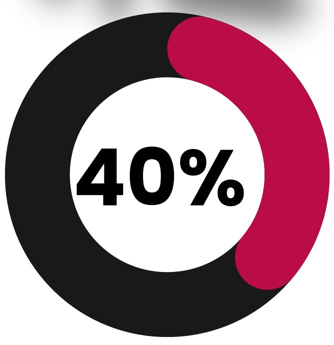
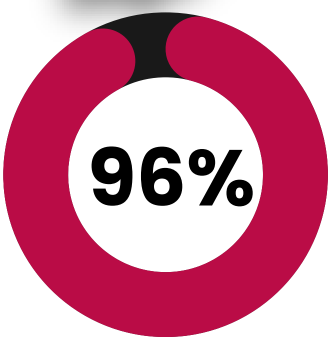
Understanding the current state of healthcare

Healthcare organizations are vulnerable to a wide range of attacks, whether it's collecting a past-due payment for services, fulfilling an order for medical devices, or a simple gesture of sending flowers to a loved one's bedside, making it a vulnerable industry compared to others.

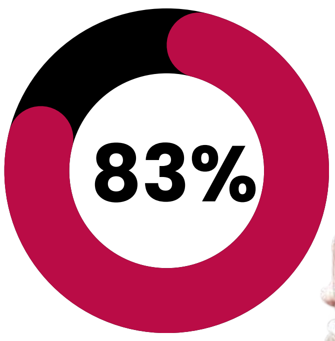
Patients



40% of American customers stopped doing business just after **ONE** poor customer service experience



96% of consumers say that customer service is an essential fact that affects their choices



83% of consumers in the US claim they will immediately stop spending after a security breach and **21%** will never return to that organization

Contact Center

One and four data breaches come from the lost or stolen devices - a problem that will persist with the increase in remote and hybrid workers

95% of data breaches are caused by human error and are the root causes of security breaches

43% of all breaches are insider threats within the organization

Organization

Only **5%** of an organizations' data is properly protected and **54%** of companies say their IT department are not prepared enough to handle a cyberattack

$10M

A data breach in healthcare industry costs **$10.93 million dollars** on average

On average, it takes **4.5 days** of a ransomware to be detected and **75 days** to contain a data breach

What to look for when partnering with a payment security provider.

- ✓ **Flexibility & scalability**
- ✓ **Frictionless patient journey**
- ✓ **Secure & compliant**
- ✓ **Security across all channels**
- ✓ **Future-proof technology**

Patients today have choices regarding their healthcare options. Give patients the confidence to choose your organization by partnering with a vendor that prioritizes secure engagements and protects their sensitive personal data.

Discover more at **eckoh.com**

Eckoh