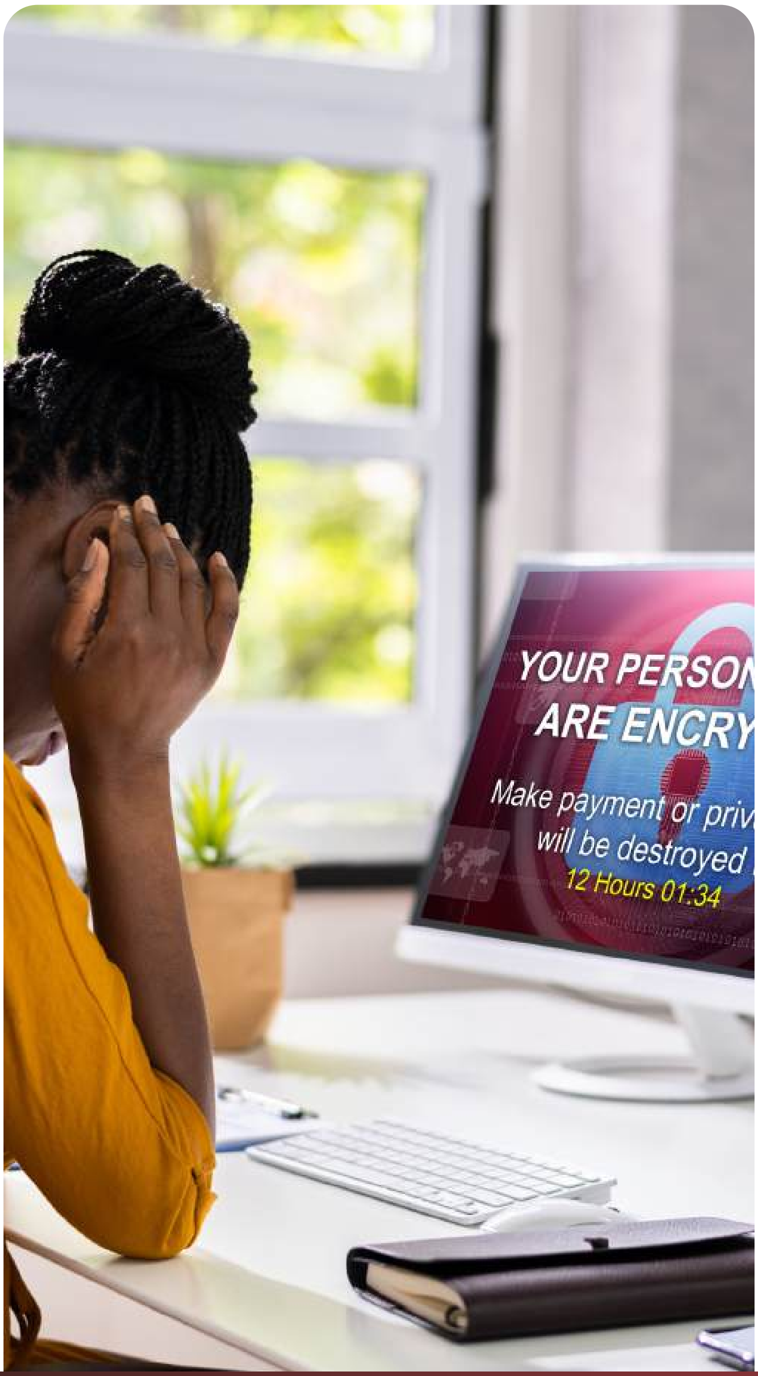
SECURITY BRIEF

# Ransomware:

## A Growing Threat to Your Businesses

Ransomware has emerged as one of the most serious cyber threats facing organizations across every business sector. Here’s a look back on its impact in 2024, and the problem is likely to get worse in 2025. Please take a few minutes to read this Security Brief from Rize Technologies. It’s vital that you understand the potential impact that ransomware can have on your business.



## What is Ransomware?

Ransomware is a type of cyber attack where criminals lock up an organization's computer systems or data and demand money (a ransom) to restore access. Think of it like digital kidnapping - but instead of a person, the criminals hold your important business information hostage.

## The Alarming Numbers

The threat of ransomware reached new heights in 2024. A shocking 83% of organizations experienced at least one ransomware attack in the past year. Even more concerning, 74% of victims were attacked multiple times within the same year, with some being hit several times in just one week.

## The Cost is Skyrocketing

The financial impact is staggering:

- The average ransom demand reached $1.57 million in 2024
- The average ransom payment jumped 500% in one year, from $400,000 to $2 million
- Recovery costs (excluding the ransom) increased to $2.73 million, up nearly $1 million from 2023
- A record-breaking $75 million ransom was paid to a group called Dark Angels - almost double the previous highest known payment

## When and Who They Target

Criminals are getting sneakier about when they attack:

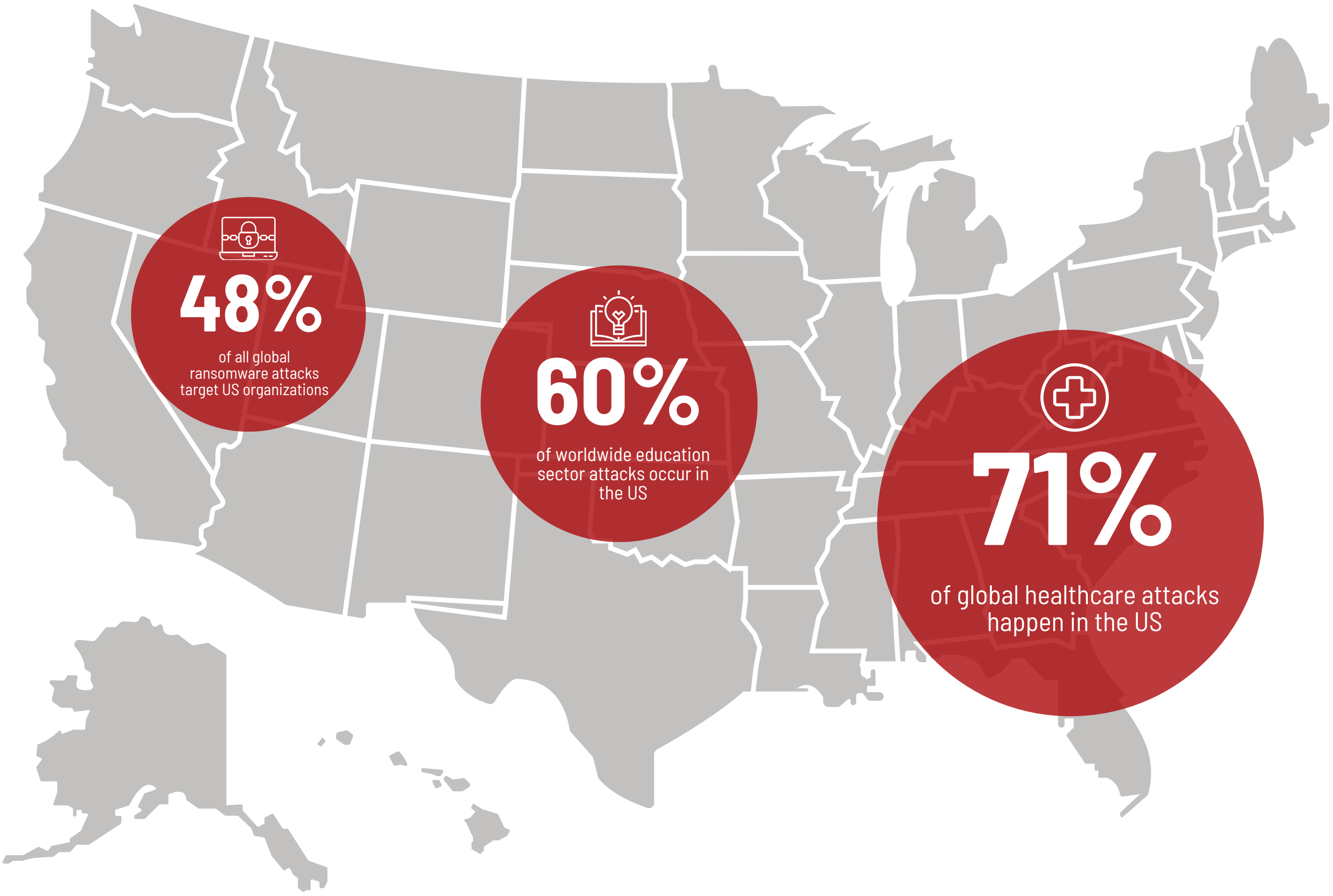
Most ransomware attacks happen between **1 AM and 5 AM** when IT staff are typically off duty

Weekend attacks are increasing

Small and medium businesses are prime targets - over 50% of victims had fewer than 200 employees

## The United States Under Attack

The US is particularly vulnerable:



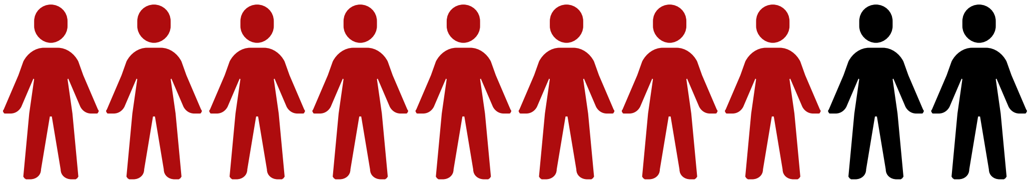
**48%** of all global ransomware attacks target US organizations

**60%** of worldwide education sector attacks occur in the US

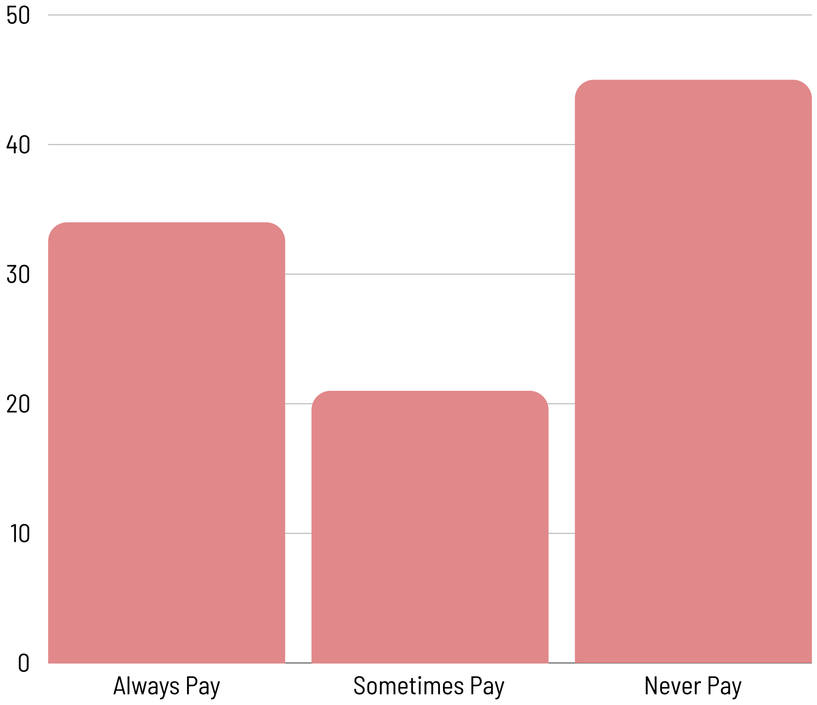
**71%** of global healthcare attacks happen in the US

## To Pay or Not to Pay?

Organizations are divided on handling ransom demands:



78% of targeted organizations paid the ransom



34% always pay, 21% sometimes pay, and 45% never pay

Among those who paid, 72% had to pay multiple times

Worryingly, even after paying, one in three organizations still couldn't recover their data

## The Future Outlook

Companies are increasingly viewing ransomware as inevitable:

**97%**

of companies say they would pay a ransom to recover their data

**67%**

would be willing to pay over $3 million

**35%**

would consider paying over $5 million

This data paints a clear picture: ransomware is becoming more frequent, more expensive, and more sophisticated. Organizations of all sizes need to take this threat seriously and invest in prevention measures, as paying the ransom offers no guarantee of data recovery.

## Protect Your Business

Rize Technologies is a managed IT services provider that has been working with growing businesses for more than a decade. To help safeguard your business against cyberattacks like ransomware, we offer a complimentary penetration test service. It's a quick and painless professional service performed by our cybersecurity experts to identify the specific areas of your network that are vulnerable to cyberattacks. It can help you ensure your business has a strong security posture to defend against ransomware.

Operating remotely and without any disruption to your network or business, our expert team will:

- Test the security strength of 10 endpoint devices.
- Analyze vulnerabilities and assess potential damage.
- Provide a detailed report and a 30-minute call with a security expert

Take advantage of this zero-cost, zero-obligation professional service offering. Your firm's security depends on it. Schedule your complimentary penetration testing here.