Blumira PRESENTS

THE TRUE COST OF RANSOMWARE

The actual ransom is only a fraction of the cost of a ransomware attack.

Several factors come into play:

DOWNTIME

Downtime and disrupted business operations means a loss in revenue, especially for companies without a disaster recovery plan. **Downtime costs related to ransomware are on average nearly 50 times greater than the ransom, according to a Datto study.**

DAMAGE TO REPUTATION

A ransomware attack can make customers feel uneasy, leading to damaged reputation, and subsequently, customer churn. **86% of people are less likely to deal with companies that experienced a data breach, according to a Semafone study.**

CUSTOMER COMMUNICATION

Companies must follow up with their affected customers after a ransomware attack, and cover costs related to credit monitoring and identity protection services.

LEGAL COSTS

If customer data was breached as a result of the ransomware attack, then companies must incur legal costs related to third-party claims.

REMEDIATION

Remediation costs include implementing forensics and investigative work, as well as containing the actual breach. **Remediation costs grew from an average of $761,106 in 2020 to $1.85 million in 2021, according to Sophos.**

COMPLIANCE FEES

Paying a ransom could breach OFAC regulations and result in needing to pay compliance fees on top of that ransom.

WHAT'S THE TOTAL?

The average cost of ransomware is **$4.4 million**, according to a Ponemon study.

The same study found that organizations can save $1.12 million on average if they are able to detect and contain a breach in less than 200 days.

That's why the cost of ransomware far outweighs a cloud SIEM investment.

START YOUR FREE TRIAL TODAY

www.blumira.com/trial

Blumira