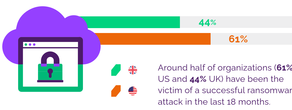
MENLO SECURITY

Ransomware is now a full-blown crisis

Remote working is an ideal environment for cybercriminals. With ransomware paydays hitting $40 million, it's no surprise they're on the rise.

FACT:
1 in 3 organizations now report **WEEKLY** ransomware **attacks.**

FACT:
41% of IT security leaders worry that ransomware attacks have **evolved** beyond their **teams' capabilities.**



Around half of organizations (**61%** US and **44%** UK) have been the victim of a successful ransomware attack in the last 18 months.

We need to keep talking about ransomware.

While ransomware may have fallen off the news agenda, the **ongoing barrage** of attacks shows **no signs of slowing.**

It's a proven and effective mechanism for hitting a huge payday in one shot, with payouts totaling as much as **$40 million.**

As work-from-home becomes embedded across the public and private sectors, **vulnerability to ransomware has spiked.**

The insider threat hasn't gone away.

FACT:
Partners, suppliers, and contractors are seen as serious security risks.

FACT:
Employees are seen as cybersecurity's "weakest link."

FACT:
1 in 3 say remote workers are their biggest challenge when defending against ransomware.

Perception VS reality:
The real cost of remediation.

IT security leaders **estimate the average** total cost of recovery from a ransomware attack at **$326,531**

The **real average** total cost of recovery in 2021 was **$1.4 million**

> "Security professionals are coming under increasing pressure as organizations face an unprecedented number of highly sophisticated threats like ransomware."

Mark Guntrip
Senior Director of Cybersecurity Strategy, Menlo Security

Battle ready?

"Less than half (45%) of **IT security leaders implement a data backup** or recovery plan as step one in a ransomware attack.

"Just 37% **inform their employees** about an **attack** and 33% tell customers.

"Only 29% **contact the CEO** or Board in the first instance.

"One in 10 admit **they don't know** what step one is.

How should IT security leaders react?

- Formulate a detailed response plan outlining immediate steps in the event of an attack.
- Consider unmanaged devices as a key part of IT security strategy.
- Focus on mobile as a leading attack vector.
- Calculate the real cost of recovery from an attack.

Adopt a prevention-driven approach that stops attacks before they can happen.

Prime vectors for ransomware attack:

A better defense

Our study shows that current ransomware defenses need to shift towards prevention, empowering CISOs with the tools, technologies and solutions needed to reduce operational burdens and provide greater peace of mind.

Find out more at www.menlosecurity.com

Download a copy of the report here.

MENLO SECURITY

Contact Us
menlosecurity.com/contact
ask@menlosecurity.com

About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation 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 financial services institutions.

© 2021 Menlo Security, All Rights Reserved.

SOURCE:
Forbes Research, 2020 Impact: Ransomware attacks and preparedness, a survey of 200 IT security decision makers at US and UK organizations with more than 1,000 employees