



CYBER DIGITAL WORLD

NEWSLETTER

Volume: 57

MAY 2026

Securing the Cloud: Avoiding Costly Misconfigurations in Caribbean Organizations



INTRODUCTION



Dr. Ronald Walcott
Managing Director

Cloud technology has transformed how organizations operate. Across Trinidad and Tobago and the wider Caribbean, businesses are rapidly adopting cloud platforms to improve flexibility, scalability, collaboration, and cost efficiency. From financial services and healthcare to retail and government operations, cloud adoption is accelerating digital transformation throughout the region.

However, while cloud technologies create tremendous opportunities, they also introduce new cybersecurity risks. One of the biggest misconceptions organizations make is believing that moving to the cloud automatically makes systems secure. In reality, many cloud breaches

occur not because cloud providers fail, but because organizations misconfigure their own environments.

At Precision Cybertechnologies, we have seen firsthand how small configuration errors can expose sensitive data, weaken identity controls, and create visibility gaps attackers actively exploit. This month's newsletter explores the risks associated with cloud adoption, the importance of understanding the shared responsibility model, and why continuous cloud security monitoring has become essential for Caribbean organizations.

UNDERSTANDING CLOUD SECURITY RISKS

1. The Caribbean's Growing Dependence on Cloud Services

Organizations throughout the Caribbean are increasingly relying on cloud platforms such as, Mi-

crosoft 365, Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) & SaaS business applications.

Cloud adoption supports remote work, business continuity, and digital service delivery. For many organizations, the cloud reduces infrastructure costs while improving operational agility.

However, cloud migration often occurs faster than security maturity develops. Organizations focus heavily on deployment and availability while overlooking critical security configurations.

This creates an environment where attackers can exploit weak identity controls, exposed storage systems, and poorly monitored cloud activity.

2. Misconfigurations: The Leading Cause of Cloud Breaches

One of the most important realities in cloud security is this:

Most cloud breaches are caused by customer misconfigurations, not cloud provider failures.

CONTINUED ON PAGE 2

IN THIS ISSUE:

SECURING THE CLOUD: AVOIDING COSTLY MISCONFIGURATIONS IN CARIBBEAN ORGANIZATIONS

UPCOMING EVENTS

Misconfigurations occur when cloud resources are deployed insecurely or monitored improperly.

Common examples include: - **Publicly exposed cloud storage buckets, Weak or excessive user permissions, Disabled logging and monitoring, Misconfigured firewalls and security groups, Unsecured APIs and integrations and even Unpatched cloud-hosted applications.**

Even a single incorrectly configured setting can expose sensitive customer records, financial data, or internal systems to the internet.

Cybercriminals actively scan cloud environments looking for these weaknesses because they know many organizations fail to validate configurations after deployment.

3. Understanding the Shared Responsibility Model

A major challenge in cloud adoption is misunderstanding the shared responsibility model.

Cloud providers secure the infrastructure itself including physical data centers, networking, and underlying hardware. However, organizations remain responsible for securing:

- User identities and accounts
- Access permissions
- Data protection
- Endpoint security
- Application security
- Configuration management
- Monitoring and logging

For example, if an organization exposes sensitive files through a publicly accessible cloud storage bucket, the cloud provider is not responsible for that exposure.

Understanding where provider responsibility ends and customer responsibility begins is critical for effective cloud security.

4. Identity Security: The New Cloud Perimeter

Traditional network perimeters continue to disappear as organizations move applications and data into cloud environments.

Today, identity has become the new perimeter.

Attackers increasingly target: - Weak passwords, Poorly enforced multi-factor authentication (MFA), Over-privileged accounts and Stolen credentials.

Once attackers gain legitimate cloud credentials, they often blend into normal activity, making detection difficult.

Common cloud identity risks include:

- Shared administrator accounts
- Lack of conditional access policies
- Inactive accounts with elevated privileges
- Insufficient monitoring of login anomalies

Strong identity governance is now one of the most important components of cloud security.

5. Why Visibility Matters in Cloud Environments

One of the biggest cybersecurity challenges in cloud environments is maintaining visibility.

Unlike traditional on-premise infrastructure, cloud systems are highly dynamic:

- New resources are deployed rapidly
- Remote users connect from multiple locations
- Applications integrate through APIs
- Workloads scale automatically

Without centralized monitoring, organizations may struggle to identify:

- Unauthorized access attempts
- Suspicious administrator actions
- Data exfiltration activity
- Compromised accounts
- Misconfigured services

Many organizations assume cloud environments are self-monitoring, only to discover during incidents that logging was incomplete or disabled entirely.

Continuous visibility is essential for detecting threats before they escalate.

6. Cloud Threats Facing Caribbean Organizations

As digital transformation expands regionally, Caribbean organizations face growing exposure to cloud-based attacks.

Common threats include:

Credential Theft

Attackers steal Microsoft 365 or cloud platform credentials through phishing attacks and use them to access sensitive data.

Business Email Compromise (BEC)

Compromised cloud email accounts allow attackers to impersonate executives or vendors.

Ransomware Targeting Cloud Backups

Threat actors increasingly target connected cloud backup repositories to prevent recovery.

Shadow IT

Employees sometimes deploy unauthorized cloud applications without security oversight, increasing risk exposure.

Insider Threats

Misuse of privileged cloud access can result in accidental or intentional data exposure.

Organizations must recognize that cloud adoption expands the attack surface significantly if security controls are not properly implemented.

7. The Role of MSSPs in Cloud Security Monitoring

Many organizations lack the internal resources or expertise required to monitor cloud environments continuously. This is where Managed Security Service Providers (MSSPs) play a critical role.

At Precision Cybertechnologies, cloud security monitoring focuses on:

- Continuous threat detection
- Identity monitoring and anomaly detection
- Log analysis across cloud platforms

- Security posture assessments
- Incident response support
- Configuration auditing

Through Managed Detection and Response (MDR) and Security Operations Center (SOC) services, MSSPs help organizations maintain visibility across complex cloud environments.

Rather than reacting after a breach occurs, MSSPs help organizations identify suspicious activity early and reduce attacker dwell time.

8. Building a Secure Cloud Strategy

Cloud security is not achieved through a single tool or platform. It requires ongoing governance, monitoring, and operational discipline.

Organizations should prioritize:

Multi-Factor Authentication (MFA)

MFA significantly reduces the effectiveness of stolen credentials.

Least Privilege Access

Users should only have access necessary for their roles.

Continuous Monitoring

Cloud activity should be monitored in real time.

Security Awareness Training

Employees remain a major target for credential theft attacks.

Regular Security Assessments

Cloud configurations should be audited frequently to identify exposure risks.

Backup Validation

Cloud backups should be tested regularly and isolated from production systems where possible.

A proactive approach to cloud security reduces the likelihood of costly breaches and operational disruption.

Organizations that invest in secure cloud architecture and continuous monitoring position themselves to grow confidently in an increasingly digital economy.

9. Cloud Security Is Business Security

Cloud environments now support critical business functions, customer communications, financial operations, and sensitive data storage.

As a result, cloud security is no longer simply an IT concern - it is directly tied to:

- Business continuity
- Customer trust
- Regulatory compliance
- Financial stability
- Organizational reputation



UPCOMING EVENTS

RSA CONFERENCE 2026 – SAN FRANCISCO, USA
Sessions covering cloud security, identity protection, and AI-driven threat detection

AWS RE:INFORCE 2026
Focused on cloud security strategy, compliance, and architecture best practices.

SANS INSTITUTE CLOUD SECURITY TRAINING SERIES 2026
Hands-on cloud defense and incident response workshops.

CARIBBEAN CYBER SECURITY CENTRE REGIONAL DIGITAL TRANSFORMATION FORUM 2026
Discussions on securing digital innovation across Caribbean industries.



Frequently Asked Questions:

DOES MOVING TO THE CLOUD AUTOMATICALLY IMPROVE SECURITY?

No. Cloud providers secure the infrastructure, but organizations remain responsible for securing their data, identities, configurations, and access controls.

WHAT IS THE BIGGEST CLOUD SECURITY RISK TODAY?

Misconfigured cloud resources and compromised identities remain the leading causes of cloud-related breaches

WHY IS MULTI-FACTOR AUTHENTICATION SO IMPORTANT IN CLOUD ENVIRONMENTS?

Cloud services are accessible from anywhere. MFA helps prevent attackers from accessing accounts even if passwords are stolen.

CAN SMALL ORGANIZATIONS BENEFIT FROM CLOUD SECURITY MONITORING?

attackers assume they have weaker defenses and less monitoring visibility.



868-610-7237



info@precision-cyber.com



www.precision-cyber.com



Ground Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad