October 5th, 6th, 2017

Cyber3 Conference Tokyo 2017 Summary

General Information

Dates	Thursday, 5th and Friday, 6th October, 2017
Venue	Keio University Mita Campus, 2-15-45 Mita, Minatoku, Tokyo
Organizer	Nikkei Inc.; Nikkei Business Publications, Inc.
Co-Organizer	Cyber Security Research Center, Keio University Information-technology Promotion Agency, Japan National Institute of Information and Communications Technology
In association with	Japan Cybersecurity Innovation Committee（to be established）
Knowledge Partner	PwC Japan Group World Economic Forum (WEF)
Chairman	William Hiroyuki Saito (Special Advisor, Cabinet Office, Government of Japan)
Official Support	Cybersecurity Strategic Headquarters; Ministry of Internal Affairs and Communication; Ministry of Foreign Affairs; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Economy,Trade and Industry; Ministry of Defense; National Police Agency; Personal Information Protection Commission; Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); British Embassy Tokyo; French Embassy in Tokyo; Israel Economic and Trade Mission; Embassy of the Kingdom of the Netherlands in Japan; Embassy of the Republic of Singapore in Tokyo; U.S. Commercial Service Japan, Embassy of the United States of America; INTERPOL; InterNational Cyber Security Center of Excellence (INCS-CoE)= Keio University, The University of Tokyo, Waseda University, Tokyo Denki University, Institute of Information Security, Kyushu University, Stanford University, Northeastern University, University of Maryland-Baltimore County, Harvard, Massachusetts Institute of Technology, Carnegie Mellon University, Georgia Institute of Technology, University of Delaware, University of Cambridge, Imperial College London, University College London, Royal Holloway-University of London,Queen's University Belfast

Executive Summary and Proposal

The theme of Cyber3 this year was “Tokyo Olympic/Paralympic Games in 2020 and beyond”. 2020 year will be a critical one for management of cybersecurity, and we need to think about how cybersecurity will be advanced beyond 2020. The Cyber3 Conference is constantly evolving just as cybersecurity is evolving to tackle new and unexpected threats. Multiple stakeholders must come together to discuss beyond their own domain to tackle the challenges of this new era. With industry-academia-government collaboration, this year IT human resource development was also a key theme.

- Society 5.0 is the new government growth strategy for future innovation though digital transformation of the Japanese society, for which cybersecurity is a critical requirement.

- Spread of cyber risks cannot be fought by a single organization - we need to work in unity between business, government and academia, and also globally. Many SMEs do not have cybersecurity expertise in house and therefore the government needs to provide tools and resources to help them in this area.

- Organizations need to assume perimeter defenses will be compromised and have mechanisms in place to stop the spread of infection and minimize damage in order to maintain resilience, with solid BCP measures in place. We must also recognize that cyber attackers are taking many evolving forms with diverse motivations.

- Communication is indispensable for cybersecurity and the Cyber3 Conference is one way of furthering it. Cybersecurity also requires leadership and speaking out to share information, and the conference encourages conversations that go beyond the official two days.

Background

The 1972 Munich Olympic Games were marked by violence, and cybersecurity is necessary to counter modern threats to the upcoming Tokyo Olympics, as evidenced by the ever increasing level of cyberattacks upon each Olympic Games in recent years. Tackling issues requires political commitment and also awareness at the CEO level. Partnership and collaboration is required at all levels, between companies, between sectors, between countries.

US and Japan are both strong, vibrant, well connected economies that rely on computer systems to support their way of life, making them uniquely vulnerable to cyber-threats. Cybersecurity is a critical area of U.S.-Japan cooperation and a subject of discussion between President Trump and Prime Minister Abe.

UK Prime Minister May issued a joint communique with Prime Minister Abe to bring Japan-U.K. cooperation on security to a new level, with cybersecurity as a central area of focus. In UK, the NCSC was established in 2016, which collaborates with the private sector and academia as well as countries around the world, including countries with which it does not have a traditional security relationship.

Private sector cooperation is critical. Joint expertise and collaboration with academia and industry has helped in countering cyberattacks.

Connect Track

With the spread of IoT, the proliferation of devices that are connected to the Internet is resulting in diversification of cybercrime. Cybersecurity is even more important than before. By connecting various systems through IoT there is an emerging System of Systems. Unlike with just information systems, in this case it is essential to ensure measures are taken at each layer and incorporate security into the devices, the network, the platform and each service. This must be done in cooperation among multiple stakeholders, which can be done effectively under an approach incorporating five pillars: the creation of a structure to take measures to address vulnerabilities, advancement of research and development, promotion of security measures by private sector companies, strengthening of human resource development, and international cooperation.

When considering cybersecurity, it is of course important to prevent problems from

occurring, but it is also important to enhance resiliency and to give priority consideration to what needs to be done so that systems can rebound after an incident has occurred.

In Japan there is a tendency to aim for zero risk. However, in the world of cybersecurity there is no possibility of zero risk. It is important to accurately identity the various risks that exist and consider this to be a managerial exercise in determining where and how to allocate the available resources.

The tendency to treat any cyber incident as a very big problem results in the creation of a corporate culture in which incidents are hidden and not reported. As such there is a tendency for a delay in developing the truly important measures and for sharing information. Academia can play a role in changing this as it is perceived to be in a neutral position and able to make independent evaluations.

In this digital age OPEN API are essential for all financial services. This includes proprietary systems developed by banks and data and systems that are commissioned and open to vendors. This will make it possible to develop highly convenient financial services. When making use of an OPEN API it is essential to ensure a balance between safety and convenience. In order to do succeed in doing that it is important to establish access controls in line with the use and objectives of financial institutions, FINTECH firms and users and to create a community, strengthen regulations and to foster governance underpinned by an understanding from the financial sector.

The concept of Society 5.0 integrates the database layer and the service layer and will result in the promotion of innovative services. AI, big data and cybersecurity will provide a platform for this.

The world is focused on what is being called Industry 4.0. In Japan what is being called Society 5.0 is very much focused on people. Society 5.0 will make use of data to quickly and efficiently implement actions across a wide spectrum to provide people with various benefits. However there remain many issues including data reliability, cybersecurity, developing regulations on the use of personal information and others.

Architectures must be made to be Secure by Design and to incorporate Privacy by Design. Establishing authentication mechanisms (identification, authentication, authorization) for authentication of people, data and devices is essential for building overall trust, which is

required if we are to realize Society 5.0.

Autonomous driving (AD), electric vehicles (EV) and connected cars (CC) can be combined to create the ability to provide extremely high level mobility services. We should not only focus on the evolution of mobility. We must aim for the development of highly convenient services that are closely linked together across all business segments.

Even in Japan where there is a high focus on security and safety and a highly developed social infrastructure including automobiles, there will be a severe check focused on deep learning, which is the core of autonomous driving.

However, by building knowledge in this environment Japan will be able to emerge as a leader in this sector and this should serve as an engine for developing technologies that are competitive and closely integrated into society and people's lifestyles.

Crime Track

The discussions in the Crime Track this year focused on the evolving identities and motivations of cybercrime, as well as the roles of government and the private sector and strengthening collaboration between them. The track suggested the need for two mechanisms: a nationwide intelligence gathering mechanism for creating actionable intelligence, and a confidence building mechanism for public-private partnerships.

Cybercrime is constantly evolving to take new forms, reach new stages of threat, and fuse the cyber world with the "real" world. However, awareness is still far too low and countermeasures and cooperation need to be strengthened. Collaboration involving diverse aspects such as cyber threat intelligence gathering must increase on inter-organizational, national, and international levels.

We must recognize that cyber attackers are taking many evolving forms, including online criminals, hacktivists, terrorists, and nation states, with diverse motivations that respectively include financial goals, ideological causes, forcing change, and national interest. In addition to striving to identify the "who" behind cyberattacks, we should also concentrate on the "why," "what," and "how" to gain a holistic view of attackers and patterns of attack.

Businesses, especially senior managers who are often the most lacking in awareness,

must recognize the seriousness of cybercrime and conduct comprehensive risk assessments that take into account information leaks, business interruption, and physical damage to people and infrastructure. They must appropriate proper budgets to cyber insurance and dedicated cybersecurity staff, rather than just forcing everything on overworked IT departments.

There is currently a debate over the extent of the role government should play in cybersecurity, often colored by a deep-rooted distrust of government due to concerns over privacy. However, we must ask ourselves why cybersecurity gets a pass on regulation and liability compared to industries like automobiles, food, and medicine when the risk is so high and growing daily. Due to their overarching nature, governments can play a dynamic role in pushing cooperation and encouraging research. For example, since academic researchers and hackers themselves are often the best sources of information about cyberattacks, the government can push past company reticence to support real-life hacking research on company products to expose and defend against vulnerabilities.

Relationships of trust between governments, the private sector, and academia are key. Governments can set penalties and liabilities, but they should also proactively collaborate with the private sector to tackle underreporting of cyber threats. More collaborative information sharing is also necessary, so companies do not think they are throwing their information into a black hole. In turn, the private sector needs to share information but also recognize what constitutes actionable information and have reasonable expectations for results.

There is a gap between technology advancement and policy set by governments around the world. Governments must constantly evolve their approach to security issues or be left behind. Japan in particular greatly lags on policy despite striving to achieve the concept of Society 5.0. Given that Japan will host the first Olympics in the era of the IoT, its government and private sector should view the Games as an opportunity to bolster cybersecurity and achieve technological policy goals.

Security Track

AI has already been used in the industry for many years to assist with processing very high volumes of events at the scale of 1 trillion security events per month, using AI to augment the abilities of human operators to make rapid decisions, and dealing with rapidly evolving

security threats.

AI has the potential to significantly help to reduce false positives so that more threatening alerts are easier to identify. For AI development both security analysts and AI specialists need to work together so that the AI team can understand what will support the security analysts in effectively carry out their role on behalf of the customer. AI and deep learning are already now used in many services. One area where AI and deep learning is used is in analysis of logins to identify attacks through suspicious activity or typical attack patterns.

The prevailing attitude in Japan is of trying to adapt to new regulations as quickly as possible, rather than to be proactively involved in rulemaking. Companies will need to change their mentality to become more proactive. When systems are developed secure by design is a basic requirement, but a test environment is required to ensure this, and the costs of development escalate in line with the degree of testing carried out, so a balance must be found.

Each country has its own data protection laws, but when data is transferred across borders it is not possible to know how the data will be protected in all countries. Awareness of GDPR in European companies is still too low, with some countries or industry sectors having only a very small proportion or organizations fully prepared for the regulations coming into effect in 2018.

Japanese corporations need to be aware of new definitions of PII, including biometric information, numbers such as driving license numbers, but also data such as cookies or IP addresses or other information that may be linked to a specific individual which may also be considered as PII depending on the region.

Privacy impact analysis and Privacy by design are essential to comply with privacy regulations, and senior management should be engaged with a full budget and ownership. In terms of protecting information, it is not just PII but also corporate information that must be protected from theft. In this regard cybersecurity measures are an investment which can also contribute to improvement of business processes.

Each company has its own structure at the executive level, but in general in Japan only around 40% of companies have a CISO in place, and in many cases this role is held concurrently with other roles. Whatever the structure in place, there needs to be clear

accountability for implementation of security policies.

Next Actions

METI is promoting the Connected Industries Initiative 2017 with a view to 2020 and beyond. Cybersecurity measures are indispensable for these connected industries to ensure the safe transfer and handling of data. METI and IPA (Industrial Cyber Security Center of Excellence) carried out an initial joint exercise in the field of cybersecurity with experts invited from the US (DHS and ICS-CERT), and METI and IPA will continue to collaborate with US, EU and others in this field.

States need to agree on the actions that they will not engage in in the cyber realm in terms of attacks on critical infrastructure, but this is both a significant challenge to achieve and difficult to enforce. Cybersecurity was developed by practitioners which means that fundamental questions were left untouched, such as the problem of attribution.

There is a lot more work to be done around the world to continue to shift the perception of cybersecurity from one of being a technical issue to being a national security and policy issue. The problems in different countries are often the same, but the solutions are particular to each country due to the political structure as well as societal differences.

An important characteristic of cybersecurity is to reduce the conflict between security and privacy, and significant research and investment will be required to address the issue. In addition to privacy and security, there is also an enduring conflict between innovation and security.

Cybersecurity is the foundation for all ICT activities. As the 2020 Tokyo Olympic Games approach, a cybersecurity task force has been established and initiatives have been set in place as Japan accelerates its cybersecurity efforts in preparation. The Olympic Games represent a significant risk for attacks by various threat actors, but provide an opportunity for Japan to put in place effective infrastructure that will provide benefits long into the future. In addition, the best preparation is development of overall resilience, human resources, and effective processes, rather than focusing on specific threats, since the threat landscape changes so quickly.

There are various services and infrastructure required for the Olympic Games and it is

important to carry out a risk assessment and consider how we are going to protect ourselves. Attacks can come from various sources, and there may be crimes of opportunity. The Olympic Games is seen as just as important a marketing opportunity by malicious actors as it is by official sponsors and organizations.

The Government is pursuing five areas: setting up a system for IoT vulnerability, fostering research and development, promoting security measures in the private sector, human resource development, and international as well as government-academia-private sector collaboration.

The Government is working to realize Society 5.0, for which cybersecurity is indispensable. Relationships of trust between governments and the private sector are a key part of effective cybersecurity. Leadership needs involvement of expertise from private sector and research in order to make the best policy decisions.

Cybersecurity needs to broaden its focus to encompass understanding of business risks and context. Curiosity and a thirst for continuous learning is imperative. This will also contribute to building networks of trust. People are the most important element. There is a shortage of cybersecurity experts, so we need more capacity building.

The importance of cybersecurity has been shifting from confidentiality of data towards availability and integrity of data. We need to understand why we are being attacked and also understand how we can be attacked in order to defend ourselves. Companies should assess their risks (both physical and cyber), allocate resources, and share information for their own benefit as well as others.

In the past year we have seen an increase in large-scale influencing of elections through fake news, and ransomware attacks which appear to have actually been state-sponsored attacks. In addition, we have seen the massive Equifax data breach, and manipulation of markets by hackers for monetary gain.

We cannot limit our thinking on security to cyberspace. In light of the broad impact on society, if five years from now we are still discussing this topic in "Cyber" conferences then we will have missed the key point of these discussions.

Documentation: