

# **A Call for Reinforcement of Cybersecurity**

## To Realize Society 5.0

December 12, 2017

Japan Business Federation (Keidanren)

# A Call for Reinforcement of Cybersecurity

## To Realize Society 5.0

### I Introduction

–Background & aims

### II Fundamental Perspectives

1. Value creation
2. Risk management

### III Specific Matters to Be Addressed

1. Raise awareness
2. Secure resources
  - (1) Train personnel
  - (2) Share information
  - (3) Technical measures
  - (4) Promote investment
3. Establish cybersecurity framework
  - (1) Establish government-affiliated organizations & enable collaboration
  - (2) Establish frameworks inside & outside companies
4. Develop legal system & norms
  - (1) Japanese legal system
  - (2) Technical standards
  - (3) International cybersecurity norms

### IV Keidanren's Action Plan

1. Promote understanding among top management
2. PR/publicity activities
3. Global links

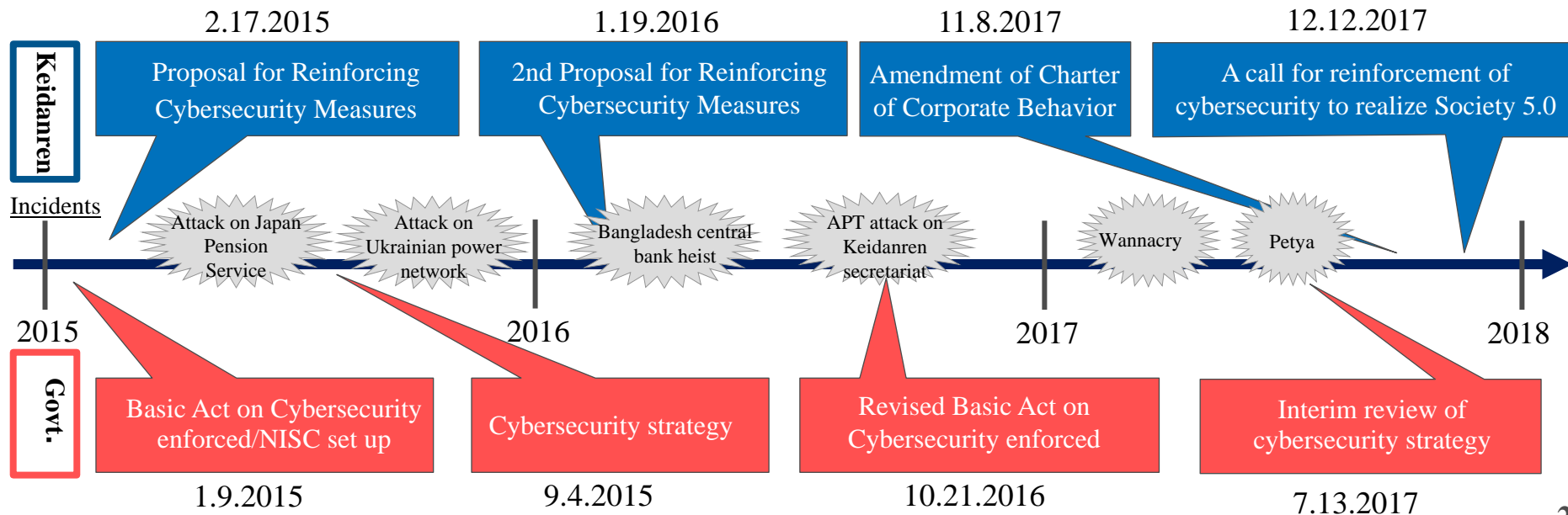
### V Conclusion

–The run-up to the Olympics/Paralympics

Keidanren proposed reinforcement of cybersecurity measures twice in the past, as well as amending its Charter of Corporate Behavior to state that companies should address cybersecurity as a social responsibility.

Damage from cyberattacks is growing worldwide, and has reached a new level

Keidanren is renewing its proposal to push further for specific initiatives in companies and organizations of all types, as well as collaboration among all involved



# The Importance of Cybersecurity in the Society 5.0 Era

**Society 5.0**, in which all kinds of objects, people, and concepts **will be linked** by data, is coming. **Ensuring cybersecurity is important** to prepare for a society that solves issues using technology and data.



It is important to work proactively to ensure cybersecurity from two perspectives: as a **precondition for creating value** via Society 5.0, and for **risk management**.

## Value Creation

**Security is necessary as a precondition for creating value in cyberspace in the Society 5.0 age**



- ◆ Maintain/enhance ability to compete by providing safe, worry-free products & services with cybersecurity assured
- ◆ Ensuring business conditions within global markets and enhancing security self-sufficiency are also necessary perspectives

## Risk Management

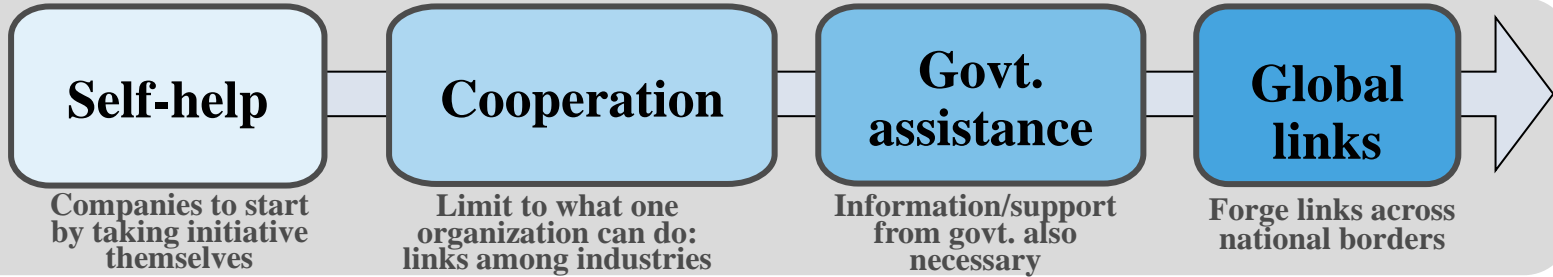
**If measures against cyberattacks are neglected, companies will be unable to continue in business, with potentially major impacts on stakeholders and citizens**



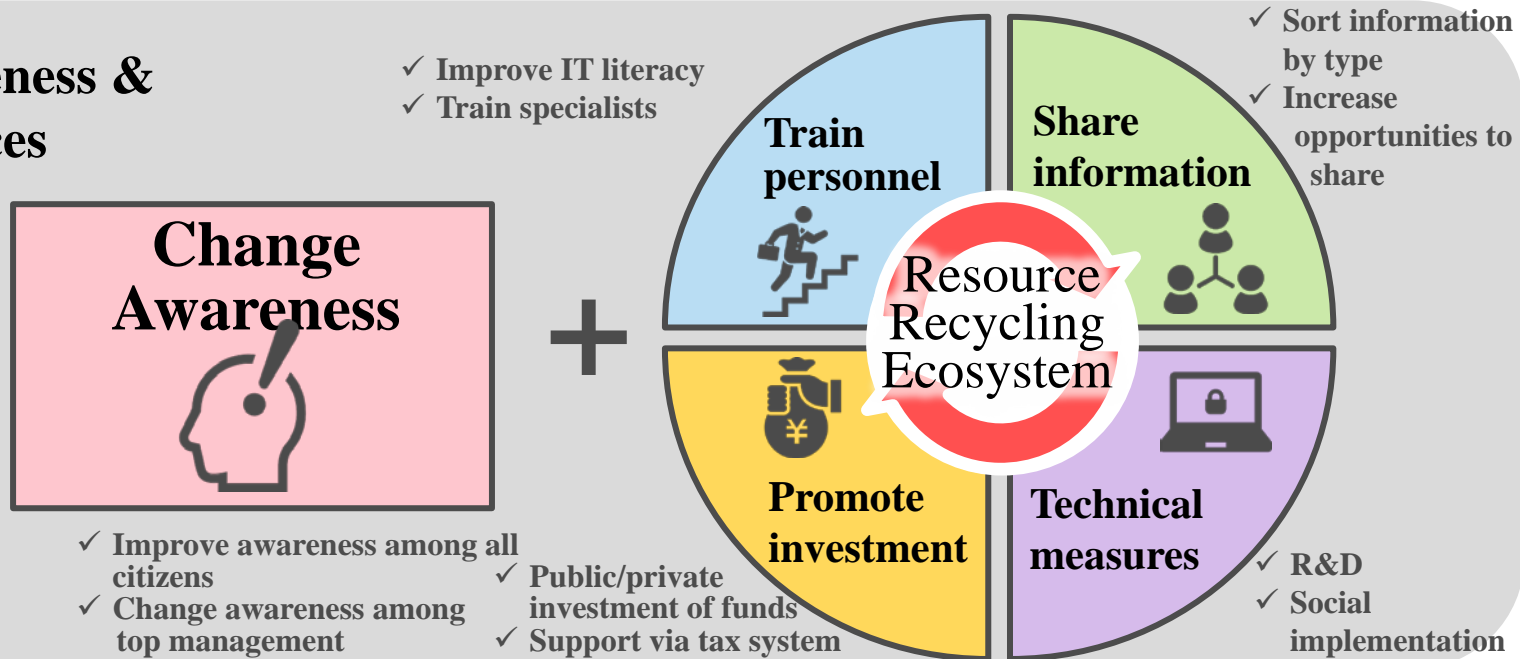
- ◆ Companies need to take initiative to develop measures as social responsibility
- ◆ However, full protection is impossible; cyberattacks should be regarded as unavoidable risks like natural disasters
- ◆ To ensure business continuity, emphasize response/recovery by detecting attacks early and preventing damage from spreading

# Overview of Cybersecurity Measures

## Approach



## Change awareness & secure resources



## Develop frameworks as foundation







It is necessary to improve awareness of cybersecurity throughout Japan.  
In particular, changing awareness among top management in each organization is key.

## Security by design

- ✓ Being aware of security from the product/service **planning & design stages**

## Raise awareness among top management

- ✓ Top management to **recognize** cybersecurity as the **most important management issue**
- ✓ Cybersecurity issues to be regularly reported to/discussed at board of directors meetings, etc.; top management to take responsibility for decisions
- ✓ **Secure appropriate resources, e.g., personnel & budgets**

## Spread recognition that full protection is impossible

Even if baseline measures are implemented, it is impossible to protect fully against cyberattacks

- ✓ Emphasize **efforts to minimize damage** after an attack
- ✓ **Foster a social climate** that does not needlessly blame companies that sustain damage despite taking measures to prevent attack, but instead encourages them to actively disclose information

# Train Personnel (1)



Most cybersecurity incidents are attributable to human factors; it is therefore important to improve IT literacy throughout society.

Moreover, personnel who can take responsibility for cybersecurity measures are severely lacking in terms of both quality and numbers; it is therefore necessary to build an ecosystem for training and retaining personnel.

## Improve IT literacy throughout society

### Schools

- ✓ IT literacy education starting in elementary/junior high school
- ✓ Build up no. of teachers who can teach IT literacy

### Organizations

- ✓ Continuous education and training for staff/employees

### Top Management

- ✓ Top managers themselves to deepen their understanding of IT & cybersecurity

## Discover outstanding young personnel

### Provide chances to compete

- ✓ Need to provide chances to try out skills, such as security contests, CTF, etc.



### Ethics education

- ✓ Ethics education is required so that outstanding young personnel do not get involved in wrongdoing



# Train Personnel (2)

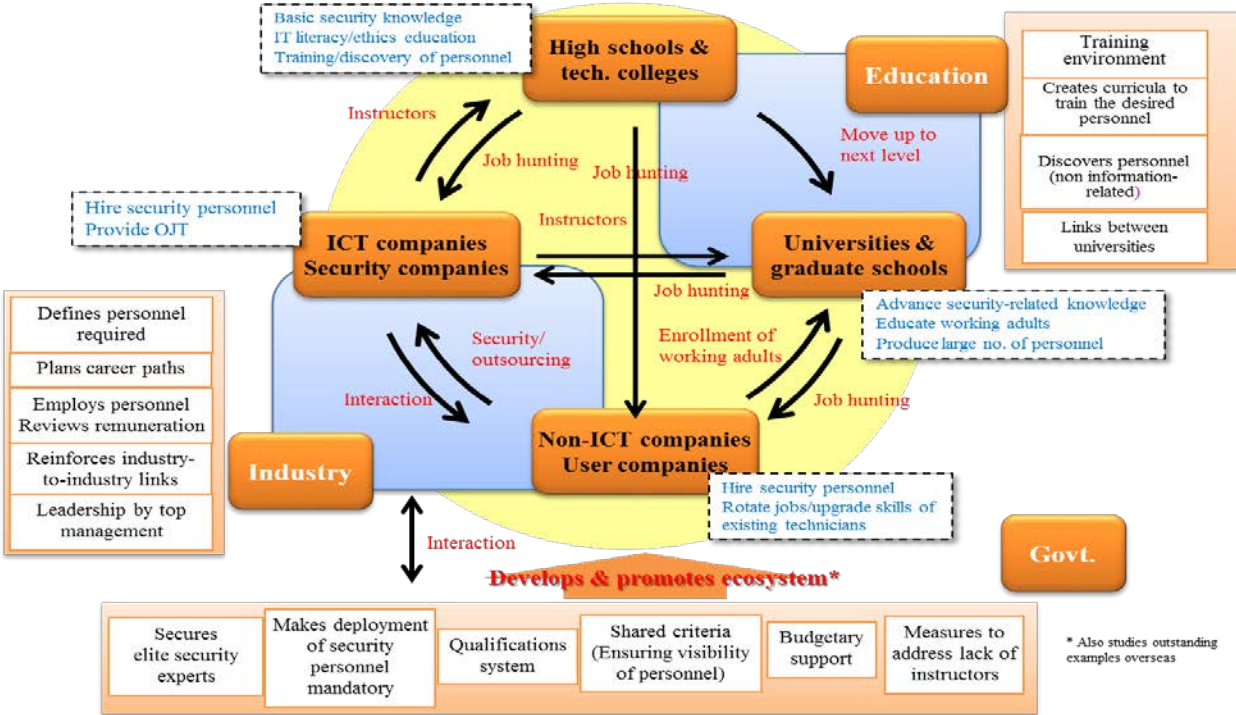
## Build an ecosystem to train & retain specialist/highly skilled personnel

### Education/ Training

- ✓ Ensure that training measures & educational curricula reflect the types of personnel required by industry
- ✓ Provide training/re-training for working adults & recurrent education
- ✓ Popularization of qualifications & global links

### Career Path

- ✓ **Improve remuneration, actively hire highly skilled personnel inside & outside Japan**
- ✓ **Go beyond existing HR systems** in public/private sectors  
(system enabling personnel to play active roles with special remuneration regardless of age or past career)



# Share Information (1)



**To prepare for cyber attacks, it is important to gather, share and utilize information.**

**We need a mechanism to promptly share information across companies, industries, public and private sectors, and national borders.**

## Clarification of 5W1H

- Although the importance of information sharing is being understood, the construction of concrete framework is not progressing.
- Although there are various information such as "vulnerability / technical information", "analytical information", "threat information" from "know-how · best practices", the necessary information and way of correspondence also differs depending on the receiving position.



- ✓ It is necessary for public and private organizations and organizations to organize and standardize 5W1H (purpose, type, place, position, timing, method, etc.) of information to be shared / utilized.

## Expand framework for sharing information

Some industries are making progress in organizing opportunities for sharing information, e.g., by establishing Information Sharing and Analysis Centers (ISACs), but they need to be increased further.

- ✓ **Increase no. of fields with ISACs & improve how existing ISACs function**
- ✓ Establish Information Sharing and Analysis Organizations (ISAOs) that cut across industries
- ✓ Provide media such as mailing lists and portals, etc., for sharing information

## Create mechanism for government assistance

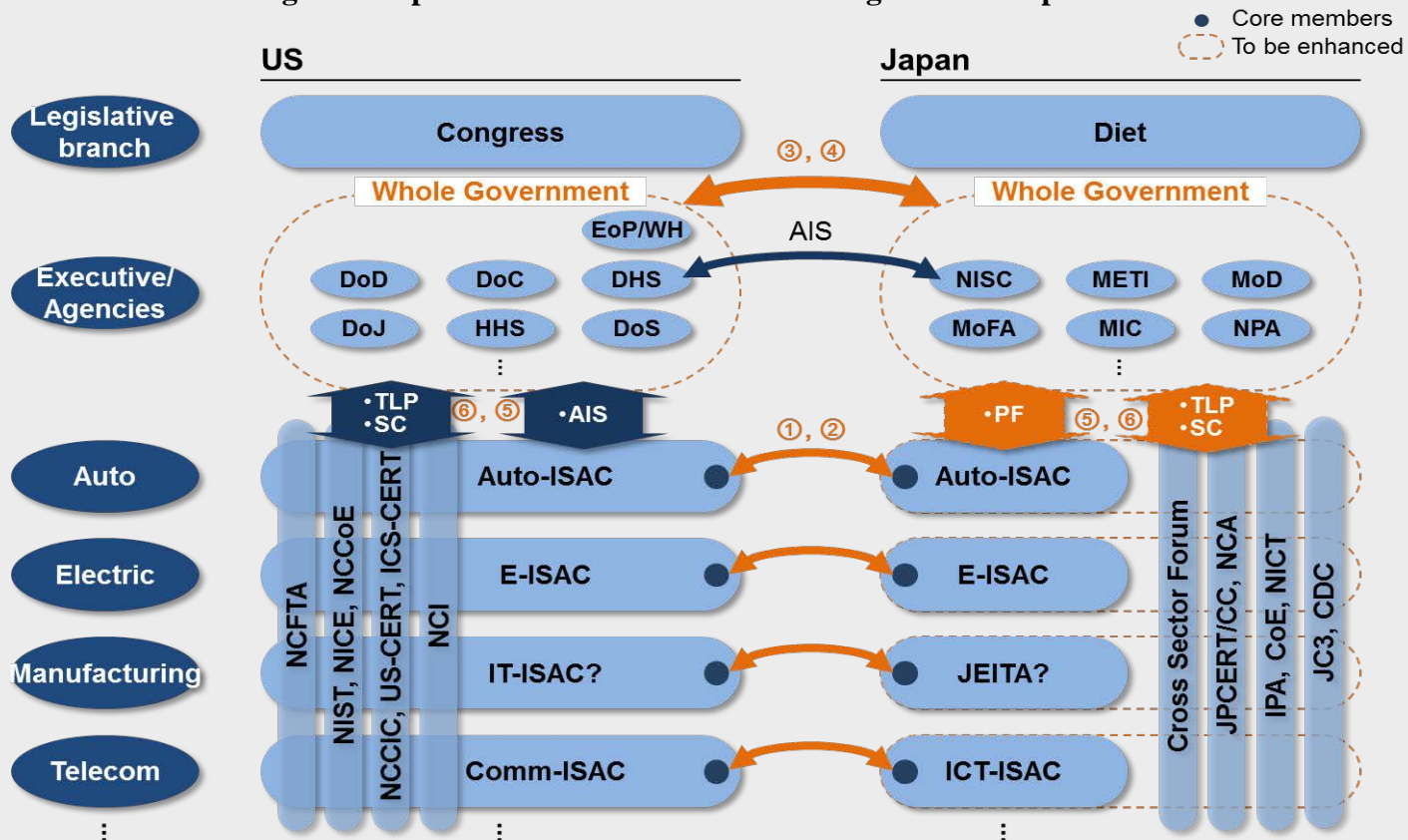
The potential for information collection/sharing by private-sector companies alone is limited; government assistance is required.


- ✓ Take lead in sorting information & support information-sharing organizations
- ✓ **Establish cross-sectoral mechanism providing information to private sector about threats**  
under certain conditions
- ✓ Integrate existing Traffic Light Protocols & promote their use
- ✓ Examine scope & conditions of system authorizing who can handle information (security clearance), etc.
- ✓ Mechanism enabling information provider to limit extent of sharing

## Global links

- ✓ Mechanism to enable **real-time information sharing with US** and other **relevant countries involving both public & private sectors**
- ✓ Japan should aim for **information sharing among governments & companies and global links among ISACs**

Figure: Proposed Future Information Sharing between Japan and US



 It is essential to reinforce technical measures to make up for lack of personnel & IT literacy. Public & private sectors should work together to pursue technical R&D and expedite social implementation.

## Measures in individual organizations


- ✓ Update OS & software
- ✓ Employ anti-virus software
- ✓ Use passwords & encryption technology
- ✓ Manage access rights
- ✓ Employ multiple defenses inc. physical security

## Technical development, etc.

- ✓ Increase R&D for security technologies (warning sign detection, anonymization, encryption technology, etc.)
- ✓ Measures for OT/IT & linkage of diverse devices
- ✓ Use latest technologies such as AI & blockchain
- ✓ Pursue research on attackers

## Measures for SMEs

Difficult for SMEs to secure resources alone; cooperative use of technology & personnel is required

- 
- ✓ Promote use of cloud among SMEs
  - ✓ Popularize convenient cloud services

## Provide products & services

- ✓ Enact measures based on various guidelines
- ✓ Make full use of reward schemes, etc., for discovery of information on vulnerabilities

## International standardization

- ✓ Take initiative in proposing specs for technical standards
- ✓ System for mutual certification with US & European countries



Realizing Society 5.0 requires focused investment of funds in personnel, information & technology; creating mechanisms & systems to ensure efficient fund flow is essential.

## Investment by companies

- ✓ Invest **adequate funds in personnel, technology, development of systems, etc.**
- ✓ Use insurance, etc., to cover risks
- ✓ Support measures at subsidiaries, business partners, etc.
- ✓ Set up organizations such as ISACs, think tanks, etc.



## Measures by SMEs

- ✓ **Found mutual aid association** enabling SMEs to share information in return for low premiums
- ✓ Establish **national organization that can provide across-the-board support** for cybersecurity measures, auditing, information sharing, handling incidents, dealing with insurance, etc.



## Government assistance

Establishing/maintaining organizations & groups imposes a considerable burden. It is also difficult for SMEs to take measures using only their own resources.

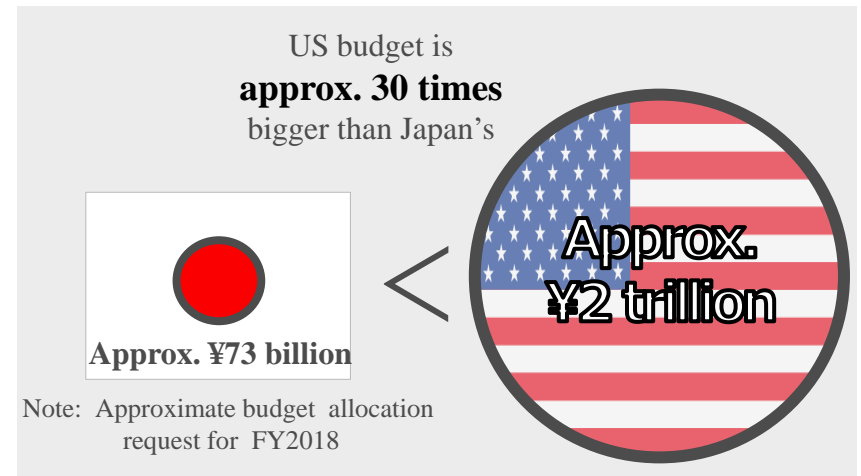
→ Requires government support in promotion of corporate initiatives

- ✓ **Institute tax breaks** for purchase of systems & services, etc.; **upgrade tax system to facilitate investment by SMEs**; provide support via subsidies
- ✓ Provide support via tax system for costs of measures at domestic subsidiaries borne by parent companies
- ✓ Provide subsidies toward costs of setting up/operating organizations (ISACs, think tanks, etc.)

## Government budgets

- ✓ Position cybersecurity as a form of public infrastructure provision
- ✓ Focus investment on personnel, technology, etc., by **significantly expanding government budgets**

Figure: Comparison of Japanese and US Cybersecurity Budgets



The Cyber Security Strategy Headquarters formulates government strategy; individual government departments secure budgets & implement measures.

Compartmentalizing can result in measures being duplicated/fragmented; government departments' respective roles are unclear.

- ✓ Clarify roles of relevant government departments/organizations; **integrate measures and inform all parties of order of priority**

## Strengthen NISC's command center function

- ✓ Authority to propose & decide establishment/combination/abolishment of individual departments' measures
- ✓ **Increase personnel/budget**
- ✓ **Direction/management/ supervision** of personnel training, collection/analysis/sharing of information, global standards/links, etc.
- ✓ Extend public awareness activities
- ✓ Single contact point for reports/consultation regarding attacks
- ✓ Links with physical security

## Issues in the future

- ✓ **Consolidate relevant organizations and ensure political leadership** to facilitate integrated reinforcement of measures

**In addition to developing an in-company framework including a CISO & security response unit, BCP and related considerations are also important.**

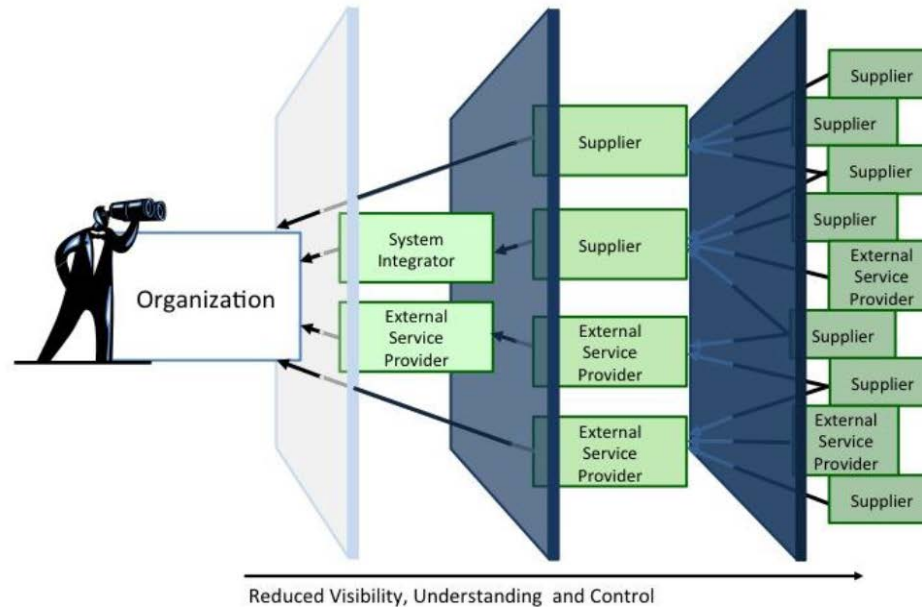
## Develop in-company framework

- ✓ **Appoint a CISO or other individual** with responsibility for security measures & ensure adequate support staff
- ✓ **Set up security response unit** (CSIRT, PSIRT, SOC, etc.) **with links to top management**
- ✓ Provide continual awareness-raising/education via employee training & practice exercises
- ✓ **Formulate business continuity plans, etc.**, targeting prompt recovery & conduct regular drills

Given that companies of all types and sizes are connected via IT, it is necessary to ensure rigorous management of cybersecurity throughout the entire supply chain including outsourcing contractors & business partners.

## Ensure cybersecurity in supply chain

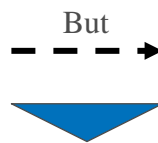
- ✓ Set up digital supply chain ISAO
- ✓ Employ process management at each stage
- ✓ Make use of SOC reports & a variety of other reports when checking on outsourcing contractors/ business partners



Legal system/norms are currently not adapting quickly enough to rapid advances in technology. Development of legal system & norms is required to make cyberspace safe and worry-free.

## Japanese legal system

In order to reinforce cybersecurity, research on attacks, identification of the sources of attacks, etc., are essential



Instead, risk of infringing on **Act on Prohibition of Unauthorized Computer Access, Copyright Act, Telecommunications Business Act**, etc., impedes research and measures to reinforce security

- ✓ **Development of reference guidelines and sufficient reexamination of the laws is required**

## Technical standards

US introduced cybersecurity technology-related framework and certifications (NIST SP800/FedRAMP, etc.) and is contributing to progress of cloud storage for all national records



- ✓ Japan should learn from these initiatives and their operation, incorporating private-sector opinion to **formulate internationally applicable technical standards & guidelines for measures soon**

## International cybersecurity norms

In the UN and elsewhere there are moves to create an international framework & norms to make cyberspace safe and worry-free



- ✓ Japan also needs to ensure repeated dialogue among parties involved, including all relevant government agencies & private sector organizations so that **industry, academia, and government can collaborate to actively participate in and lead moves to establish international cybersecurity norms**

Keidanren itself regards reinforcement of cybersecurity measures as the key issue in realizing Society 5.0 and will implement its own initiatives to promote change.

## 1 Action to promote understanding among top management

- 🎯 Formulate Keidanren Cybersecurity Management Declaration
- 🎯 Offer seminars/training/off-sites for top managers



## 2 Action relating to PR/publicity

- 🎯 Conduct surveys of cybersecurity measures at individual companies/publication of case studies, etc.
- 🎯 PR/publicity via newsletter/briefings/dispatching instructors, etc.
- 🎯 Cooperate in events organized by government/other organizations
- 🎯 Disseminate information to stakeholders in Japan & overseas



## 3 Action to promote global links

- 🎯 Participate in Japan-US Cyber Dialogue, Japan-US Policy Cooperation Dialogue on the Internet Economy, Japan-EU ICT Strategy Workshop, etc.
- 🎯 Forge links with the World Economic Forum, etc.





## **Conclusion**

**Reinforcement of cybersecurity is a pressing issue in the run-up to the 2020 Tokyo Olympics & Paralympics.**

**Collaboration by all types of stakeholders will be essential: companies/organizations, politicians, government/local authorities, universities/educational institutions/research institutes, media, investors, citizens, etc.**

**Japan's prowess in basic technologies, emphasis on quality, and a national tendency to work hard can contribute to reinforcing cybersecurity worldwide.**

**Keidanren will pursue concrete initiatives in collaboration with the government and other organizations.**