Information Age

What every healthcare technology leader needs to know about cloud data and security

William Klusovsky is the Global Cybersecurity Strategy, Governance, Risk and Compliance Offering Lead at Avanade spoke to Information Age about cloud data and security.

With most healthcare organizations continuing to digitize services and increasingly move workloads to the cloud, any healthcare technology leader must prioritize cloud data and security in this expanding virtual environment.

The reduction of administrative work leading to an improvement in overall patient care, combined with the benefits of technologies like the Internet of Things (IoT), which are changing the face of medicine and healthcare, demonstrate the importance of a digital-first approach.

However, as these digital transformation initiatives continue to expand an organization's virtual ecosystem, it is imperative that cyber security and cloud data protection practices are prioritized and baked into the business strategy.

This is crucial, as nearly two-thirds of global healthcare organizations have experienced a cyber attack in their lifetime, with over half being attacked within the last 12 months, according to research by Keeper Security.

Knowing your data

As organization's transition to the cloud, technology leaders should take responsibility and ownership of that journey, while building out a comprehensive security framework from the beginning. In the scenario of a data breach, for example, someone must be accountable and steer the organization through their governance and compliance requirements.

Knowing where an organization's data resides, who owns that data and what type of data it is, will ease any security incident and any legal or compliance implications. It will also ease an organization's ability to manage risk and improve their response over time.

Commenting on the importance of knowing your data, William Klusovsky, Global Cybersecurity Strategy, Governance, Risk & Compliance Offering Lead at Avanade, said: "Often, technology leaders will forget that asset management is not just about keeping track of hardware, it means knowing where your data is, where your data flows and who owns that data."

The challenge of having a holistic view of an organization's data landscape is intensified by the problem of Shadow IT — the procurement of software and tech without IT's knowledge. As new systems and applications are onboarded by various departments it's easy to lose track of these, and what data sits within them, without a strong systems acquisition process.

With healthcare specifically, the rapid introduction of IoT medical devices and all the new data they're generating, exemplifies this. Every new device needs to be monitored and secured, because even one vulnerable device — which is very simple to procure — could be used as gateway for a hacker to enter a healthcare providers network.

Article originally published in Information Age, Healthcare Sector, May 2021

What every healthcare technology leader needs to know about cloud data and security

Start at the top

"It's important to start at the top," said Klusovksy,"We bring in executive level experts to talk about building a comprehensive security strategy, then bring in architects to look at the policies and processes within the organization, before defining what technology is needed and how to implement it.

"By partnering with clients as opposed to offering a service, there is little or no knowledge transfer required — because it should be communicated and trickled down across various levels of the business, from strategy to policy process and technology implementation."

Learn more at:
Avanade.com/health

Developing a cloud security strategy in healthcare

Protecting the personal information of patients must be a priority for any healthcare technology leader. Here, Klusovksy provides four tips for developing an effective, holistic cloud security strategy:

1. Planning — leaders must assess their organization, understand their current security posture and define what's achievable from the beginning. The plan should also "live" and be continuously reevaluated against the changing risk and compliance landscape.

2. Aligning security to business goals — security should be built into the development of the business strategy. The two must be aligned. Technology leaders, therefore, should look at the goals of the business before making any purchasing or strategic decisions when it comes to security.

3. A governance framework — despite the huge variety of regional regulation, healthcare organizations must develop a baseline standard way of doing business, which should account for all the things you have to do from a compliance and risk standpoint. Having a governance framework in place, knowing where the risk lies, gives organization's the roadmap for what it should be doing to continually manage and improve things.

4. Skilled resources — it's important to understand your skills and capabilities. If you're a healthcare organization that does not have strong cloud skills, for example, then partner with someone who does. It will help get the job done right the first time, saving time and money.

The evolution of cloud data security: Zero Trust

Moving forward, adopting a Zero Trust framework into an IT or security strategy is necessary. The concept of Zero Trust, assuming businesses can't trust anything, be it a user, a device or network, means that mechanisms need to be built in to create that trust.

From a healthcare angle, looking at the explosion of IoT medical devices and wearable technologies that are now active on a provider's network, those devices can't be trusted and the data they produce that sits in the cloud must be secured. Regardless of the IoT device, whether a smart watch, an MRI machine or thermostats, they need to be monitored and security teams need the ability to detect when malicious activity is occurring.

"Protecting IoT requires the ability to be able to monitor it, which is different than typical security monitoring. Tools like Azure Defender for IoT provide the capability and insight to get the work done," explained Klusovsky.

"In a broader sense moving to Zero Trust requires the same planning that a cloud migration strategy would. Organizations need to look at their processes, infrastructure, data flow and business operations and begin mapping out the path to zero trust. It requires strong identity management and access controls using products such as Azure Active Directory, among many other things," he continued.

"If you're looking at new innovations and wanting to move forward, a healthcare technology leader must make security part of the plan from the beginning of the transformation journey," he added.