Leadership Masterclass

How to Communicate Risk in Business Terms
April 28th, 2026

Disclaimer: The views and opinions expressed herein are intended solely for general informational purposes and to support community contributions. They are those of the presenter and do not reflect the official policy, position, or endorsement of PLZ Corp.

Agenda


INTRODUCTION
Why Risk Communication Fails
Translating Risk into Business Impact
Practical Playbook that Works
Driving Decisions in Today's Reality

Pal Vankayalapati
CIO PLZ CORP

A leader in Product Manufacturing
We enable brands to grow and outperform

PLZ CORP

Introduction

As a forward-thinking CIO specializing in cybersecurity and risk management, I lead AI-driven strategies that enhance resilience and fuel business growth. I apply AI/ML and advanced analytics to enable proactive threat detection and risk-informed decisions, while building high-performing teams and positioning security as a strategic business enabler.

Security Fails when it Doesn't Speak Business

- Too technical → not tied to revenue or operations
- Vulnerability talk vs real business impact
- Disconnect between security teams and leadership priorities
- Executives care about growth, continuity, reputation, compliance
- Lack of clarity on why act now

Why Risk Communication Fails

Make Cyber Risk a Business Conversation

- Translate threats → revenue loss, downtime, brand damage
- Ask: “What happens if this fails?”
- Quantify in dollars, time, and customer impact
- Turn security into trust with customers & partners
- Use simple, business-first language

Translating Risk into Business Impact

Focus on What Matters Most

- Prioritize top 3 risks—not 30 findings
- Use real-world scenarios, not technical reports
- Protect employees, customers, and critical systems
- Take practical, high-impact actions (avoid over-complexity)
- Show before → after:
  Risk → action → outcome

Practical Playbook that Works

From Risk Awareness to Business Decisions

- Cyber threats are faster, smarter, targeting mid-market
- AI is changing both risk and defense landscape
- Focus on high-impact actions vs expensive tool sprawl
- Frame decisions as business trade-offs (action vs inaction)
- Prove ROI and build credibility through consistency

Driving Decision in Today's Reality

Balanced use of preventive and reactive measures to safeguard company data

Preventive:

Adequate Training & Protection

Training & Awareness

- Annual Security Awareness training
- Role based security awareness training
- Targeted phishing simulations with training assigned after failures.

Adequate Protection

- **Identity & Access Security**: MFA enforced for all external and privileged access
- **Endpoint Protection & Encryption**: Advanced threat protection with full device encryption
- **24/7 Threat Monitoring & Response**: Continuous SOC-led monitoring across endpoints, network, and logs
- **Network Security & Segmentation**: Controlled access, traffic monitoring, and isolation of critical systems
- **Email& Web protection**: Phishing prevention and blocking of malicious sites and content

Reactive:

Cyber Insurance & Recovery Preparedness

Cyber Insurance

- Cyber insurance

Incident Response Plan

- A documented Incident Response Plan with clearly defined Incident Response Team (IRT) roles and members.

Recovery Preparedness

- Redundant Backups for Disaster Recovery
- Redundant Internet links at manufacturing locations for failover
- Annual live disaster recovery testing.
- Security Operations Center(Cyber Agent) monitors all traffic and escalates alerts to Cybersecurity and Infrastructure teams as needed.

Cybersecurity Risk Management Framework

- Every employee is both a line of defense and a potential risk—security starts with you
- If something feels suspicious, report it to IT—don’t click links or open attachments
- Never share your login credentials—your user ID and password are yours alone
- Cybersecurity is everyone’s responsibility—not just IT or the security team

Cybersecurity starts with you

Questions


Thank you