VERITAS
The truth in information.

#RANSOMWARE
Are you protected?

The Growing Threat

Ransomware has quickly emerged as one of the most dangerous cyberthreats facing both organizations and consumers, with global losses now likely running to billions of dollars each year. Adopting a unified approach to backup helps ensure you are protected, regardless of where your data resides.

91% of cyberattacks begin with a spear-phishing email commonly used for ransomware[1].

Ransoms can be as high as $10,000 per user, paid in untraceable Bitcoin[2].

71% of organizations targeted by ransomware end up infected[3].

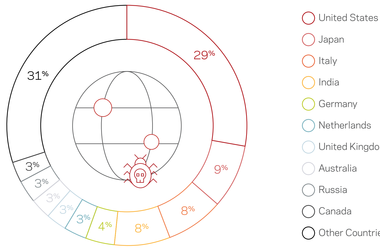
Global ransomware damage costs are predicted to reach $20 billion annually by 2021[4].

Ransomware is a threat to all major operating platforms:

iOS — Apple iOS™
Windows — Microsoft Windows™
Android™
Linux™

Ransomware infections by country[5].

More than any other country, the United States remains the most affected by ransomware attacks. The U.S. may be heavily targeted because a reported 64% of victims will pay the ransom demanded.



Businesses are experiencing ransomware attacks more frequently than ever[6].

Beginning of 2016	End of 2016	End of 2019	In 2021
Every 2 minutes	Every 40 seconds	Every 14 seconds	Every 11 seconds

The Big Question: Should you pay?

Victims need to be aware that paying the ransom does NOT always work. Some attackers will continue to demand ransom after receiving the initial payment. The decryption process, if poorly implemented, can damage files. And what's worse, 20% of those who do pay never receive a decryption key.[7]

Four Steps to Comprehensive Data Protection.

Adopting a multilayered approach minimizes the chance of infection. Here's what Veritas recommends you do to safeguard your organization from loss:

Educate

Make sure employees know the dangers and what to avoid:

- Websites they don't know.
- Emails from unfamiliar senders.
- Physical media from unknown sources.
- Pop-up browser windows.
- Software with optional installs.

Secure

- Install security software.
- Keep it up-to-date. No exceptions.
- Ensure that OS, software and firmware stay patched on all devices.
- Set antivirus and antimalware to auto scan and update.
- Configure access controls and permissions appropriately.

Back Up

- Make regular, frequent backups.
- Store backups separately and off-site.
- Unify backup across your physical, virtual and cloud environments.
- Test to help ensure recoverability.

Unify

Adopting a unified solution could be the best way for businesses to protect their data everywhere:

- Harden backup servers with the same level of protection as other systems.
- Resolve problems that prevent backups from completing successfully.
- Update backup software frequently to address known vulnerabilities.
- Run test restores on a regular cadence.

Get the Guide

Learn more about the steps you can take to protect your organization with our short guide Ransomware and NetBackup: What backup professionals need to know.

References:

1. 91% of cyberattacks begin with spear phishing email
2. Intermedia Ransomware 101: What your business needs to know about ransomware attacks
3. Must-Know Ransomware Statistics 2018
4. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
5. US remains the country most affected by ransomware
6. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
7. Why you should NOT pay ransom to malware creators

VERITAS
The truth in information.