MARSH

Calculating Cybersecurity Return on Investment

La gestión del riesgo cibernético debe pasar de la intuición a decisiones basadas en datos. Marsh combina datos de seguros, incidentes, señales externas, dark web y análisis de controles para estimar exposición, priorizar inversiones y fortalecer la asegurabilidad. Para la Dirección, la clave es identificar qué controles reducen más riesgo, dónde invertir primero y cómo conectar ciberseguridad con continuidad, resiliencia y protección financiera.

1 **Los modelos ayudan a decidir mejor**
No predicen el futuro con certeza, pero ordenan datos complejos, comparan escenarios y priorizan inversiones según impacto esperado en riesgo, pérdida y asegurabilidad.

2 **MFA debe implementarse sin brechas críticas**
Cualquier MFA es mejor que no tener MFA, pero los métodos resistentes al phishing reducen más el riesgo. Las excepciones en cuentas administrativas o por ubicación pueden debilitar el control.

3 **EDR reduce probabilidad de brecha**
Un incremento de 25% en despliegue de EDR se correlaciona con una reducción de 2% a 3% en probabilidad de brecha. Los beneficios completos se observan con 75%–100% de despliegue.

4 **La Dark web y señales externas anticipan exposición**
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 **La asegurabilidad exige controles demostrables**
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.

Cuantificar el riesgo cibernético permite a la Dirección priorizar inversiones, demostrar madurez ante aseguradoras y fortalecer la resiliencia financiera y operativa de la organización.