HOGUE TECHNOLOGY

Cybersecurity Outlook

The 70/30 Trap: Why Most Business Owners Are Spending Their Cybersecurity Money in Exactly the Wrong Way

Abstract

Most businesses still allocate ~70% of their cybersecurity budget to prevention tools (firewalls, antivirus, etc.) and only 30% or less to detection and response. 2025 industry data show this outdated "build a bigger wall" approach fails: 88% of breaches involve stolen credentials that bypass every preventive control. Companies that flip the ratio — moving to roughly 40/40/20 (prevention / detection / response) — detect attacks faster, save millions per incident, and recover with minimal disruption. Two composite real-world examples illustrate the dramatic difference in outcomes. Business owners can protect what they've built more effectively, often at the same or lower cost, by focusing on seeing and stopping intruders quickly instead of hoping the front door holds.

Colonel Doug Hogue, CEO/Founder

doughogue@hoguetechnology.com

Executive Summary

Most businesses still spend ~70% of their cybersecurity budget on prevention tools and only ~30% on detection and response. 2025 industry data shows this no longer works: 88 % of breaches start with stolen credentials that bypass every preventive control.

Companies that rebalance to roughly 40/40/20 (prevention/detection/response) save an average of $1.9 million per incident, cut attacker dwell time from weeks to days, and often pay less overall thanks to lower insurance and faster recovery.

Two composite cases — a large retailer that lost nine figures and a mid-sized manufacturer that stopped attacks in hours — prove the difference.

Bottom line: The fastest way to reduce risk and cost today is to stop overinvesting in walls and start investing in eyes, ears, and a rapid-response team.

The Hard Numbers (All from 2025 Industry Reports)

- **88 % of breaches involving stolen credentials succeed even when every "keep-them-out" tool is in place.** Source: Verizon 2025 Data Breach Investigations Report (DBIR)
- **Companies with strong detection and response saved an average of $1.9 million per breach compared to prevention-heavy organizations.** Source: IBM Cost of a Data Breach Report 2025
- **Organizations that detect intruders internally now do so in a median of 10 days — versus weeks or months when they wait for someone else to tell them.** Source: Mandiant M-Trends 2025

Translation in plain English: Spending most of your money trying to build an unbreakable wall is no longer the most innovative way to protect your company.

Two Composite Stories (Real Patterns, No Real Names)

Story 1 – The large retail chain (composite)

This example combines patterns seen in several well-publicized 2023–2025 breaches (including incidents at UnitedHealth/Change Healthcare, Snowflake customers, and a major pharmacy chain).

A national retailer had spent tens of millions on the latest firewalls, endpoint protection, and cloud security suites — the whole "castle and moat" package. An attacker used a stolen contractor password, lived quietly inside the network for over two months, and left with customer data. The stock dropped roughly $1.4 billion in market value in the days after disclosure.

Story 2 – The 350-person Midwest manufacturer (composite)

This is a blend of outcomes from four actual mid-market manufacturing clients I've reviewed in the last 18 months.

Total annual cyber spend: under $60,000. Instead of buying another expensive wall, they paid about $4,000 a month for 24/7 monitoring and rapid response. Twice in the past year, attackers got in using stolen credentials — and both times the monitoring team spotted and stopped them within 12 hours. Zero ransom paid. Zero downtime.

Same threat landscape. Dramatically different outcomes.

A Simpler, Smarter Way: The 40/40/20 Rule

- 88 % of breaches involving stolen credentials succeed even when every "keep-them-out" tool is in place. Source: Verizon 2025 Data Breach Investigations Report (DBIR)
- Companies with strong detection and response saved an average of $1.9 million per breach compared to prevention-heavy organizations. Source: IBM Cost of a Data Breach Report 2025
- Organizations that detect intruders internally now do so in a median of 10 days — versus weeks or months when they wait for someone else to tell them. Source: Mandiant M-Trends 2025
- Translation in plain English: Spending most of your money trying to build an unbreakable wall is no longer the most innovative way to protect your company.

The Two Questions Every Owner Should Ask This Week

1. Of the money we spent on cyber last year, what percentage went to “keep-them-out” tools versus watching and rapid response?
2. If someone logs in with my stolen password at 2 a.m. on Saturday, how fast will we actually know?

If the answer to #1 is “70/30 or worse” and #2 is “probably weeks — or when the ransom note arrives,” you’re spending exactly like the companies that keep making headlines for all the wrong reasons.

You’ve worked too hard to leave your business exposed to an outdated strategy.

If you’d like an impartial look at your own numbers (no sales pitch, no jargon), drop me a message with your rough spend and split. I’ll tell you, in plain English, where you stand compared to the companies quietly winning.

The wall-building era is over. The new winners focus on seeing trouble fast and shutting it down faster. Everything else is hope dressed up as strategy.

References

- Verizon 2025 Data Breach Investigations Report (DBIR)
- IBM Cost of a Data Breach Report 2025
- Mandiant M-Trends 2025 Report