PULSE Lookout

# 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
- What makes an organization vulnerable to ransomware
- Why ransomware attacks have been increasing

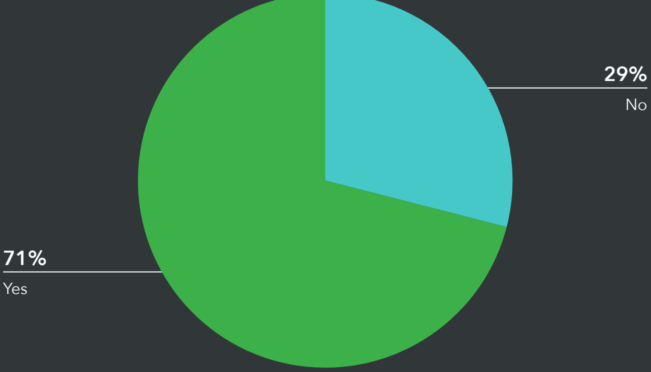
Data collected from June 26 - August 28, 2021

Total respondents: 331 tech decision-makers

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

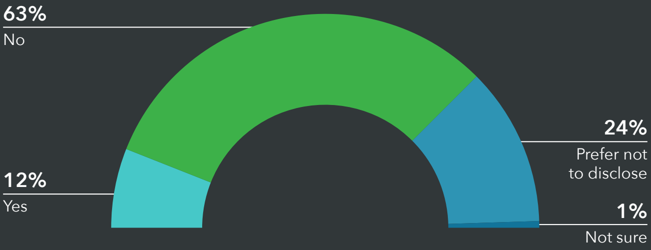
Almost three-quarters (71%) of leaders have worked in an organization that has experienced a ransomware incident.

**Have you ever worked at an organization during a ransomware incident?**



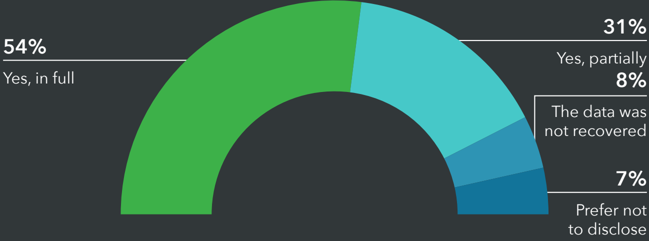
At least 12% of those ransomware incidents involved payments.

**Was the ransomware paid?**



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).

**Was the ransomed data recovered?**

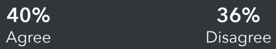


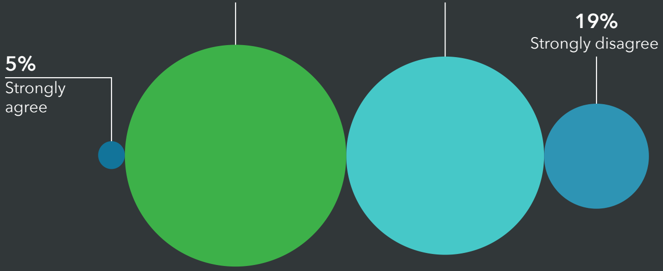
> "Ransomware is emerging as one of the major threats worldwide and it should be properly managed."
>
> - Director, medium-sized mining company

## 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.

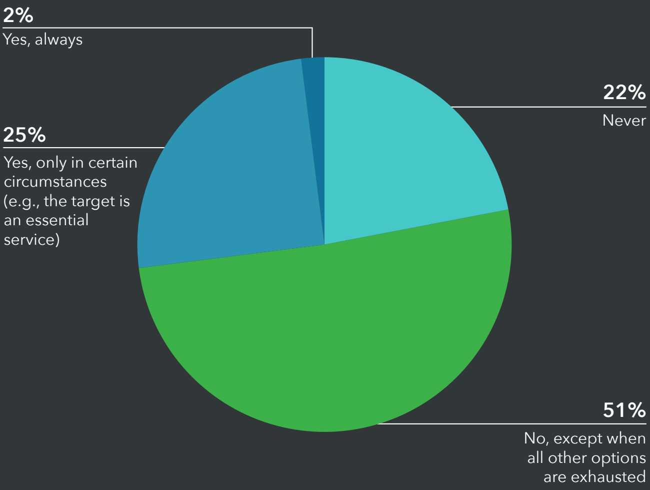
**To what extent do you agree with the following: "Ransomware payments should be considered an operating cost for businesses."**





And most (51%) believe ransomware demands shouldn't be paid unless all other options are exhausted.

**Should organizations pay ransomware demands?**



"[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 penalty than pay the criminals.”

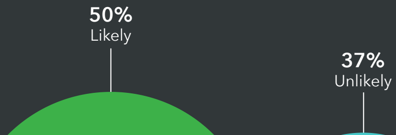
- VP, large education company

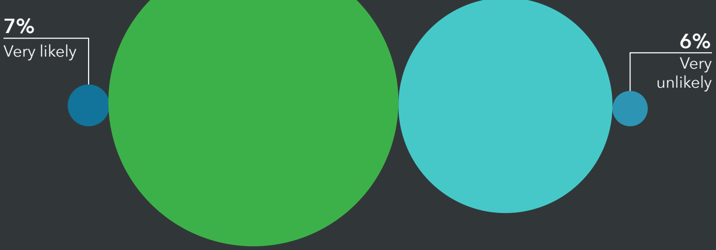
## Most believe a ransomware attack is likely on their current organization within the next year and fear business reputational damage as a result

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 already 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 = 97).

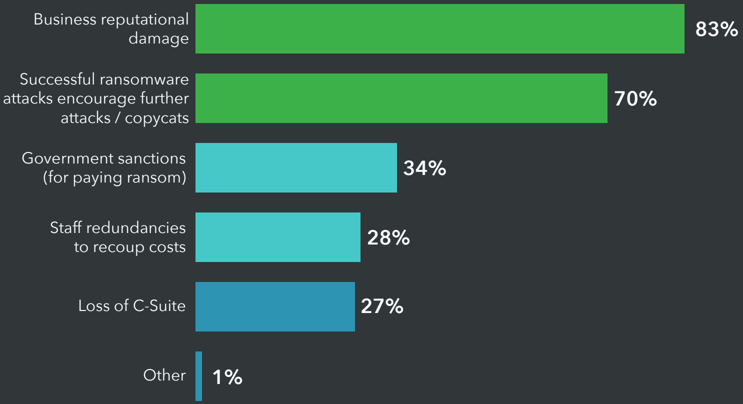
**How likely is it that your organization will experience a ransomware attack in the next 12 months?**





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/copycat ransomware attacks (70%).

**From an organizational viewpoint, what do you fear are the main consequences of a successful ransomware attack?**

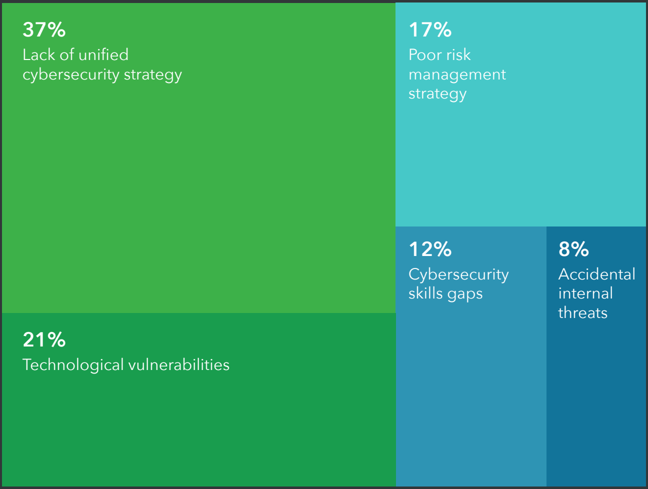


> “Ransomware attacks are getting more generic than specific: Hackers are casting a wide net, since most organisations are using the same third party products.”
>
> - VP, software company

## Lack of unified cybersecurity strategy is the top reason given for why orgs fall 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%).

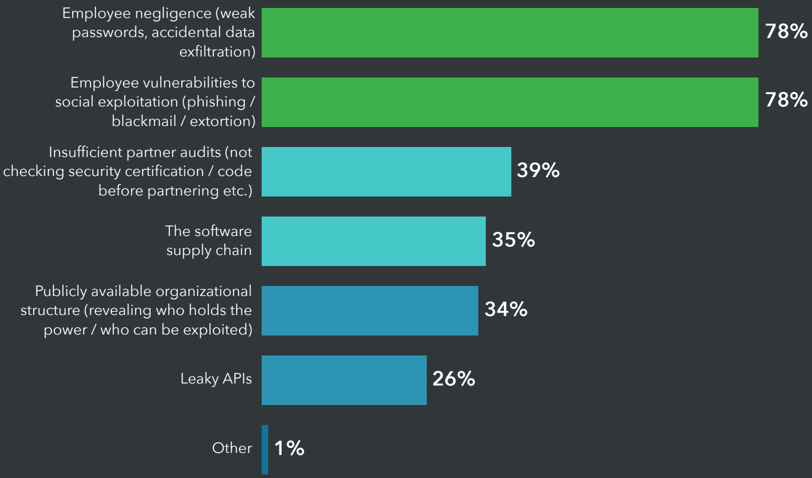
**In your opinion, what is the single main reason an organization falls victim to a ransomware attack?**



Malicious internal threats (**2%**), Disgruntled ex-employees (**1%**), None of these (**1%**), Other (**1%**)

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%).

**What are the main organizational vulnerabilities that malicious attackers exploit when engaging in a ransomware breach?**

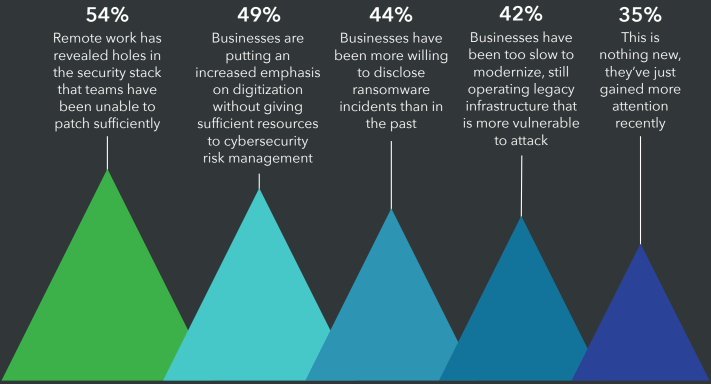


> “Almost all the threat vectors for cyber [breaches] have increased, spurred on by [the] COVID-19 pandemic, the uptake of remote working, and geopolitical instability.”
>
> - C-suite, medium-sized healthcare company

# 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%).

**Why have so many high profile ransomware incidents been reported in the news in recent months?**



The financial incentives of ransomware are greater than the financial incentives of holding a legal cybersecurity technical position **(35%)**, The proliferation of cryptocurrencies makes it harder to trace cybercriminals **(34%)**, The proliferation of third-party SaaS has increased the surface area for attack **(22%)**, The deterioration of international relations has led to an increase in state-sponsored cybercrime **(19%)**, Other **(2%)**, None of these **(1%)**

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

**Which industries do you fear are the biggest target for ransomware attacks?**

**79%**
Energy infrastructure (E.g., power plants, energy grids)

**72%**
Healthcare institutions

**71%**
Government institutions

**59%**
Supply chain command centers

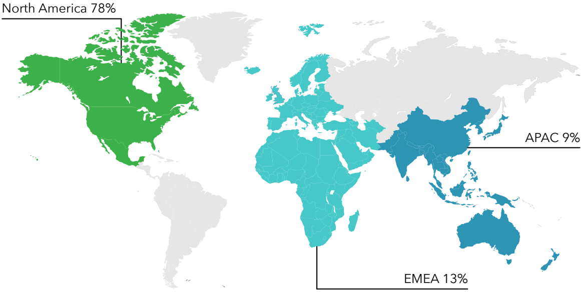
**36%**
Educational institutions

Food processing **(24%)**, Sport franchises/events **(11%)**, Other **(1%)**

> "Until cyber currencies 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

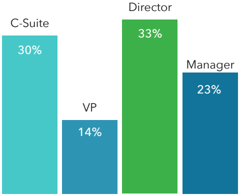
## Respondent Breakdown

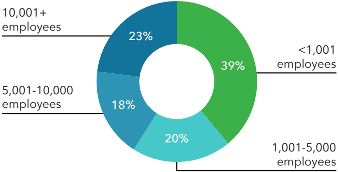
### Region



### Title

### Company Size





Insights powered by PULSE