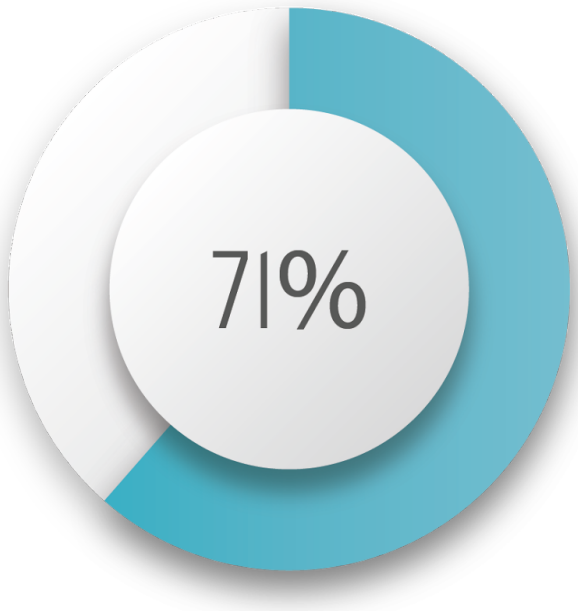
CopyStrong Combats Insider Threat for Healthcare Organizations

According to new research from IBM, in 2016 1 out of every 4 cyber attacks in the healthcare sector was the result of insider threat, a far higher rate than any other major industry (see below).



OF **UNSECURED DATA LOSS** IS DUE TO **INSIDER ATTACKS** AND **LEAKS**.

ACCORDING TO PUBLISHED STATISTICS

Healthcare organizations are at particular risk for the exfiltration of sensitive information by insider cyber-criminals. Healthcare is the only major industry in which insider attacks are more common than those from outside.

When electronic records replaced paper records, the digitization came with new vulnerabilities, such as direct breaches (in the case of insider threats) and through indirect compromise (such as third-party Electronic Medical Record (EMR) breaches), placing patient information at much greater risk. The most recent Breach Barometer report from Protenus, identified 31

breaches in February 2017, involving more than 206,000 patient records. *Of the 31, insiders were responsible for 18*.

On average 200 people have access to a patient's medical record during a three-day hospital stay. Nurses, doctors, technicians, and other employees have legitimate access to proprietary systems, which shields them from traditional cybersecurity defenses. While IT security teams spend most or all of their budgets securing their servers and databases, they are ignoring the dangers inherent in the patient record applications to which their users have access. This is a massive misalignment in the security posture of most healthcare organizations.

Such was the case with an emergency room employee at Florida Hospital who used his access to collect information on patients injured in car accidents, which he then sold to chiropractors and lawyers. This went undetected from 2009 to 2011. After he was terminated, his wife (who was an employee at the same hospital) continued the scheme. This sort of delayed detection and ineffective response is worryingly common for organizations at risk for insider threat.

Stolen personal identifiable information (PII) has generated Deep Web markets worth an estimated $120 billion dollars. Any employee might decide to exfiltrate sensitive information from their organization in order to sell it on Deep Web markets like Alphabay. There they can easily exchange company databases and other PII for the right sum. A departing executive could easily exfiltrate and sell troves of employee or patient data and expect to make up to $363 dollars per record, according to the Ponemon Institute and IBM.

Why is personal identifiable information (PII) so valuable? Credit card details fetch as little as $5 on the dark web, but a PII record can be worth well over $300. This is because, while a credit card can be quickly cancelled and replaced, records from within the healthcare system often

contain personal data, such as social security numbers, that can be used undetected for long periods of time, and which are difficult (or impossible) to cancel or replace.

Bad actors within an organization can take the data from an Electronic Medical Record (EMR) and use it for a number of further criminal activities, for example, to buy drugs and medical equipment or in the case mentioned, selling them as leads. The IRS breach of 2015 was so harmful because the health records gave enough information to allow fraudulent tax claims to be made in real people's names.

As more sophisticated bad actors are predicted to concentrate their efforts on client-side applications, CopyStrong has launched a front-end security solution for healthcare organizations, providing advanced dual functionality on both internet and intranet environments while integrating into ERMs and other applications. CopyStrong protects against today's cyber security vulnerabilities, delivering solutions that will foil perpetrators best efforts to steal your data. Our software allows healthcare organizations to get ahead of data breaches and minimize the loss of sensitive information while avoiding the disruption to operations, financial losses, and reputational damage a data breach involves.

CopyStrong alerts administrators to possible attacks and launches its own pre-configured safeguards to track and recover the data being removed, adding further insight into the nature of the attack.

CopyStrong works by structuring your security data in a relational method, providing you with insightful and actionable intelligence in real time. Because of its patented technology and counter-intelligence features, CopyStrong is in a league of its own.