

**Apirath Limmanee\***  
apirath.li@kmitl.ac.th\*

Department of Engineering Education, School of Industrial Education and Technology,  
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520 Thailand

\*Corresponding author E-mail: apirath.li@kmitl.ac.th

**Received:** June 29, 2026 **Revised:** June 30, 2026 **Accepted:** June 30, 2026

**Citation reference:**

Limmanee, A. (2026). Cyber security measures in Tokyo 2020 Olympic games: a case study.  
**International Journal of Industrial Education and Technology**, 8(1), A1-A4.

 **ABSTRACT**

This article reviews the cyber security measures and strategies used in Tokyo 2020 from its official report, an academic article, and some security guidelines. The topic includes basic risk management policies, risk assessment, security working units and personnels, cyber security measures before and during the Games, and conclusion on the success factors.

**Keywords:** Cyber security, Risk assessment

---

## **I. INTRODUCTION**

Organizing a gigantic event like Tokyo 2020 Olympic Games requires extremely rigorous planning, especially in terms of risk management. There are several risk categories to be considered, such as the weather, the crowd, the logistics, or even the terrorist attack. There is, however, another kind of risk that is equally, if not more, difficult to manage, the risk of cyber-attacks.

This article reviews the cyber security measures and strategies used in Tokyo 2020 from its official report, an academic article, and some security guidelines. The topic includes basic risk management policies, risk assessment, security working units and personnels, cyber security measures before and during the Games, and conclusion on the success factors.

## **II. BASIC RISK MANAGEMENT POLICIES**

From the official report, there are five basic risk management policies as follows (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).

- 1) Operating the Games Safely
- 2) Completing the Games as Planned
- 3) Preserving the Social Reliability of the Tokyo 2020 Organizing Committee
- 4) Operating the Games through Appropriate Finance
- 5) Achieve the Satisfaction of All Relevant Parties of the Games

### III. RISK ASSESSMENT

In the official report of Tokyo 2020, risk assessment for cyber security consists of risk identification and risk evaluation (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022). The risk identification part identifies prioritized risks and records them into a risk register. However, to be more precise, risk assessment is defined by ISO/IEC 27000:2018 as consisting of risk identification, risk analysis, and risk evaluation, as shown in Figure 1.

| Process             | Definition in ISO/IEC 27000:2018 (JIS Q 27000:2019)                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk Assessment     | Overall process of risk identification, risk analysis and risk evaluation                                                                          |
| Risk Identification | Process of finding, recognizing and describing risks                                                                                               |
| Risk Analysis       | Process to comprehend the nature of risk and to determine the level of risk                                                                        |
| Risk Evaluation     | Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable |
| Risk Treatment      | Process to modify risk                                                                                                                             |

**Figure 1:** Definitions of key terms

Source: Information-Technology Promotion Agency, Japan (2022, p. 3)

The functional areas of risk management (RSK) proposes the same set of generic attack scenarios for all venues, but they are customizable for each in terms of possibilities of damage and loss. This enables unique identification for each venue while maintaining consistent risk management across all venues.

### IV. FORMING SECURITY WORKING UNITS AND PERSONNELS

Several security working units are formed. They coordinate with one another to ensure that the security policies are met (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).

- 1) Security Bureau (SEC) was founded to implement security planning and system considerations at early stages.
- 2) Chief Security Officer (CSO) has jurisdiction over total crisis management for the
- 3) Tokyo 2020 organizing committee.
- 4) Security Operation Center (SOC)
- 5) Technology Operation Center (TOC)
- 6) Security Coordination Center
- 7) Cyber Security Response Coordination Center
- 8) Security Information Center
- 9) Computer Security Incident Response Team (CSIRT)
- 10) Chief Information Security Officer (CISO)

### V. CYBER SECURITY MEASURES

Cyber security measures of Tokyo 2020 are divided into two stages, before the Games and during the Games.

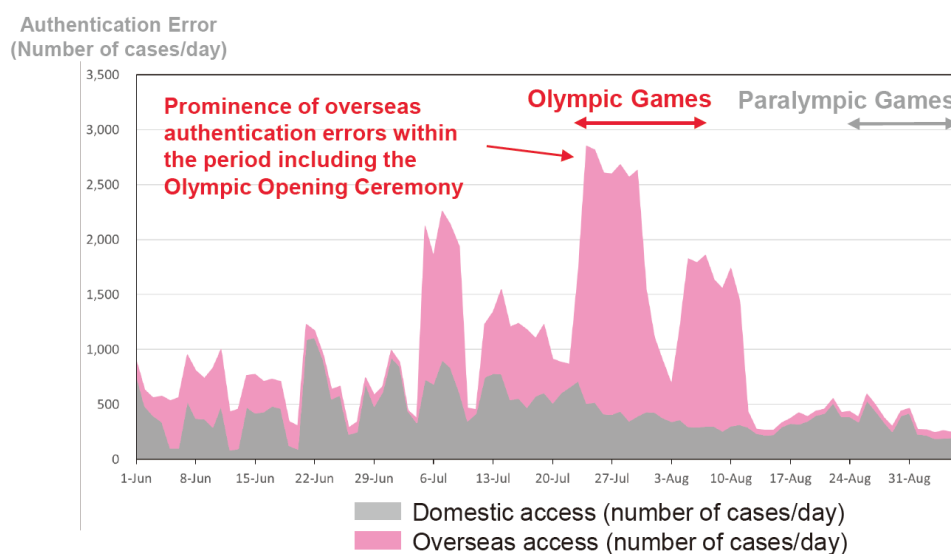
#### A. Before the Games

As preparation before the Games, four types of security measures are taken as follows (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).

- 1) Cyber security exercises: Training, network-based e-Learning training and “awareness training,” are conducted. The awareness training includes training on dealing with targeted email cyber-attacks. For cyber-attacks on critical systems, tabletop exercises are carried out with various simulated scenarios. This involves several participating bureau staff.



- 2) Cooperation with relevant authorities: Those authorities include the Cabinet Secretariat Olympic and Paralympic Games Tokyo 2020 Promotion Management Team, the National Centre of Incident readiness and strategy for cyber security (after “NISC”), and the Tokyo Metropolitan Government Office for Strategic Policy and ICT Promotion. The collected and analyzed information on threats was shared with stakeholders such as the IOC, OBS, marketing partners, and related functional areas.
- 3) Venue cyber security support: The targets of cyber-attacks include not only the information systems (IT) but also the operational technology (OT) such as central monitoring control systems, as well as power and air conditioning monitoring control installed in facilities. Both permanent (legacy) systems and temporary (overlay) systems are protected. Checklists are created to specifically address cyber security concerns.
- 4) Establishing the security operation center (SOC)

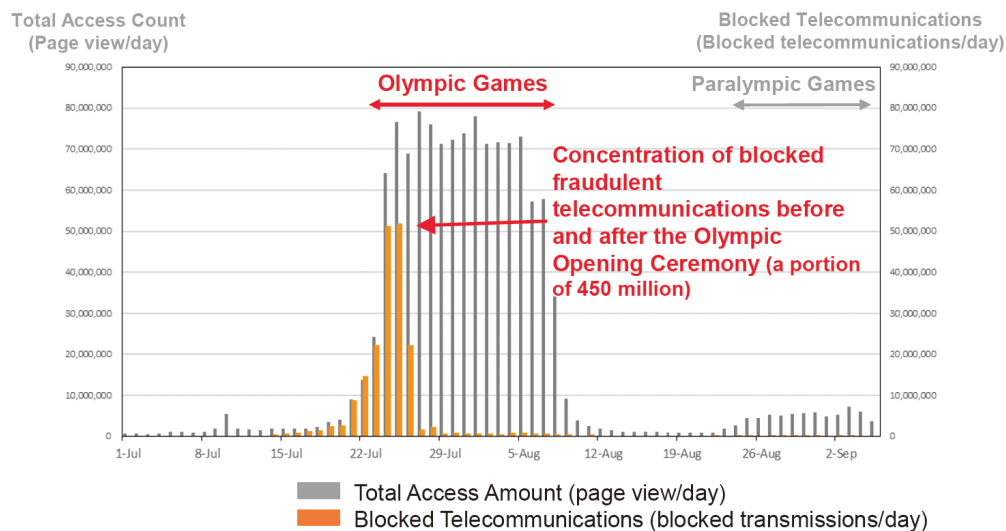


**Figure 2:** Authentication errors observed in back-office network environments  
Source: The Tokyo Organizing Committee of the Olympic and Paralympic Games (2022, p. 267)

### B. During the Games

The Security Operation Center (SOC) established within the Technology Operation Center (TOC) is used for monitoring networks and various information systems. It also operated a system of coordination through real-time chains of communication between key broadcasting stakeholders. The SOC also worked to fine-tune security solutions and improve technician proficiency through four field training exercises, two large-scale comprehensive technology training exercises, and three disaster recovery training exercises (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).

The issues observed during the Tokyo 2020 Games includes many cases of authentication errors in back-office environments reported to be password brute force attacks using IP addresses from participating countries as shown in Figure 2. There are also many security incidents on networks including sport networks, back-office networks, and stakeholder networks, as well as on the official website and mobile apps. A total of 450 million security incidents were blocked (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).



**Figure 3:** Blocked telecommunication in the server environment of the official website/mobile applications

Source: The Tokyo Organizing Committee of the Olympic and Paralympic Games (2022, p. 267)

## VI. CONCLUSION: THE SUCCESS FACTORS

The official report of Tokyo 2020 summarizes a few success factors that make cyber security measures a success, i.e., there is no cyber-attack incident significantly impacting the event. We mention those factors here in terms of action taken, rather than the personnels involved, as follows (The Tokyo Organizing Committee of the Olympic and Paralympic Games, 2022).

- 1) Deployment of cyber security experts as the Internal Staff of the Organizing Committee: These experts are involved in implementation of information security management systems from the start, e.g., establishing necessary regulations and procurement rules.
- 2) Improvement of the architectural design of the information systems and telecommunication networks
- 3) Proactive security measures
- 4) Field training exercises and security audits
- 5) Cooperation with the government and other relevant authorities

## REFERENCES

- The Tokyo Organising Committee of the Olympic and Paralympic Games. (2022). *Tokyo 2020 official report: Volume 1*. Olympic World Library. <https://library.olympics.com/Default/doc/SYRACUSE/2954165/tokyo-2020-official-report-the-tokyo-organising-committee-of-the-olympicand-paralympic-games>.
- Information-Technology Promotion Agency, Japan. (2019). *Security Risk Assessment Guide for Industrial Control Systems*. <https://www.ipa.go.jp/icscoe/j5u9nn000000a3y4-att/j5u9nn000000cmcm.pdf>.

**The content, as well as the use of language in the article, is the responsibility of the author.**

