CopyStrong

The Problem: Insider Threat & Cyber Attacks within Healthcare Organizations

The percentage of healthcare organizations that have reported a cyber attack has risen from 20% in 2009 to 40% in 2013. The period between 2013 and 2014 saw a 72% increase in cyber attacks. According to an annual survey conducted by the *Ponemon Institute,* in the past 2 years more than 90% of healthcare organizations suffered at least one data breach exposing patient records. During the same period, 39% of healthcare organizations suffered between two to five breaches, while 40% experienced more than five breaches.

These cyber attacks cost healthcare organizations $6 billion per year. A report issued by ID Experts found these costs to average $2.1 million per organization.

With a quarter of all medical data breaches being carried out by insiders (whether maliciously or unknowingly) medical data is proving to be particularly attractive to cyber-criminals. Stolen health records can fetch as much as $363 per record, according to data from Ponemon.

Healthcare organizations may not be aware of the damage from insider threat because current research shows that 75% of all insider crime goes unnoticed. Below are recent examples.

- Between 2009 and 2011, an emergency room employee at the Florida Hospital used his computer to access and collect information on people injured in car accidents. He then sold this information to a Polk County man. After this employee was terminated, his wife, and fellow hospital workers continued the theft. All three eventually plead guilty in federal court. Cases of insider threat and data breaches continued throughout 2012 and 2014 at Florida Hospital.

- A Miami respiratory therapist reportedly sold patient's' personal information for up to $150 per person; buyers then used the data to illegally file and claim patient's' tax returns.

- On Oct. 2nd, 2014, health system officials discovered a University Hospital staff member had been snooping into the EMRs of 692 patients from January 2011 through June 2014. The staff member was able to gain access to patient names, medical diagnoses, health insurance numbers, dates of birth, home addresses and treatment data.

- The Queens, N.Y., district attorney charged two employees of Jamaica Hospital Medical Center with illegally accessing emergency room patients' medical records and personal identification information, and selling that data to individuals.

“To understand why one Medicare number can sell for close to $500, consider that these records typically include names, birth dates, social security numbers, policy numbers and billing information that can be used for an equally exhaustive list of profitable activities.”

In a *2010 CyberSecurity Watch Survey,* 67% of respondents stated that insider breaches were more costly than outsider breaches. The response indicated a much larger than anticipated problem, as the majority of these insider attacks go unreported.

Over 92% of healthcare IT professionals agree that their healthcare organizations are vulnerable to insider threats, while 49% felt very or extremely vulnerable.

The Survey also demonstrated that "the public may not be aware of the number of incidents because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement". There are a variety of reasons why companies choose not to report insider cases; in particular, lack of evidence to prosecute, damage levels that were insufficient to warrant prosecution, inability to identify the perpetrator, and fear of public embarrassment.

Based on the study along with collaboration from other industry leaders, it is believed that most insider crimes go unreported not because they are handled internally, but because they are never identified in the first place, or, by the time they are, the damage has already been done.

- Cleveland, Ohio-based University Hospitals earlier last year notified nearly 700 patients of a HIPAA privacy breach after one of its employees was caught snooping on confidential medical records. The employee was able to inappropriately access patient medical and financial records for nearly three and a half years without University Hospital knowing.

“75% of healthcare organizations believe employee negligence is their biggest security concern.

The Solution: CopyStrong Combats Insider Threats, Offering Tracking, Monitoring and Predictive Responses.

Copy**Strong**’s next generation cybersecurity software provides true digital protection on both internet and intranet environments, as well as offering customized integration solutions with EMR and EHR systems. Copy**Strong** is designed to protect against insider threats, such as removal of code, content, data and images.

By utilizing Copy**Strong**’s unique Digital Identity algorithms and predictive configurations, Copy**Strong** offers healthcare organizations the ability to initiate “bait and switch” functionality. This functionality allows preconfigured fictitious content (documents, patient records, numbers, data) to serve up to an attacker upon an attempted breach or alerting activity. This fictitious content hosts tracking numbers and other security features providing further analysis and insight into the breach.

Healthcare organizations using Copy**Strong** would be able to configure high-level mitigation strategies, reduce monetary loss from insider threat and data breaches, assess probability and minimize the severity of identified risks, implement pre-configured actions to minimize the impact or likelihood of insider threat occurrences, and provide real time alerting of probable insider threat conditions.

Copy**Strong** is device-centric and platform agnostic, and can function inside remotely accessible environments. Copy**Strong** can act as middleware or integrate with existing programs and/or software that may already be in place within a healthcare organization. Copy**Strong’**s proprietary tracking algorithms span into several different branches, including pattern recognition, predictive modeling, data analytics and a real-time advanced recovery protocol (ARP).

The use of Copy**Strong** inside healthcare organizations offers huge potential benefits. These include intelligence, encryption, recovery, theft protection, identity tracking and a variety of advanced technological features not commonly applied within healthcare organizations. With the current Federal mandates for healthcare and growing requirements for digital record keeping, in combination with the demand for increased speed of deployment of EMR technologies, incidents of insider threats and breaches will continue to grow exponentially without the use of aggressive preventative measures.

Copy**Strong** is the only solution for healthcare organizations offering this diversification in cybersecurity, providing advanced functionality in areas such as intelligence, analytics, predictive modeling, and pattern recognition. Copy**Strong** protects against today’s cyber-security vulnerabilities within healthcare organizations, delivering next-generation solutions that will foil any perpetrator’s efforts.

.