CAN YOUR FIRM FIND AN ACTIVE DATA BREACH BEFORE CLIENT ASSETS ARE AT RISK?

80/100

largest law firms breached since 2011

Source: Legal Tech News

19%

of breaches are self-detected

Source: Trustwave in Computerworld UK

Can your firm pass a client security audit without the means to quickly and accurately detect an active data breach?

79%

of enterprises had a security incident in the past 12 months.

47%

said new security technology is a priority

Source: survey by PwC, CERT, Carnegie Mellon Software Engineering Institute and U.S. Secret Service

$5 TO 40,000,000

Cyber Insurance coverage by most large firms

$1 TO 10,000,000

Cyber Insurance by Mid-sized firms

Source: Global cash access in Bloomberg article

4 TOP REASONS WHY EXISTING SECURITY CAN'T SPOT AN ACTIVE ATTACKER

1. Too much focus on prevention. Preventative security is essential but not sufficient. A motivated cybercriminal will find a way into your network.
2. Hooked on Malware – most "detection" solutions today are really preventative security looking for statically defined signs of malicious software.
3. Drowning in Security Alerts. The hundreds or thousands of daily alerts are beyond anyone's ability to find a real indication of a breach
4. Lack of true detection of breach behavior – no means to see the tel-tale operational behaviors of an intrusion.

WHAT'S AT STAKE?

- Client's confidential material information
- Intellectual property
- Case strategies and supporting documents
- Internal emails

72%

of firms have not assessed and scaled the cost of a data breach based on the information it retains.

Source: Marsh, More Cyber Preparedness Needed

LIGHTCYBER

LIGHTCYBER.COM • (844) 560-7976