IRON MOUNTAIN®

ARE YOU READY?

WHEN **RANSOMWARE** STRIKES, DO YOU HAVE A PLAN TO RECOVER?

Ransomware attacks and cybersecurity threats are on the rise and can disrupt your business, resulting in data loss, security breaches, and possible financial and brand damage. Hackers don't discriminate: if your IT infrastructure is vulnerable, they will find a way in. Once inside, ransomware spreads, causing extensive damage as it moves through your organisation's systems and devices. Even if you find it immediately and begin remediation, most infections aren't uncovered for at least 24 hours. And the longer the ransomware spreads, the longer it will take to remove it. Not to mention, hackers may have stolen data and are demanding payment to release it.

ARE YOU AWARE?

Ransomware will attack a business every **11 seconds** by the end of **2021**.
(Cybercrime Magazine)

ENERGY

ARE YOU AWARE?

In **2020**, the severity of ransomware attacks increased **47%**, with a **100%** spike in the number of attacks.
(Department of the Treasury)

Oil and gas pipelines span millions of miles around the world and are prime targets for sabotage, as evidenced by the Colonial Pipeline ransomware attack. Recent Frost & Sullivan research states that much of the world's pipeline infrastructure lacks real-time monitoring and that the oil and gas industry is long overdue for technology upgrades to safeguard data and modernise infrastructure. Also, the utilities industry is at a crossroads: grid modernisation, increased use of smart meters, consumer demand for affordable, reliable, and environmentally sustainable electricity, as well as growing compliance and government regulations, while operating with a lean workforce and aging systems, are just a few of the challenges you face. The last thing you need to deal with is a ransomware attack.

HEALTHCARE

The healthcare ecosystem has seemingly infinite sources and formats of data, and it's growing – at a CAGR of 36 percent. At the same time, roughly 60 to 80 percent of IT budgets are tied up in maintaining legacy applications and mainframe components. It's extremely difficult for health IT leaders to allocate the full scale of budget and resources required to ensure that both IT infrastructure is protected and that data is retained as expected for compliance reasons. Yet budget isn't the only challenge. The complexity of managing cybersecurity has grown exponentially. The pace at which cybercriminals evolve their attacks has accelerated, while the sheer volume of attacks continues to climb.

ARE YOU AWARE?

Today, only **4** to **7%** of a health system's IT budget is in cybersecurity, compared to about **15%** for other sectors.
(Healthcare Finance News)

FINANCIAL SERVICES

ARE YOU AWARE?

53% of financially motivated breaches were caused by malicious attacks with the average cost of **$3.86M**
(IBM Security and the Ponemon Institute)

With the increasing frequency and severity of ransomware attacks, in order to reduce the losses caused as much as possible, it is recommended that you regularly back up, air gap, and password protect backup copies offline and use multifactor authentication where possible. Modernising IT will require breaking down traditional silos, while also finding ways to protect and retain access to legacy data, and building out stronger, more resilient data protection strategies for the future.

ALL ORGANISATIONS

Security and compliance mandates are driving you to look at how you are protecting your organisation from ransomware attacks and other cyber threats. With a limited IT budget, you need solutions that protect your organisation's data but that are cost-effective, secure, and can also help you recover should the worst-case scenario happen.

ARE YOU AWARE?

July **2020** Gartner report predicts that cybersecurity threats and ransomware attacks will impact **95%** of organisations through **2024**.
(Gartner)

THE THREAT IS REAL; NOW IS THE TIME TO PREPARE

Since ransomware can happen to any organisation at any time, you need a cost-effective, long-term storage solution with built-in safeguards for ransomware recovery to protect your data. With Iron Mountain, you can create an **air-gapped gold** copy of your valuable data that is stored offline and retrievable using multifactor authentication to ensure secure recovery. You have the ability to fail over to Iron Mountain to keep day-to-day business operations going if the worst-case scenario occurs, you can also verify your data is not corrupted before you restore.

READY TO PREPARE?
READY TO RECOVER?
Contact Iron Mountain today.

0861 476 668
IRONMOUNTAIN.CO.ZA