



HomePublicationsNewsContact



Search

The Need for Developing a Cyber Security Ecosystem of Professionals

February 8, 2017 by Shiva Bissessar



Snapshot showing Caribbean 'attack' activity from Norse

Over the period 6th and 7th February, 2017, it was my honour and privilege to participate in, and make contributions to, a closed expert group meeting to assess future threats as executed by a national intelligence agency. The following is the paper I presented on developing cyber security capacity to meet future challenges.

Introduction

The cyber security implications of technological advancements, such as, the Internet of Things (IoT) or smart technologies, along with the possibility of cyber warfare and realities of cybercrime are thought-provoking areas around which intelligence agencies must develop threat awareness. However, a more significant threat which will affect the cyber security of Trinidad and Tobago over the next five years is lack of an environment which can stimulate and foster the growth of local cyber security professionals.

Indication of such a deficient environment can be gleaned from the examples below.

- At a government agency with responsibility for implementation of the national strategy towards Information and Communication Technology (ICT), a senior position with responsibility for cyber security has been vacant since 2010.
- At “M4 an event by Microsoft” held in Nov 2014, Mr. Roberto Arbelaez, Chief Security Advisor for the Americas at Microsoft, stated that he knew many world class Information Security professionals of Trinidadian heritage. However he went on to state that unfortunately they all worked outside of Trinidad and Tobago.
- At a 2016 Christmas dinner event for an association of lawyers, a prominent lawyer lamented that Trinidad lawyers, having opted not to pursue continuing education, were lacking in areas of increasing import including cybercrime[1].

While this may be considered anecdotal evidence, the lack of attention to cyber security does not allow for formal research to provide proper evidence on the state of cyber security locally.

Cyber security ecosystem of professionals

Within their research **Thomas et al** illustrate the cybercrime underground economy as a complex ecosystem of actors within a value chain where profit centres are built upon underlying support infrastructure. This allows criminal entrepreneurs to devise scams by procuring the necessary resources *al a carte*; taking advantage of specialization and economies of scale and resulting in a web of interactions which potentially span the globe. One can argue that such a criminal ecosystem, like many other cyber security threats, can only be disrupted by an equally powerful cyber security ecosystem of professionals.

provides cyber security capacity building exercises to law enforcement across the globe previously divulged that suitably qualified private sector experts can participate in these exercises if they are appropriately recognized by law enforcement personnel.

Hence, a more inclusive approach needs to be found to ensure that a national pool of talent, at all levels, is being developed today to address unknown future needs. The status quo will forever bind us to a dependency upon the importation of expertise or hopefulness towards the return of qualified diaspora who wish to contribute to developing cyber security. The up-skilling of a national pool of experts also presents Trinidad and Tobago with opportunity in providing exportable resources both regionally and internationally as others seek to develop cyber security.

Beyond the need for a coordinated approach to develop a cyber security pool of talent, there seems to have been an emphasis on getting legislation in place while the technical controls, which can actually prevent threats from becoming exploited, are not given due attention. This position was also **articulated by Mr. Arbelaez, at the Caribbean Stakeholders Meeting (CSMI) in May 2014.**

Are we lagging behind regionally?

Awareness, capacity development and technical controls are all areas which require attention to adequately build threat response capability over the next five years and there is much we can learn from our own Caribbean neighbour, Jamaica. Having delivered presentations in November 2016 at three conferences in Jamaica as hosted by the **Jamaica Computing Society**, UWI Mona (**4th National Cyber Security Conference**) and the Jamaica Bar Association (Continuing Legal Education)[2], I can personally attest to a comparatively more mature response towards cyber security.



Presented on UN ECLAC sponsored research into opportunities and risk of digital currency within the Caribbean at the Jamaica Bar Association, Continuing Legal Education, Annual Week-end Conference 2016

Such fora have been productive towards supporting and encouraging local capacity development of technical capabilities in the private sector and building public awareness on cyber security. At Jamaica's 3rd National Cyber Security Conference in 2015, the audience was challenged to **consider cyber security as an opportunity for the growth of an industry and economic development, rather than a threat**, in the same vein as highlighted above. It is interesting to note that these fora also exemplify what a cyber security professional ecosystem should look like with active participation from technical professionals, policy/regulatory/legal professionals, academics and civil society.

Moving forward

We need to ask some difficult questions if we are to position ourselves to cope with future cyber security threats:

- Can we define if there is a community of experts exists in Trinidad and Tobago focusing on cyber security; and if yes, who are the persons comprising this community?
- Is this a formal community or a loosely defined community which comes together temporarily during exercises such as this one?

- Does its membership lean towards greater participation from the public sector or the private sector?
- Is there recognition that private sector interest from a Small Medium Enterprise (SME) is not the same as the private sector interest of a large commercial entity?
- How are potential candidates encouraged to contribute within this community?
- Is the community comprised in such a way that both of fresh ideas and a wealth of experience are expressed in deliverables?
- Do the participants of this community come from different professions, back grounds and skill sets?
- Can such a community adopt value chain relationships to be transformed into an active ecosystem[3] of professionals seeking to promote national cyber security?
- Can this forum be the catalyst in the formation of such an ecosystem?

Recommendations

In conclusion the following recommendations can be put forward for consideration in the development of the aforementioned ecosystem of professionals

1. Cyber security must be given recognition as a field of specialization and not be simply lumped under ICT. Such recognition should extend to the appointment of national champion to oversee the development of cyber security locally.
2. Establish a national consultative body for cyber security which can serve as a sounding board for various plans towards developing cyber security. The membership of such a body cannot be exclusively comprised of public sector employees and large corporate entities. It must include cyber security focused SMEs. This formal body will lead to the formation of the informal cyber security ecosystem of professionals.
3. Encourage participation from the private sector in local and regional meetings being facilitated by the aforementioned international bodies, for example ComSec and OAS. Appropriately qualified entities from this set should also be invited to participate in the training and capacity building exercises arising from such meetings. Support for such entities should include financial assistance to participate.
4. Assessment of institutions which are deemed critical infrastructure as well as a key Ministries and agencies. The organizational structure of these bodies should reflect cyber security maturity extending to the roles and responsibilities of key personnel dedicated towards cyber security. A comprehensive set of Information Security policies and audit mechanisms also need to be defined for such organisations.
5. Information Security Governance training needs to be administered to boards and senior management of various key organisations. Additionally, Information Security Awareness training needs to be administered for the general population of employees.

6. Alignment between the academic institutions, the national development needs scholarship system and the intake of graduates into the public and private sectors needs to take place to ensure that Information Security professionals are being developed academically and professionally. There also needs to be coordination with corporate entities towards the creation of funding for cyber security research.
7. The Government needs to facilitate the creation of opportunities within the private sector to build and develop competencies which they can call upon in the future. We need security researchers, writers, lecturers, practitioners, policy makers, legal specialists and technical experts to name but a few. The government must lead by example and procure services from fledgling entities seeking to provide services in cyber security.
8. Information Security awareness training needs to be conducted extensively within the primary and secondary school system.
9. Take advantage of training and capacity development exercises from international bodies and multinational corporate entities to up-skill the national pool of experts (public and private sector) towards the goal of developing cyber security for economic development.

[1] CNC3 News, Nov 2016


[2] Presentation to the Jamaica Bar Association was on the digital currency which also has emerging threat and cyber security dimension to it.

[3] It is important to recognize that an ecosystem differs from a community in that an ecosystem speaks to a non-siloed approach, coordination and symbiotic relationships towards growth of entities.

Share this:



Blog

 awareness, capacity building, Caribbean, Commonwealth, ComSec, critical infrastructure, cyber hygiene, cyber warfare, cybercrime, cybersecurity, digital currency, ecosystem, governance, internet of things, IoT, OAS, policy, risk, threat

- < Are we on track for sustainable Caribbean cyber security development?
- > T&T Cybercrime bill demands multi-stakeholder input (July 2014)

Leave a Comment

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

Post Comment

