The Due Diligence Question You're Not Ready For

Cybersecurity is now a capital readiness issue — and founders who aren't prepared are losing deals. Here's what you need to know before your next raise, acquisition, or government contract.

KEEP SCROLLING →

A Deal Almost Died Over One Question

A founder Rod Loges worked with was deep in due diligence. Revenue was strong. The deal was moving. Then the acquirer asked: **"Walk us through your cybersecurity posture."**

> He had antivirus software and a firewall. He thought that was enough. It wasn't.

The deal eventually closed — but at a lower valuation and on a longer timeline. Six weeks of scrambling. Real money lost. The cost of not being ready wasn't stress. It was dollars.

THE THREAT LANDSCAPE

What Is Q-Day — and Why It Matters Now

⚡ The Moment

Q-Day is when quantum computers become powerful enough to break the encryption protecting nearly everything online — financial data, IP, contracts, email.

📅 The Timeline

Most experts place Q-Day in the early 2030s. Google has warned it could arrive **as early as 2029.**

🎯 The Attack Today

Adversaries are already running **"harvest now, decrypt later"** operations — stealing encrypted data today and storing it to unlock later.

⚠ **If your data needs to stay confidential for more than 5 years, the threat is current — not future.**

AI-DRIVEN THREATS

The Door Is Being Unlocked Faster Than You Can Lock It

George Hyek — former US Army intelligence officer and fractional CISO at TrinSec Seven — shared a sobering reality on the MilCom Founders Podcast.

> "It's happening instantly and at a scale that companies simply can't patch. They cannot come up with the time to make the patch, to remediate it, to fix it. To lock the door." — George Hyek, TrinSec Seven

Anthropic's AI platform **Mythos** identifies vulnerabilities and writes exploit code — in record time. The security landscape founders thought they understood is shifting beneath their feet.

BY THE NUMBERS

Small Business Is in the Crosshairs

43%

Attacks on Small Biz

Nearly half of all cyber attacks target small businesses — most founders have no idea they're already in the fight.

2029

Earliest Q-Day

Google's projected earliest date for quantum decryption capability — less than 5 years away.

6 Wks

Recovery Time

How long one founder scrambled to get security in order after a due diligence red flag — at significant cost.

Source: George Hyek, TrinSec Seven / Rod Loges, One Degree Financial

READY FOUNDER™ FRAMEWORK

Cybersecurity = Capital Readiness

Pillar 6 of the Ready Founder™ framework: capital readiness goes far beyond clean books and strong cash flow. It means **can your business survive scrutiny?**

Investors

Ask about cybersecurity posture during due diligence — increasingly a dealbreaker, not a footnote.

Acquirers

Evaluate data protection as part of risk assessment before any transaction closes.

Government Contracts

CMMC, HIPAA, and other compliance frameworks are now gatekeepers to even bidding on contracts.

A breach can wipe out years of value in a single incident — no matter how strong your revenue looks.

Security as a Competitive Advantage

> "I see the security through your lens. I try to make the security a business asset for you that supports your business objectives. The minute security becomes an obstacle, people go around it — which just creates a bigger vulnerability." — George Hyek

Done right, security isn't a burden — it's a differentiator. Founders who build security into operations signal maturity, protect valuation, and win deals their unprepared competitors lose.

ACTION PLAN

4 Steps to Get Your House in Order

1	**Get a Vulnerability Assessment** Bring in a qualified security professional. If the idea feels uncomfortable, that's exactly why you need it.
2	**Ask Vendors the Hard Questions** What are they doing about post-quantum encryption? What's their incident response plan? No clear answer = red flag.
3	**Think Like an Owner, Not an Operator** Security protects revenue, customer data, IP, and valuation. A breach costs more than money — it costs trust.
4	**Add Security to Your Capital Readiness Checklist** Right next to clean financials, cash flow projections, and investor materials. It belongs there.

What Is a Fractional CISO — and Do You Need One?

A **fractional Chief Information Security Officer** provides enterprise-grade security strategy to companies on a part-time or contract basis — without the cost of a full-time executive hire.

Full-Time CISO

$250K–$400K+ annually. Enterprise scale. Often out of reach for growth-stage companies.

Fractional CISO

Senior expertise, flexible engagement. Right-sized for small businesses preparing for capital events.

For founders preparing for fundraising, M&A, or government contracting — a fractional CISO can be the difference between a deal that closes and one that doesn't.

Don't Let Cybersecurity Be the Reason You Lose the Deal

The question is coming. Investors, acquirers, and contract officers will ask about your security posture. The founders who answer confidently — and credibly — are the ones who close.

MILCOM Founders Podcast – Episode 45

Listen Now

Episode 45: George Hyek, TrinSec Seven on the MilCom Founders Podcast

Share This Post

Tag a founder who needs to hear this before their next due diligence call.

Rod Loges, CEO — One Degree Financial

Ready Founder Framework | Pillar 6: Capital Readiness