



Lethal Cybersecurity Lies That Can Doom Your Business

A CEO's Strategic Guide
to Cybersecurity

**RICHEY
MAY**

Cyber

Lethal Cybersecurity Lies That Can Doom Your Business

As a CEO, inherited beliefs can silently erode your competitive edge. For example, assuming your offerings face no rivals, only to watch market share vanish to unseen substitutes.

In cybersecurity, six common lies pose even greater risks: they turn a vital defense into a hidden liability, costing millions in breaches, lost trust, and regulatory fines. We prepared this guide to expose these lies and reveal truths that position cybersecurity as a strategic advantage that boosts ROI, protects customer relationships, and enables agile decision-making.

Embrace these insights now: identify the gaps in your approach, build adaptive defenses, and transform potential crises into opportunities for leadership.

LIE #1

“I Won't Get Breached”

THE TRUTH

Odds Are You Will Get Breached

Breaches are becoming an inevitability. Hackers exploit weak spots faster with AI tools. What once took weeks now happens in hours. This shifts focus from prevention alone to rapid detection and response.

Hope is a liability. Believing “I won’t get breached” is a misguided approach to cyber. Hope alone can’t save you.

Perimeter defenses fail when threats slip through. Compliance certificates offer false security against modern attacks. Result: higher costs and business disruption.

A national fast-food chain ignored breach warnings and fired their consultant. The attack hit anyway, amplifying damage through delayed action. Avoid this by preparing for breaches to protect revenue and reputation.

LIE #2

“Compliance Equals Security”

THE TRUTH

Static Defenses Fail Against Evolving Threats

Compliance builds basic layers like firewalls and training. But threats evolve exponentially with AI. Static approaches leave gaps that erode competitive advantage.

Treat cybersecurity like dynamic business risk. Build adaptive systems that evolve with threats. This ensures resilience and supports strategic growth.

While rivals chase minimum standards, invest in defensive resilience. The result? Elevating your cyber resilience not only reduces breach risks but also secures a stronger position in the market.

LIE #3

“Our IT Person Has Cybersecurity Covered”

THE TRUTH

IT ≠ Cybersecurity

IT handles networks and software. Cybersecurity demands expertise in attacker tactics and defenses. Confusing the two creates catastrophic gaps.

Assessments often reveal these shortfalls in crises which are too late. Small and mid-sized companies skip specialists due to cost, but the alternative proves far more expensive.

Hire or partner with true experts. This safeguards assets and enables confident decision-making on risks that impact the bottom line.

LIE #4

“I Can Delegate Cybersecurity Leadership”

THE TRUTH

Only You Can Build a Security-First Culture

You set the “why” behind security efforts. No one else aligns it across functions as a strategic priority.

Cyber risk equals business risk (like financial or legal threats). Champion it positively: frame protocols as protecting customers to inspire compliance.

Model sincere diligence: use multi-factor authentication yourself, publicly support your cyber team, and allow no exceptions. Your involvement signals priority, boosting ROI through reduced incidents.

LIE #5

“A Breach Is Just Another Crisis”

THE TRUTH

Breaches Damage All Stakeholder Relationships at Once

Unlike fires or disruptions, breaches shatter trust with employees, customers, vendors, and investors simultaneously. This demands coordinated response across departments.

You must lead preparation: define roles for legal, marketing, PR, HR, finance, and IT before incidents hit. In a breach, focus on scope, containment, impact, evidence, and resources.

Communicate wisely: verify facts first, share what stakeholders need, show concern, and provide actions. Hasty statements, like Valve Corporation's error, amplify harm. Strong prep turns crises into trust-building moments.

LIE #6

“If We Have the Right Systems and People, We’re Secure”

THE TRUTH

Odds Are You Will Get Breached

You set the “why” behind security efforts. No one else aligns it across functions as a strategic priority.

Cyber risk equals business risk (like financial or legal threats). Champion it positively: frame protocols as protecting customers to inspire compliance.

Model sincere diligence: use multi-factor authentication yourself, publicly support your cyber team, and allow no exceptions. Your involvement signals priority, boosting ROI through reduced incidents.

The Ultimate Cybersecurity Truth

Answer this post-breach: “Did I do everything possible to protect customer data and respond well?”

A “yes” requires preparation. Contemplate the human stakes = leaked data ruins lives. This mindset drives decisive action.

The Johnson & Johnson Model

In 1982, cyanide-laced Tylenol killed seven. J&J recalled products nationwide, cooperated with authorities, and redesigned packaging at huge cost.

Their credo guided quick, decisive response building greater customer (and regulator) trust. Apply this: clear convictions on data protection enable fast breach handling without hesitation.

The Competitive Advantage of Truth

Well-prepared firms emerge stronger from incidents. They prove reliability, deepening customer loyalty.

Poor prep destroys reputation forever. Invest now to gain an edge: demonstrate leadership under pressure.

What This Means for You

Start today with these actions:

- **Set the cultural tone:** Make cybersecurity a visible leadership priority.
- **Evaluate your team:** Security belongs with specialists, not generalists.
- **Plan for crisis:** Develop and test response procedures.
- **Layer defenses:** Go beyond perimeters for comprehensive protection.
- **Build your team:** Identify internal and external experts.
- **Assess posture:** Use outside validation to test defenses.

Preparation costs less than recovery.

Your Next Steps

Breaches are certain. Readiness is your choice.

Contact Richey May's cybersecurity team for a full assessment.

Prepare now to lead through any incident.