MARSH

Calculating Cybersecurity Return on Investment

A gestão do risco cibernético deve passar da intuição para decisões baseadas em dados. A Marsh combina dados de seguros, incidentes, sinais externos, dark web e análises de controles para estimar exposição, priorizar investimentos e fortalecer a segurabilidade. Para a Diretoria, a chave é identificar quais controles reduzem mais risco, onde investir primeiro e como conectar cibersegurança com continuidade, resiliência e proteção financeira.

1 **Os modelos ajudam a decidir melhor**
Eles não preveem o futuro com certeza, mas organizam dados complexos, comparam cenários e priorizam investimentos de acordo com o impacto esperado em risco, perda e segurabilidade.

2 **O MFA deve ser implementado sem brechas críticas**
Qualquer MFA é melhor do que não ter MFA, mas os métodos resistentes a phishing reduzem mais o risco. Exceções em contas administrativas ou por localização podem enfraquecer o controle.

3 **EDR reduz a probabilidade de violação**
Um aumento de 25% na implementação de EDR está correlacionado com uma redução de 2% a 3% na probabilidade de violação. Os benefícios completos são observados com 75%–100% de implementação.

4 **A dark web e os sinais externos antecipam a exposição**
Hallazgos en mercados de dark web se asocian con tasas de pérdida de 8,69% frente a 3,61% sin hallazgo. Credenciales expuestas y señales OSINT también elevan la probabilidad de pérdida.

5 **A segurabilidade exige controles comprováveis**
MFA, EDR, backups probados, PAM, gestión de parches, respuesta a incidentes, formación y gestión de proveedores digitales son controles clave para mitigar riesgo y sostener capacidad de seguro.

Quantificar o risco cibernético permite à Diretoria priorizar investimentos, demonstrar maturidade perante as seguradoras e fortalecer a resiliência financeira e operacional da organização.