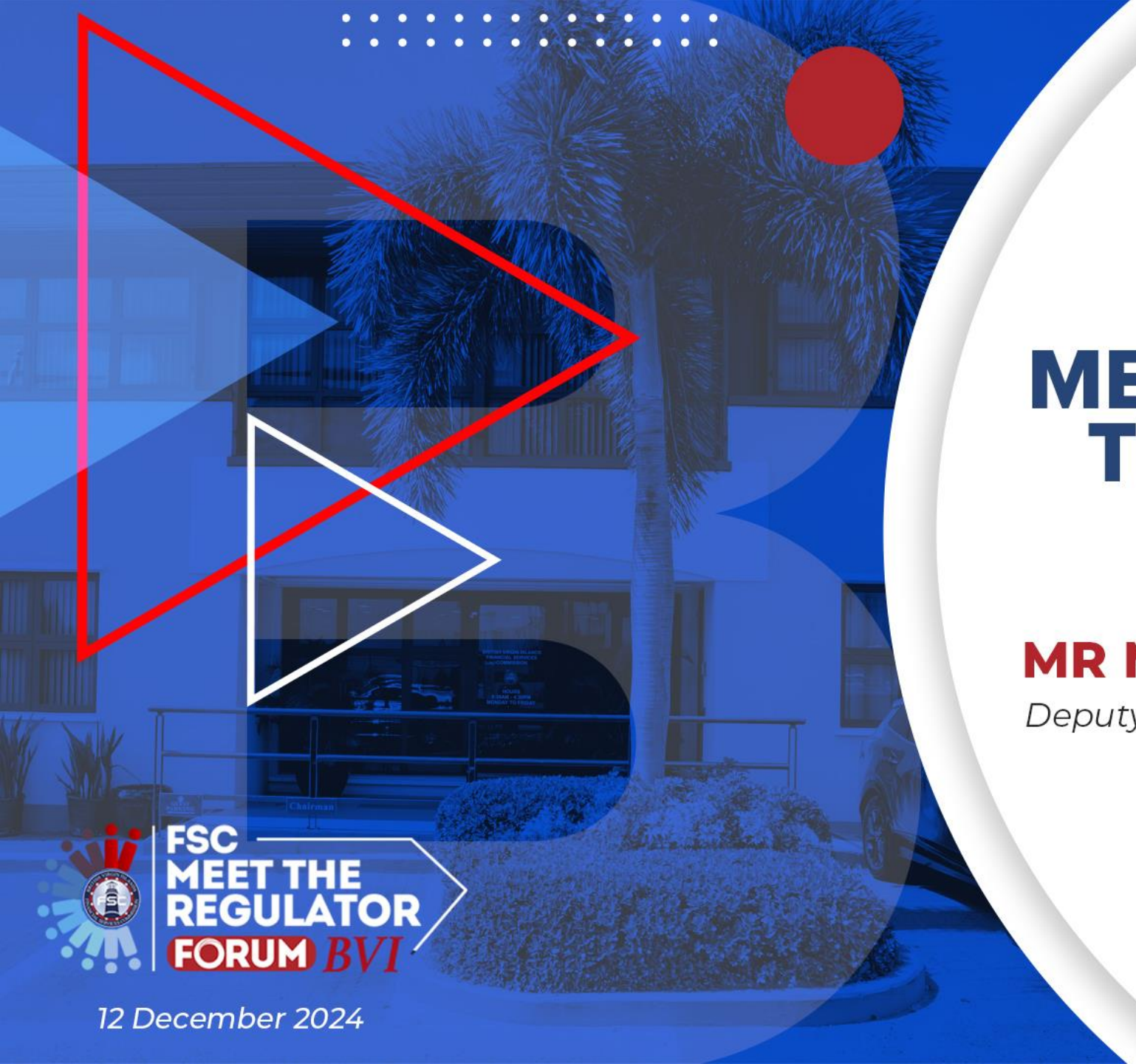


FSC MEET THE REGULATOR FORUM BVI

12 December 2024

SECURITY MECHANISMS AND THE BO SYSTEM

MR MICHAEL GEORGE

Deputy Director, Information Technology

Security and Confidentiality

- Security and confidentiality of all data in VIRRGIN as FSC's highest priority

ISO 270001-certified resources

world-class security partner resources manage our technology solutions

User Authentication

- **FSC Internal Users**:
  - Authenticated via FSC's Active Directory (User ID and password).
  - Requires MFA
- **Role Based Access Control**
  - Users only see what they are permitted to
- **Agent Users and Non-Agent Users**:
  - Authenticated by User ID and password issued by VIRRGIN system.
  - ***NEW* Multi-Factor Authentication (MFA)**:
    - Required for all users to access VIRRGIN.

Geographic Access Restrictions

Agent and Non-Agent Users:

- Access restricted to the British Virgin Islands (BVI).
- System checks every connection to VIRRGIN to ensure connection originates from BVI.

VIRRGIN Lite

- Restricted access to verified users for specified transactions

Access Control Mechanisms

- **Password Protection**:
  - Passwords transmitted and stored using one-way encryption.
  - Prevents anyone, including administrators, from reading passwords in clear text.
- **Granular Access Control:**
  - Fine-tuned permissions ensure sensitive data is accessible only to those who need it for their role.
- **Automatic Logout**:
  - Disconnects inactive users after 30 minutes of inactivity.
- **Failed Access Attempts**:
  - Monitors consecutive failed login attempts.
  - Locks account after reaching a set threshold.

Audit and Encryption

Comprehensive Audit Trails:

- All user activities within the application are logged and monitored.
- This creates transparency and allows us to identify and address suspicious behaviour quickly.

End-to-End Encryption:

- Data is encrypted both in transit and at rest
- Ensuring it is unreadable to unauthorised users even if intercepted.

Infrastructure Security

- **Endpoint Protection**:
  - Protects against viruses and malware.
  - Intrusion Prevention System (IPS) protection.
- **Network Security**
  - Firewalls that provide additional IPS protection
  - Network segmentation
  - Enforces rules to limit types of traffic in and out of the network and between servers and switches.
- **Access Limitation**:
  - Limits access to VIRRGIN from BVI IPs, Hong Kong / VIRRGIN Lite agent IPs.
  - HTTPS connections via SSL for external access to VIRRGIN.

Continuous Monitoring and Protection

Ongoing Monitoring:

- Detection and response on all VIRRGIN hardware, both on-premises and in the DR.
- Dedicated team of cyber security engineers monitoring logs and our network traffic

Vulnerability Scanning:

- Continuous scanning and remediation of vulnerabilities.

Managed Risk

- Network End-Point scanning, assessing and mitigating

How These Measures Protect You

- **Reduced Risk of Unauthorised Access:**
  - By combining MFA, geographic restrictions, and AD-controlled access, the system ensures that only the right people get in.
- **Data Integrity and Confidentiality:**
  - Encryption and network safeguards maintain data privacy.
- **Accountability:**
  - Audit trails and access controls provide transparency, so actions are always traceable.
- **Quick Incident Response:**
  - MDR services enable rapid containment of threats to minimize risk.

How can you help?

We, the users, are the weakest link

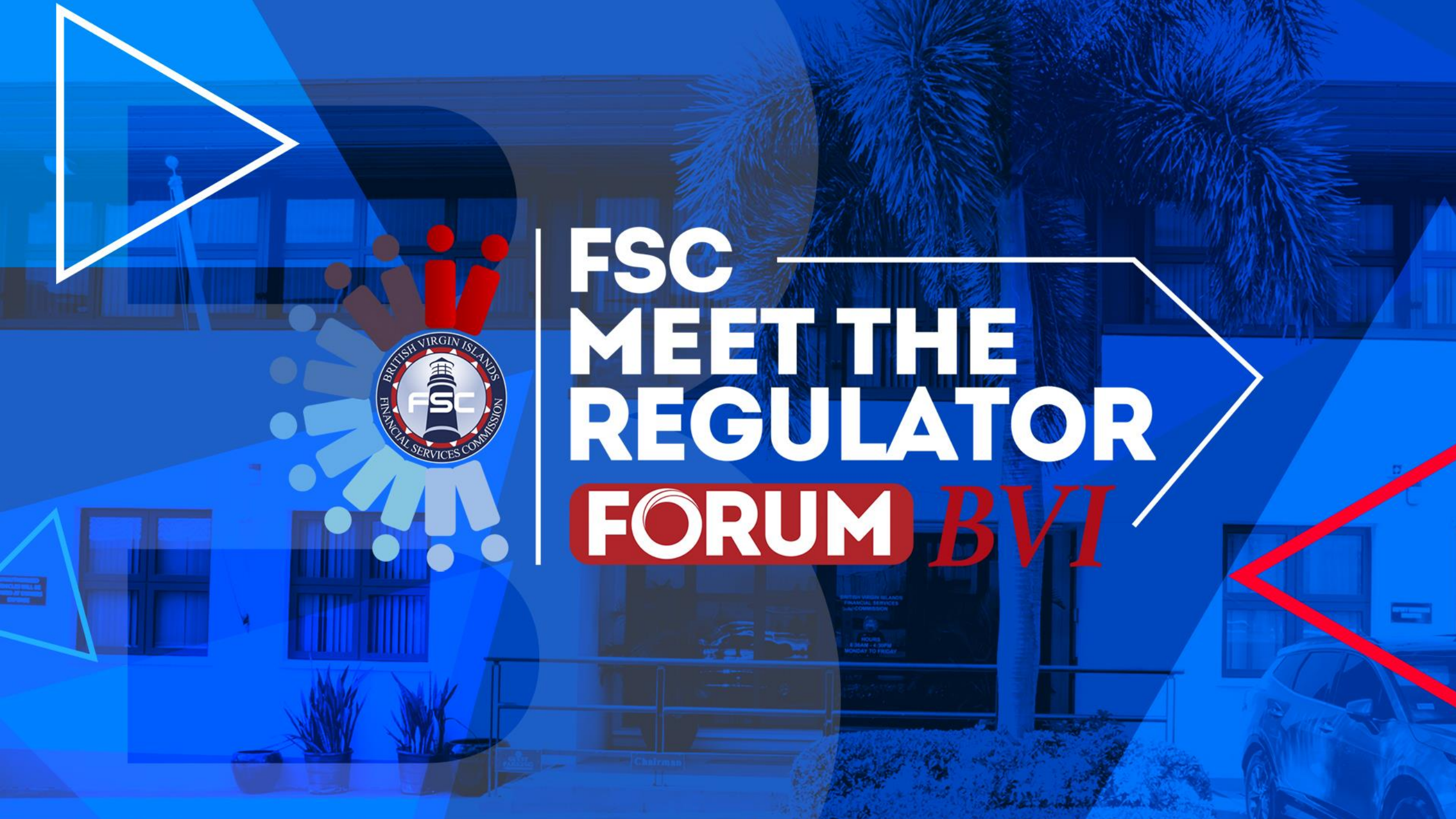
You may recall the various breaches in recent years

- Most, if not all, were a result of something done or not done by a user.

Partner with us to ensure that your staff is trained to recognise security red flags; awareness is key!

Cyber Security engineers are coming up with more and more ways to get to our corporate and personal data.

Stay Vigilant!


FSC
MEET THE
REGULATOR
FORUM BVI