

EXECUTIVE CYBER BRIEF

EVERY GROWTH-FOCUSED EXECUTIVE SHOULD KNOW

Five Emerging Cybersecurity Risks



Pillar Technology
P A R T N E R S





introduction

Cyber risk isn't slowing down — and neither are you.

Mid-market organizations are experiencing the same threat volume as Fortune 500s — but with leaner teams and faster growth targets. Whether you're preparing for acquisition, scaling operations, or protecting customer trust, cybersecurity is no longer a technical concern. It's a business-critical function.

This brief outlines five threats that every growth-focused leader must have on their radar — and the strategic responses that can turn each risk into a resilience opportunity.

Ransomware Targets Mid-Market

1



Coveware reports a strategic pivot by ransomware actors toward mid-market companies, exploiting limited in-house cybersecurity capabilities (coveware.com)

Mid-sized companies are now prime ransomware targets — seen as profitable, yet underprotected

STRATEGIC SAFEGUARDS



Engage a reputable incident response (IR) firm under contract and on-call to accelerate containment



Regularly back up critical data — and test your recovery procedures like your business depends on it (because it does)

Assuming “Security Debt”²



“Security debt” — the result of postponed cybersecurity maintenance — compounds over time, leaving systems exposed (theimagingchannel.com)

STRATEGIC SAFEGUARDS



Conduct regular cybersecurity audits to surface outdated systems and neglected protocols



Invest in modern infrastructure and proactive updates to reduce your long-term attack surface

Deferred patches and rushed tech decisions quietly build up risk over time — until it explodes

Third-Party Exploits



The 2023 MOVEit breach exploited a vulnerability in a widely used file transfer tool, compromising data from hundreds of global organizations (wired.com)

**Cybercriminals
are breaching
large
organizations
through smaller,
connected
vendors**

STRATEGIC SAFEGUARDS



Conduct comprehensive cybersecurity assessments of key suppliers and partners



Implement stringent third-party risk management protocols that include contractual security standards

Credential Theft and Executive Targeting

4



In 2024, over 3.2 billion credentials were compromised, with 75% stemming from infostealer malware campaigns (asisonline.org)

Executives are the bullseye — with credentials increasingly compromised by stealthy malware

STRATEGIC SAFEGUARDS



Implement multi-factor authentication (MFA) across all executive accounts — no exceptions



Provide targeted cyber training for executives through programs like Pillar's Cyber Wellness, which builds personal cyber awareness and workplace resilience

Reputation and Share Value Impact

5



In April 2025, SK Telecom's breach led to an 8.5% stock drop and widespread customer concern (reuters.com)

Data breaches now impact more than compliance — they hit valuation, customer loyalty, and brand trust

STRATEGIC SAFEGUARDS



Maintain a tested crisis communication plan that includes executive visibility and board readiness



Establish a pre-negotiated IR retainer to reduce response time and reputational fallout



What Growth-Focused Companies Often Get Wrong About Cybersecurity

Growth exposes gaps — not just in tech, but in assumptions.

Many mid-market leaders believe cybersecurity is something to scale after growth. In reality, it's what enables growth to continue without interruption, litigation, or reputational loss.

Here are 3 common missteps we see:

OUTSOURCING WITHOUT OVERSIGHT

Third-party vendors are assumed to be secure — until a breach proves otherwise. Risk isn't transferred, it's shared.

ASSUMING I.T. HAS IT COVERED

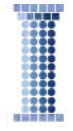
Most I.T. teams are built for availability and uptime — not threat intelligence, incident response, or regulatory navigation.

OVERINVESTING IN TOOLS, UNDERINVESTING IN STRATEGY

Tech stacks grow faster than governance. Without a clear strategy, security becomes reactive, fragmented, and fragile.



The fix? Start with risk visibility and an executive-aligned plan — not tools. Cybersecurity isn't a compliance check; it's a growth enabler.



executive cyber checklist

- ✓ **Third-party risk protocols in place?**
- ✓ **IR firm retained and briefed?**
- ✓ **MFA implemented across executive accounts?**
- ✓ **Cyber Wellness training for senior leaders?**
- ✓ **Crisis communication plan up-to-date?**
- ✓ **Regular security audits scheduled?**
- ✓ **24x7 Managed Security in place with oversight?**



conclusion

In today's hyper-connected digital economy, growth-focused organizations face an evolving threat landscape that extends far beyond traditional IT boundaries. For executives at mid-market enterprises, cybersecurity is no longer just a technical issue — it's a strategic business imperative.

Cybercriminals are becoming more sophisticated, targeting the supply chain, exploiting deferred maintenance, and zeroing in on high-value executive credentials. Meanwhile, the consequences of a breach — reputational damage, financial loss, and operational disruption — have never been higher.

We highlighted five critical cybersecurity risks every executive should understand and act on now. With practical, boardroom-ready insights and real-world examples, it's designed to help you lead with confidence, resilience, and foresight.



Pillar Technology
P A R T N E R S

Pillar Insights

Explore more insights and resources for security leaders:

Cybersecurity Risks of AI

Actionable roadmap empowering CISOs to assess, prioritize, and accelerate cybersecurity maturity through strategic alignment, governance, and risk-informed decisions.

> AI Risks

Unexpected Emergency

Learn more how we work hand-in-hand with organizations large and small to resolve complex incidents and protect critical data.

> Incident Response

Complete Security Program

Gain insight how we offer a customized cybersecurity program tailored to give control over risk, protect sensitive data, and fortify defenses. How we provide what you need, when you need it.

> Managed Security

Security Leadership & Coaching

Security programs can be overwhelming. Even the most effective leaders benefit having a trusted coach who sharpens strategy, challenges blind spots, and offers a different perspective. Find more information how we help security leaders lead with confidence.

> Leadership & Coaching

Strategic Cybersecurity for Growth-Focused Organizations

At Pillar, we help high-growth companies protect their momentum.

Our approach is proactive, executive-ready, and tailored for the fast-moving challenges facing mid-market healthcare, tech, manufacturing, and PE-backed firms.

Contact Us

Partnering with Pillar means proactive protection, executive-level security leadership, and a pragmatic strategy for cybersecurity aligned with your growth trajectory.

Security starts with a conversation, contact us at:



678-304-9099



info@ptechcyber.com



www.ptechcyber.com



YOUR TRUSTED PARTNER IN MID-MARKET AND HEALTHCARE CYBERSECURITY



Pillar Technology
P A R T N E R S