BULLWALL FOR THE LEGAL SECTOR

Ransomware attacks increasingly target the sensitive data that law firms manage. In the UK, successful cyber attacks against law firms surged by 77%, rising from 538 incidents in 2023 to 954 in 2024. This escalation is mainly due to the valuable personal and financial information these firms hold, which attackers use for ransom demands or sell on the dark web.

A SUCCESSFUL RANSOMWARE ATTACK DOES MORE DAMAGE THAN SIMPLY REDUCING THE BANK BALANCE.

The most obvious impact of a ransomware attack is financial. However, this is often the least costly impact of an attack that an organization faces. For instance, In 2021, Campbell Conroy & O'Neil, a U.S. law firm representing major corporations like Apple and Boeing, was hit by a ransomware attack, exposing sensitive client data and leading to legal repercussions. The reputational damage of this attack was crippling, even before the firm factored in the loss of revenue and recovery costs.

WHY BULLWALL?

BullWall provides a specialized ransomware containment solution that protects legal organizations from ransomware that has bypassed their preventative security solutions.

By instantly detecting and halting ransomware attacks before attackers can encrypt or exfiltrate data, BullWall protects you from not only the financial impact of an attack but also the loss of reputation that an attack would cause.

77%

surge in ransomware attacks against the legal sector in the last 12 months

$2.47M

is the average ransomware demand

Today's Family Lawyer

Comparitech

> ***Ransomware resilience is now essential.*** *Cybersecurity teams must be ready to contain and recover swiftly, recognizing that blocking every threat is no longer possible.*
>
> **BRIAN MURPHY**
> Head of Cybersecurity at MJ Flood Technology

HOW LEGAL ORGANIZATIONS BECOME A RANSOMWARE TARGET

PHISHING EMAILS

99%

of the UK's top 100 law firms lack sufficient measures to protect themselves against email fraud, indicating widespread susceptibility to phishing attacks.

UNPATCHED SOFTWARE & VULNERABILITIES

<!>

In 2023, attackers used the MOVEit file transfer vulnerability to breach multiple law firms.

INSIDER THREATS (MALICIOUS OR NEGLIGENT EMPLOYEES)

60%

of identified data breaches in the UK legal sector were caused by insiders, per data from the UK's Information Commissioner's Office.

THE IMPACT

The impact of a ransomware attack has far-reaching consequences for legal firms, which makes the initial financial cost seem almost trivial by comparison.

REPUTATIONAL DAMAGE

A ransomware attack on a law firm can severely damage its reputation, leading to a loss of client trust, as clients may seek their legal services elsewhere due to confidentiality concerns. If the breach results in the public exposure of sensitive information, it can attract widespread media attention, further tarnishing the firm's image. Even after recovery, the lasting impact on the firm's reputation may cause long-term client loss, especially in industries where confidentiality is critical.

LEGAL AND COMPLIANCE CONSEQUENCES

If sensitive client data is exposed or compromised in a ransomware attack, the firm could face penalties for violating data protection laws such as GDPR or HIPAA. Clients may also file lawsuits for failing to protect their data, especially if it results in financial or reputational harm. Additionally, regulatory bodies may initiate investigations, potentially imposing fines or requiring the firm to revise its cybersecurity practices.

LOSS OF SENSITIVE INFORMATION

A ransomware attack on a law firm can compromise sensitive data, such as legal case files, financial information, and intellectual property, leading to severe consequences for both the firm and its clients. If private client information is exposed, it can undermine attorney-client privilege, a fundamental right in legal practice. Additionally, the loss or corruption of critical case files and legal documents can disrupt ongoing litigation, causing delays and potentially negatively affecting case outcomes.

WHAT IS RANSOMWARE RESILIENCE?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.

PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.

CONTAINMENT

Minimize the impact to business operations when ransomware gets through, and significantly reduce recovery efforts.

RECOVERY

Resilient organizations recover quickly to limit operational downtime and return stronger.

BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

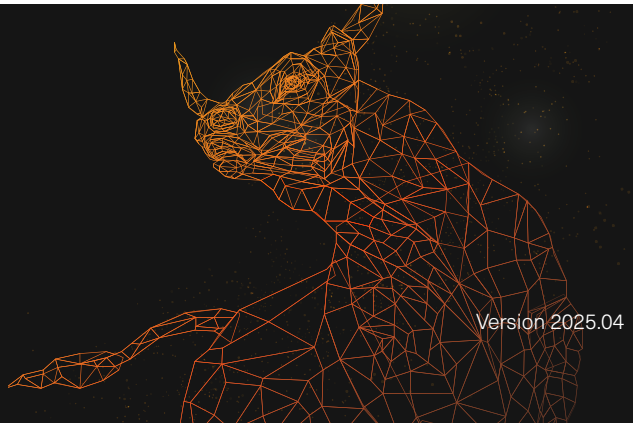
Phishing emails are the easiest way for cybercriminals to get in and access the valuable data that law firms possess.	**Once the payload triggers, BullWall instantly isolates and quarantines the user** and stops the attack.
Known weaknesses and unpatched systems are easy targets for ransomware attackers.	**BullWall addresses unpatched software and systems** to protect the legal sector from ransomware.
The actions of associates and staff, either knowingly or unintentionally, can represent a threat to the organization.	**BullWall protects against insider threats,** whether they are malicious or unintentional.

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware.

Learn more at www.bullwall.com.

BULLWALL



Version 2025.04