Building Enterprise Cyber Resilience Capabilities for Modern Network

ISSA-NOVA Meeting

Reston, Virginia

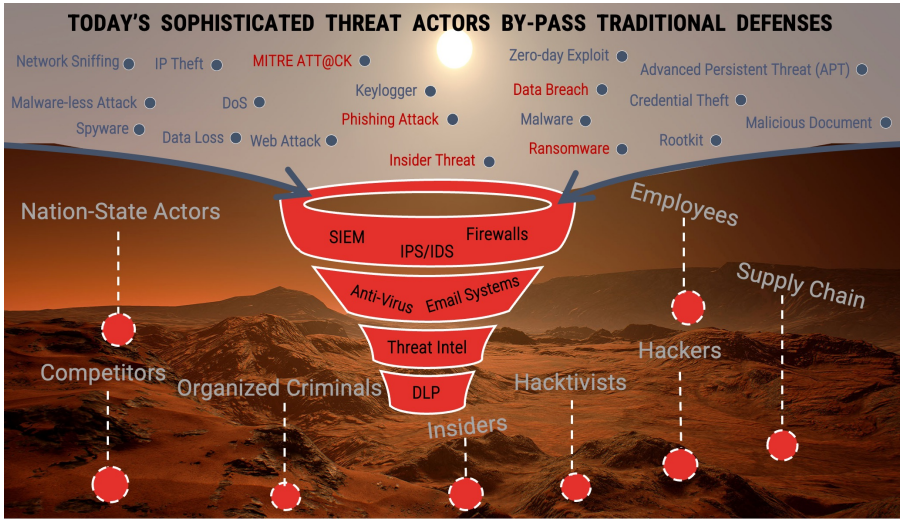
Innocent "Inno" Eroraha, CISSP-ISSAP, ISSMP, CISM, CISA, CHFI, CCSA, CCSE
Founder & CEO
NetSecurity Corporation
Dulles, Virginia, USA

netSecurity®

February 15, 2024

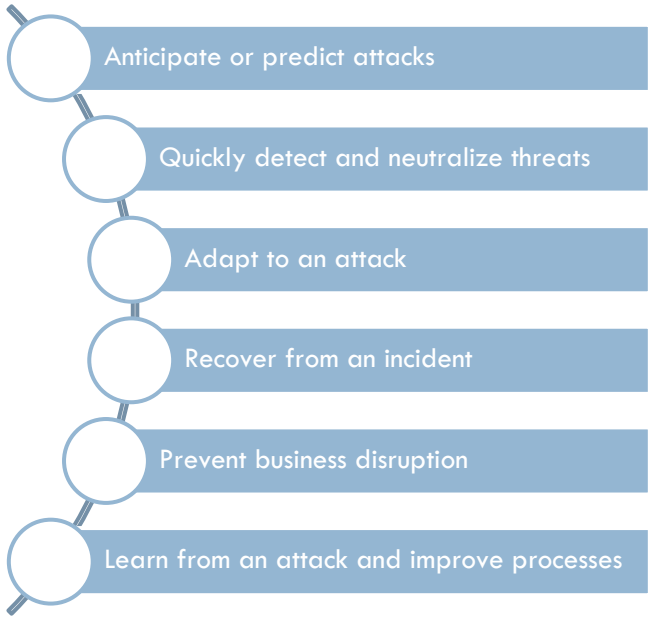
The Threat Landscape

- The ever-evolving cyber threat landscape
- Increasing frequency and sophistication of attacks
- Financial losses, data breaches, and reputational damage
- Importance of proactive cyber resilience strategies



What is Cyber Resilience?

- The ability to anticipate, withstand, recover from, and adapt to cyber attacks
- Holistic approach encompassing people, processes, and relevant technologies
- Continuous improvement and learning from previous incidents
- Building a security awareness culture



Key Pillars of Cyber Resilience

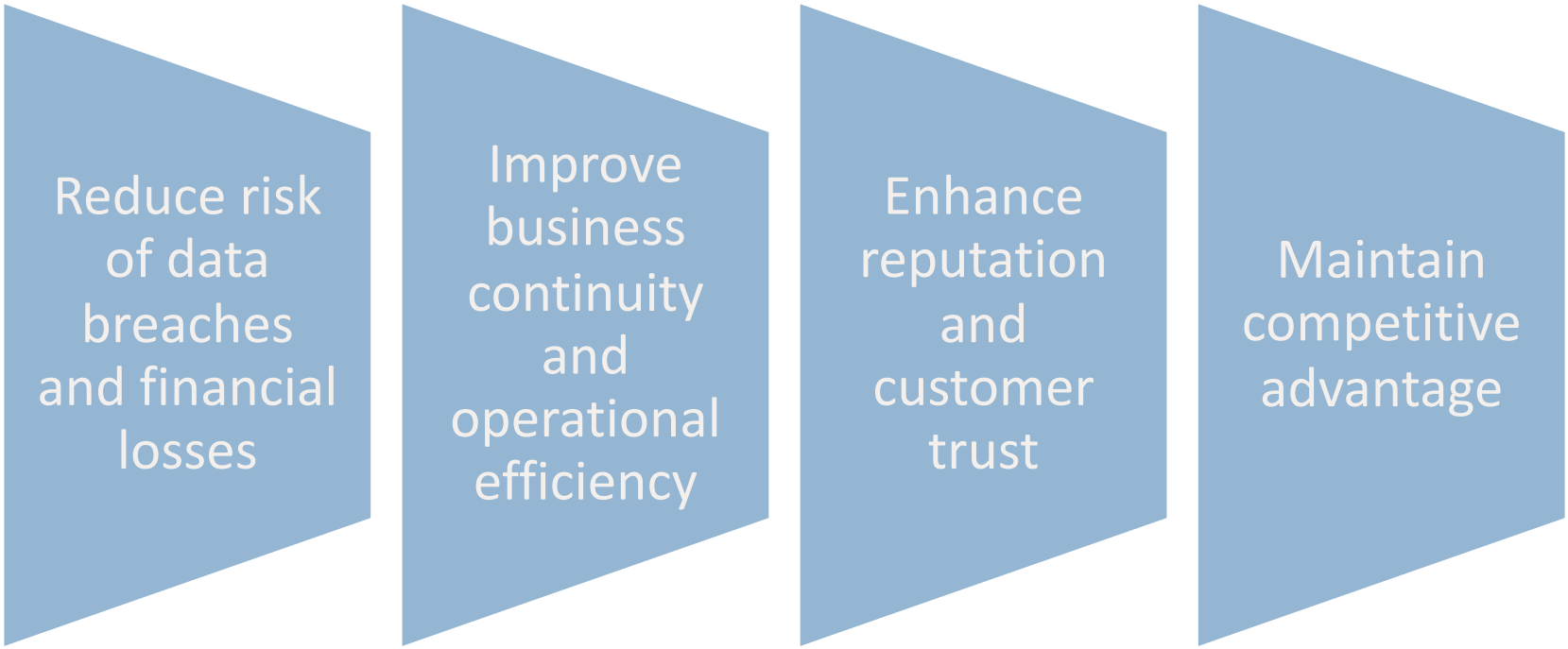
People: Training employees on cyber security best practices, fostering a security-conscious culture

Processes: Implementing clear security policies, incident response plans, and risk management frameworks

Relevant Technologies: Utilizing robust (endpoint) security tools, vulnerability management solutions, and data encryption

Security Culture: Promoting a culture of collaboration, communication, and transparency regarding cyber security

Benefits of Building Cyber Resilience



Building a Cyber Resilience Program

Conclusion


Cyber resilience is an essential investment for any organization
Proactive approach protects your business, data, and reputation
Invest in solutions and practices specific to modern network challenges
Start building your cyber resilience program today