## Forward looking toward Olympic

# Cyber Security in 2020

2017/04/26

Trend Micro Incorporated

# Agenda

- Considering the year 2020 for Japan
- Understanding importance of Security Master Design
- Essential Components for Next Generation Cyber Security

# Considering the year 2020 for Japan

# What would the year 2020 mean to Japan

- **Stage to present Japanese technology, culture, hospitality ?**
  - IoT, AI, Robot, UAV, Autonomous Car ??
- **Or Japan to show the political leadership ?**
  - Completion of post WWII, US-Japan alliance, Pan-Pacific ?
- **Or Japan to be a potential target of terrorism ?**
  - ISIL, Al-Qaeda, Hizb Allāh, Partiya Karkerên Kurdistan
- **Or the best appealing stage for global activist group ?**
  - Anti-Capitalism, Anti-Commercialism, Anti-Japan…

# Major International sports events have been targeted

… because, it is seen by all-of-the-world, best situation to appeal their claims.

**1972年 Munich Massacre [Black September]**
1983年 Rangoon bombing (Seoul Olympic Related)
1986年 Gimpo International Airport Bombing（〃）
1987年 Korean Air Flight 858 Bombing（〃）
1996年 Manchester Bombing (UEFA CS)
1996年 Centennial Olympic Park bombing (Atlanta)
1998年 Three Lions' bench Bombing （France WC）
2002年 Stadium Bombing in Madrid
2004年 Bombing attack in Athens
2008年 2008 Kunming bus bombings
2008年 2008 Weliveriya bombing (Sri Lanka Marathon)
2009年 2009 attack on the Sri Lanka national cricket team
2010年 July 2010 Kampala attacks (South Africa WC)
**2013年 Boston Marathon Bombing**


"All the News That's Fit to Print"

The New York Times

LATE CITY EDITION

VOL. CXXI ... No. 41,634 NEW YORK, WEDNESDAY, SEPTEMBER 6, 1972 15 CENTS

9 ISRAELIS ON OLYMPIC TEAM KILLED WITH 4 ARAB CAPTORS AS POLICE FIGHT BAND THAT DISRUPTED MUNICH GAMES

MRS. MEIR SPEAKS

A Hushed Parliament Hears Her Assail 'Lunatic Acts'

A 20-HOUR DRAMA

2 Others Are Slain in Their Quarters in Guerrilla Raid

©New York Times

# What happened in RIO2016


## Major Cyber Incident (by NCFTA*1 report)

- Petrobas Oil Company Hacked (February 2, 2016)
- Brazilian Government Websites DDoS (August 1, 2016)
- Brazilian Olympics Website DDoS and Data Breach (May 22, 2016, August 5, 2016)
- Cyrela Hacking and Data Breach (August 12, 2016)
- International Weightlifting Federation's Website Defaced (August 17, 2016)

## Other noteworthy threat

- A lot of new ransomware targeted Brazilian Olympic Committee
- Legacy threat, such as phishing, DDOS, can be seen a lot as usual.



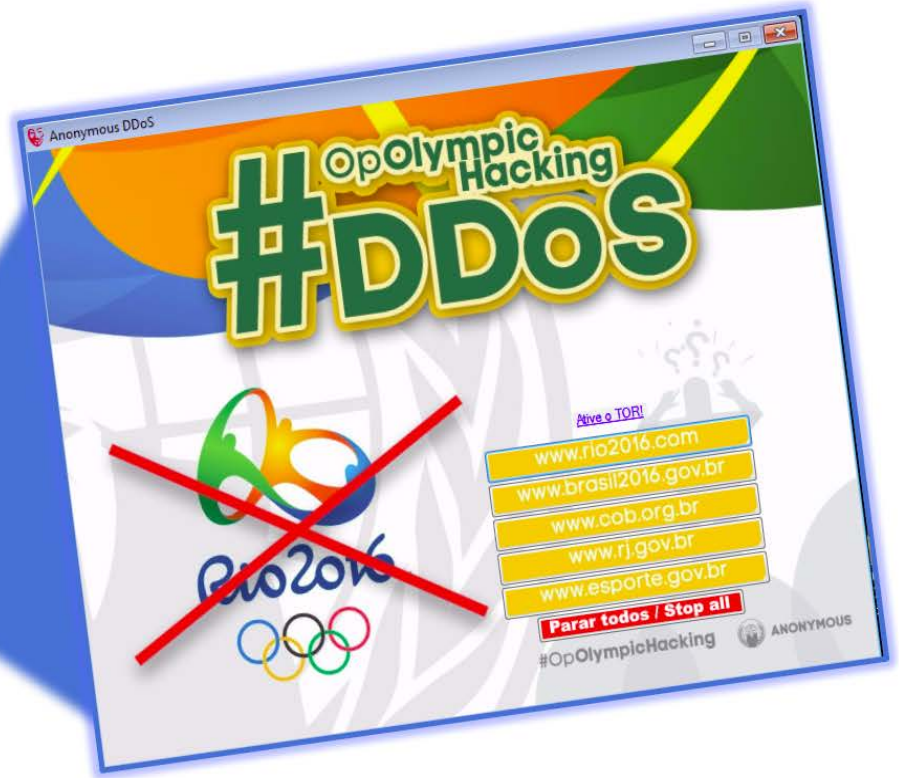

*1 NCFTA : National Cyber-Forensics & Training Alliance

Anonymous Brasil
8 August ·

#Anonymous #OpO
4 more database ha
We are Anonymous
Link: https://ghostbi
Anonymous







# What does the year 2020 mean to organizations ?

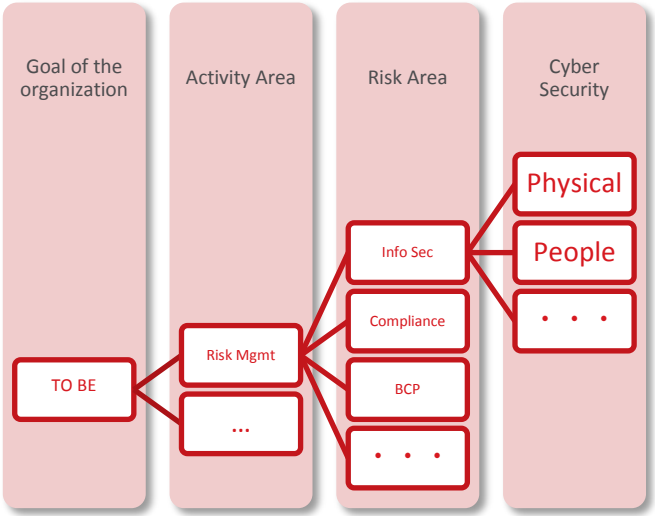
- Japanese Company will be the major target, as past Olympics.
- Sponsoring Company will be at the higher risk.
- Critical infrastructural company will be at extremely high risk.
- New eco-system based on IOT and ICT will generate higher economical value that means simply be targeted by money-motivated attackers.
- The population of TOKYO becomes 120% of usual time frame.

**Large number of organizations in Japan would face major RISKs in 2020**

# Importance of Security Master Design

# Security Master Design

**A Holistic Design of Security Framework**, based on the organization's vision, goal, raison d'être, etc, where all involved activities are thoroughly integrated with all business processes.

# Importance of the Security Master Design

- If “cyber security activities” are isolated from the business process, it may not become the essential portion of business itself.
- If individual activities are not be well integrated, the cost will be much higher.
- “Method” becomes “Objective” such as ISO certificates, which will easily low down the motivation of the people concerned.
- Security will become lower priority in each function blocks.
- Once people concerned becomes “passive”, decision-cycle becomes “reactive” and incident driven.

# The Structure of Security Master Design

## Prerequisite

Ideal State [TO BE], such as goal, objective, vision, success measure

## Process to define the master plan (Integrated Risk Management)

| Risk Identification | Risk Analysis | Risk Response / Incident Response Plan | Risk Reduction Plan/ Drill (IR) plan | Implementation of risk reduction, drill against incident | 3rd Party Review |
|---|---|---|---|---|---|
| Executives<br>Biz Owners<br>Risk Management Dept | Risk Mgmt Dept<br>Org at biz OPS<br>SME | Risk Mgmt Dept<br>Org at biz OPS<br>SME | Executive<br>Biz Owners<br>Risk Mgmt Dept<br>SME | Riks Mgmt Dept.<br>Org at biz OPS<br>SME | SME<br>Executive<br>Org at biz OPS<br>Risk Mgmt Dept<br>Biz Owners |

## Major Stakeholders

# Essential Components for Next Generation Cyber Security

# Essential Components for Cyber Security in Next Generation

1. Integrated Risk Management ⇒ Cyber as the organization risk
2. PDCA Model + ⇒ PDCA + OODA*1 loop
3. Ethical Hacker ⇒ Attackers' point of view
4. XGEN people development ⇒ Body of Knowledge based
5. Information Sharing ⇒ That monitored by OODA

Based on the existing security management system, it is mandatory to put the model which is based on the impact and then strategic defense strategy.




*1 OODA : Observe, Orient, Decide, Action by John Boyd

# 1. Integrated Risk Management

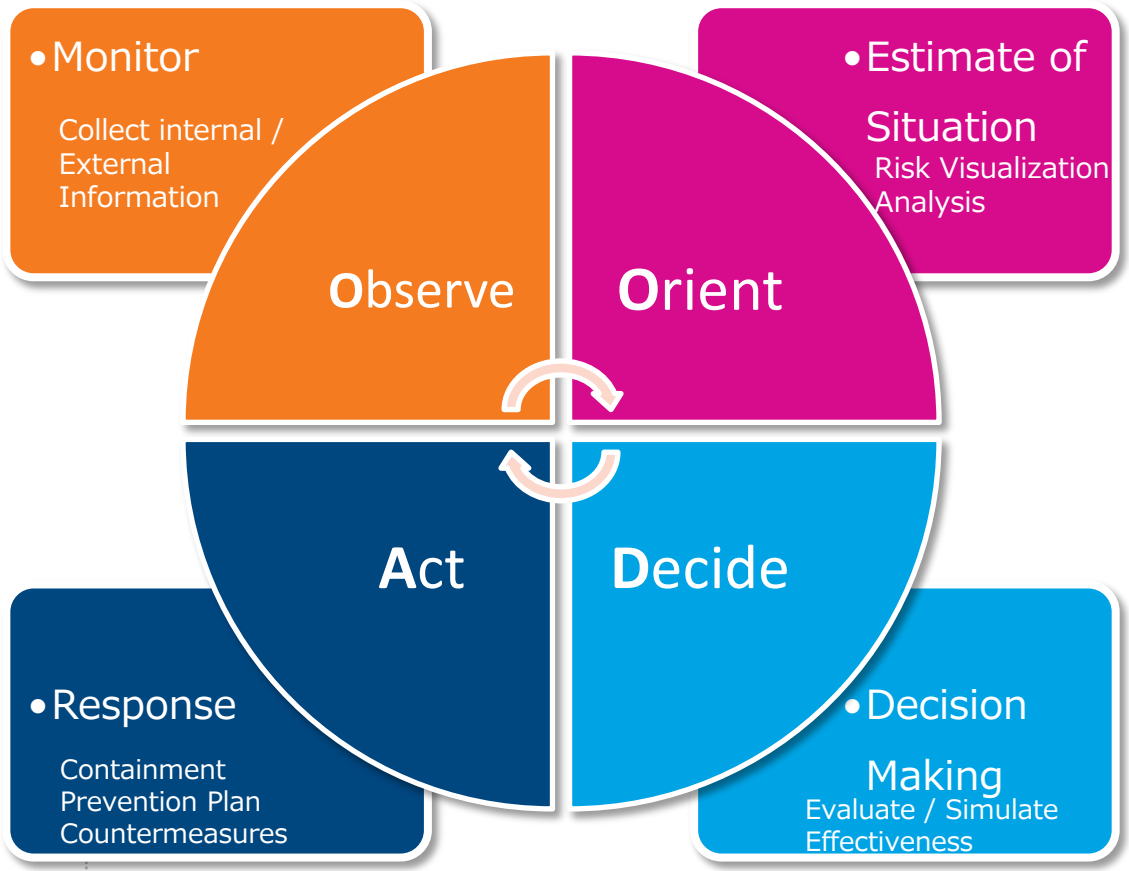
- Back Ground
  - Fast-glowing new ICT Ecosystem through the IoT Innovation
  - Time frame from sign of risk to actual incident is shortened
  - Higher tension across international relations
  - Rapid change in attacking methods and attacker's motivations

All risk areas interrelates and affect each other, so that silo type of management will no longer work.


**What's needed ?**

- ✓ Estimate of situation
- ✓ Prompt & right decision making
- ✓ Risk Management
- ✓ Incident Response
- ✓ No Silo

# 2. OODA for Cyber Security



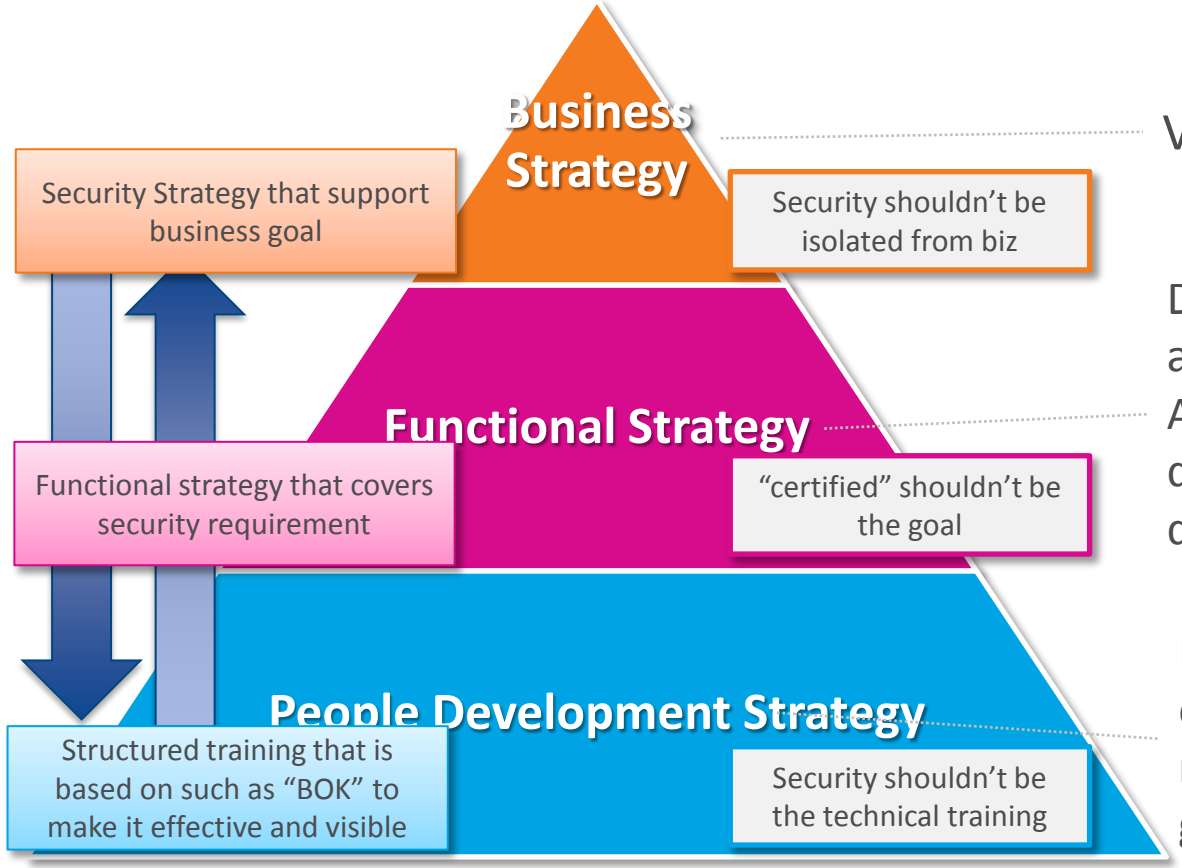

**OODA Loop**

- ✓ A decision cycle of observe, orient, decide, and act
- ✓ Originally developed by US military strategists & USAF Colonel John Boyd
- ✓ Focuses on Fast Response
- ✓ Often used to implement process to handle unexpected events & incidents.

# 3. The Ethical Hackers

1. Think from the attackers point of view （purpose, intent, method, timing etc…）
2. Being aware of hacker’s point of view would lead to true visualization of critical components to organization, vulnerable area.
3. “Standards / Regulations” such as ISO are methods and being certified is not objectives on security, having ethical hackers would provide better optimized compliance to them.
4. Offence vs Defense would become real time battle and ethical hacker’s would contribute in fast response.

# 4. Organization Capability Building




Vision / Goal of the organization

Define the required capability to achieve the functional mission. And need the people development plan based on the definition.

Define the required skills, experience and maturity level that needed for achieving functional goal.

# 5. The importance of information sharing

1. Difficult to grasp holistic picture of threat by alone.
2. Too much related information that makes difficult to generate actionable intelligence.
3. The effect of cybercrime involves multiple stakeholders

1. The Chambers of Commerce took lead on info-sharing in US.
2. Homeland Security establish the information hub for public-private collaboration.
3. NCFTA*1 starts public-private joint research.
4. Information sharing by ISAC*2 has been driven by EO#13691.

*1 National Cyber-Forensics & Training Alliance
*2 Information Sharing & Analysis Center

# Steps to enhance the security based on “master design”

Corporate Vision / Goal

Risk Identification

Vulnerability Analysis

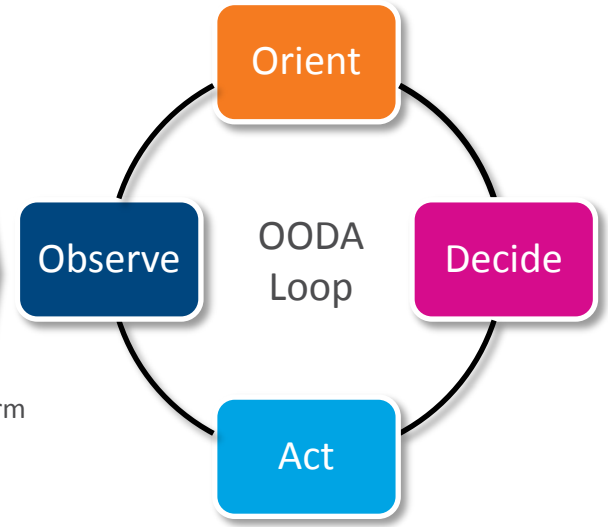
Cyber Triggered Risk Identification

Risk Scenario Identification

Risk Assessment per Scenario


Monitoring Start

Info-Sharing Platform



# Thank You

THANK YOU