffany is currently the Emerging Growth Leader for the Cyber & Strategic Risk practice at Deloitte. She has had a distinguished career holding various leadership and operational roles in the technology industry, White House, government, and US military.*

**Digital extortion goes corporate**

The threat landscape has evolved to become surprisingly professional—albeit remaining illegal. Modern ransomware operators maintain help desks, negotiate terms, and even provide "customer service" for their victims. These digital desperados have

1: "The VC Investors Leading the Way in Cybersecurity," PitchBook, Jacob Robbins, February 29, 2024.

built a surprisingly successful business model—if only they could apply their skills to a more honest profession.

What's just as concerning is the sophisticated targeting of companies during crucial business events: IPOs and M&A transactions. These cybercriminals have mastered the art of strategic timing, actively monitoring news about potential M&A or funding rounds and taking advantage of those events by actively launching ransomware or data breach campaigns targeting those entities.

**The zero trust revolution**

There was a 400% increase of Internet of Things (IoT) malware attacks across various industries, according to Deloitte's Annual Cyber Threat Trends Report.[2] In response to these types of evolving threats, organizations are increasingly adopting "zero trust" principles. This approach, based on the premise of "never trust, always verify," requires verification at every step, whether accessing internal systems or communicating with third parties. Every login and connection become the digital equivalent of an airport security check. "Zero trust provides a scalable framework that grows alongside your business," says Tiffany.

**Smart threats, smarter defense**

Similar to other facets of business these days, AI plays a big part in cybersecurity, emerging as both a threat and a solution. While AI enables more sophisticated attacks, including very convincing deepfakes that can fool even C-suite executives, it's also powering defense mechanisms that can spot a digital intrusion faster than you can say "unauthorized access." This technological race can push companies to strengthen their security positions and improve their data governance practices. Get ready for a new mantra in today's corporate environment: Data governance isn't just good housekeeping—it's key to survival.

**The CFO's cybersecurity awakening**

Move over, balance sheets—there's a new line item keeping chief financial officers (CFOs) up at night. They're finding that cybersecurity has become an unexpected but crucial part of their portfolio. Tiffany says, "At recent industry conferences, while nearly all CFOs acknowledged their involvement in cybersecurity decisions, few felt adequately educated on the topic." The result? A mad dash for cyber literacy among the spreadsheet-and-depreciation crowd, who suddenly need to understand why that seven-figure cybersecurity investment might be as important as next quarter's earnings report.

**2025's cybersecurity survival guide: Stop wishing, start preparing**

Protecting your company starts with undergoing a due diligence process. Work with a trusted advisor to conduct an in-depth assessment of your cybersecurity network including past incidents and current staffing. We can advise on policy reviews, cybersecurity tool stacks, and your organization chart, in addition to regular security assessments with independent National Institute of Standards and Technology (NIST) framework evaluations. We can also provide advice for your incident response plan and risk-appropriate insurance options.

Tiffany notes an important statistic: "According to the Deloitte 2023 Global Future of Cyber Survey,[3] 91% of companies reported at least one cyber incident or breach." Deloitte's cybersecurity team is here to assist you in transforming your security strategy from a wish list into an actionable plan. Contact us to start the conversation—your next security assessment is closer than you think.

Take a deeper dive by downloading our annual Cyber Threat Trends report.

Contact our team today.

---



2: "Annual Cyber Threat Trends Report: Insights, Emerging Threats, and Their Potential Impact," Deloitte, 2024, accessed December 18, 2024.
3: "2023 Global Future of Cyber Survey," Deloitte, 2022.

Deloitte.

# Capture.
# Organize.
# Done.

## The new way to audit prep.

**EGC Knowledge Share** empowers emerging growth companies to get audit-ready from day one. Our digital survey tool transforms traditional audit prep from a reactive scramble into a proactive process. By capturing and organizing your baseline audit knowledge early, you're reducing the number of adhoc requests that will be needed. Learn more about our trusted five-step approach to first-time audits and watch how our EGC Knowledge Share tool advises you on the ways to put it into practice.

**Learn more**