BACKBOX

A CHECKLIST TO **FOSTER COLLABORATION** AND **BUILD CYBER RESILIENCE**

To strengthen your organization's cyber resilience, create a collaborative environment between ITOps and SecOps teams. **Here's a checklist of five best practices:**

ESTABLISH **SHARED GOALS.**

A strong relationship starts with a shared understanding of protecting the organization's assets and data and maintaining confidentiality, integrity, and availability. This helps establish priorities, clarify roles, and identify areas of collaboration for mutual success.

HAVE A COMMON WAY TO **ASSESS AND MANAGE RISK.**

Network teams focus on operational risk related to network infrastructure availability and performance. Security teams focus on incident prevention and risk mitigation to keep the business moving forward. Developing a common way to assess and manage risk ensures both teams work together in the business's best interests.

BECOME PARTNERS **IN COMPLIANCE.**

Organizations often need to work on collaborating for compliance. During audits, the security team requests reports from the network team, leading to rushed responses. Work together to implement controls and processes that meet legal, industry, and internal requirements, then leverage audit tools to help maintain secure and compliant systems.

BRING IT FULL CIRCLE WITH **INCIDENT RESPONSE.**

Despite best efforts, incidents happen. Cyber resilience requires a shared plan that both teams trust to maintain business continuity and integrity. When something happens, you will have established how to investigate, contain, remediate, and restore normal operations.

REMOVE **BUDGET BARRIERS.**

Coordinating security and IT operations is crucial for cyber resilience. It highlights overlooked areas in IT operations that are essential for security. Managing network device vulnerabilities is foundational, requiring funding for automation tools.

Strengthening cyber resilience is the best way to mitigate the impact of cyberattacks.
Coordinate SecOps and ITOps to ensure network availability and prevent incidents for a more cyber-resilient organization.