SOLUTION BRIEF

FBI CYBERSECURITY WARNING IS TURNING THE HEAT UP ON COLD STORAGE

The FBI recently announced that healthcare providers can expect a new wave of ransomware attacks, accelerating the need for cold storage solutions to protect your data.

Iron Mountain recommends healthcare providers use a multi-tiered data protection strategy that embraces cold storage as an air-gapped deterrent to these risks and threats.

HOW WE GOT HERE (TIMELINE)

- Over the course of October 2020 experts tracked a 71% increase in ransomware attacks against US hospitals.
- Within a span of two days, six U.S. hospitals were hit by ransomware attacks prompting the federal authorities and IT security experts to issue an industry-wide warning.
- By month's end, the Federal Bureau of Investigations (FBI), Human Health and Services (HHS) and the Cyber Security and Infrastructure Security Agency under the Department of Homeland Security issued a warning to healthcare providers to elevate protection against ransomware which is responsible for 75% of attacks

THE PERFECT STORM

These attacks come at a time when providers are feeling most vulnerable.

- **Growth Outpacing Infrastructure:** In today's healthcare ecosystem there are seemingly infinite sources and formats of data – which is growing at a CAGR of 36%. At the same time, roughly 60 to 80% of IT budgets are tied up in maintaining legacy applications and mainframe components. In the face of these dynamics, it is extremely difficult for health IT leaders to allocate the full scale of budget and resources required to ensure their data protection infrastructure and policy keep up. In fact, today only 4% to 7% of a health system's IT budget is in cybersecurity, compared to about 15% for other sectors such as the financial industry.
- **Connected Devices and IoT Creating New Vulnerabilities:** The increased adoption of connected devices in healthcare has advanced the quality of care and transformed care delivery. Yet, it has also introduced new cybersecurity vulnerabilities that elevate risk.

"THIS IS THE MOST SIGNIFICANT CYBER THREAT I'VE SEEN IN THE UNITED STATES IN MY CAREER..."

Charles Carmakal, chief technology officer of cybersecurity firm Madiant, told The Wall Street Journal

IRON MOUNTAIN®

DID YOU KNOW ONLY 4% TO 7% OF A HEALTH SYSTEM'S IT BUDGET IS IN CYBERSECURITY, COMPARED TO ABOUT 15% FOR OTHER SECTORS SUCH AS THE FINANCIAL INDUSTRY?

According to Gartner, more than 25 percent of cyberattacks in healthcare delivery organizations will involve the Internet of Things (IoT). In other words, criminals now pose a threat to more than PHI. They have the means to deploy attacks that put patient health and safety at risk.

- **Regulatory Bodies Softened Security Requirements in the Wake of COVID:** As COVID emerged, regulating bodies relaxed security requirements to enable providers to quickly spin up telehealth support and scale COVID-19 testing sites. While this change was very necessary to safely and rapidly meet care delivery demands, it has undoubtedly created gaps in healthcare providers' data protection program that have left them more vulnerable to cybersecurity threats.

IN THE FACE OF RISING THREATS, COLD STORAGE EMERGES A CRITICAL ELEMENT IN ENABLING DATA PROTECTION AND CONTINUITY OF CARE

In order to evolve with the ever-expanding security risks of today's increasingly virtual healthcare environment, IT leaders need to rethink how they protect growing archives of data and the hardware and systems used to manage it. Using a multi-tiered approach to data protection that includes cold storage, providers can effectively control costs while keeping up with the changing face of cybersecurity threats and requirements.

Iron Mountain's Iron Cloud Secure Offline Storage (SOS) lets organizations easily move inactive data from cloud (or disk) to tape, decreasing storage costs, ensuring long-term archival data compliance and protecting against ransomware. By moving inactive data offline to reliable tape, data is now protected in a secure air-gapped vault. Iron Cloud SOS's Vault Lock option offers another layer of protection by using multi-factor authentication for the safe retrieval of offsite data.

HOW IT WORKS

1. upload data and objects to a secure storage bucket (S3)
2. data and objects are then transferred to Iron Mountain's Iron Cloud
3. once received, data is downloaded to air-gapped tape where it is stored offline in a highly secure, climate-controlled vault for safekeeping
4. to retrieve data, simply make a request online
5. Iron Mountain verifies your credentials and returns the requested data via a secure storage bucket (S3)

Fight Cybersecurity Threats and Ransomware with a Vendor You Trust

Iron Mountain works with you to determine the best data strategy to securely store and protect your data. Our technology-agnostic approach lets you:

1. migrate all your data based on use – active or inactive – providing right place, right price savings
2. move data from cloud (or disk) to resilient offline storage without paying egress fees
3. integrate your backup applications and archival systems with our geo-redundant, energy-efficient Iron Cloud
4. keep data accessible with easy retrieval and data restore options

LEARN MORE AT
www.ironmountain.com/sos

WE PROTECT WHAT YOU VALUE MOST™

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.