MARSH

# Lessons learned from Cyber Incident Response

A apresentação mostra por que uma estratégia centrada em evitar violações já não é realista. Para a alta direção, a prioridade é preparar a organização para resistir, responder e se recuperar rapidamente: governança de crise, ativos críticos identificados, continuidade, backups protegidos, cenários testados e decisões pré-aprovadas.

**América Latina: alvo de ataques**

A região tornou-se um alvo atraente para grupos sofisticados. Os ataques de ransomware na LAC passaram de 302 em 2023 para 432 em 2025. O Brasil concentra 32%, o México 17% e a Argentina 12%.

**Ransomware: prioridade executiva**

Os ataques de ransomware foram classificados como a principal preocupação dos CISOs em 2026. A perda média global atinge USD 1,53 milhão, sem considerar pagamentos de extorsão, e 49% das empresas afetadas pagaram a extorsão.

**Recuperação: o desafio crítico**

Apenas 16% das organizações conseguem se recuperar de um ataque de ransomware em menos de um dia. Os RTO/RPO devem ser validados diante de cenários catastróficos, e não apenas frente a interrupções operacionais convencionais.

**Erros que aumentam o impacto**

As falhas mais críticas incluem planos não testados, backups sem monitoramento, ausência de continuidade, desconhecimento da superfície externa, inventário tecnológico incompleto e falta de pré-aprovação para ações de alto impacto.

**Resposta como ciclo integral**

A preparação deve abranger prevenção, testes, resposta e pós-incidente: avaliação de capacidades, planos e protocolos, simulações de crise, testes de Red Team, análise forense, gestão de sinistros e lições aprendidas.