BLACKSWAN CYBERSECURITY

State Bar of Texas Ransomware Attack

A Lesson for Legal Firms

Overview—Could This Ransomware Breach Have Been Prevented?

In mid-2023, the State Bar of Texas experienced a ransomware attack at the hands of the INC group—a relatively new but highly effective cybercrime syndicate. The result? A breach that compromised names, Social Security numbers, financial data, and other sensitive information belonging to attorneys and staff.

This was more than an inconvenience. It was a reminder that the legal profession is squarely in the crosshairs of modern cyber threats. And the lessons learned here carry urgent relevance for law firms and legal institutions everywhere.

A Breach Breakdown: What Went Wrong?

Based on public disclosures and INC's known tactics, several key points of failure likely contributed to the success of the attack:

1. Spear Phishing

INC ransomware operators have a history of using highly targeted phishing emails. These messages trick staff into clicking malicious links or downloading attachments that open the door to your network. Legal professionals, due to their public-facing roles and high-value data, are frequent targets.

2. Unpatched Vulnerabilities

Known vulnerabilities in software—like **CVE-2023-3519**, which INC is believed to have exploited—are one of the lowest-hanging fruits for attackers. When security patches are delayed or missed, you're essentially leaving the front door unlocked.

3. Lack of Real-Time Monitoring

The breach wasn't detected until the data was already exfiltrated. Without 24/7 monitoring, there was no opportunity to stop the attack midstream or limit its impact.

How Blackswan Cybersecurity Could Have Stopped It

At Blackswan, our services are designed to close these exact gaps—before they become front-page news. Here's how:

24/7 Security Monitoring

- Our team actively monitors network activity around the clock, identifying suspicious behavior before it becomes a crisis.
- We don't just wait for alerts—our SOC analysts investigate anomalies in real time and take action immediately.

855-BLK-SWAN
contact@blackswancybersecurity.com
blackswancybersecurity.com

Vulnerability Management

- Regular scanning and patch verification ensures your systems are hardened against known exploits like the ones INC used.
- We help legal firms prioritize updates based on actual risk—not just available patches.

Phishing Defense & User Training

- Our simulations and awareness programs reduce your firm's exposure to social engineering.
- We test staff regularly and provide training that sticks, not just check-the-box compliance.

Incident Response Planning

- We prepare your firm for the worst-case scenario, so even if attackers gain a foothold, the damage is contained quickly.
- Rapid response reduces downtime, legal exposure, and reputational fallout.

Why Law Firms Shouldn't Wait

Legal organizations hold extremely sensitive information—case strategies, client financials, privileged communications. Cybercriminals know this. They know that a single breach can shake client trust, trigger lawsuits, or lead to ethics complaints.

That's why the legal industry is an increasingly common target. And that's why passive cybersecurity measures are no longer enough.

Final Thoughts

What happened to the State Bar of Texas could happen to any legal organization without a modern cybersecurity partner in place. But it doesn't have to.

Blackswan Cybersecurity exists to make sure your firm stays secure, compliant, and resilient—no matter what threat actors are out there. Let's make sure your firm doesn't become the next headline.

If you're experiencing a security incident or breach, contact us immediately: 855.BLK.SWAN (855-255-7926)

855-BLK-SWAN
contact@blackswancybersecurity.com
blackswancybersecurity.com