PULSE | Coalfire

Ransomware in 2021

Incidents of ransomware, when attackers use malware to seal off data until a ransom demand is met, continue to create headlines. What are tech decision-makers' experiences of ransomware?

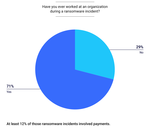
In this One-Minute Insight Report, Pulse surveyed over 300 decision-makers to learn:

- How many have experienced ransomware, and what the outcomes were
- Which industries are particularly vulnerable to ransomware
- Why ransomware attacks are increasing in 2021 and beating

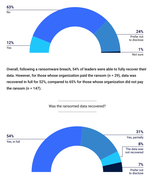
Data collection from June 30 - August 30, 2021 | Total respondents: 321 tech decision-makers

Many have experienced ransomware attacks in their career, though most incidents didn't result in payment, and data recovery was successful in most cases

Almost three quarters (71%) of leaders have worked in an organization that has experienced a ransomware incident.



At least 12% of those ransomware incidents involved payments.

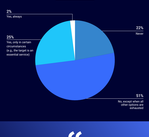


Overall, following a ransomware breach, 54% of leaders were able to fully recover their data. However, for those whose organization paid the ransom (n = 29), data was recovered in full for 52%, compared to 65% for those whose organization did not pay the ransom (n = 147).

> "Ransomware is emerging as one of the major threats worldwide and it should be properly managed."
>
> – Director, medium-sized mining company

Leaders divided on whether ransomware payments should be considered operating costs—but most would only pay as a last resort

Overall, a small majority of leaders (55%) disagree that ransomware payments should be considered an operating cost for businesses.



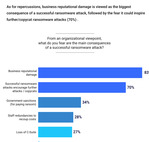
And most (55%) believe ransomware demands shouldn't be paid unless all other options are exhausted.

> "[Ransomware] is a problem we made ourselves. Insurance companies have made it worse by offering coverage and just [rewarding] extortionist behavior without consequences."
>
> – C-suite, small-medium education company
>
> "People are paying, so there is a market. Frankly, I'd rather pay the ransom than pay the criminals."
>
> – VP, large education company

Most believe a ransomware attack is likely on their current organization within the next year and fear business reputational damage as a result

Overall, most leaders (57%) believe their organization is likely to be hit by a ransomware attack in the next 12 months.

However, of those who have experienced a ransomware attack (n = 234), 62% believe an attack is likely, compared to 45% of those who haven't experienced a ransomware attack (n = 87).



As for repercussions, business reputational damage is viewed as the biggest consequence of a successful ransomware attack, followed by the fear it could inspire further/repeat ransomware attacks (78%).

> "Ransomware attacks are getting more generic than specific. Hackers are casting a wide net, since most organizations are using the same third party products."
>
> – VP, software company

Lack of unified cybersecurity strategy the top reason given for why organ-hit victim to ransomware—with employees the main vulnerability

The main reason leaders think an organization falls victim to a ransomware attack is a lack of a unified cybersecurity strategy (37%).

Malicious internal threats (8%), Disgruntled employees (2%), None of these (1%), Other (0%)

Leaders point to employees as the main vulnerability points exploited by ransomware attackers, with the top 2 vulnerabilities being employee negligence (78%) and the social exploitation of employees (78%).

> "Almost all the threat vectors for cyber [breaches] have increased, spurred on by [the] COVID-19 pandemic, the uptake of remote working, and geopolitical instability."
>
> – C-suite, medium-sized healthcare company

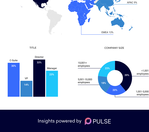
Remote work (and an insufficient security stack) the main reason ransomware is in the news—and leaders highlight energy and healthcare industries as the top targets

As for why ransomware has been making the news more often recently, leaders believe it's mainly due to the fact that remote work has revealed holes in the security stack that teams have failed to patch (54%).

The financial incentives of ransomware are greater than the financial incentives of holding a target organization's data hostage. This is why ransomware attackers increasingly target the biggest and most cybercriminals (58%). The proliferation of third-party SaaS has increased the surface area for attack (58%). The deterioration of international relations has led to an increase in state-sponsored cyberattacks (49%).

Other (0%), None of these (0%)

As for the industries most likely to be hit by ransomware attacks, leaders highlight energy infrastructure (79%) and healthcare (72%).



Food processors (34%), Sport franchises/venues (31%), Other (2%)

> "Until cyber criminals are more regulated (or made illegal to use for ransom payments), the rate of incidents will only increase in the future."
>
> – Director, large education company

RESPONDENT BREAKDOWN

REGION

TITLE

COMPANY SIZE