

► The Future of Risk
Management –
Adapting to a New
Era of Threats

THERAPY FOR SECURITY



> whoami

- Aspiring photographer
- Proud Slytherin
- CISO + jack of several trades
- <https://linkedin.com/in/whoami>



Is risk
management
working?



New cast, same issues

- We constantly face the **distraction cycle** of shiny object syndrome and risk reporting theater
- Incident fatigue is a reality. We need to make leaders care about risk that despite incidents occurring daily without much consequence
- Human error still accounts for the majority of successful attacks
- Just patch already!





Risk ownership is dysfunctional – who owns it?

- IT owns the assets, not the risk decisions
- Security finds the risks, but cannot mandate fixes
- Business creates the risk, but doesn't manage them
- Compliance reports, but doesn't drive outcomes



$$f(\text{risk}) = \text{Security}$$

Exhaustive Security Checklists

Security checklists often cover all possible threats but can become overly detailed and rigid.

Dynamic Cybersecurity Reality

CISOs face constantly evolving threats that require flexibility beyond fixed checklists.

Need for Adaptable Approaches


Bridging the gap calls for adaptable security strategies that evolve with emerging risks.

► Is it all doom
and gloom?





What can we actually do?

- Don't forget the foundations over the shiny toys
 - Build partnerships and establish JOINT ownership of risk
 - Frame for the business. “We have a 23% chance of a 4+ hour outage this month” instead of “We have 1,000 critical vulnerabilities OMG”
 - Develop a risk framework that maps technical risks to business processes, with as much quantifiable impact as possible.
 - Build outcome-driven controls. E.g. Prevent unauthorized access Authentication controls
MFA/SSO
 - Automate the basics, and implement continuous assurance to validate risk posture in real-time
- 

ANY QUESTIONS?

imgflip.com