PACIFIC FORUM INTERNATIONAL

Key Findings
US-Singapore Tech & Innovation Virtual Dialogue Session 3:
Forging Digital Standards: Challenges in Intellectual Property and Supply Chains
January 26, 2022 (US) | January 27, 2022 (Singapore)

On January 26, 2022, with the support from the US Embassy Singapore, the Pacific Forum hosted the third session of the US-Singapore Tech & Innovation Virtual Dialogue, "Forging Digital Standards: Challenges in Intellectual Property and Supply Chains" with over 30 participants (excluding speakers or staff) from the government, private sector, academia, and other non-governmental organizations.

Andreas Kuehn, Senior Fellow at the Observer Research Foundation America, and **Priya Mahajan**, Head of Asia Pacific Public Policy & Regulatory Council of Verizon Communications, discussed the challenges of supply chain security. The session examined the landscape of digital crime in the APAC region, explored the complex nature of supply chain security, and debated the age-old question of how much government intervention is too much.

Key findings from this meeting are described below.

Cybersecurity Landscape of the Asia-Pacific

In 2007, Verizon Communications began its Data Breach Investigation Report (DBIR) to answer the who, what, where, when, and how of cyber security breaches. Over the course of 14 years and with contributors from 88 different countries, the DBIR provides intricate details of the cybersecurity landscape.

Among the three regions examined by the DBIR (North America, Asia, and Europe, Africa, and the Middle East), 34% of all security breaches occurred within the arts, entertainment, and recreation sector. This sector has become particularly lucrative for hackers given the digital transformation catalyzed by Covid-19. Of the 29,207 worldwide incidents analyzed by the DBIR, 5,258 were confirmed breaches, with ransom incidents twice as common as they were in 2021. The vast majority of data breaches contained a human element and focused on web applications as the attack vector. The DBIR further identifies specific patterns in breaches (the loss or unauthorized access to an organization's network, data, applications, or devices) and incidents (an event outside of normal operations that disrupts organizational operations). With breaches, social engineering, basic web applications attack, and system intrusions were most common. For cybersecurity incidents, denial of service was the most common – comprising roughly half of these incidents – while occurrences of basic web application attacks and social engineering accounted for most of the remainder.

The DBIR report also reveals patterns unique to the APAC region. The DBIR analyzed a total of 5,255 regional incidents – 1,495 with confirmed data disclosure – finding that the most common type of data breach within APAC was social engineering operations, e.g., manipulating unsuspecting individuals to engage in behavior such as bank transfers or the purchase and transfer of gift cards to fraudulent parties. Out of the 1,130 confirmed data breaches against top industries in APAC, public administration was the most targeted, accounting for nearly 60% of all incidents. While espionage and amusement were found to be occasional motivations for hacking, financial goals accounted for 96% of all breaches. Finally, the most commonly compromised form of data was credentials at 96%, followed by personal data at 3%. Ultimately, the vast majority of cybercrimes are financially motivated.

Supply Chains and Cybersecurity

ICT supply chains have not only economic but also national security implications and are increasingly subject to geopolitical tensions. Supply chain security is challenging to ensure on a technical, organizational, and political level given the complex and transnational nature of today's global supply chains. For example, Apple has over 200 suppliers in 43 different countries. However, links within supply chains, whether related to the economy, digital infrastructure, or critical technologies, are ideal targets for digital crime. Ensuring supply chain security is therefore essential, and as an initial step, governments have begun to develop relevant security standards and risk frameworks.

Stakeholders must confront a spectrum of challenges to achieve supply chain security. Imposing accountability for bad behavior is difficult and there is a long way to go to rectify issues of attribution. A lack of norms also presents concerns. Frameworks, standards, the role of government, and accountability of vendors across different sectors urgently requires discussion at the domestic and international levels. At present, a lack of incentives has precluded private sector cooperation in implementing the type of frameworks needed to achieve greater supply chain security. Vendor and buyer accountability, including issues over the legality or security implications of products sold, also needs to be addressed.

Several factors have influenced contemporary developments in supply chain security. First, the digital landscape has recently – especially since the pandemic – gone through significant transformation. As supply chains expand in scope and scale, so too does cybercrime. A prime example is Singapore's smart city strategy, which has increased attack vectors as more devices connect to critical national infrastructure. With more digital actors and connections, a reduction in the relative cost of hacking, and greater professionalism from cyber criminals, supply chain security should be re-framed to incorporate cybersecurity considerations at its core.

Second, techno-nationalism has increasingly become the norm, as evidenced by the willingness of governments to place restrictions on foreign technologies and favor domestic suppliers over national security and economic concerns. While such measures can be justified on the grounds of national security, they can also have detrimental economic impacts. U.S. chip suppliers, unable to export to China due to government restrictions, have keenly felt the consequences of techno-nationalist policies.

Third, supply chain security becomes significantly more complicated when considering issues of geopolitics and technology. China seeks to become a dominant force in the critical and emerging technology space to reduce its foreign dependence on key inputs while extending its ability to exercise pressure on other states. Thus, these states have come to see an overreliance on foreign supply chains as dangerous. Yet this danger falls on a spectrum. Lack of 5G access might be considered an inconvenience for most but a failure to secure semiconductor supplies could have cataclysmic implications for a nation's well-being.

These challenges are significant but not insurmountable. As a start, supply chain security and resilience should be addressed at three fundamental levels. First, buyers should focus on risk management when purchasing information and communication technology products, while vendors should follow international standards and best practices. Second, vendors should establish a consortium through which they are able to provide risk assurances, participate in norm setting, and commit to vulnerability disclosures. Finally, at an ecosystem level, regional transparency and certification standards need to be developed complementing the United Nations' efforts in creating cybersecurity norms of state behavior.

Intervention vs. the Market

Supply chain security is an emerging issue that governments have been approaching from a variety of angles. Washington, for example, has recently folded supply chain security into its cybersecurity framework, with nine presidential executive orders addressing supply chain security and resilience. Another example is the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certificate, a program which acts as a "unifying standard and certification model to ensure that DoD contractors properly protect sensitive information."

The case for direct government cybersecurity intervention in form of hard, legally binding requirements remains contentious, however. Those in favor of increased intervention argue that the government should intervene when an industry is slow to adopt standards or is ineffectively handling cybersecurity. Others argue that increased government intervention stifles innovation. In APAC, many governments have been enacting well-intended supply chain policies that have dampened trade and investment. If companies are forced to comply with non-uniform standards and regulations, the cost and difficulty of conducting business increases. While the IT industry is generally not in favor of government regulation, there must be a conversation about effectively securing systems and protecting consumer data and privacy and the conditions under which intervention might be necessary. Regardless of one's position, close collaboration between government and industry is crucial.

The private sector should seek ways to work with governments rather than waiting for direct intervention. The willingness of the private sector to share information among its constituents and with the government remains crucial to building secure supply chains. However, without an ecosystem of trust between members of the private sector and the government, information sharing will continue to lack uniformity. This lack of trust is especially prevalent in Southeast Asia where the demand for liability clauses has been growing at pace with the frequency of data breaches and ransomware attacks. Without adequate guarantees and protections, the private sector is unlikely to seek full cooperation. To this end, frameworks that are conducive to cooperative solutions, such as operational information sharing, are an important step. Such frameworks would facilitate the flow of pertinent information within the private sector, allowing them to work together to solve security issues quickly. By working toward a collective solution, the private sector can help avoid excessive government regulations that may hamper innovation.

Regardless of government approaches, responses will need to be holistic and capable of generating trust. Given that supply chain security is a group exercise between vendors, operators, and buyers, government intervention may be a necessity to help coordinate policy or when issues of national security arise. Policymakers must walk a fine line between protectionism and security as even legitimate reasons for excluding products or vendors from a supply chain could incur significant economic costs and loss of industry investments and technological leadership in the long run.

Supply chain security is a relatively nascent topic and any solution at a micro level will require cooperation between the private and public sectors. Similarly, any effective solution at a macro level will need to be collaborative rather than unilateral. Thus, as supply chain security issues continue to evolve, they offer ample opportunities for the U.S. and Singapore to strengthen their partnership.

This document was prepared by Daniel Mitchum. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Vice President of Pacific Forum. These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.