7 Financial Impacts of a Ransomware Attack

The Ransom

You should NOT pay the ransom. There's a risk that the ransom will only be raised, recovered data have been damaged from the encryption, or you will simply never hear back....
> Read more

Legal Expenses

You must always inform your clients immediately about a breach of personal data according to the EU's GDPR regulation. Also, in some industries a data breach can result in fines by default ...
> Read more

Cost of Downtime

As long as your systems are down, your whole operation is paralyzed and you're unable to service clients, sell or produce products, etc. The negative impact is counted in minutes rather than hours ...
> Read more

Data Loss

Even if you are able to restore from your backup, there is a risk that not all of your files were backed up completely or correctly, meaning you might have forever lost valuable data ...
> Read more

Labor Cost

While your IT resources are focused on restoring your systems, most other employees are dependent on access to data, resulting in a backlog of work throughout your organization ...
> Read more

Collateral Damage

Hackers trade stolen data and credentials and have become highly organized. After having resolved an incident there is still a risk that your company data could be exploited in future ...
> Read more

Brand Reputation

You can restore data, but a damaged reputation is hard to fix. And remember: the public includes not only your customers, but also your employees, investors and other stakeholders ...
> Read more

The financial burden of a ransomware attack is a combination of the cost of downtime and lost business due the above-mentioned factors. Have a backup strategy in place that includes a complete mapping and classification of your data, restore testing and an incident response plan. Read more at b4restore.com/financial-ransomware

B4RESTORE
0100001001000101001 | EVERY BIT COUNTS |