EXECUTIVE BRIEFING · CYBERSECURITY STRATEGY

The Breach Is Already Inside

Why Organizations Keep Falling Victim — and What AI Changes for Everyone

Dominic Vogel | Cybersecurity Strategist

30-MINUTE EXECUTIVE BRIEFING

CASE STUDY

April 28, 2024: **A Wake-Up Call for Canada**

79 Stores
CLOSED

Across four Western Canadian provinces — overnight

10 Days
DARK

Full retail shutdown; pharmacists filled prescriptions by hand outside locked doors

$25 Million
RANSOM DEMANDED

By LockBit ransomware group — London Drugs refused to pay

Employee Data
STOLEN

Corporate files exfiltrated; 2 years of credit monitoring offered to all staff

> *This was not a small startup. This was a household name with 79 locations, trusted by millions.*

SCOPE OF THE PROBLEM

This Is Not an Isolated Incident

The Numbers
Behind the Headlines

57%

HCLTech 2024–25

And many don't discover the breach until nearly a year after it happens.

01

$57 Billion

Ransomware Reports 2024

Against only $813 million actually paid in ransom — the real cost is operational chaos.

02

90%

Accenture 2025

Most organizations are fighting a new war with old weapons.

03

GLOBAL 2024–2025

ROOT CAUSES

Three Reasons the **Breaches Keep Coming**

1 Brittle Legacy Systems

Outdated infrastructure wasn't designed for today's threat actors. Deferred modernization creates exploitable gaps that attackers know how to find — and use.

- **64% cite legacy tech debt as their #1 barrier to cyber resilience**

2 Leadership Blind Spots

Only **37% of security leaders** say they effectively communicate cyber risk to the C-suite. Cybersecurity is still treated as an IT problem — not a business strategy.

- **87% of CISOs say cyber risk is invisible at the board level**

3 Digital Complexity

Cloud migration, remote work, SaaS sprawl, and AI adoption have **expanded attack surfaces faster than defenses can adapt.** Every new tool is a potential entry point.

- **83% of firms struggle to secure cloud infrastructure**

These three forces interact and amplify each other — London Drugs is a textbook example of all three converging.

Sources: HCLTech 2024–25 · Dynatrace 2024 · Accenture 2025

LEADERSHIP DISCONNECT

The **Dangerous Gap** at the Top

What the C-Suite Believes

- We have an IT security team
- We passed last year's audit
- We have cyber insurance

CONFIDENT — COMFORTABLE — UNAWARE

VS

What the CISO Knows

- **87%** of CISOs say cyber risk is a board-level blind spot
- Only **37%** can effectively brief the board on security posture
- **70%** of executives say security teams speak in jargon, not business terms

ALARMED — ISOLATED — UNHEARD

Cybersecurity is not an IT problem. It is a *leadership* problem.

LEGACY SYSTEMS — DEEP DIVE

Most organizations are fighting a **2026 war** with **2010 weapons.**

— Dominic Vogel

- 64% cite legacy tech debt as top barrier
- 83% of firms struggle to secure cloud infrastructure
- Average breach discovery: nearly 12 months after intrusion

Meet the New Attacker: **Faster, Smarter, Cheaper**

Artificial Intelligence has become a force multiplier for criminals

AI-Generated Phishing

Hyper-personalized, flawless phishing emails at massive scale. **No typos. No red flags.** Indistinguishable from a real CFO.

29 min

Machine-Speed Attacks

Median time from breach to lateral movement. AI compresses the entire attack chain — **recon, exploit, exfiltrate** — before defenders can react.

Malware on Demand

Tools like **FraudGPT** let criminals generate sophisticated malware with zero coding skills. Entry barriers have completely collapsed.

389%

Surge in Ransomware Victims

Year-over-year spike driven by AI-enabled automation. **LockBit** and its successors operate like professional criminal enterprises.

⚠ This is not science fiction — this is the threat landscape your organizations are navigating right now.

Sources: CrowdStrike 2025 · Fortinet 2026 · FraudGPT threat intelligence

The Same Technology **Defending Us**

AI is also the most powerful tool defenders have ever had

1 Threat Detection at Machine Speed

AI systems monitor billions of events per second, catching anomalies no human team could spot. IBM's autonomous systems now detect and respond in **seconds, not hours** — compressing response timelines by orders of magnitude.

Seconds
IBM AUTONOMOUS RESPONSE TIME

2 Predictive Vulnerability Management

AI maps attack surfaces **continuously**, identifies risky patterns, and prioritizes patching before criminals exploit them. No more waiting for annual audits — exposure is monitored and remediated in real time.

24/7
CONTINUOUS SURFACE MAPPING

3 AI-Powered Incident Response

When an attack begins, **agentic AI** can contain the threat, isolate systems, and begin remediation automatically — without waiting for human intervention. With CrowdStrike's 29-minute breakout window, every second counts.

29 min
ATTACKER BREAKOUT WINDOW

The defenders who embrace AI now will be the ones still standing.

RISK INTELLIGENCE

The New Risk Equation Every Leader Must Understand

Cybersecurity is now inseparable from enterprise strategy

29 min

SPEED OF MODERN ATTACK

Median time from breach to full lateral movement across a target network

CrowdStrike 2025

73%

CEO CYBER CONCERN

of CEOs were directly affected by cyber-enabled fraud in the past year

WEF 2025

87%

BOARD BLIND SPOT

of CISOs say cyber risk is invisible at the CEO and board level

Dynatrace Research

90%

COMPANIES UNPREPARED

lack the maturity to defend against AI-enabled threats

Accenture 2025

THE LEADERS WHO KNOW THESE NUMBERS WILL BE THE ONES WHO ACT

What Cyber-Ready Leadership Looks Like

A practical framework for boards and executive teams in 2026

PHASE 01

Speak the Language

Demand business-risk briefings from your CISO — not technical jargon. Translate vulnerabilities into financial and reputational exposure.

CISO ↔ Board Dialogue

1

PHASE 02

Retire the Legacy

Make technology modernization a board-level budget priority. Legacy debt is not an IT issue — it is a business liability.

Board Budget Priority

2

PHASE 03

Test Before Crisis

Commission regular tabletop exercises and red-team simulations. You practice fire drills. Practice breach response.

Red-Team + Tabletop

3

PHASE 04 CRITICAL

Govern AI Proactively

Establish AI governance policies before your adversaries exploit the gaps. **77% of organizations** lag in AI security practices.

AI Governance Policy

4

GOVERNANCE IMPERATIVES — NOT IT RECOMMENDATIONS

EXECUTIVE BRIEFING

What You Take Away Today

5
KEY POINTS

1 **No organization is immune** — London Drugs proves that size and reputation offer no protection from sophisticated attackers.

2 **The causes are predictable** — legacy systems, leadership disconnects, and digital complexity are known problems with known solutions.

3 **AI has permanently changed the threat calculus** — attacks are faster, cheaper, and more convincing than ever before.

4 **AI is also your best defense** — organizations that harness it proactively will be significantly more resilient.

5 **Cybersecurity is a leadership discipline** — not an IT function. Boards and executives set the culture, the budget, and the urgency.

“The question is no longer whether your organization will be targeted.
It is whether you will be *ready*.”

— Dominic Vogel

CONTINUE THE CONVERSATION

SPEAKER
Dominic Vogel

ROLE
President

WEBSITE
vogelleadershipcoaching.com