Executive Summary and Proposal

- As a wide variety of devices and data are digitized and connected to the Internet, the Internet of Threats (due to cyber crime, denial of service, etc.) is also exploding. Cooperation between enterprises, the public and private sectors and the international community is indispensable to ensuring cybersecurity.

- To promote multi-stakeholder cooperation, a system that smoothly shares information on cyber-related threats must be established by creating incentives for sharing information and permeating a “Need to Share” mindset.

- The government must create a cyberspace-related framework that addresses matters such as the establishment of international rules, and the promotion and definition of regulations and guidelines.

- Each enterprise must initiate cybersecurity measures to help themselves in their own areas of responsibility, which requires that enterprise management have a security mindset. Management must see cybersecurity measures as an “investment” instead of a “cost” and make effective investment decisions with a firm understanding of cyber risks.

- Regardless of enterprise scale, security must be permeated through the entire supply chain starting with major enterprises, their subsidiaries and affiliated companies, and down through the network of small and medium-sized enterprises (SMEs).

- There is a shortage of security human resources, both in quality and quantity, which creates the need to raise the standard of HR to meet the needs of society, and create resources that can succeed globally. The use of technology such as AI to supplement the lack of human resources should also be considered. Furthermore, to ensure smooth communication between management and front-line staff, cyber-related risks must be discussed in business terms instead of technical terms.

- By fully leveraging Japan Quality, Japan has the opportunity to initiate and lead the next phase of digitalization of industry, dubbed “Industry 4.0”. To generate the momentum required to realize this, the government must display strong leadership. Industry, government and academia must cooperate and promote growth strategies that seize the chance presented by the 2020 Tokyo Olympics.

Background

The Cyber3 conference provides a multi-stakeholder venue to discuss issues related to cybersecurity as the changing landscape of the world becomes dominated by data. The conference's three tracks discussed the impacts of increasing interconnectivity, the cybersecurity aspects of these connectivity changes, and cyber crime aspects, which are closely interlinked.

With the arrival of self-driving cars, consideration needs to be given to the interconnections between cars and connections between cars and other devices such as smartphones. When different classes of objects are connected, the security of the communications must be ensured, with a clear definition of the responsibilities. The Japanese Government has implemented a cybersecurity strategy, and a General Security Framework for Safe IoT Systems, which is a meta standard framework for individual sectors, and it is planned to propose this as an international standard together with interested countries.

Global changes in the structure of industry and society are driving the adoption of digital technologies, and the Japanese Government is proposing the Super Smart Society, Society 5.0, as a unified approach to addressing these broad challenges, focusing not only on technology but also operational knowhow. The rapid expansion of IoT presents many new cyber threats to the lifelines that society is heavily dependent upon. The Japan Business Federation has made policy proposals to reinforce cybersecurity which have contributed to the government's activities in this area.

ConnectTrack

There are both great opportunities and great risks in the connected world that can only be solved by public-private partnerships and a better understanding of the risks. We must keep in mind the pace of change of technology, where the exponential growth patterns mean that over five or ten years the changes seen will be enormous.

Issues regarding autonomous cars on the business front include the establishment of standards for assessing the performance of autonomous cars, how to establish the public/social infrastructure, and the construction of legal regulations and standards. Establishing the public/social infrastructure is a very difficult matter. Infrastructure for automated driving at the level where the driver is engaged will soon be in place. However, debate is necessary not only in Japan but also internationally on automated driving at the level where the system assumes complete control. Using the initiatives in the IT industry as a model, the automobile industry should have their own unique security requirements. Clarification of the boundaries to the scope of the responsibility of auto manufacturers and service providers is also a challenge in terms of the reliability and accuracy of AI systems.

The difference in risks of IT and OT (Operational Technology) needs to be made clear. It is particularly necessary to bear in mind that OT carries not only the risk of economic loss through property damage, but also the risk of harm to human lives. The market for cybersecurity insurance is not yet sufficiently developed, and many challenges remain to be addressed in this area. Different regions have different regulatory regimes for data management. This is the most difficult area, and coordination is not being properly conducted, with each region implementing its own policies for the regional environment. It is important to consider how to protect yourself from liability for actions in different regions. There should be an evaluation of the costs involved with potential risks and the investment required to alleviate these risks. Wherever there is a potential effect on social infrastructure, this needs to be taken into account.

Currently all of the demand in IoT is for functionality, with no demand for security, meaning that the attack surface is exploding. As some nations move to smart cities there are concerns that these are being built on a foundation of sand. Standardization of the IoT is required, with security included. This can be considered an investment in growth as a safe IoT will create a strong position for global competition and will allow the realization of sustainable economic growth. The development of security experts and education to raise the basic knowledge of users are indispensable to the future of the IoT. There must be a change in information sharing practices and thinking through public awareness that cybersecurity is a risk that affects our nation and our children.

Organizations can utilize big data to increase productivity and create new business opportunities, but this requires businesses to rapidly implement AI and big data in the same way as many companies competed to implement new ideas in the early days of the Internet. For example, new insurance services will be developed using big data and AI in the future. Big data analysis of gas turbines (500 GB/day) made it possible to predict failure. The use of big data can lead to accurate predictions in various fields, including detection of suspicious and abnormal activity. AI is replacing many roles in organizations that can be automated, eliminating the need for human operators. In the point of view of exporting Japanese big data and AI solutions, high quality is one of the key points of differentiation. Japanese architecture (e.g. the strength of the field organization) is also a strength of Japan. To obtain big data from the Internet there must be standardization and norms.

CrimeTrack

The CrimeTrack based its discussions on the outcomes of the previous Cyber3 conference, which centered on information sharing to increase situational awareness on cyber threats, strengthening collective defense, and enhancing law enforcement capabilities. As threats evolve rapidly, so must countermeasures. We also need to assess the stumbling blocks to sharing of actionable information.

Global cooperation is critical as most cyber crime originates from foreign countries. Measures such as system security auditing are currently becoming important to manage cyber risk. Consideration must be given to policy measures and what constitutes ‘personal information.’ Best practices to protect organizations from internal attacks must also be taken as activities such as outsourcing increase risk in this area. Guidelines on cybersecurity measures must be updated regularly to keep pace with advances in cyber crimes. Cybersecurity and national security go hand-in-hand as critical infrastructure is often involved, and the government should take an interest in this. Financial institutions are among the most important critical infrastructures, and so are held to higher standards. Countermeasures to new technologies and developing risks must be considered in advance since it will be too late to counter them effectively once the technology is developed.

There is a huge gap between skills and techniques of hackers and the security practices of government and industry. Criminals can share information more rapidly and broadly based on building trust among their communities for their activities. Meanwhile, government and private sector management of cybersecurity is often fragmented and operating in silos, and many cyber crimes go undocumented. In addition, legacy IT is very difficult to update and defend. A diffusion of power is taking place, with power shifting from state actors to non-state actors. Voluntary schemes and frameworks for private sector collaboration and information sharing are needed to increase private sector resilience.

A majority of organizations agree that sharing information on best practices to combat cyber threats would be beneficial for their respective industries overall. These organizations still compete on product, but willingly share threat intelligence. The more vendors that share threat intelligence, the more benefit the industry will have. And at the security level, solutions are often consistent between sectors. However, making these security solutions easy to use is a challenge. There is a need for an anchor of trust, and there was discussion on how this could be standardized. There was also discussion on the possibility of mandating rules and how to build an international consensus for this.

Through the evolution of AI and robotics, it is now possible for a robot to acquire and distribute information autonomously. The barrier between the cyber and real worlds has disappeared. It is now possible to cut the electrical supply either through cyber or real terrorism. Those who can utilize cyber technology will become strong and those who cannot will be left weak, creating a gap. The state is already weak in terms of the Internet and cyber technology compared with both the private sector and potential competitors.

SecurityTrack

Recent world events have shown that anything can happen and that we should not be surprised by unexpected events. While the future is unpredictable, we should prepare so that differences of culture and language do not lead to communication issues during an incident. There needs to be very clear ownership of issues to minimize gaps that can be attacked. Most action needs to be taken by the private sector, and this creates trust issues, so those trust relationships must be developed early, before a crisis. In addition to building relationships, tests and rehearsals must be conducted to identify gaps. The Olympic Games provide a great opportunity to focus attention on the right things with a common goal and deadline. The time remaining to the Olympic Games is a long time for the attackers who are already preparing, but a short period of time for the defender. In exercises it should not be forgotten that the “red-team” (attackers) generally wins now, which reinforces the need to conduct such exercises to strengthen the capabilities of the defenders.

There is value in data and information, and this motivates cyber criminals. Cybersecurity management therefore requires well-balanced approaches integrating people, process, and technology. For the “people” aspect, this means hiring the appropriate people, constructing a system to evaluate their appropriateness, and retaining and retraining high quality employees. In terms of “process,” a good manual should be created. That will help in the education of new personnel and transparency during audits. In the rapidly changing field of “ technology,” this means taking measures to mitigate weaknesses, improve defenses and enhance resilience. Complying with static international standards is not sufficient, as technology is constantly changing and active efforts to adjust standards to reflect these changes should be made continuously.

In the area of security, different skills are needed in different business divisions, which requires a very good understanding of the business and the acceptable levels of risk. For board members it is very important to develop an ability to make sound judgements in the face of cyber-related and other challenges. Training programs in Japan focus on knowledge rather than judgement, and while a certain level of knowledge is required to make a decision, judgement is a separate skill that needs to be developed. There is a tendency for management to refuse to implement new technologies due to fear of the risks involved, but at the same time it is difficult to remain competitive without implementing new technologies.

In a group company structure, the budget and manpower put into security will be different according to the member companies. However, reputation risk applies to the whole group, and the security level of the whole business is only as good as the weakest link. Understanding the business and its structure, as well as its vendors, is key to understanding how to manage information security and how to rapidly react to an incident. Good corporate governance with clear policies is also vital, backed by an effective structure for implementing security policies in each business reporting up to management, while allowing flexibility to fit the policies to the needs of the individual businesses. It is difficult for any individual organization to conduct cyber-defense activities by itself, and therefore external collaboration is vital. It is a business decision how much risk you are willing to accept, and the costs that you are willing to bear. It is important to have a very clear dialogue with the business leaders to help them understand the business impact of a breach and the level of risk in order to get buy-in from leadership. The guidelines for cybersecurity released by the Ministry of Economy, Trade and Industry (METI) in 2015, which stated that cybersecurity should be addressed in subsidiaries and vendors, gave a great boost to security teams in justifying to management the need to take action in this area. The inclusion of a message that cybersecurity is an investment (rather than a cost) is also very positive. However, as this is a guideline there is no absolute requirement to implement actions based on it.

Next actions

While IoT has several positive aspects, connectivity of devices also brings many risks as criminals move into smart cyber crime, leading some to refer to the “Internet of Threats”. Malware targeting IoT devices is a major new attack vector, and has already been used in DDoS attacks that can paralyze large parts of the Internet. Actors in cyber attacks include terrorists, online criminals, nation states and hacktivists. In addition to digital theft from financial institutions and accounts, the incidence of ransomware is also rapidly rising. Not only PCs and smartphones, but also internet connected TVs and other smart devices are vulnerable to ransomware and being incorporated into botnets for denial of service attacks. The INTERPOL Global Complex for Innovation (IGCI) in Singapore was created to focus on resilience, with experts from the private sector working alongside INTERPOL in order to improve information sharing. The change of mindset from “need to know” to “need to share” is vital to address the risks from cyber. There is a tendency in Japan to refer to data “leaks,” rather than data “theft,” which understates the urgency of the threat.

There must be a clear focus on cybersecurity among top executives, with appropriate resources allocated to prevention, detection, and mitigation, along with reporting of incidents to the authorities, and a focus on the three Cs of Collaboration, Cooperation, and Coordination.

Cybersecurity is a complex phenomenon that can seem to be overwhelming, so there is a serious question of how the boards of public and private companies can approach this issue. In Japan the concept of training of directors is not very common, and there needs to be a sense of crisis in the board room with regard to the lack of awareness and preparation in this area.

The National Association of Corporate Directors has a Cyber Risk Oversight directors’ handbook, which sets out the important principles on cybersecurity risk awareness for businesses. There is no “right answer” for cybersecurity, but there is a “right process”. For cybersecurity, management is critical, but discussions must also involve representatives of legal and HR in addition to IT. Boards must require a holistic risk evaluation framework, including cybersecurity, but not limited to cybersecurity. As someone said, the key cybersecurity decisions need to be made in the board room, not the server room.

Principles outlined in the METI guidelines. There are complicated cross-border issues with data protection regulations. Human resources for war gaming may come from Cyber Security Incident Response Teams (CSIRTs) established in some companies, but this is not yet common enough. Data is the oil of the digital economy, and we need to learn how to deal with oil spills for the 21st century.

Cybersecurity from The Perspective of Diplomacy Strategies

With the increase of cyber attacks, including upon critical infrastructure, there is no country that is left unaffected, with the consequences affecting the lives of citizens. The cost of cyber attacks is already estimated to be tens or even hundreds of billions of dollars each year and is growing rapidly. The lack of visibility into the source of attacks and the difficulty of attribution means that the attacker has the advantage, and therefore governments must work together to address these threats, in partnership with the private sector. A global discussion is underway on ensuring the rule of law with regard to cyberspace, and the application of existing international law to cyberspace is suggested to be the best approach to achieving this. The UN has established a Group of Governmental Experts (GGE) to discuss the application of international law and the responsible behavior of States in the cyber-sphere, but it was pointed out that discussion of GGE participation needs to be more inclusive and that the elements of the reports should be implemented by many countries including non-members of GGE. The Counter-Terrorism Committee Executive Directorate (CTED) of the UN has a mandate to monitor the implementation of comprehensive counterterrorism measures. Attacks by terrorists on critical infrastructures impacting large numbers of civilians can be used as a means of gaining maximum exposure for their activities. Prevention requires not only increased security measures but also better prosecution, which in turn requires international rules for preservation of digital evidence. There is a discussion of appropriate norms such as that countries should protect their own national infrastructure through active cyber defense measures, in addition to cooperating in the event of attacks on other countries’ infrastructure. The G7 has also been comprehensively discussing the issue, and has created a working group to continue to move the discussions forward. Many bilateral discussions are underway to promote confidence building, and an important challenge is to build the capacity of the vulnerable countries in the area of cybersecurity, as this is not an issue that can be solved by any one country alone.

What Specific Actions Japan Should Take as a Leader in Asia

In January last year the Basic Act on Cybersecurity was enacted in Japan, with the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) as the leading agency. However, following the attack on the Japan Pension Service the scope of monitoring activities by NISC has been expanded, and recognizing that government agencies abilities in cybersecurity were still insufficient, new posts for cybersecurity were created in each ministry at the deputy director-general level. METI has taken a particularly serious approach to this area, as it is in charge of various key industries. One action taken is the creation of cybersecurity guidelines for small and medium sized enterprises. There is also a cyber rescue team that can help to triage incidents.

IoT, big data, and artificial intelligence (AI) are key for Japan's continued economic success, underpinning the fourth industrial revolution which will be critical for Japan to overcome changes in society. However, last year a cyber attack on a Japanese institution occurred every five seconds against the Japanese Government. Therefore, cybersecurity is an indispensable part of the country's growth strategy, and the government established the cybersecurity headquarters as a control tower for the government's efforts in this area.

In September 2015 a revised Cybersecurity Strategy was adopted, which highlighted the importance of private sector cybersecurity-oriented management teams with an investment mind-set, development of human resources in cybersecurity, both in quality and quantity, even from the primary school level, and the protection of the nation and the general public from the effects of cyber attacks. In August this year the common norms were modified and we are reviewing the action plan for critical infrastructures. At the Ise-Shima Summit the G7 members agreed to work together to build a safe cyberspace, and Japan also is looking through ASEAN to promote partnership for capacity building among ASEAN countries.

In some respects, when preparing for a major event such as the G7 summit, looking back at past history is not that useful given the rapid changes that are taking place in this area. Rather, it can be more useful to carefully monitor what has been happening in recent months throughout the preparations. For the Olympic Games Japan needs to be imaginative in visualizing what might happen and to have a framework for broad information sharing to take advantage of the experiences of people in all areas.

2020 will also be a test for IoT. Security needs to be implemented in IoT systems, and METI and the Ministry of Internal Affairs and Communications (MIC) should be working together to come up with a way to incorporate a security gateway into IoT systems. For industrial systems it is very difficult to apply straightforward textbook study to the security, rather it needs imagination to apply the principles to different systems. METI would like to raise the overall cybersecurity level and also improve the abilities of the private sector, so that businesses can more easily identify and analyze the potential impact of true threats and so that taking cybersecurity measures is not seen as a cost but as an investment for their growth and stability.