CLOUD COMPUTING
BUILDING A SOLID BACK-UP INFRASTRUCTURE AND DISASTER RECOVERY STRATEGY

SAVVAS DELIS

SALES MANAGER - MARPOINT

MarPoint

A BIT OF HISTORY

All four of the world's largest shipping companies have now been hit by cyber-attacks

1. **APM-Maersk** - ransomware/wiper - 2017.
2. **Mediterranean Shipping Company** - unnamed malware.- April 2020
3. **COSCO** - ransomware - 2018.
4. **CMA CGM**, ransomware, in September 2020 / leak of data, September 2021

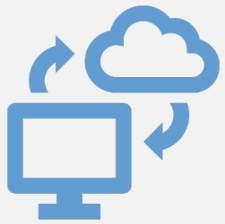
IS THE CLOUD A GOOD INVESTMENT ?

IS THE CLOUD EXPENSIVE?

- No capital expenses for hardware procurement. Infrastructure is acquired and used as needed and is billed only for the resources consumed.

- AWS's on-demand model for disaster recovery is far more cost effective for the enterprise than complex systems in-house.

IS THE CLOUD CAPACITY LIMITED?



Marpoint has the experience to offer AWS services for any given organization or business case; be it bandwidth-demanding or compute-heavy, there is basically no IT-based need that our customers' business has, that AWS cannot handle.

IS THE CLOUD SAFE?

- First of all, AWS now spans 77 Availability Zones within 25 geographic regions around the world.
- AWS data centers and network architectures are built to meet the requirements of the most security-sensitive organizations.
- Shared Responsibility: You will provide security and configurations of your software components and AWS will provide security for its infrastructure.
- Customer-Only Responsibility: You are fully responsible for guest operating systems, deployed applications, and select networking resources (for example, firewalls).
- AWS-Only Responsibility: AWS manages the cloud infrastructure, including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software.

DISASTER RECOVERY AS A SERVICE

DR in the cloud

- No upfront hardware investment needed
- Only pay for rightsized compute/storage when actually needed
- Lower IT management overhead
- (MUCH!) More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days!)

DISASTER RECOVERY PLAN – THE IMPORTANCE OF RTO AND RPO

WHAT IS THE DIFFERENCE BETWEEN RTO AND RPO?

- Since Recovery Time Objective (RTO) is the timeframe in which applications and systems must be restored following a disaster.

- On the other hand, Recovery Point Objective (RPO) looks at how much data an organization can lose before it begins to impact business operations.

- So, what do RTO and RPO have in common? Ideally, the numbers should be as close to zero as possible.

MULTIPLE LEVELS OF DR ACROSS A SPECTRUM OF COMPLEXITY AND TIME

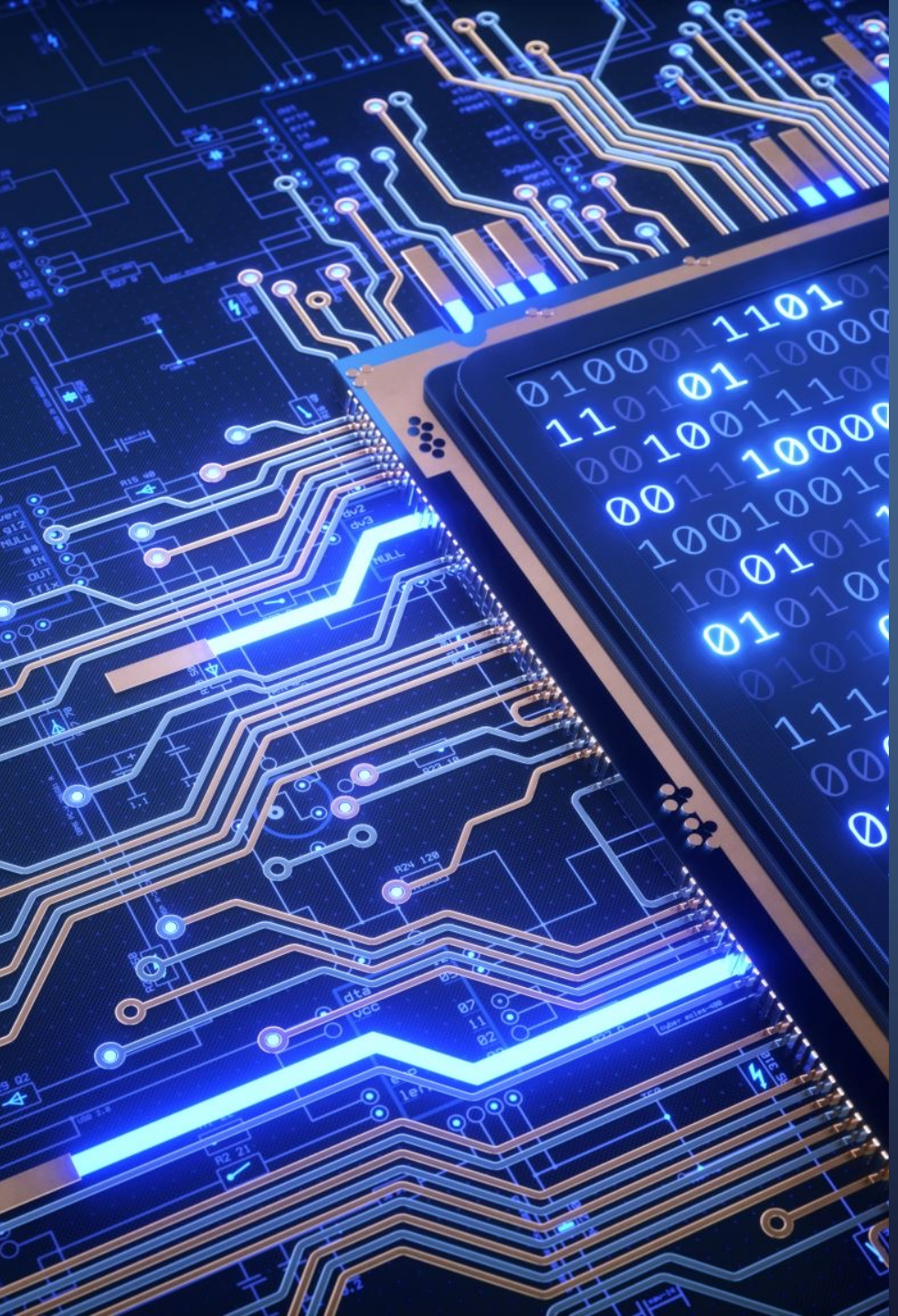
Lower priority use cases	Auto-failover of your environment in AWS (Real-time)
• Solutions: Amazon S3, • AWS Storage Gateway • Cost: $	• Cost: $$$$

CLOUD DISASTER RECOVERY PLAN – MIGRATION TO THE AWS CLOUD

This journey starts with…

- Understanding your infrastructure and outlining any risks
- Conducting a Business Impact Analysis
- Creating a DR Plan based on your RPO and RTO
- Building your Cloud DR infrastructure
- Putting your Disaster Recovery Plan on paper
- Testing/Testing/Testing your DR Plan often

In relation to this, Marpoint comprehensive Cloud DR migration strategy involves working with you to provide a robust cloud migration assessment of your applications and dependencies before delivering your migration solution



2. HOW DOES THE ROLE OF IT MANAGED SERVICES CHANGE IN SHIPPING?

MarPoint

WHY IT MANAGED SERVICES?

1. Remote Access 24/7/365, total control over IT operations, peace of mind to stakeholders

2. Focus solely On Your Business Objectives

3. Minimized & Predictable Costs

4. Increase Efficiencies & Improve Response Times

5. Data Security, Compliance, and Risk Management

A CONCLUDING NOTE

Looking beyond the COVID-19 crisis., at Marpoint, are OPTIMISTIC. We believe that working together with you, we can exploit the merits of technology, business good practices and social well-being so as to build a better Maritime IT Services world!