APR 2020 - VOLUME III

Language Barriers and Their Implications

A Cyber Security Perspective

INTUITION PUBLISHING PTE LIMITED

Language barriers are a common struggle across industries and countries, and can have different meanings depending on where you are. Initially when we talk about a language barrier, we imagine the tourist situation. There are also technical language barriers, for example between different business departments with different goals. People from cyber security will talk about technical operations and cyber defence, and that can be their sole focus. People from the finance department speak the language of revenues and expenses. There is a plethora of information on the importance of overcoming these internal operational "language barriers".

As our increasingly interconnected and globalised lives bring us all closer together, we often face the age-old problem of language barriers in cyber security, particularly across APAC.

Over the last few years there have been some notable cyber incidents with global ramifications. The speed at which cyber attacks can spread and cause significant disruption and cost can leave system administrators scrambling to obtain information and threat intelligence that requires translation. The demand for such translations has surged, showing the need for information sharing during and after cyber incidents.

Increased requirements in any one individual language can also be linked to national cyber incidents. In Japan in 2016, cyber attacks on Japanese companies caused 12.6 million breaches, compared to 2.07 million in 2015, where over 600 networks in Japan were hit by the notorious WannaCry ransomware attack.

There is a notable reaction to high profile cyber incidents where non-native English-speaking countries are demanding translations. This also highlights how there could be an increased level of risk posed due to the delay of vital cyber intelligence. While some of the major multinational corporations may feel relatively isolated from such risk, the smaller companies and local infrastructure providers may be your Achilles-heel. It's all well and good if your corporation has a global cyber security response and can quickly mitigate threats; but what about the country's infrastructure that your business relies on? Loss of utilities, transportation & communications can still cause a major disruption to your operations.

Nations and companies should have proactive ways of translating and distributing information to all. How to measure the associated level of risk can be difficult, a Recent CISCO report shows that Thailand may be lagging in cyber security. This study found 29% of respondents in Thailand experienced a downtime of 24 hours or more, compared with just 4% globally and 23% in Asia-Pacific. It showed 45% of respondents in Thailand reported receiving more than 50,000 threat alerts a day, with only 23% globally. Kerry Singleton,

director of cyber security in ASEAN for Cisco, said that 23% of respondents in APAC faced cyber security breaches costing over $2.5 million, compared with 15% globally.

Language barriers work both ways, it's not only the defensive side of the equation that struggles. Western cyber security researchers and threat hunters are struggling to keep up with the growing cybercrime industry emerging in APAC. It is no longer enough to monitor cybercrime activities typically associated with Russian, North Korean or other English-speaking cyber groups. Language barriers, cultural differences and government-imposed access restrictions make it incredibly difficult for threat hunters to access and blend in with Asian underground communities to effectively perform threat reconnaissance. Researchers need to navigate linguistic and cultural differences to be effective in combating the growing cybercrime industry.

It is a difficult task to research and monitor the dark web landscape, government laws and attitudes towards cyber activity, and key threat actors, especially in a foreign language.

Studies show Chinese Internet forums are used by hackers who are not even using openly accessible anonymous networks, mainly due to increasing restrictions on the use of TOR and VPN services in China. This has created an interesting dynamic between the Chinese government and its cyber citizens, leading to several additional challenges threat hunters must work around.

Russian forums rarely publish data dumps from Russian firms. By contrast, data dumps and malware sourced from Chinese firms are usually only found on Chinese forums. Chinese nationals are internationalists, often active on Chinese, English and Russian forums. In contrast, few native Russian or English speakers would use Chinese forums. The increasing restrictions in China are pushing Chinese hackers to use foreign forums. The result is data and malware, once unique to Chinese forums, becoming more accessible internationally. This trend has the potential to increase in spread and become a cyber threat that is bolstered by language barriers.

Intuition – Blended Learning

The Intuition online learning library consists several tutorials related to this article:

- **Cyber Security Awareness**
  - Passphrases
  - Preventing Identity Theft
  - Device Security
  - Malware & Breach Recovery
  - Social Engineering
  - And more…
- **More from the Know-How Library**
  - Digital Banking
  - UK Cybercrime

For Intuition blended learning related to this article, some of our popular workshops include:

- Cyber-Warfare the Fourth Dimension of War
- Human Cyber-Security Risk
- Holistic Technology Risk Management Framework
- Artificial Intelligence
- Digital Banking Masterclass
- Insights into GRC in New Digital Age and Impact on Financial Advisory and Capital Market Representatives

Get in touch with your Intuition account manager at apacinfo@intuition.com for more details

Download the Asia Perspectives free app to get the latest news and articles.

Get the app

Related News Articles

- Cybersecurity experts come together to fight coronavirus-related hacking – 26 Mar Reuters
- Language barriers are not the best for cybersecurity – Aug 17 StartupBeat
- Overcoming the cybersecurity language barrier with your peers – Jun 18 AT&T Business
- Cybersecurity's dual mission during the coronavirus crisis – Mar 20 McKinsey & Company
- Remote working due to COVID-19 raises cyber security concerns – 23 Mar AFR

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours.