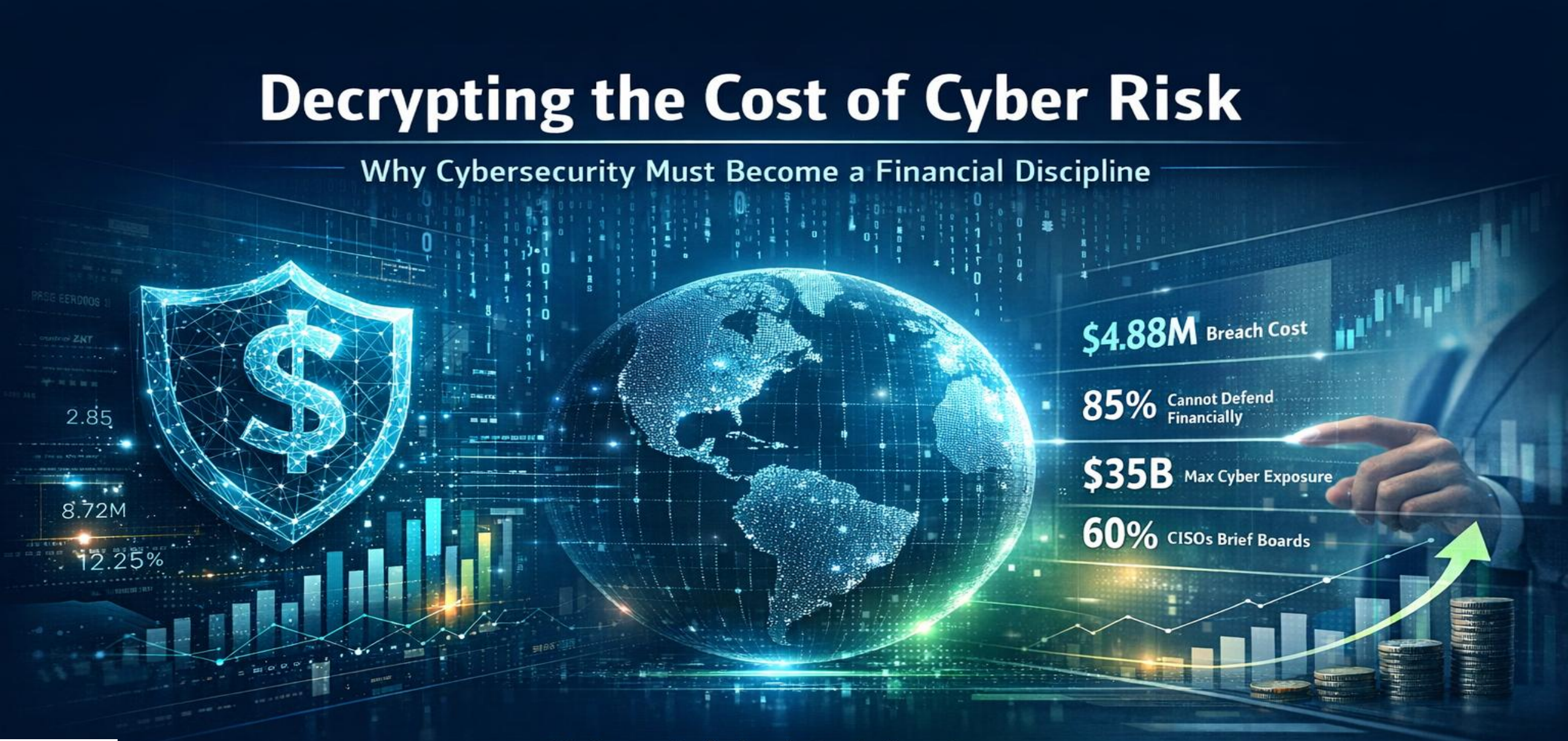
Decrypting the Cost of Cyber Risk

Why Cybersecurity Must Become a Financial Discipline



Oleksandr (Alex) Godzilevsky

Founder, RAP Consulting LLC & CIFER

DECRYPTING THE COST OF CYBER RISK

WHY CYBERSECURITY MUST BECOME A FINANCIAL DISCIPLINE

OLEKSANDR (ALEX) GODZILEVSKY

CYBERSECURITY IMPACT & FINANCIAL ESTIMATION OF RISK (CIFER)

FOUNDER, RAP CONSULTING LLC & CIFER

WHY I BUILT CIFER

Why I Built CIFER

- 24+ years in cyber & national security

- We defend everything… but cannot financially justify anything

- Decisions made without:
  - Quantified loss
  - Financial accountability

➡️ It's not a technology problem
➡️ It's a culture problem

CULTURE PROBLEM

Cybersecurity Has a Culture Problem

- We measure:
  - Alerts
  - Vulnerabilities
  - Compliance
- But not:
  - Financial exposure

Current Culture:

- Activity-driven
- Tool-driven
- Compliance-driven

➡️ Future: Financial accountability

FINANCIAL GOVERNANCE IMPERATIVE

85% of U.S. executives cannot defend cybersecurity decisions financially
— Harvard Business Review

$4.88M average breach cost (~40% reputational damage)
— IBM & Ponemon (2024)

60% of CISOs brief boards 3–4x/year
— World Economic Forum

$35B documented extreme cyber exposure scenarios
— Economic Impact Study

CORE PROBLEM

We Are Asked to Justify What We Cannot Measure

- No financial loss baseline
- No defensible risk position
- Boards receive:
  - Scores
  - Heat maps
  - Compliance reports

➡️ None translate to dollars

GOVERNANCE GAP

The Governance Gap

- No documented financial cyber-risk position
- Weak board engagement
- Reactive vs proactive investment
- Security seen as cost—not risk control

MARKET FAILURE

Why the Industry Has Not Solved This

Vendors optimize for:

- Detection
- Prevention
- Compliance

Not for:

- Financial loss estimation

Result:

Activity ≠ Outcome

Spend ≠ Risk Reduction

WHY THE MARKET CAN'T FIX IT

Why Financial Transparency Doesn't Exist

- Quantification limits vendor pricing power
- Legal liability suppresses modeling
- Pricing hides risk asymmetry
- Compliance ≠ financial resilience
- Ambiguity sustains fear-based sales

THE SHIFT

The Shift That Must Happen

From: Are we secure?

➡️ **What is our financial exposure?**

From: Tools

➡️ **Financial outcomes**

From: Compliance

➡️ **Financial resilience**

INTRODUCING CIFER

CIFER: Cybersecurity Impact & Financial Estimation of Risk

- **Patent-pending methodology**
- **Built on 19 critical risk factors**
- **Translates:**
  - **Threats**
  - **Vulnerabilities**
  - **Controls**

➡️ **Into projected financial loss**

HOW CIFER WORKS

How CIFER Works

- **10 Risk Amplifiers**
- **9 Mitigation Factors**
- **Produces financial loss ratio**

Applied to business revenue

➡️ **Outputs projected financial impact**

IMPACT

What Changes When You Quantify Cyber Risk

- Board-level clarity
- Defensible financial cyber-risk position
- ROI-driven decisions
- Insurance alignment
- Strategic investment prioritization

Q&A / DISCUSSION + CONTACT

Discussion / Q&A

- How are you currently justifying cyber risk to leadership?
- What challenges do you face translating risk into financial terms?
- Where would financial quantification change your decision-making?

https://cifer-decrypt-cost.replit.app

Oleksandr (Alex) Godzilevsky
Founder, RAP Consulting LLC & CIFER

Email: info@rapconsultingllc.com
Cell: 410-340-9816