Healthcare's Growing Crisis: Risk of Data Loss

In the 2018 Cost of a Data Breach Report, IBM and the Ponemon Institute found that healthcare data breach costs average $408 per record, the highest of any industry for the eighth straight year and nearly three times higher than the cross-industry average of $148 per record.

> *"Most healthcare breaches are motivated by financial gain, with healthcare workers most often using patient data to commit tax return and credit fraud."*
>
> - VERIZON 2018 Protected Health Information Data Breach Report (PHIBDR)

Additionally, a February 2017 survey from Accenture reveals that healthcare data breaches have affected **26% of U.S. consumers**, or more than one in every four Americans.

Why is Healthcare being targeted?

Regardless of the size of the organization, healthcare companies are at risk for data loss. If you consider what healthcare data is made up of – patient name, date of birth, address, phone number, medical and social insurance numbers, employer, insurance information, age, gender, ethnicity, height, weight, color hair, color eyes, health details etc., having access to that information, could effectively lead to a number of ways that it could be used - including the theft of a person's complete identity.

Additionally, because of all the ways that healthcare information can be misused, the effective life cycle of personal health data is much longer than say financial data; where the usability of that information quickly diminishes to almost nothing, once a person changes their credit card number.

As one of the biggest and most attractive targets, the healthcare industry continues to suffer costly data loss. So why aren't current measures stopping these attacks?

Attacks and breaches are inevitable, more focus is needed on understanding data risk and implementing better data protection; not cybersecurity defenses, but protection on the data itself. Key is understanding the risk of sensitive data.

Within your organization, is there a process for the assignment of risk? Does the organization know who owns the risk for data loss? Does your organization understand where sensitive data resides, and how it's being accessed and shared? Does your organization have a prioritized list of risks? Does your organization have plan to address risk?

There are a lot of questions to answer however, an understanding of each of these, enables an organization to recalibrate the data loss conversation.

The ability to measure risk against a known security framework and achieve the goal of HIPAA's "Privacy Rule" is a critical first step – specifically as it pertains to data loss. Understanding how risk is being measured, enables an organization to be able to do something with that risk, and prioritize how to mitigate risk. This includes things like acceptance, transference and remediation.

> *"58% of healthcare security incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization."*
>
> - Verizon 2018 PHIDBR

Having answers to those questions will help to close the gap with respect to data loss.

"The number of exposed records more than doubled year over year, from 5,138,179 records in 2017 to 13,236,569 records in 2018."

- HIPAA Journal

Freezing risk levels by implementing compensating or validating existing controls, allows organizations to accept risk. Implementing or revamping a vendor management program supports the transference of risk. While either implementing or strengthening existing policies, processes and technologies, enables organizations to remediate risk.

The ability to close these data loss gaps is foundational to understanding what an organization needs to do next. Taking stock of existing processes and solutions will help the organization to understanding where from here. Is there a new technology that's going to be required, or is there an existing technology that simply needs to be modified? Is there a need for new policies or processes to be implemented, or are the current programs enough? Would the organization benefit from data loss prevention awareness training? Does the organization perform annual risk assessments to identify new areas for improvement?

There are many things that need to be considered, however the key takeaway is to proactively protect the organization from data loss by identifying, assigning ownership, measuring, and treating risk. Putting the necessary investment in these foundational activities will mean the difference between effective risk mitigation and the repercussions of an unwanted headline.

data security by ConnectWise is partnering with Informatica, leveraging the Informatica Data Privacy solution, to help healthcare organizations mitigate the risk associated with data loss. Please visit our website **Data Security Services by ConnectWise** to find out more about our solutions. Please visit Informatica at **Informatica Data Governance and Compliance** to find out more.