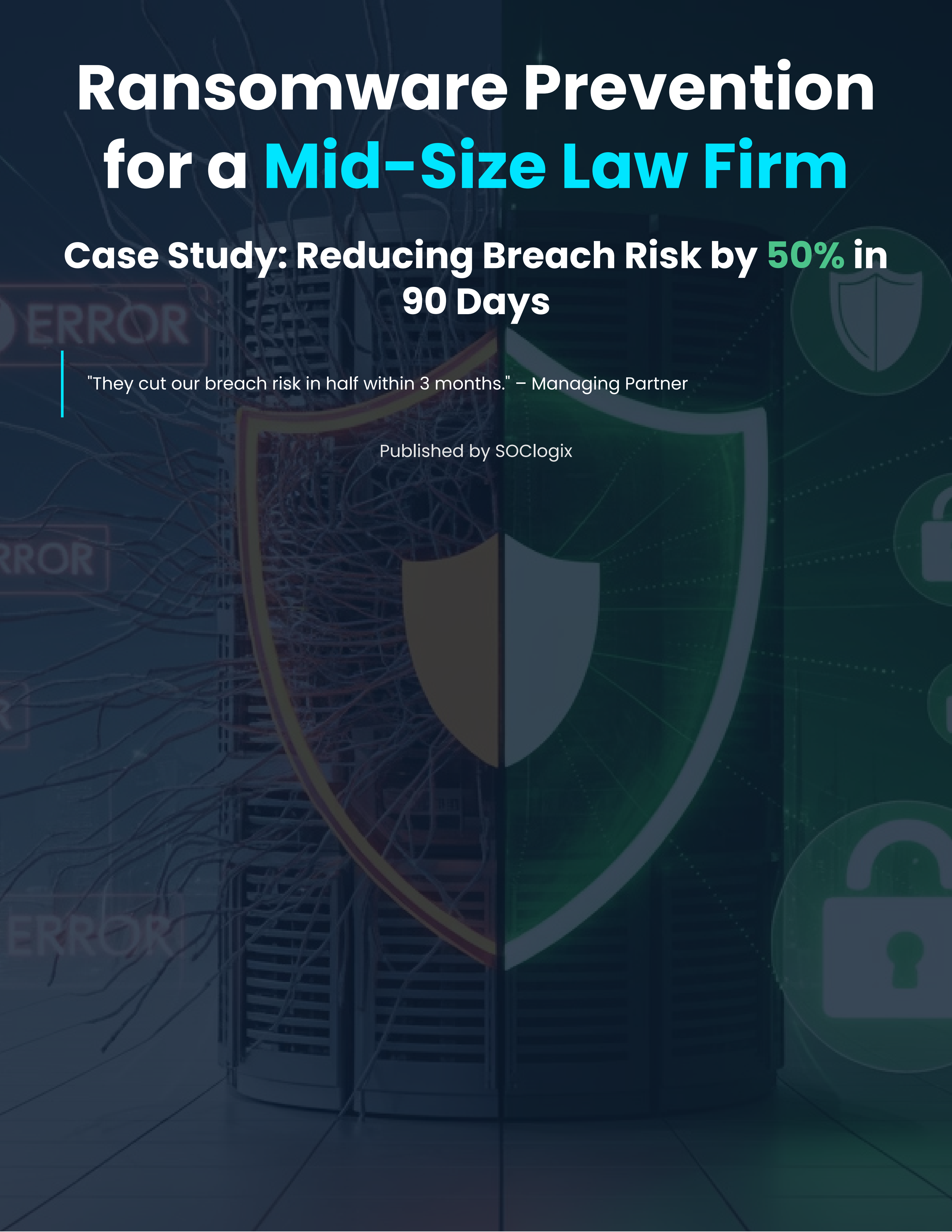
Ransomware Prevention for a Mid-Size Law Firm

Case Study: Reducing Breach Risk by 50% in 90 Days

> "They cut our breach risk in half within 3 months." – Managing Partner

Published by SOClogix



Executive Summary

A mid-size law firm with 150 employees faced a rapid rise in ransomware threats targeting sensitive client case files. Over six months, phishing emails and malicious attachments bypassed outdated security tools, exposing the firm to potential operational downtime and reputational damage.

We implemented a comprehensive 90-day defense program combining advanced threat monitoring, upgraded phishing protection, and targeted staff training. This layered approach reduced the firm's breach risk score by 50% within three months.

Key results:

0

Ransomware Incidents

Zero successful ransomware incidents in the past 12 months

0.82%

Phishing Click Rate

Reduced from 33% to 0.82%

100%

Ransomware Blocked

All attempted ransomware payloads blocked before execution

4.5

Response Time

Incident response time improved from 47 minutes to 4.5 minutes

The project not only addressed immediate risks but also established long-term security resilience, meeting both operational and compliance requirements.

Client Profile

Industry

Legal Services

Employees

150

Locations

3 offices across Maryland DC

Core Systems

Cloud-based document management, email, case management software

Compliance Requirements

ABA Cybersecurity Guideline

The Challenge

The law firm saw a 200% increase in ransomware-related activity over a 6-month period. Attackers targeted high-value legal files containing sensitive client data.

Pain points identified:

Frequent phishing attempts

Averaging 120 suspicious emails per week

Weak filtering

Legacy email gateway missed 47% of malicious attachments

Limited monitoring

No centralized visibility into endpoint threats

Untrained staff

No structured phishing awareness program in place

High breach cost risk

Estimated potential downtime cost per day of $180,000

Leadership feared both financial loss and reputational damage if attackers succeeded.

The Solution

We designed and deployed a 90-day ransomware defense program:

1. Threat Monitoring and Incident Response

- Implemented a full soc package with AI-driven detection for ransomware behaviors
- Established a 24/7 Security Operations Center escalation protocol
- Linked all endpoints to a centralized SIEM for correlation and alerting
- Set up automated containment rules to isolate infected devices within seconds

1. Phishing Defense Upgrade

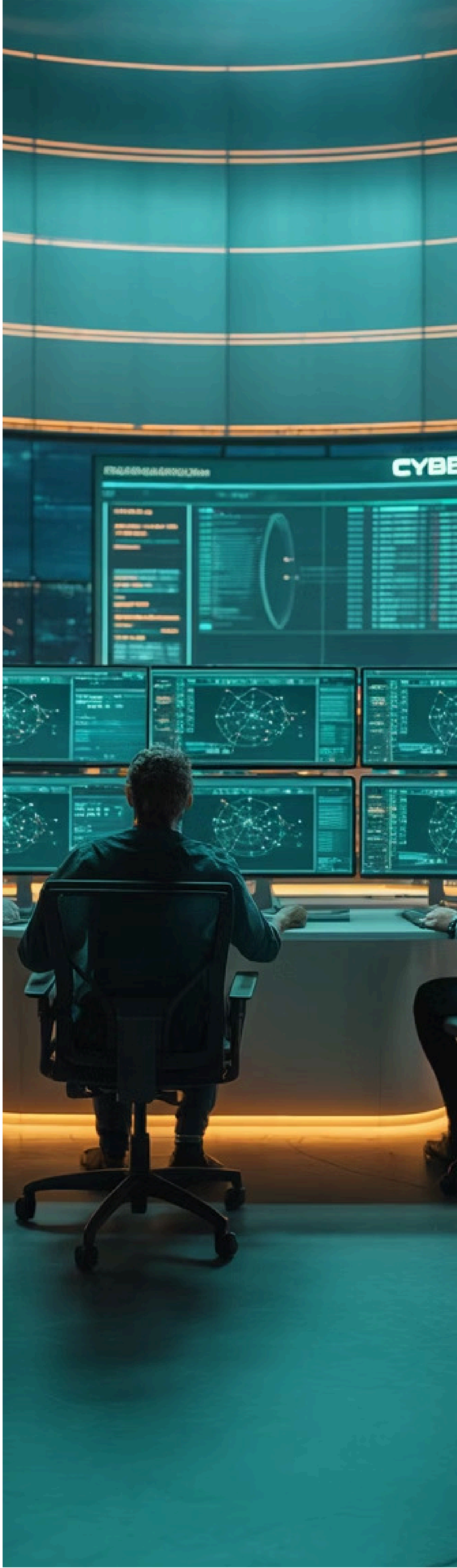
- Replaced outdated email filtering with INKY e-mail security solution
- Added attachment sandboxing to block suspicious files before delivery
- Configured DMARC, SPF, and DKIM to reduce spoofing

2. Security Awareness Training

- Delivered interactive phishing training to all staff, including attorneys and paralegals
- Launched simulated phishing campaigns every 2 weeks to measure progress
- Created a "Report Suspicious" button in Outlook to streamline reporting

3. Policy and Process Reinforcement

- Updated incident response playbook with ransomware-specific workflows
- Conducted tabletop exercises with leadership to rehearse breach scenarios



How the Numbers Stack Up

50%

Risk Reduction

Breach risk score dropped from 76 to 38

0.82%

Phishing Click Rate

Fell from 33% to 0.82%

32

Blocked Attacks

Attempted ransomware payloads blocked pre-execution

0

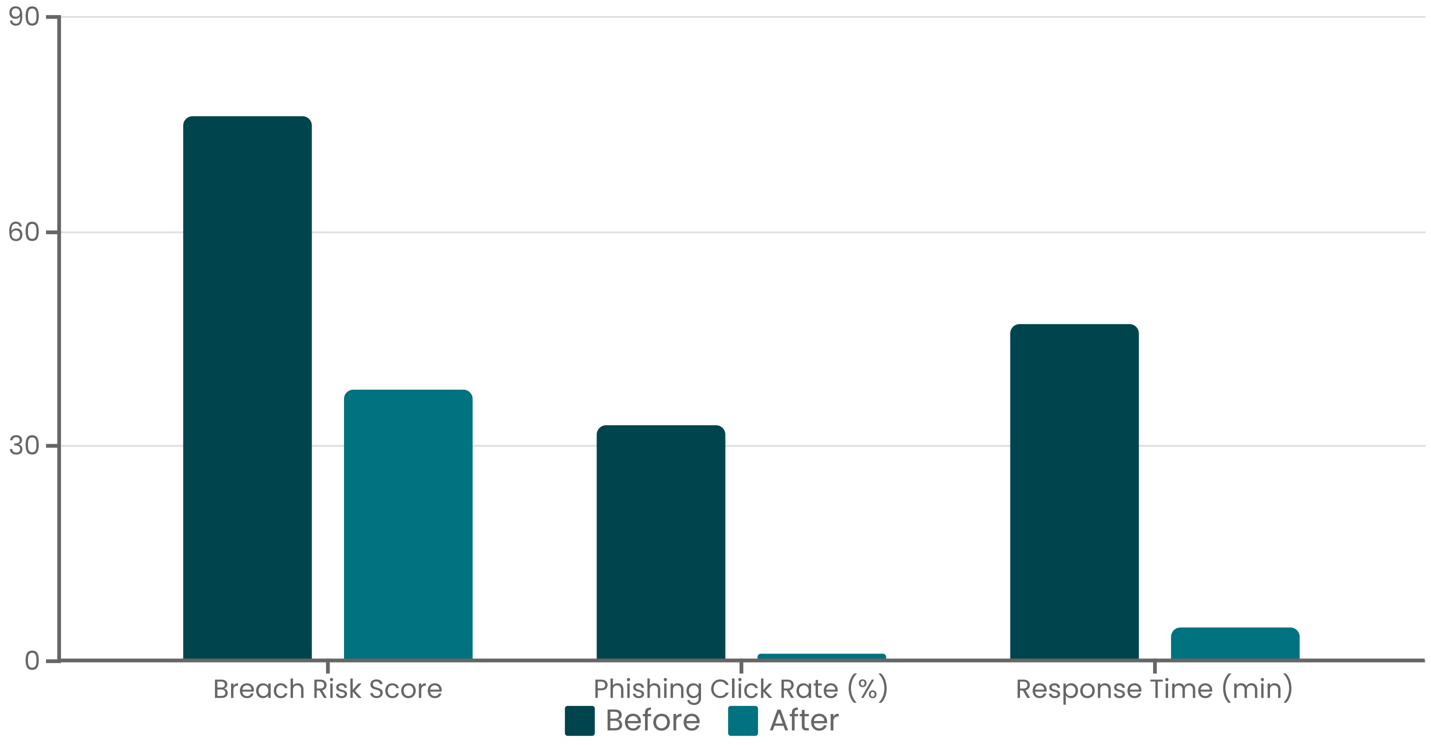
Successful Attacks

Zero successful ransomware incidents in the past 12 months

4.5

Response Time

Incident response time reduced from 47 minutes to 4.5 minutes



Client Feedback

> "They cut our breach risk in half within 3 months. Our team is more confident, and our systems are better protected." – Managing Partner, [Firm Name]

Key Lessons for SMBs

Balanced Defense

Ransomware defense requires both technology and human vigilance

Speed Matters

Fast detection and automated containment can prevent major data loss

Culture of Security

Ongoing training builds a security-aware culture that reduces mistakes

Want to learn how we can help your organization reduce ransomware risk? Contact SOClogix today for a free security assessment.