40 ANNIVERSARY
STABLE | TRANSFORMATIVE | ACCOUNTABLE | RESILIENT

AML/CFT NEWSLETTER

ISSUE 9 MARCH 2023

WHAT'S THE BUZZ ABOUT VIRTUAL ASSETS?

Virtual Assets

While there has been a rapid growth of virtual assets (VAs) worldwide, a study conducted by the Caribbean Financial Action Task Force (CFATF)[1] reported a lack of knowledge, and to some extent, confusion about what VAs are.

The Financial Action Task Force (FATF) defines a VA as any digital representation of value that can be digitally traded, transferred and can be used for payment or investment purposes. It does not include digital representation of fiat currencies or securities[2]. The presence of VAs has grown rapidly and is becoming part of the financial landscape throughout the Eastern Caribbean Currency Union (ECCU) and the wider Caribbean. Therefore, it is important that persons understand what are VAs and how it may impact us.

THIS ISSUE'S CONTENT

Virtual Asset Service Providers

We cannot discuss VAs without speaking about Virtual Asset Service Providers (VASPs). VASPs are natural or legal persons who are not covered elsewhere under the FATF 40 Recommendations. VASPs as a business, conducts one or more of the following activities or operations, for or on behalf of another natural or legal person:

- Exchange between VAs and fiat currencies;
- Exchange between one or more forms of VAs;
- Transfer of VAs;
- Safekeeping and/or administration of VAs or instruments enabling control over VAs; and
- Participation in and provision of financial services related to an issuer's offer and/or sale of VAs.

Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF) concerns related to VAs and VASPs

VAs aim to make payments easier, faster, cheaper, more convenient and provide an alternative payment to persons without regular financial products. However, as with any other financial product, criminals identify opportunities for misuse of VAs, to facilitate laundering of criminal proceeds or finance their illicit activities. If not adequately monitored and regulated VASPs can assist these criminals in their abuse of the financial system. According to a 2022 blockchain analysis report by Chainalysis[3], criminals laundered $8.6b in 2021 through the use of cryptocurrency, representing a 30.0 per cent increase from 2020. Associated predicate crimes include large-scale fraud, child abuse material, theft, ransomware, and terrorist financing. Concerns may surround customers' transaction patterns, anonymity, source of funds and geographic risks.

What is expected from Licenced Financial Institutions (LFIs)

The treatment of VAs is no different from any other business relationship an LFI engages with. To mitigate the risk associated with VASPs' relationships and VAs transactions, LFIs are required to:

- Understand the legislative framework related to VAs and VASPs;
- Draft and implement a framework for identifying, verifying and monitoring VASPs;
- Understand the unique features of VAs and how criminals can acquire, move and store them;
- Understand the associated risks and determine their appetite for establishing business relationships and conducting transactions involving VAs and VASPs;
- Identify and conduct adequate due diligence on beneficial owners, directors and officers of VASPs;
- Monitor business relationships and transactions involving VAs and VASPs; and
- Report suspicious activities involving VAs transactions.

1 https://www.cfatf-gafic.org/
2 Fiat currency refers to currency that is declared as legal tender and backed by a country's government. For example, the Eastern Caribbean Dollar or United Stated Dollar.
3 https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

REGULATORY UPDATES

1

THE JUDICIAL COMMITTEE OF THE PRIVY COUNCIL JUDGMENT: JAMAICAN ATTORNEYS–AT–LAW TO COMPLY FULLY WITH PROCEEDS OF CRIME ACT AS DESIGNATED NON-FINANCIAL INSTITUTIONS

On 29-30 November 2022, the Judicial Committee of the Privy Council (JCPC) heard the appeals relating to whether Jamaica's Anti-Money Laundering Legislation, as it applied to lawyers (also known as attorneys), was attuned with the Constitution of Jamaica. The Jamaican Bar Association, which represents attorneys, argued that that the duties imposed by the Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) regime upon Attorneys-at-Law were unconstitutional on a number of grounds. The JCPC declared on 9 February 2023 that the AML/CFT regime of Jamaica did not breach constitutional rights of attorneys and clients. Therefore, the decision of the Full (Constitutional) Court of Jamaica upholding the relevant AML/CFT legislation as it applies to Attorneys-at-Law should be restored.

READ MORE

https://www.cfatf-gafic.org/home/what-s-happening/776-the-judicial-committee-of-the-privy-council-jcpc-judgment-jamaican-attorneys%E2%80%93at%E2%80%93law-to-comply-fully-with-proceeds-of-crime-act-as-dnfisl

RESULTS OF THE FEBRUARY 2023 FATF PLENARY

The second Plenary of the FATF under the Presidency of T. Raja Kumar of Singapore, took place in Paris over the period 22-24 February 2023.

2

The Plenary discussed the ongoing Russian invasion of Ukraine, noting that it was one (1) year after the Russian Federation's illegal, unprovoked and unjustified full-scale military invasion of Ukraine. As a result, the FATF Plenary suspended the membership of the Russian Federation. Following the statements issued since March 2022, the FATF reiterated that all jurisdictions should be vigilant to emerging risks from the circumvention of measures taken against Russia in order to protect the international financial system.

FATF members agreed to release finalised guidance related to Recommendation 24, as it relates to beneficial ownership transparency for legal persons and agreed amendments to Recommendation 25, which aims to improve beneficial ownership transparency for trusts and similar legal arrangements. The guidance was published in March 2023.

The FATF also noted that the scale and number of ransomware attacks has increased significantly in recent years. The FATF completed research that analyses the methods that criminals use to carry out their ransomware attacks and the methods by which the ransom payments are laundered. This report was published in March 2023 and includes a list of risk indicators that can help public and private sector entities identify suspicious activities related to ransomware.

The Plenary reiterated its focus for VAs and VASPs by agreeing on a roadmap to strengthen implementation of FATF Standards on VAs and VASPs. The roadmap will include an assessment of the current levels of implementation VAs regulatory frameworks across the global network.

The FATF has also finalised a report that explores the link between ML, art and antiquities. The report includes a list of risk indicators that can assist public and private sector entities towards the identification of suspicious activities in the art and antiquities markets. It also emphasized the importance of rapidly identifying and tracing cultural objects involved in ML or TF. This report was published on 27 February 2023.

In concluding, the Plenary announced that Mr Jeremy Weil, from Canada had been selected as the next FATF Vice President.

https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html

UPDATES TO FATF BLACK AND GREY LISTS

On 24 February 2023, the FATF added Nigeria and South Africa to its list of jurisdictions under increased monitoring known as the *"grey list"*. The FATF also noted Cambodia and Morocco's progress in improving their respective AML/CFT regimes covered by their individual action plans and as such both countries were removed from the grey list.

Additionally, there were no changes to the group of high-risk jurisdictions that have significant strategic deficiencies in their regimes to counter ML, TF, and PF, known as the "*black list*".

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2023.html

BRITISH VIRGIN ISLANDS, COSTA RICA, MARSHALL ISLANDS AND RUSSIA ADDED TO EUROPEAN UNION LIST OF NON-COOPERATIVE JURISDICTIONS FOR TAX PURPOSES

The European Union (EU) added four (4) countries to its list of Non-Cooperative Jurisdictions for Tax Purposes as at 14 February 2023. These jurisdictions included the British Virgin Islands, Costa Rica, Marshall Islands and Russia. The EU list now consists of sixteen (16) jurisdictions.

Anguilla remains the only Eastern Caribbean Currency Union (ECCU) member territory on the list having been added to the EU list of Non-Cooperative Jurisdictions for Tax Purposes on 4 October 2022. The Bahamas and Turks and Caicos Islands, Trinidad and Tobago, Panama and the US Virgin Islands are the other Caribbean jurisdictions currently listed by the EU.

https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/taxation-british-virgin-islands-costa-rica-marshall-islands-and-russia-added-to-eu-list-of-non-cooperative-jurisdictions-for-tax-purposes/

LAWMAKERS ADVANCE EU AML ACTION PLAN

The European Parliament on 28 March 2023 approved comprehensive plans to overhaul the bloc's AML regime, including establishing a new, EU-wide AML Supervisor.

The proposed AML regime include establishing the Anti-Money Laundering Authority (AMLA), development of a new AML directive and an AML regulation, that will apply uniformly across the EU member states. The parliament also recommended a number of amendments to further strengthen the measures including lowering the threshold at which financial institutions must identify the beneficial owners of legal entities they serve, and reducing a proposed €10,000 limit on cash payments to €7,000.

The proposed AMLA will directly supervise a limited number of financial institutions and serve as an information-sharing hub for financial intelligence units. Members of the EU Parliament also wants the AMLA to become the bloc's coordinator for sanctions, amid concerns over uneven implementation and enforcement of EU financial and trade embargos by member states. The Parliament will enter negotiations on the AML package with national governments and the European Commission, the bloc's executive arm, later this year.

READ MORE

MoneyLaundering.com :: Changes in Bank Regulations, Financial Compliance Regulations, Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training

MONEY LAUNDERING AS A SERVICE

Money Laundering as a service (MLaas) refers to the provision of ML services by individuals or entities. This can involve providing tools, techniques, and services to help criminals launder their funds, often for a fee or commission. It can involve the use of cryptocurrency exchanges, online recruitment campaigns and machine learning to facilitate ML. For example, in order to grow their criminal enterprises, cyber-criminal organisation may use money mules. Money mules are individuals who are recruited to assist with the laundering of money, at times they may be recruited under false pretences, with the promises of legitimate jobs, only to realise they were recruited to launder illegally obtained funds. Traditionally, this was done using wire transfers, however, criminals are increasingly using crypto-currencies to avoid leaving an audit trail. This is due to their anonymous nature and the lack of adequate regulatory oversight.

The United Nations Office on Drugs and Crime, estimated the amount of money laundered globally per year was between 2.0 to 5.0 per cent of global gross domestic product or USD800.0b to USD2 trillion. Due to increased advances in automation, this trend is expected to worsen and MLaas are anticipated to increase.

In order to address the rise of MLaas, it is important for LFIs and regulators to collaborate and share risk information. This must be supported by good cyber hygiene practices and capacity building measures aimed at raising awareness.

1 Overview (unodc.org)

Sources

How Cybercriminals Are Operationalizing Money Laundering and What to Do About It (darkreading.com)
FinCEN's Financial Trend Analysis

SEEING IS BELIEVING... OR IS IT?
DEEPFAKE - IMPLICATIONS FOR COMPLIANCE

Have you seen convincing videos or photographs of famous persons making statements, you believed that were genuine, only to be informed overtime, that they were fake?

Deepfakes[1] refer to artificial intelligence sounds and images which are combined with machine learning algorithms that can manipulate media, visuals and can therefore replace an individual's voice, image, or both with similar artificial voices or likeness. They are increasingly used for nefarious purposes to create audio content and images that are fake, or make real people appear to say or do things they did not say or do.

Deepfakes are a common tool used by cybercriminals to spread misinformation or commit fraud and extortion scams. They can be used in ML schemes through the use of financial institutions. It is therefore critical that compliance professionals, regulators and other competent authorities understand the threats posed by cybercriminals using deepfake technology and adopt and implement mitigating measures. Deepfakes technology and its application can cause security and mass disinformation concerns, personal reputational and financial damage, as well as facilitate identity theft.

Deepfakes can be used in phone calls, biometric verification and email scams. Cyber criminals armed with this tool, can manipulate employees into believing that their customer or employer has provided instructions requesting the transfer of funds or other private business details. Deepfakes can be used to make traditional fraud scams more difficult to detect, for example payment fraud, email hacking or ML.

Therefore, it is important that financial institutions are aware of the risks posed by deepfake technology.

With advancement in technology, financial institutions have improved their internal processes in order to be more efficient, deliver added value to customers and to remain competitive. It is important, however, that institutions utilising technology in the customer identification and verification process, implement the necessary controls to combat deepfake advances. Particular attention should be placed on processes for on-boarding of new customers, processing transactions, communicating with customers and verification of documents received.

Investing in cybersecurity solutions and providing relevant and timely training on the risk posed by new and emerging technologies, can assist institutions in reducing the probability of successful deepfake attacks.

Red flags indicators of deepfakes include[2]: delayed or slower than normal speech, unnatural colouring of the skin, unnatural facial expressions or eye movements, facial morphing, digital background noise, awkward body positioning, varied fluctuations or intonations in voices, bad lip syncing and poor lighting.

Employees should be aware of the following red flags when receiving instructions from customers and always remember, "*when in doubt, stay out*":

1. Inconsistent communication or speech;
2. Suspicious requests or activity;
3. Urgent request and constant follow ups; and
4. Requests for secrecy and non-disclosure to other persons.

[1] What are deepfakes – How to spot a deepfake | Norton
[2] What are deepfakes – How to spot a deepfake | Norton
Source: Deepfake 101: A Threat to FIs - ACAMS Today

ECCB PROVIDES TRAINING TO LFIs IN SAINT VINCENT AND THE GRENADINES ON UPDATED ML/TF/PF RISK FACING THE BANKING SECTOR

As part of its ongoing initiatives to raise awareness on emerging ML, TF and PF risks, the ECCB hosted a virtual workshop geared at sensitising and engaging LFIs with respect to AML/CFT/CPF developments and trends in Saint Vincent and the Grenadines (SVG). The virtual workshop was held on 30 and 31 January 2022, and included presentations and discussions on the following:

- A summary of SVG's 2020 ML/TF National Risk Assessment;
- Findings of the ECCB's December 2022 Banking Sector ML/TF/PF Risk Assessment;
- The banking sector's role in the mutual evaluation process;
- Techniques for demonstrating effectiveness, presented by the Director of the Financial Intelligence Unit; and
- Risk Assessments and AML/CFT/CPF Governance Structures.

The workshop was attended by over fifty (50) participants including representatives of each LFI, the Financial Intelligence Unit and Financial Services Authority of SVG.

FEATURE

SUCCESSFUL RECIPIENT OF THE ECCB-ACAMS SCHOLARSHIP

The ECCB continues to administer the technical assistance project received from the Caribbean Development Bank, towards improving the integrity of financial transparency in the ECCU. The overall objective of this technical assistance is to strengthen AML/CFT/CPF frameworks within the ECCU and to increase the technical capacity of financial institutions and regulatory authorities. The project is subdivided into three (3) components, which included the certification of regulators as Anti-Money Laundering Specialists (ACAMs).

Accordingly, a total of fifty (50) scholarships towards certification of AML specialists were issued to regulators across the ECCU. Over the period 29 August to 1 September 2022, scholarship awardees participated in a boot camp to prepare the recipients in preparation for their certification exams. Mr Patrick George was one of the successful recipients of the ACAMs scholarship.

Mr. Patrick L. George
CAMS | CAMLFC | CFRMP | CCFTP | CCSP | CRAMLFC | CFCPAP

Mr Patrick L George is a Senior Financial Investigator with the Financial Intelligence Unit (FIU) of the Commonwealth of Dominica (Dominica). He serves as a member of Dominica's Mutual Evaluation (MEVAL) Technical Working Group that focuses on the implementation of the FATF's 40 Recommendations. Mr George has acquired over 24 years of experience in the public service inclusive of 21 years of experience in the field of AML/CFT. He is a trained 3rd and 4th Round CFATF Assessor and has participated in the assessment of Belize as the Law Enforcement Assessor.

Mr George has a certificate in Criminology from the University of the West Indies and holds certificates as an Instructor in the following fields: Anti-Money Laundering and Financial Crimes Specialist (CAMLFC), Fraud Risk Management (CFRMP), Counter-Financing of Terrorism (CCFTP), Cyber Security (CCSP), Regulatory Examiner – AML-CFT-CPF (CRAMLFC), Foreign Corrupt Practices Act -UK & US (CFCPAP).

Proficient in the installation and configuration of analytical software systems, Mr George has assisted the following jurisdictions with training in and installation/configuration of IBM i2 iBase and Analyst Notebook: Tortola, Bahamas, Trinidad and Tobago, Turks and Caicos, Grenada, Suriname, Cayman Islands, Antigua and Barbuda, Saint Vincent and the Grenadines, Guyana, Barbados and Saint Christopher (St Kitts) and Nevis. He is a trained United Nations (UN) expert in the implementation of the UN Convention Against Corruption (UNCAC), and has participated in assessments of Dominica, Qatar, Guatemala, Afghanistan and Israel regarding the implementation of the UNCAC. Mr George is a trainer of the CFATF Egmont-Developed Strategic Analysis Course.

Reflection on the ACAMS Certification

"*As a member of the FIU and the MEVAL Technical Working Group of Dominica, it was humbling to have been selected to participate in this project as the benefits of the ACAMS certification program are significant. FIUs are generally responsible for collecting and analysing financial intelligence to support law enforcement and regulatory agencies in the detection and prevention of ML, TF and other financial crimes. However, due to their hybrid structure, some FIUs are also AML/CFT/CPF Supervisory Authorities of financial institutions including designated non-financial businesses and professions (DNFBPs). Though Dominica's FIU does not have regulatory functions, by completing the ACAMS certification, I was able to further enhance my knowledge and expertise in AML/CFT/CPF and stay up-to-date on the latest trends and best practices in the field. This opportunity allowed me to gain insight into the broad scope of factors that are considered by varying private sector entities in their fight against ML/TF/PF.*

Some of the topics that stood out to me in the ACAMS certification program were: banks and other depository institutions, ML/TF red flags within various sectors and the facets of an investigations initiated by a financial organization. However, the most interesting chapter within the course content, was the characteristics of a ML/TF/PF risk assessment, in particular the distinction and principled similarities that was evident to me between a national risk assessment and an institutional risk assessment.

Through the program, FIU professionals who are also engaged in supervisory examinations of either financial institutions or DNFBPs can also learn about the latest regulatory requirements and compliance standards, which can help them stay ahead of the curve in their work.

One of the most important lessons reinforced through the ACAMS certification program was the importance of collaboration and communication in AML/CFT/CPF. FIUs and supervisory authorities must work closely with law enforcement and regulatory agencies to effectively combat ML and financial crimes. Through the program, professionals can learn how to build effective partnerships and communicate effectively with stakeholders in the AML/CFT/CPF ecosystem.

In conclusion, the ACAMS certification program continues to be an invaluable resource not only for me but also for other participating competent authorities (supervisory authority, legal and customs and excise), who are collectively responsible for identifying, preventing, and responding to ML, TF and other financial crimes, and mitigating the risk associated with these threats and vulnerabilities. By completing the program, I was able to enhance my knowledge and skills in AML/CFT/CPF, stay up-to-date on the latest trends and best practices in the field, and build effective partnerships with key stakeholders in the AML/CFT/CPF ecosystem.

Hence, on behalf of myself and my colleagues, I take a moment to express my sincere gratitude to ECCB (and their many partners) for selecting me to be a recipient of the ECCB-ACAMS Scholarship. I am truly honored and excited to have been given this opportunity to expand and sharpen my knowledge and skills in this field.

I understood the importance of this training, and remain committed to making the most of this opportunity.

Very humbly, thank you."

ML/FT/PF Risk Management

By Patrick L. George

An institutional ML/FT/PF risk assessment is an essential and comprehensive process geared at identifying, assessing, understanding and mitigating the risks associated with ML/FT/PF. It is a key component of an AML/CFT/CPF compliance programme, and is very often a regulatory requirement. The key aspects of such an assessment includes:

Risk Identification: The first step is to identify the potential ML/FT/PF risks faced by the institution. This includes assessing the institution's products, services, customers, transactions, and geographic locations, as well as considering the vulnerabilities that exist within its internal controls (i.e. record keeping, customer due diligence, transaction monitoring and reporting). Increased emphasis is placed on its products, services and customers that are contextualized by the transaction analysis and consideration of the risks posed by evaluation of the geographical factors.

Risk Evaluation: Once these risks are identified, they need to be evaluated in terms of their likelihood and potential impact. This includes, among other things, considering the internal controls and mitigating measures that are in place and their impact (or effectiveness) on the identified risk. At this stage, consideration should also be given to developing an institution-wide risk-rating mechanism that allows for the assignment of qualitative and quantitative risk-ratings and risk-scores to various aspect of the business. This measure will assist in the effective implementation and management of a risk-based approach, geared at treating with the varying risk classifications previously established.

Risk Mitigation: Based on the risk evaluation, the institution needs to develop and implement effective enterprise-wide risk mitigation measures that are risk-based. This may include enhancement to policies, procedures, and processes to prevent, detect, and report suspicious activities, increasing the frequency of reviews of high-risk customers, products and related transactions and executing targeted training to varying levels of staff, in particular customer-facing staff, among other actions.

Monitoring and Review: The institution needs to continuously monitor and review its AML/CFT/CPF risks and mitigation measures, implemented in furtherance of its corrective action plan, to gauge their effectiveness and determine whether the desired outcomes are being achieved. This includes, but is not limited to, conducting transaction analysis and evaluating customer behaviour, conducting regular reviews of policies and procedures, and updating risk assessments periodically.

CASE STUDY: BUSINESS EMAIL COMPROMISE

Cybercriminals are impersonating accountholders by sending emails designed to deceive financial institutions into assuming that the instructions contained in the email are from their clients and consequently prompt them into making wire transfers, processing payments or taking other actions, which result in the transmission of funds to the fraudster.

The ECCB encourages LFIs to practice heightened vigilance in responding to email instructions received on behalf of clients. Entities are to ensure account holders' email credentials, messages and instructions are adequately scrutinized prior to execution of the request.

See below case study on Business Email Compromise Fraud submitted by the *Office of National Drug and Money Laundering Control Policy* – Antigua and Barbuda.

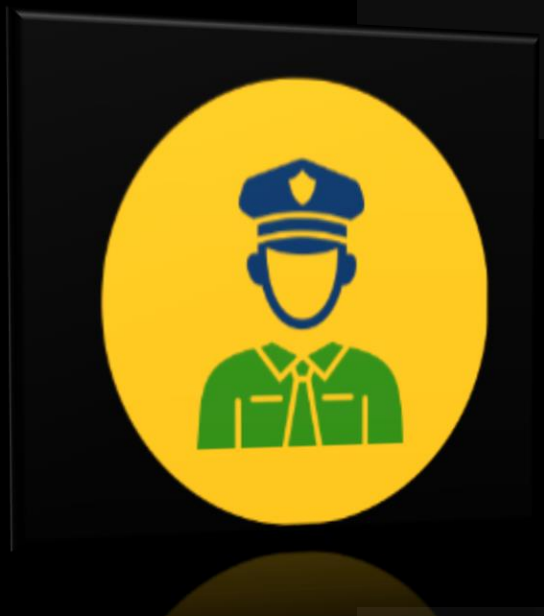
Case Study

- Sunny Castus Supplies (SCS) has an account at YourBank.
- YourBank receives an email from SCS requesting a wire transfer of USD40,000.00 to Newmoon Supplies (NS).
- YourBank processes the wire to NS.
- While reconciling the account, SCS observes the transaction and contacts YourBank.
- SCS denies the transaction request.

Did you consider?

1. How the instructions were received and whether an unusual mode or method was used by SCS?
2. Whether SCS's email address was an exact match to the SCS email address that YourBank has on record?
3. If the beneficiary was the recipient of other wire(s) from SCS, or was a company SCS did business with previously?
4. YourBank's current risk exposure to cyber related activities?
5. If the procedures that YourBank requires to thoroughly scrutinize emailed instructions were followed?
6. Any other verification steps that YourBank could have initiated prior to completing the transaction?

BUILDING A 'SECURITY AWARE' CULTURE



Culture can best be defined as the customs, accomplishments, values, norms and general beliefs of a certain group of individuals[1].

From an organisational perspective this can be interpreted as the spoken and unspoken behaviours that define how an organisation functions. Management consultant Peter Drucker was famously quoted as stating that *"culture eats strategy for breakfast"*[2] and this can be interpreted to mean that without employee commitment at all levels, the best strategies, plans and procedures are unlikely to be successful. The security culture that exists in organisations are a subset of the overarching enterprise culture, and it is important to note that a positive organisational culture does not guarantee a strong '*security aware*' culture.

There are four (4) essential features of a sustainable security aware culture:

1. ***It is deliberate and disruptive*** - Security culture must be disruptive to an organisation and deliberate with actions to foster change and improve security.
2. ***It is engaging and fun*** - Employees are compelled to participate in a security culture that is enjoyable and a challenge.
3. ***It should be rewarding*** - For employees to invest their time and effort, they need to understand what they will get in return.
4. ***It provides a return on investment (ROI)*** - The reason anyone does security is to improve an offering and lower vulnerabilities.

Building a security-awareness culture in an organisation requires a comprehensive approach that includes training, policies and practices. At the very least the following should be given priority:

- **Assessment of the organisation's current security culture:** The first step to realisation should always be to acknowledge the status of the security culture within an organisation. Once there is an understanding of where the culture stands, an actionable plan can be created with the aim of achieving the organisation's security goals.

1 https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/understanding-developing-organizational-culture.aspx
2 https://www.thecorporategovernanceinstitute.com/insights/lexicon/what-does-culture-eats-strategy-for-breakfast-mean/

- **Establish a Security Incident Response Plan:** It is important to develop a security incident response plan that outlines the steps to be taken in case of a security breach. All employees must be familiar with the plan and understand what to do in the event of a security incident.

- **Make security awareness ongoing:** Building a strong security culture takes a sustained and consistent effort, as it cannot be created overnight. Scheduling security training once a year is no longer considered adequate. Using internal communication avenues such as staff meetings, newsletters, table top exercises, the company intranet and targeted emails are great ways to engage employees and drive behavioural change. Additionally, creativity needs to be added to the awareness efforts to capture the interest of employees.

- **Ensure Executive Support:** Regardless of industry, executive management have a great influence due to the nature of their roles, as they often set the tone for the rest of the organisation. This means that management should be taking security awareness training, following best practices regarding securing data and openly encouraging others to do the same.

- **Develop sound Security Policies and Procedures:** Comprehensive security policies and procedures need to be easily understood if they are to be followed as they form the basis of a sound security culture. These policies and procedures also need to be regularly updated in keeping with the current threat landscape.

Building a security aware culture cannot and should not be a one-time project in any organisation. A balance needs to be found between an organisation's core business activities and business security. With the right training, employees will better understand their role in keeping their organisation safe.

The human factor is often quoted as being the weakest link in cyber security and this will not change. What is critical is the need for continuous development of a security aware culture, that will help organisations turn their weakest link into their strongest asset and formidable last line of defence.

Have you read the previous issues of the AML/CFT Newsletter?

Download your copy from the Publications section of the ECCB Website at https://www.eccb-centralbank.org/documents

Thank you!

The Eastern Caribbean Central Bank

P O Box 89
Basseterre
St Kitts and Nevis
West Indies

Tel: (869) 565-2537
Fax: (869) 565-9562

The ECCB welcomes your feedback and suggestions towards improving the utility of this newsletter to your institution. Please make your submissions to:
Email: AMLSupervisoryUnit@eccb-centralbank.org

@ECCBConnects

https://www.eccb-centralbank.org/

@ECCBConnects

Eastern Caribbean Central Bank