Pay Up

Or you'll never see your data alive again.

Ransomware is on the rise, and the targets are in every industry. In this type of malware, attackers hold your files or system for ransom, and demand payment in order to regain access.

But how serious is the threat?

The FBI estimates ransomware costs will **reach USD1 billion in 2016.**[1]

8 out of 10 security leaders are seriously concerned.[2]

In just the first quarter of 2016, **more than USD209 million** in ransoms have been paid.[1]

Take action to avoid attack

By adopting a unified incident management process, you can be better prepared to proactively prevent and limit the devastating consequences of ransomware attacks.

Best practices for fighting back

- Back up data before it is too late.
- Train users to beware of threats.
- Prohibit attachments with executables.
- Keep anti-virus solutions up to date.
- Maintain an updated patch management policy.

Don't let your data be held hostage.

IBM

Learn how to prevent, detect and remediate the risks of ransomware. Download the Ransomware Response Guide now.

[1] David Fitzpatrick and Drew Griffin, "Cyber-extortion losses skyrocket, says FBI," *CNN Money*, April 15, 2016. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

[2] Robert Lelewski, "The Silver Lining of a Ransomware Infection," *IBM Security Intelligence*, March 30, 2016. https://securityintelligence.com/the-silver-lining-of-a-ransomware-infection/