MENLO SECURITY

The million-dollar question: Should you pay ransomware attackers?

Menlo says NO.

Menlo research highlighted that 62% of organizations[1] were targeted by ransomware attacks in 2020. Ransomware is big business.

Payday for ransomware attackers

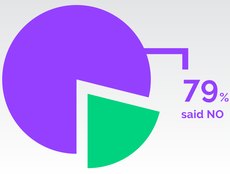
Recent data shows global losses will exceed $20 billion rising to $265 billion by 2031

Average ransom **$312,493**

In 2020, ransomware attacks increased by more than **130%**[2]

Colonial Pipeline in the US paid over **$4 million** in Bitcoin ransom

But the question is, **how many respondents think organizations** should defy their attackers and **not pay?** Menlo's Twitter poll investigates – and here is what you said:



Menlo agrees that it is time to take a stand worldwide alongside

the White House | the UK Home Office | law enforcement agencies | cybersecurity experts

> *"Ransomware isn't going away any time soon and with the rise of ransomware as a service it's an increasingly easy way for cyber criminals to launch a profitable attack. It's time for governments, organizations and individuals to take a stand. If companies continue to pay ransom demands, then these criminal groups will continue to see the technique as an easy way to make massive monetary gains."*
>
> Mark Guntrip, Senior Director, Cybersecurity Strategy, Menlo Security

Although **20%** of respondents said they would **pay to regain control**, it seems they are **resistant to demands for large sums**

The Twitter poll shows **two in five** would pay **no more than $100**

Taking a proactive stand on ransomware – time to protect users, applications and data

69% demand more **government intervention** with prison sentences for attackers

16% concede that attackers are currently **unlikely to be apprehended**

Menlo is supporting the fight back against ransomware risk

Start the fight back today with an isolation-powered approach to zero trust

Your organization's cyber resilience plan to mitigate the risks from ransomware should include but not be limited to:

- Maintain regular off-site backups and prevent lateral ransomware movement between your backup and primary network/cloud instance
- Patch regularly and maintain a list of critical assets
- Implement a secure email gateway, with link-rewriting/isolation
- Ensure external active content from documents, such as macros, have limited or zero ability to execute on your network
- Execute fire drill exercises that equip teams to combat ransomware threats – test, test and test again

Gartner recommends security and risk management leaders look beyond the endpoints to protect organizations from ransomware. SWGs and web isolation can help.

Learn more about how to prepare for ransomware attacks by downloading the **Gartner Report: How to Prepare for Ransomware Attacks**

MENLO SECURITY

Contact Us
menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and eight of the ten largest global financial services institutions, and is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit **www.menlosecurity.com**

[1] 2021 Cyberthreat defense report
[2] Breach Insights - Q3 2020, Beazley Group