

CYBER RISK **WEBINAR**

Are You Prepared?



Envision
Technology Advisors, LLC



TODAY'S SPEAKERS

KLR



Jason Albuquerque
COO

 999 Main St., Suite 703
Pawtucket, RI 02860

 401-272-6688

 jason.albuquerque@envisionsuccess.net

 www.envisionsuccess.net



Manuel Lobao
Director of Cybersecurity &
Compliance Services

 999 Main St., Suite 703
Pawtucket, RI 02860

 401-272-6688

 manuel.lobao@envisionsuccess.net

 www.envisionsuccess.net



What We'll Cover



The 2027 Threat Landscape

The 2027 Risk Horizon: Navigating the Intersection of Growth and Volatility

Reducing Cybersecurity Risk

The Weaponization of Intelligence: AI Agents, Deepfakes, and Integrity

Preparing for a Cyber Incident

Securing the Extended Ecosystem: Supply Chains, Software Integrity, and the Quantum Clock

The Executive 30-60-90 Day Action Plan

From Defense to Resilience: Redefining Fraud, Liability, and Business Continuity

Q&A

The Securing 2027 Blueprint: What Boards and Executives Must Do Monday Morning

KLR

The 2027 Threat Landscape

- AI compresses attack timelines
- Identity is the perimeter
- Agentic AI creates new access risks
- Post-Quantum Preparedness
- Third-parties expand the blast radius
- Back To The Basics
- Resilience is the new benchmark



Reducing Cybersecurity Risk

- Prioritize risk by business impact
- Secure identity before adding tools
- Zero-Trust
- Validate controls with real world simulated attacks
- Operationalize NIST CSF fundamentals
- Build a measurable security culture





Preparing for a Cyber Incident

- Establish governance and decision-making framework in advance
- Out of band and crisis communication playbook
- Business impact analysis and recovery planning
- 3rd party and retainer readiness
- Test the plan with a tabletop simulation
- Validate recovery, not just restoration



The Executive 30-60-90 Day Action Plan

- **Days 1–30:** Assign ownership and baseline your cybersecurity risk
- **Days 1–30:** Contain obvious critical exposures
- **Days 31–60:** Close identity, data and visibility gaps
- **Days 61–90:** Exercise response and recovery
- **Ongoing:** Govern measurable risk reduction & Continuous Improvement



You Engaged, We Listened

- AI-driven threats and resilience?
- Immediate incident actions?
- Right-sized security for small organizations?
- Google Workspace and data protection?



Five questions every Board should ask

- Which services are critical and how long can they be unavailable?
- Where are our largest identity, data, and third-party exposures?
- Can we detect, contain, and communicate a material incident quickly?
- Have we proved recovery from clean, isolated backups?
- Who owns each material risk, decision, and remediation deadline?



AI-era resilience starts with architecture

- Assume attacks move at machine speed
- Keep critical recovery paths under your control
- Prioritize Zero Trust then a data-protection
- Govern every AI agent, connector, and data source
- Test new AI exposure before production



Practical security starts with the environment

- Start with inventory, identity, updates, endpoint protection, data governance and tested/secured backups
 - Suspect an attack? Connect, Isolate, Preserve, and Activate the plan
 - Small business resilience strategy, managed outcomes not large platforms
 - Secure cloud infrastructure through identity, sharing, and admin controls
 - Match tools to risk, support capacity, and recovery needs





Open Q & A



Take-Away Resources

- **NIST CSF**

<https://www.nist.gov/cyberframework>

- **NIST AI RMF**

<https://www.nist.gov/itl/ai-risk-management-framework>

- **NIST Incident Response Framework**

<https://csrc.nist.gov/projects/incident-response>

- **Envision Security Services Page**

<https://envisionsuccess.net/services/cybersecurity>





THANK YOU

————— Let's Keep In Touch —————



MANUEL

LOBAO

*Director of Cybersecurity
& Compliance Services*



JASON

ALBUQUERQUE

COO