6 CYBERSECURITY STATS

YOUR HEALTHCARE ORGANIZATION NEEDS TO UNDERSTAND TO RESPOND TO A DATA BREACH

IPRO

Has your healthcare organization recently been exposed to a data breach? You aren't alone.

48%
of malware attacks are located in office files.

88%
of organizations have had a spear phishing attack.
This kind of attack is specifically targeted to a single organization's data.

237%
growth in phishing attacks imitating Saas Services

IPRO has compiled this critical information for healthcare organizations to show how cybercriminals are becoming more sophisticated and are able to mimic the work environment that individuals use specifically at their own organization to gain access to data.

The average time it takes to identify a breach:

228 DAYS

As data continues to exponentially grow across organizations, all the additional data accumulated during this nearly 9 month period is also exposed before the breach is caught.

$26 BILLION

Paid across the United States after a compromised account to gain back access to breached data.

This stat, from the FBI, is only the amount directly paid in ransom to a cybercriminal. It doesn't include the costs of:

- X Data remediation the data after the breach
- X Cybersecurity monitoring for the organization and affected individuals
- X Regulatory fines and private settlements

each person breached = $600

The average cost of a healthcare organization security breach with regard to how much social security number is worth on the black market and everything that needs to be done to notify the person breached and give them identity protection.

Is your organization prepared to respond to the next data breach?

Get a cup of coffee on us and learn how our solutions can help you better manage your healthcare organization's data access rights, retention policies, and remediation processes.

click here