Featured Woman of ICT
Ms Kristerbella Sookdeo

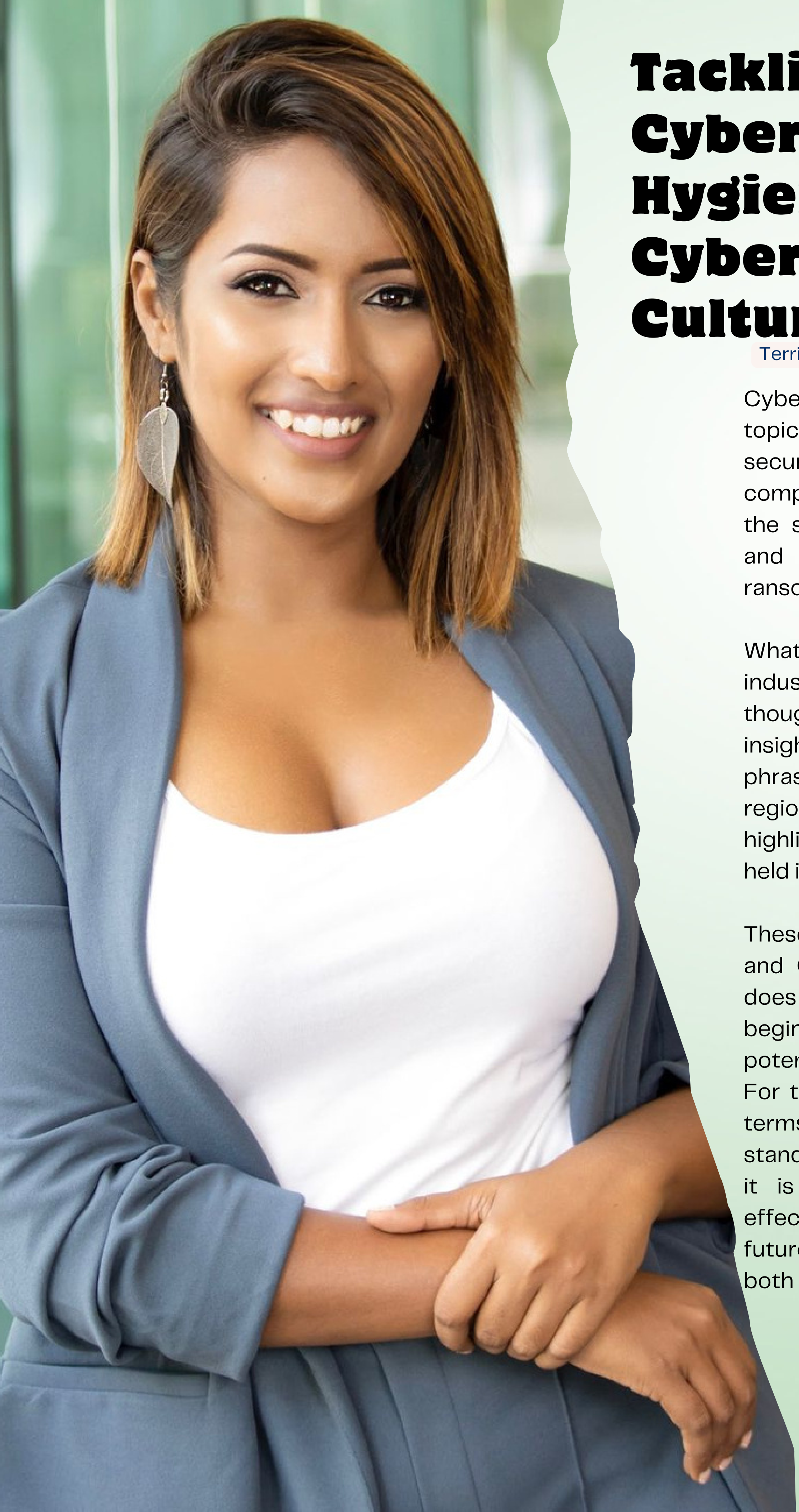
Caribbean Telecommunications Union
Shaping Caribbean ICT Development

CYBERSECURITY

IN THE K-NoW

QUARTERLY NEWSLETTER | OCTOBER TO DECEMBER 2023

TABLE OF CONTENTS



Tackling Cybersecurity Hygiene vs Cybersecurity Culture

by Ms. Kristerbella Sookdeo
Territory Account Manager, FORTINET

Cybersecurity has become a hot topic because of breaches of the security systems of various companies that have compromised the security of customer records; and because of cases of ransomware.

What is the state of the technology industry in the Caribbean? I thought that I should share some insight regarding two terms or phrases trending throughout the regional community that were also highlighted at the CTU's ICT Week held in October 2023 in Barbados.

These terms are **Cyber Hygiene** and **Cyber Culture**. What exactly does this mean, where do they begin and how can they impact our potential and immediate future?
For this article let's consider these terms from a much boarder standpoint. Let's consider first what it is and how it can be used effectively to create a safer digital future for people and businesses both currently and in future

In my recent exposure to these concepts through many conferences, forums, and personal conversations, I think these terms are being looked at within corporate organization strategies only – but is this enough? With most organizations adopting cyber resilience practices through training and development, is this going to be the only answer to a problem that requires individuals to make intentional adjustments to not only how they work but also how they function and behave in their personal lives?

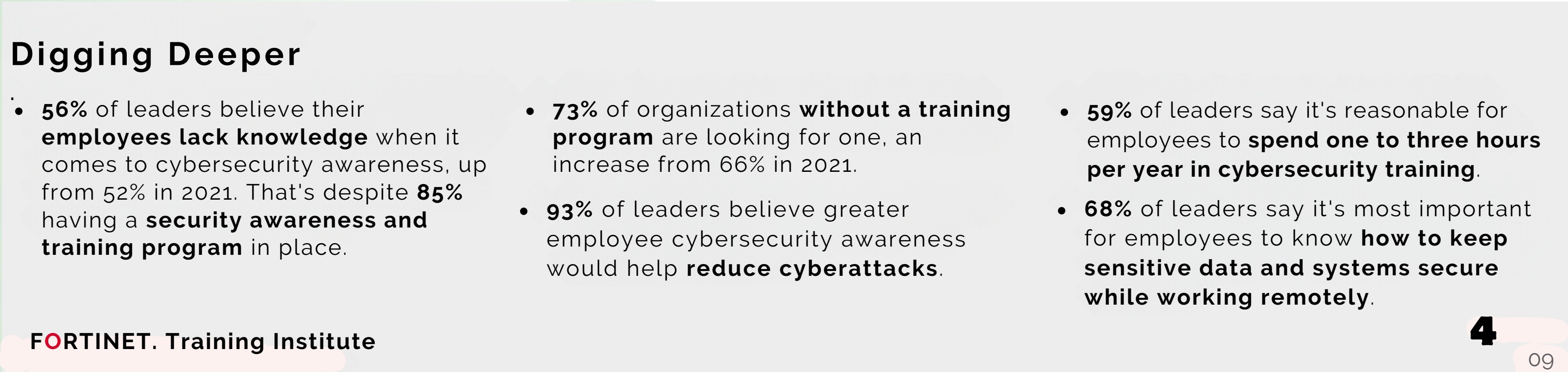
Let’s look at what we can do now that can pave the way for the current and future generations to come.I would like to suggest that whereas “hygiene” practices can and will be adopted by most organisations in the near future; Cyber“culture” should be approached from outside of the corporate office environment by positioning learning mechanisms to the growing public earlier in life.

This way we cultivate the foundation for behavioural change which is exactly what the advancement of the “cyber” space requires, as it challenges the norms of generations of people’s behavioural traits and values. Added to this, I think a simultaneous approach to addressing both topics needs to be prioritised, to really tackle the emerging cybersecurity threat.

Cybersecurity Hygiene

Cyber Hygiene (i.e. best practice) refers to the adoption of security-centric mindsets and habits that help individuals and organizations mitigate potential online breaches. This is especially important as the cybersecurity threat landscape continues to grow at a rapid rate, forcing organizations to challenge their norms and to basically play a rigorous game of continuously catching up to the newest grand cyber threat. Most organizations are now looking at measures to take to address the need for cybersecurity training and enablement internally, to avoid simple errors that can create massive inconveniences and cause an even greater risk to an organization’s success. If your organization hasn’t adopted this yet, my humble advice is that you, the reader, should encourage them to do so. Let’s look at some statistics around this,(Fortinet, 2023). 84% of leaders are reporting at least one cyber breach in the last 12 months—and nearly half citing a total cost of breaches above $1 million USD. (see below Fortinet Cybersecurity Skills Gap Report 2023)

Though this topic can evolve into a deeper discussion around the relationship or rather the tussle between Business Leaders and Cyber Leaders in relation organisation's “IT budget” vs “security priorities” regarding its infrastructure and governance, the point here is that their wouldn’t be any argument at all if the “awareness and training” aspect of Cyber Hygiene from the CEO/Board of Director Level



Digging Deeper

- **56%** of leaders believe their **employees lack knowledge** when it comes to cybersecurity awareness, up from 52% in 2021. That's despite **85%** having a **security awareness and training program** in place.
- **73%** of organizations **without a training program** are looking for one, an increase from 66% in 2021.
- **93%** of leaders believe greater employee cybersecurity awareness would help **reduce cyberattacks**.
- **59%** of leaders say it's reasonable for employees to **spend one to three hours per year in cybersecurity training**.
- **68%** of leaders say it's most important for employees to know **how to keep sensitive data and systems secure while working remotely**.

FORTINET. Training Institute

4

all the way down to organizational users was prioritized and addressed now.

Employees are an essential line of defence and many of the most common types of cyberattacks are phishing schemes, certain forms of malware, and password attacks that target users directly. Low employee cybersecurity awareness likely significantly weakens an organization's overall security posture.

The World Economic Forum (WEF) would have provided a comprehensive report around this topic and is definitely worth reading. This report highlights facts, especially in relation to Cyber Resilience, and states that organizations typically prioritize their security needs after experiencing a sophisticated cyber-attack.

This is not advisable. The organization's downtime and risk and recovery period can cripple organizational confidence, brand reputation and finances, as it forces the organization to spend a lot in a short space of time. It should instead be working with a provider or professional to create a roadmap that can be budgeted and prioritized in phases over a longer period of time.

CISOs are now challenged to assume responsibility for not just addressing technological needs but also influencing organizational cyberculture and practices across all structural levels – from end user up to C-Suite.

WEF Quote: "Dealing with these conflicts is fundamentally a task for executive leadership, and a strategic question for corporate boards of directors. Ultimately, cyber resilience will require the adoption of better governance practices."

WEF Report Link:
https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
(Global cybersecurity outlook 2023 – World Economic Forum, 2023),

2.1 Prioritizing cyber risk in business decisions

> More and more corporate boards now have true cyber experts among their members. It helps when people at board level are sufficiently cyber-literate to ask pertinent questions of their security teams but also to bring cyber into strategic business discussions. Boards also need to understand what a cyber event means for their organization. Too many business leaders still underestimate the impact a cyberattack can have on their operations, on their reputation and on their company as a whole.
> Maya Bundt, Director, Bâloise Holding; Board member, Swiss Risk Association; Member of the World Economic Forum's Global Future Council on Cybersecurity

3.1 Improving communication

> The role of the chief information security officer (CISO) is one of the most dynamic careers. We secure entire organizations as they evolve with new technologies in an increasingly digital environment. This means the CISO has a role in supporting the transformational change of a business's technology, culture and organizational structures.
> Daniel Bariusso, Chief Information Security Officer, Banco Santander

To conclude Cyber Hygiene, based on the data presented above, it's advised that organizations don't overlook the need for cybersecurity awareness training i.e.,cultivating cyber hygiene practices within their organizations. They should consider expanding their approach to it from not just one of "infrastructure and technology" needs but also assessing and adding risk management, procurement planning and business continuity planning as part of this strategy.

As stated before, employees are an essential line of defence. How they understand and interact with internal networks is critical for the organization in managing risk, and will also enhance their everyday lives. From the board level, executives could consider having cyber experts among their members to have a more comprehensive view around organization policies and investment in this space, food for thought.

Cybersecurity Culture

Cybersecurity culture refers to the attitudes, knowledge, norms, and values of the workforce of an organization. These are shaped by the goals, structure, policies, processes, and leadership of the organization. Though this sounds a little like Cyber Hygiene, let's look at cybersecurity culture from outside the organization and address it from a national, global, and holistic standpoint.

The word "Culture" refers to a system of learned and shared beliefs, language, norms, values, and symbols that groups use to identify themselves and provide a framework within which to live and work. So let's ask ourselves this, at what stage in life does a person learn culture?

That's right, we learn the fundamentals of everyday behavioural traits from early childhood stages from our parents, siblings, schools etc. Therefore, to really influence safer practices in cyber space in the present and future, we should be looking at tackling cyber culture from outside the workforce before future generations are ready to hit the job market. This can be achieved by embedding cybersecurity training and practices within the he education curriculum from as early as primary school, through to tertiary level education.

Therefore, just as we learnt to look both ways before crossing the street as a child or attended a physical education class where we were taught personal hygiene practices and self-care, let's look at the cyber space in the same light as we do with the physical world by having, for example, a "Cyber Ed" class, where the fundamentals of "online etiquette" are taught. This can influence the foundation of our future generations in many ways, by creating a digitally skilled workforce naturally and by addressing the global technology/ cybersecurity skills gap by promoting more young people to invest in technology careers.

Organisations subsequently will benefit by having a digital-minded workforce from the hiring process for any working department and industry. Additionally, at this stage, this is where we shape the morals and values of people and how they interact with each other online, addressing issues such as cyberbullying, cybercrime, online predators, personal image, and many other areas that need to be addressed with our youth for their development and for their safety.

Global technology vendors can play a particular role in providing resources towards this goal, the US government launched its K-12 initiatives this year, "The Biden administration launched an effort to beef up cybersecurity safeguards and training for K-12 schools ahead of the school year." Highlighting his quote"We need to be taking the cyber-attacks on school as seriously as we do the physical attacks on critical infrastructure", (refer below, Lauren Feiner 2023, White House to bolster cybersecurity training for K-12 schools).

Companies such as Fortinet, Amazon, Google, and many others are joining in to provide digital resources to Education Departments to guide this initiative along.

Example: Fortinet (2023) Security awareness curriculum, Fortinet K-12 Schools Curriculum. Available at: https://www.fortinet.com/training/security-awareness-training/curriculum?utm_source=website&utm_medium=pr&utm_campaign=pr-curriculum

See link above to read more:

Cyber Seven Strands

The security awareness lessons within each level will cover Fortinet's Cyber Seven Strands:

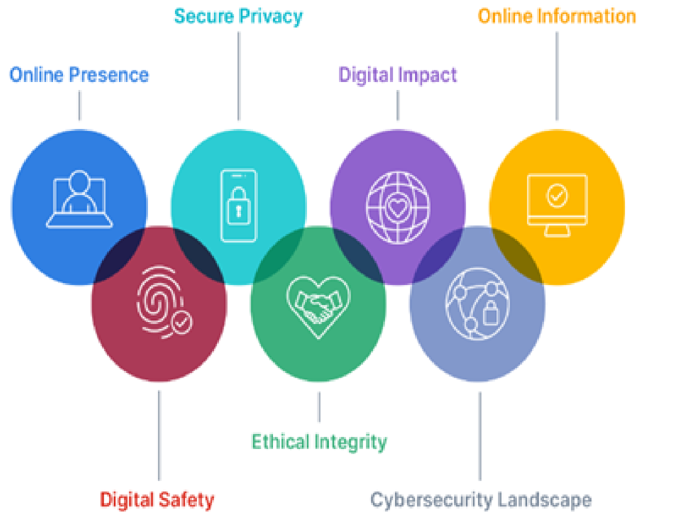
Online Presence - Maintaining a positive and safe online presence by thinking critically about identity and making mindful choices about sharing content online.

Digital Safety - Engaging in safe and respectful online interactions by recognizing online risks and knowing how to respond to difficult situations.

Secure Privacy - Protecting privacy by safeguarding personal and private information and data.

Ethical Integrity - Making informed decisions about actions and choices when using technology by understanding rights, responsibilities, and consequences of online behaviors.

Digital Impact - Using emerging technologies to improve people's lives by weighing the positive and negative impact of technology on the world.



Cybersecurity Landscape - Mitigating risks of cyberattacks by recognizing cyberthreats and bad actors' tactics and using strategies to keep people and technology secure.

Online Information - Exploring online content safely and confidently by analyzing data and recognizing reliable and relevant sources.

To conclude Cybersecurity Culture, we can agree that culture within an organization can be a very difficult task to create, influence and maintain. As the saying goes, “you can’t teach an old dog new tricks” and this may stand true when referring to creating a cyber/digital culture. Our education systems can consider evolving and adapting to not just the use of digital tools for teaching but also adjusting the content being taught.

Our future generations will be more “tech” savvy than the current adult population and may surpass the current generation with the use of technology. If we do not create a culture that addresses the morals and values of using the cyber space, we would leave room for the development of more cyberbullies and threat actors that aid the growth of cybercrime. It is very easy to be malicious with a landscape you can’t physically touch and feel.

Lastly, to address growing concerns such as the global technology skills gap and with the adoption of AI and other emerging technologies, we would need to address this topic of culture and education systems earlier on to guide our next generation of leaders and CISOs into adopting the right training and skillsat a younger age, so that the global market has a wider variety of skilled professionals to protect and innovate our future.

Speaking as someone who stumbled into this industry, I can say that I gained the lion share of the knowledge and experience as an adult within the industry; and I wish I had learnt a lot more prior to starting my career. I learnt and have been exposed to in the last 15 years of my career. Hence this topic is also a personal mission to pave the landscape for future generations of technology professionals.

Therefore, the culture topic is also a personal mission of mine to help make the landscape easier to navigate for future generations of technology innovators.

References:

Fortinet (2023) 2023 cybersecurity skills gap – fortinet, https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-security-awareness-and-training.pdf Available at: https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf (Accessed: 22 November 2023).

Fortinet (2023) Security awareness curriculum, Fortinet K-12 Schools Curriculum. Available at: https://www.fortinet.com/training/security-awareness-training/curriculum?utm_source=website&utm_medium=pr&utm_campaign=pr-curriculum (Accessed: 22 November 2023).

Global cybersecurity outlook 2023 - World Economic Forum (2023) Global cybersecurity outlook 2023 - World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf (Accessed: 22 November 2023).

Lauren_feiner (2023) White House to bolster cybersecurity training for K-12 schools, with help from the FCC, Amazon Web Services and more, CNBC. Available at: https://www.cnbc.com/2023/08/08/white-house-launches-effort-to-secure-k-12-schools-from-cyberattacks.html (Accessed: 22 November 2023).

Cyber Resilience for Development

by Mr Shernon Osepa

As the Internet continues to grow, and more and more people and things are getting online and connected, so do cyber threats also increase. That is why it is important that a secured and resilient Internet should be promoted, while focusing on all kinds of access solutions. According to different sources, World Bank included, an average of 6 percent and in extreme cases even 10 percent of a country's GDPs were observed spent on cybercrime. In Small Islands Development States (SIDS) the impact of cybercrime could be even more devastating given their already vulnerable condition.

As cybercriminals are getting more and more astute, so do defenders of an open, secured and trustworthy Internet better equip themselves. In this regard several regional and global initiatives can be observed in assisting Governments, the private sector and civil society in protecting their online resources. The Caribbean Telecommunications Union (CTU), taking its ICTs policy development role very seriously, is committed to promoting "Cyber Resilience for Development". As a result, the CTU participated recently in the "Global Conference on Cyber Capacity Building" in Accra, Ghana.

The conference was organized by:

- The Global Forum on Cyber Expertise,
- The Cyber Peace Institute,
- The World Bank,
- The World Economic Forum; and
- Hosted by the Government of Ghana.

Mr. Shernon Osepa, a seasoned policy, regulations, telecoms and Internet Governance professional represented the union in this regard. Mr. Osepa is an advisor to the CTU on Cybersecurity and Internet Governance. The primary objectives of the conference's 40 sessions were to raise awareness of the importance that every nation has the expertise, knowledge, and skills to invest in their digital future.

The 40 sessions were divided into 4 pillars:

- Making international development cyber resilient;
- Collaborating to secure the digital ecosystem;
- Cyber capacity building for stability and security; and
- Operationalizing solutions.

In addition to these sessions, an "Accra Call" was announced, which is an action framework for cyber-resilient development, endorsed by governments and several organizations across the globe. In the coming months, the CTU will be working with all regional stakeholders in the Caribbean to ensure that no one is left behind.

Stay tuned!

Regional Cybersecurity Capacity Survey

As part of its commitment to enhance the capacity of its Member States, the CTU is conducting a survey to identify areas within cybersecurity that require focus, the result of which will be used to shape and develop targeted initiatives. The CTU is actively exploring partnerships, with organisations like the Information Systems Audit and Control Association (ISACA) to develop discounted, tailored programmes to address the needs identified. Your participation is important in order to provide the CTU with guidance toward producing impactful and relevant areas for capacity development.

Click here to complete the survey.

Thank you for your time and thoughtful responses as we work together to fortify our cybersecurity landscape.

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed i
12 Hours 0
YOUR
ARE
Make paym

Ransomware is Rampant in the Caribbean

“Organizations who use unsupported operating systems, do not conduct annual risk assessment, continue to use software which cannot adequately detect and protect your information assets, will make your systems easy targets for hackers and cyber criminals, as these systems will be hardest hit as the level of vulnerabilities and exploits are high and easily available.” This is an extract from the Caribbean Cyber Security Center (CCSC) Cyber Security Predictions for 2015.

Deon Olton BSc. CEH
Cyber Security Consultant
Caribbean Cyber Security Center

Did CCSC have a crystal ball almost eight years ago? One thing for certain is that we are seeing a spike in cyber-crime and security incidents like never before in the Caribbean. The business of cybercrime has matured into a billion-dollar industry and has resulted in devastating effects for public and private sector agencies globally. Ransomware is the number one type of attack seen in security breaches over the last 11 months of 2023. These attacks are targeted and more financially driven than ever before; therefore, increasingly widespread as the cybercrime community begins to monetize their nefarious activities and lock their sight on the soft targets.

So, what really is this thing called ransomware? Like any kind of ransom, ransomware gains access to computer systems and hides the data by way of using encryption routines, before demanding payment from the victim to return access to it. Also, just like other forms of malware, ransomware tends to be effective by exploiting security weaknesses in untrained staff and or in software or operating systems. Once the ransomware is launched you will see a popup on your screen giving instructions on how much ransom to pay. There have been instances of ransom being paid and access was restored, and I am sure there is a higher number of victims who paid, and access was not restored.

All recent attacks in the Caribbean are coordinated cyberattacks which exfiltrated customer data, impacting numerous organizations including several critical infrastructure providers; sparing none in between. The massive spread and success of ransomware attacks has been made possible due to low levels of cyber preparedness and high levels of security vulnerability in far too many organisations. All these incidents being reported have one thing in common, they were exploited due to some known vulnerability which existed within each organisation.

“Known Vulnerability” means there were, and possibly still are weaknesses in the security posture of all these organisations which lead to the incidents. It could have been the use of end-of-life or unpatched computer systems, untrained end-users, and or weak passwords to name a few. The bottom line is that whatever the weakness or vulnerabilities are, the incidents were avoidable. Once an organization has a focused cyber security program the risk will be known, and the company would have the opportunity in most cases to address the risk before it is exploited. The absence of a focused cyber security program is ultimately what led to these companies being breached, and this continues to be a major problem across the Caribbean.

In the Caribbean we believe the number of companies being breached monthly is greater than what is seen in the news or reported by cyber criminals who claim ownership of these attacks. However, what is most worrying is that most countries have an immature cyber security strategy and hence there is little to no legal responsibility for companies to protect their systems or report these incidents. Sadly in countries with some reporting capability, nothing happens after the report is made. As we dig deeper and try to understand the types of organizations that have fallen victim to attacks and continue to be vulnerable it seems like the wild-wild west, any organization large, medium, or small, private, or public sector are now on the list of breached companies.

We see the cost of a ransomware attack is also on the rise globally. Of course, ransom payments aren’t the only costs associated with a ransomware attack, there is loss revenue, recovery costs, and reputational damage which you cannot put a real figure to. All the attacked organisations within the last 11 months of 2023 experienced business productivity disruptions, and downtime of mission critical applications. We do not know the average cost of those disruptions, but we can expect it to be in the tens of thousands of dollars and as was stated before, avoidable. However, it must be stated emphatically that the cost of prevention is always less than the costs associated with an incident.

Victims should avoid paying the ransom at all costs. That is because doing so does not guarantee that you will be able to recover your affected systems or data. Plus think about it, you were breached by a criminal who is asking for a payment to restore access, do you really think this is an honorable businessman? Sometimes, ransomware actors simply lack the skills to develop a decryptor that can successfully recover all your files. To compound this problem ransomware operators are now exfiltrating a target’s data before running the encryption routine and demand victims pay not only to get back access but also to get their data before it is published online.

Acknowledging the above, if you get hit with ransomware you should not pay the ransom because there is a high possibility you will not get back access to your systems nor data plus regaining access doesn’t remove the initial problem of unauthorised access by the ransomware operator. The best ransomware defence for organizations is to focus on preventing infection in the first place. There's no silver bullet to addressing ransomware or any other type of attack but a proactive approach helps. Having a cyber security program is key. You cannot rely on backups only because if you don’t have a robust backup strategy you might lose those too. You cannot rely only on Indicators of Compromise (IOCs) because your notifications are generally after the compromise, remember ransomware spreads in seconds. However, we recommend taking a defence in-depth approach to prevention by developing a cybersecurity program. First, you should ensure your staff are trained in how to identify and report suspicious email and or, system behaviour. Invest in technology that allows detection and prevention of a ransomware attack at the earliest stages. Ensure you are running the latest updates, anti-virus software and firewalling which tends to help to some extent. Back up everything, do it frequently, and ensure backups are stored off-site and off-line.

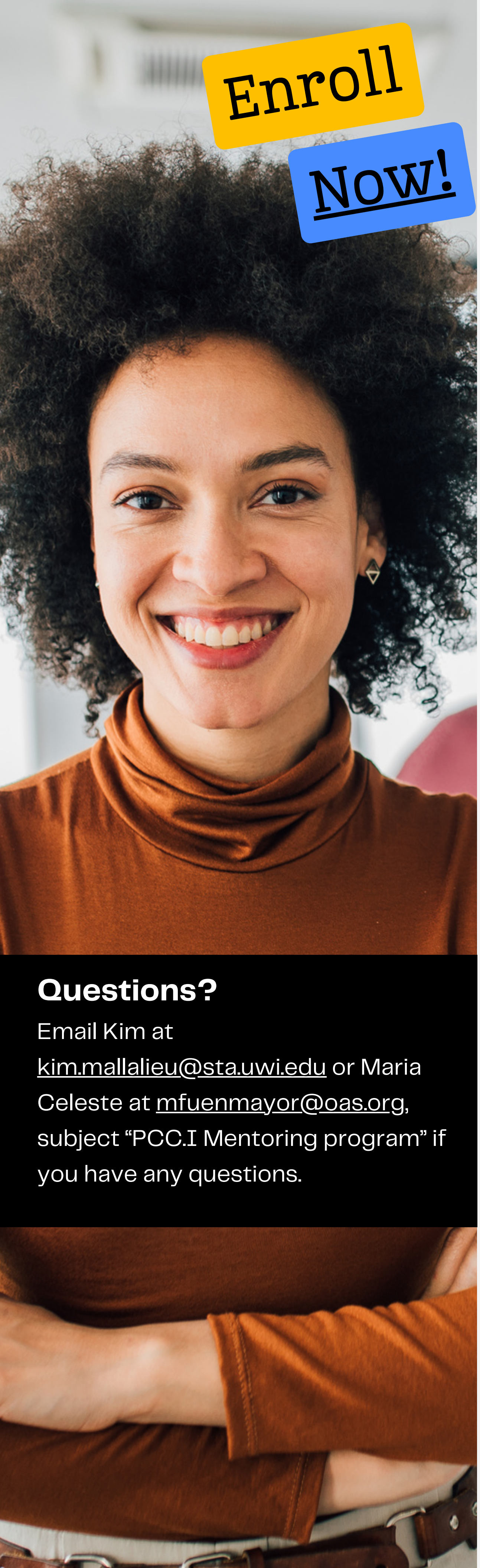
Also test backups frequently to ensure that they can be successfully restored. Spend time and money on proper prevention, or else you may be forced into considering whether it makes business sense to pay a ransom. Choose a cyber security partner to get your cyber security program developed no matter your size. Remember your company’s level of exposure tends to be a measure of how prepared you are to detect and respond to an incident. The reality is that some organizations in the Caribbean are already compromised and will feel the effects of this evolving digital threat in the coming weeks and months. We expect to see large numbers of mid and small-sized companies (who continue to neglect the implementation of a cyber security program) falling victim. This lack of preparedness for these threats will lead to Caribbean governments and private sector organizations being battered by an increasing range, type and frequency of attacks which demand a proactive and appropriately sophisticated response by those charged with cyber defence.

To book a consultation to get your cybersecurity program started and reduce the possibility of an incident whether ransomware or otherwise, give us a call at the Caribbean Cyber Security Center 1-246-232-9009 or reach us at www.caribbeancsc.com.

The Inter-American Telecommunication Commission (CITEL) & Permanent Consultative Committee (PCC)

The Inter-American Telecommunication Commission (CITEL) is the leading advisory body of the Organization of American States (OAS) on all matters relating to telecommunications/ information and communication technologies (ICTs) in the Hemisphere. Its Vision is "The full integration of the American States into the World Information Society and the digital economy, with a view to enabling and accelerating social, economic, cultural, and environmentally sustainable development for all the region's inhabitants through the development of telecommunications and ICTs" and its Mission is "To facilitate and promote the integral and sustainable development of interoperable, innovative, and reliable telecommunications/ICTs in the Americas, under the principles of universality, equity, and affordability". All 35 independent states of the Americas have ratified the OAS Charter and are members of the Organisation. CTU Member States that are CITEL members are as follows: Antigua and Barbuda, Barbados, Belize, Commonwealth of Dominica, Grenada, Guyana, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, The Bahamas and Trinidad and Tobago.

According to Article 23 of the CITEL Statute, the Assembly has the authority to create any Permanent Consultative Committees (PCCs) it finds essential for achieving its goals and carrying out its duties. In line with the CITEL Regulations, the Assembly established specific mandates for PCC.I and PCC.II. CITEL comprises a permanent executive committee, COM/CITEL, as well as two permanent consultative committees: PCC.I and PCC.II. PCC.II promotes debate and regional cooperation on issues related to the planning, coordination, harmonization, and efficient use of the radio spectrum, as well as geostationary and non-geostationary satellite orbits, for radiocommunication services. PCC.I promotes debate, cooperation and regional coordination on matters related to policies, development and standardization of telecommunications / ICT.



Questions?

Email Kim at kim.mallalieu@sta.uwi.edu or Maria Celeste at mfuenmayor@oas.org, subject “PCC.I Mentoring program” if you have any questions.

PCC.I Mentoring Program Overview

The PCC.I Mentoring Program is a comprehensive initiative designed to nurture professional development in PCC.I, most specifically to enable delegates from CITEL countries to meaningfully participate in statutory meetings and other activities of PCC.I as well as related ITU-D, and ITU-T activities.

While a significant focus is on newcomers and women, men and seasoned delegates are enthusiastically encouraged to participate and support. The Program employs various engagement strategies, support mechanisms and resources which mentor - protégé teams draw on in ways that suit their particular circumstances and preferences.

Call for Mentors

Professionals from CITEL countries with relevant expertise and leadership experience in COM/CITEL, PCC.I, ITU-D and/ or ITU-T, who highly value diversity, and possess strong interpersonal and communication skills, are encouraged to volunteer for mentoring roles in the PCC.I Mentoring Program.

Call for Protégés

Professionals eligible to represent member or associate member organisations or administrations of CITEL, and who feel that they would benefit from the Program, are encouraged to apply for protégé roles in the PCC.I Mentoring Program.

Timeline

1. Ultimate deadline for applications: January 15, 2024
2. Orientation (remote): January 22, 2024
3. Cycle 1 mentoring activities: January 22, 2024 - September 22, 2024
4. Mentors & protégés submit evaluations: September 22, 2024

Apply Now!

CALL FOR MENTORS AND PROTÉGÉS – CITEL PCC.I MENTORING PROGRAM

OAS | CITEL

PCC.I MENTORING PROGRAM

APPLICATIONS OPEN

What's this about?

The PCC.I Mentoring Program provides support for delegates from CITEL member states to meaningfully participate in PCC.I and activities related to ITU (ITU-D and ITU-T).

Who is this for?

To all CITEL members with focus on newcomers and women, though men & seasoned delegates are enthusiastically encouraged to participate and support.

What can you expect?

Direct interaction between Mentors & Proteges.

Structured content, links and courses on PCC.I Mentoring Central.

Official documents, templates, meetings, calendars & procedures.

Tools and templates.

Model documents.

Best practice.

Participation in forums, webinars, panel discussions & lots more!

Questions?

Email Kim at kim.mallalieu@sta.uwi.edu or Maria Celeste at mfuenmayor@oas.org. subject "PCC.I Mentoring Program" and we'll get back to you

Bridging the Mobile Gender Gap
Sign up now at
www.gsmatraining.com/course/bridging-the-mobile-gender-gap/

BRIDGING THE MOBILE GENDER GAP COURSE

The GSMA, OAS Inter-American Telecommunication Commission (CITEL) and the Caribbean Telecommunications Union partnered to deliver the online Bridging the Mobile Gender Gap Course to policymakers and regulators, men and women, in Latin America and the Caribbean event from the 26 September to 14 November 2023. There were a total of sixty-five (65) registrants from 29 Countries with 8 of the countries being CTU Member States. Of the registrants, we had fifty-one (51) Females and fourteen (14) Males. Please see breakdown by country and then breakdown by CTU Member States below.

A live webinar was held on 27th September 2023 served as an introduction to the course which aimed to help policymakers understand the size and drivers of the mobile gender gap in low- and middle-income countries and provides recommendations on how to improve digital inclusion for women. The session featured remarks from Mr. Oscar Leon, Executive Secretary, CITEL; Mr. Rodney Taylor, Secretary-General of the CTU; and Mr. Lucas Gallitto , Head GSMA, Latin America.

Women were encouraged share what they are doing to accelerate women's digital inclusion. It was an online, self-paced, Bridging the Mobile Gender Gap course over a seven (7) week period.

The course objectives were to:

- Gain a better understanding of the issue and the need for urgent action;
- Discover how gender perspectives can be integrated into strategies, policies, plans and budgets so they explicitly address women's needs, circumstances and preferences;
- Learn how barriers such as affordability, safety and security concerns, digital skills, access, and the availability of relevant content can be addressed;
- Learn about what other governments are doing to improve women's digital inclusion; and
- Develop an action plan for your country to reduce the mobile gender gap.

By the end of this course, participants gained a better understanding of the factors impacting the mobile gender gap; understanding the policy levers available to them; and created an action plan to address the mobile gender gap in their country.

The online course was offered through the GSMA Connected Women programme, which is funded by UK Aid and the Swedish International Development Cooperation Agency (Sida).

To learn more about what was covered click here to view the course outline.

TOTAL # OF PARTICIPANTS BY COUNTRY

COUNTRY	#
ANGUILLA	2
BAHAMAS	5
BARBADOS	1
BRAZIL	6
COSTA RICA	1
DOMINICAN REPUBLIC	4
ECUADOR	2
GAMBIA	1
GEORGIA	1
GHANA	1
GUINEA	1
GUYANA	1
INDONESIA	1
KENYA	2
MALAWI	2
MALAYSIA	2
MEXICO	2
NAMIBIA	1
NIGERIA	1
PARAGUAY	5
RWANDA, REPUBLIC OF	1
SAINT KITTS AND NEVIS	1
SAINT VINCENT AND THE GRENADINES	1
SENEGAL	1
SOUTH AFRICA	1
SURINAME	2
TRINIDAD AND TOBAGO	14
UNITED KINGDOM	1
ZAMBIA	1
TOTAL	**65**

CTU MEMBER STATES PARTICIPANTS	#
ANGUILLA	2
BAHAMAS	5
BARBADOS	1
GUYANA	1
SAINT KITTS AND NEVIS	1
SAINT VINCENT AND THE GRENADINES	1
SURINAME	2
TRINIDAD AND TOBAGO	14
TOTAL	**27**

HIGHLIGHTS

Well Done! 2023 was indeed the year for leading Caribbean Women in ICT in the international fora. We recognise and congratulate these women as trailblazers representing the Caribbean Region with excellence.

The Internet Governance Forum (IGF) is a vital global platform that enables diverse stakeholders to discuss public policy issues related to the Internet. We are delighted to announce and extend our congratulations to Ms. Carol Roach, who has been appointed as an Ex-Officio Member and Chair of the IGF Multi-stakeholder Advisory Group. This esteemed appointment reflects her significant contributions and expertise in the field.

Ms. Roach, with over 30 years of experience, is a notable figure in the ICT sector. Her role as an ICT strategist and programme lead, as well as an e-government expert for the Government of The Commonwealth of The Bahamas, has marked her as a key influencer in the digital domain.

Her regional expertise has been further demonstrated through active involvement with Red GEALC (Network of e-Government Experts in Latin America and the Caribbean), the Organization of American States (OAS), CARICOM (Caribbean Community and Common Market) and the Caribbean Telecommunications Union (CTU).

Ms. Roach is a passionate advocate for integrating the themes of People, Prosperity and Planet within the digital space.

We wish Ms. Roach tremendous success during her tenure and are confident that her leadership and insights will contribute significantly to the IGF's mission and objectives.

The participation of Caribbean Delegations at the ITU's World Radiocommunication Conference (WRC23) in Dubai from 20th November – 15th December 2023 was a resounding success. CTU Member State delegations in Dubai included Belize, The Bahamas, Cayman Islands (UK Delegation), Cuba, Grenada, Jamaica, Sint Maarten (Netherlands Delegation), Suriname and Trinidad and Tobago.

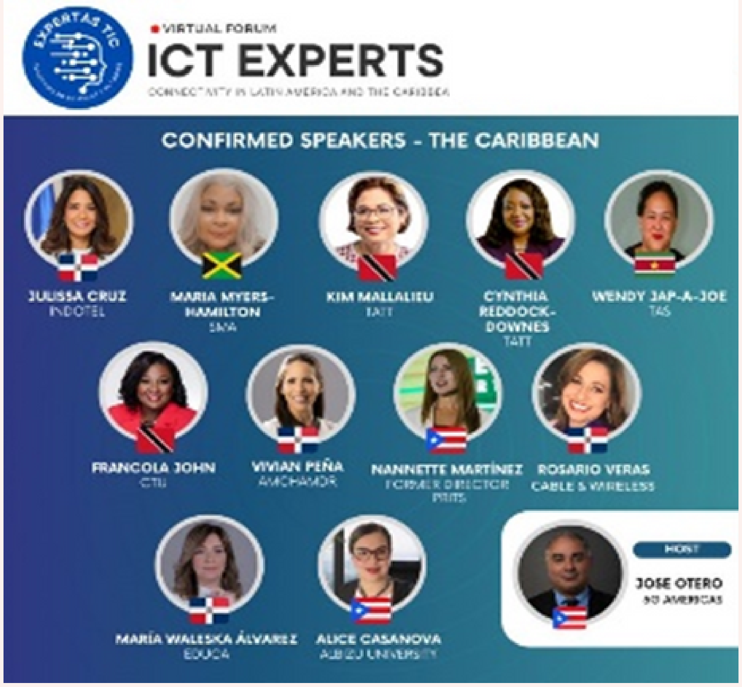
This year's event was particularly notable for the Caribbean region because for the first time ever, a leading Woman in ICT from the Caribbean, Dr. Maria Myers-Hamilton, Managing Director of the Spectrum Management Authority of Jamaica, was appointed to serve as a Vice President of Committee 4 of this treaty-based event.

Committee 4 addressed broadband applications in the mobile service such as International Mobile Telecommunications (IMT), Fixed Services, Satellite, High Altitude IMT Base Stations (HIBS) and High-altitude Platform Stations (HAPS). This appointment signifies a remarkable advancement in promoting gender equality and empowering women's roles in the specialist field of Radiocommunication on a global stage. It also highlights the region's growing influence and commitment to diversity and inclusion in the field of ICT.

The CTU congratulates Dr. Myers-Hamilton on the honour of serving as Vice Chair of Committee 4 at the ITUWRC2023.

Dr. Myers-Hamilton's interview with ITU TV at WRC23 is also accessible via the following link: https://www.youtube.com/watch?v=lyFqYClyPp8&list=PLpoIPNlF8P2PDQIp7veqBN94TQU_D6Czb&index=26

5G AMERICAS VIRTUAL MEETING OF ICT EXPERTS: CONNECTIVITY IN LATIN AMERICA AND THE CARIBBEAN



The 5G Americas Virtual Meeting of ICT Experts: Connectivity in Latin America and the Caribbean was an online event that brought together for the first time only women ICT experts from the region. The main objective addressed the current telecommunications situations in LAC from different perspectives. From amongst the CTU's membership, five Caribbean Women in ICT participated and delivered expertly during the week-long event. Presentations can be viewed via the following links:

Jamaica: Dr. Maria Myers-Hamilton
Suriname: Ms. Wendy Jap-a-Joe
Trinidad and Tobago: Dr. Kim Mallalieu
TATT: Mrs. Cynthia Reddock-Downes
CTU Secretariat: Ms. Francola John

THE CTU SECRETARIAT

At the 18th United Nations Internet Governance Forum (UNIGF), held in Kyoto, Japan, from 8th to 12th October 2023, a delegation from the Caribbean made significant headlines. This prominent presence at such a key international event highlights the growing influence and involvement of the Caribbean region in global internet governance discussions and developments.

The CTU Secretariat proudly acknowledges Ms. Nia Nanan, our Senior Research Analyst, as the driving force behind a significant milestone. Thanks to her efforts, the CTU secured a spot on the UNIGF agenda. For the first time in UNIGF's history, the CTU hosted its inaugural Open Forum, titled "From IGF to GDC: A New Era of Global Digital Governance – A SIDS Perspective", this landmark event took place on Thursday 12th October 2023, marking a pivotal moment in our organisation's journey towards influencing global digital governance.

Another accomplished Woman in ICT from the CTU Secretariat, Ms. Michelle Garcia, who serves as its Marketing and Communications Specialist, participated in the School of Digital Transformation and Innovation in Latin America and the Caribbean, held in São Paulo, Brazil in August 2023. The event was conducted strictly in Spanish and Portuguese. With her fluency in both, Ms. Garcia delivered an insightful presentation on the CARICOM Single ICT Space (CSIS), highlighting the progress of the CSIS, which has evolved from a mandate by the CARICOM Heads of Government to the implementation of various elements thanks to the continuous efforts of the CTU Secretariat.

Additionally, Ms. Garcia had the opportunity to visit the world's largest Internet Exchange Point in São Paulo, managed by NIC.br, further enriching her experience and understanding of the global ICT landscape.

CARIBBEAN TELECOMMUNICATIONS UNION (CTU) CALENDAR OF EVENTS JANUARY – MARCH 2024

#	EVENT	Date	Mode
1	SIDS at ICANN: Where we are at and how do we chart a way forward	8th January 2024	Virtual
2	CTU's 2024 1st International ICT Forecast and Industry Watch Meeting	15th January 2024	Virtual
3	The 8th annual Trinidad and Tobago Internet Governance Forum (TTIGF)	25th - 26th January 2024	Hybrid, Trinidad and Tobago
4	CANTO Connect and 40th AGM Celebration	28th - 30th January 2024	HYATT Regency Trinidad
5	CARICOM ICT CLUSTER MEETING	7th February 2024	Virtual
6	10th Latin American Spectrum Management Conference	20th - 21st February 2024	Brazil
7	Spectrum Mgt Task Force Mtg. and Workshop	21st - 22nd February 2024	Virtual
8	GSMA Mobile World Congress (MWC)	26th - 29th February 2024	Spain
9	ICANN 79	2nd - 7th March 2024	Puerto Rico
10	CTU's International Women's Day webinar	8th March 2024	Virtual
11	SMART Seas: Properties for Accessible for Communications at Sea for Small-scale Fishers Workshop	11th - 12th March 2024	Virtual
12	Govt. of Cuba, Informatica 2024 19th International Convention and Fair (Havana, Cuba)	18th - 22nd March 2024	Havana, Cuba
13	Webinar - Articial Intelligence - Opportunities and Threats for the Caribbean	22nd March 2024	Virtual

Caribbean
Telecommunications
Union

IN THE K-NoW

Network of Women (NoW) in ICT in the Caribbean

ISSUE 5 - 10-12/23

VISION OF CTU NETWORK OF WOMEN

To lead the charge in creating a strong community of Caribbean Women in ICT to drive profound and impactful transformation across the region. We envision women being equally represented and actively shaping the industry's future.

MISSION OF THE CTU NETWORK OF WOMEN

Our mission is to cultivate a supportive and collaborative community that empowers and advances Caribbean Women in ICT and STEM. Through networking, mentoring and professional development opportunities, we strive to promote gender equality, equity and parity by amplifying women's voices, and driving positive change in the industry.

OBJECTIVES OF IN THE k-NoW

The Caribbean has a staggering record of potent women leaders in telecommunications, yet there is no channel for the sharing of experiences, mentoring and encouraging women across the region to take on leadership roles in the longitudinal processes associated with ITU's statutory meetings and study groups. ITU's networks of women are available to fill this gap. At the same time, In the K-NoW provides information on key supporting resources with a Caribbean focus.

Women are a key CTU Stakeholder group. We engage them through In the k-NoW to share updates, inform on activities, data, announcements and successes of Women in ICT in our Member States and the wider Caribbean Community.

Get to know your Point of Contact for the CTU NoW: Ms Francola John, Stakeholder Engagement Specialist and CTU Focal Point for ITU's Network of Women. Tel. No.: 1-868-628-0281 Ext. 231; Email: NoW@ctu.int or francola.john@ctu.int

Be In the K-Now

Click here to subscribe to our mailing list.
Follow us on social media to be in the K-Now

OUR TEAM:

Director, Stakeholder Engagement
Mr. Trevor Prevatt
trevor.prevatt@ctu.int

Editorial
Dr. Kim Mallalieu
kim.mallalieu@sta.uwi.edu

Ms. Michelle Garcia
michelle.garcia@ctu.int