SQUIRE PATTON BOGGS

Strategies for Maintaining Information Security and Protecting Trade Secrets in Connection with Telework

Asia Pacific – Japan – June 15, 2020

Introduction

With Japan's novel coronavirus (COVID-19) emergency declaration lifted, many companies are hoping to have their employees return to working at the office. A number of companies are considering keeping in place the telework arrangements adopted in response to this crisis in order to realize benefits of streamlined work flow and improved employee lifestyle, while also maintaining measures to prevent COVID-19 infections.

Below is a summary of recommendations regarding telework that companies should keep in mind as they form their strategies for telework information security and protection of trade secrets (under the Unfair Competition Prevention Act). We standby ready to assist your organization to identify and implement telework policies and procedures to address these issues.

Overview of Telework Security

According to the Telework Security Guidelines issued by the Ministry of Internal Affairs and Communications, "telework" refers to a variety of work patterns that make effective use of time and space through the use of information and communication technology (ICT). This includes work from home, and also using mobile terminals and working in satellite offices.[1]

In office settings, it is customary for companies to implement measures to protect against computer viruses and malware, and to put in place information system administrators and administrative policies for managing paper documents and other tangible media, based on company rules. Similarly, for telework, it is necessary for companies to be aware of information security risks and to implement and maintain systems that can adequately address such risks.

In particular, companies should consider strategies such as the following.

1. Measures to Be Taken by Employers

- Formulation and regular review of security policies.
- Clarification of telework policies for handling various types of information, based on importance.
- Company-wide telework security education and awareness.

2. Measures to Be Taken by Information System Administrators

- Introduction of specific technical measures based on security policies, and adequate supervision of implementation of such measures.
- Setting access controls, encryption, printability, based on the sensitivity of information.
- Management of company devices and their users.
- Management of anti-virus software, updates, etc. on company devices.
- Confirming the status of anti-virus and other software on personal devices used for telework.
- Measures regarding prevention of information leakage through wireless local area networks, such as Wi-Fi.
- Setting and confirmation of access privileges for in-house systems.
- Separation of important electronic data from internal systems in the event of ransomware infection.
- Establishment and clarification of other rules relating to cloud storage, data sharing, social networking, etc.

3. Measures to Be Taken by Teleworking Employees

- Thorough compliance with company rules, including the information security policies and sensitivity-based information handling policies.
- Management of user devices and storage media.
- Appropriate management of authentication information, including passwords, used to access internal systems.
- Appropriate understanding of the various risks of using wireless local area networks, such as Wi-Fi.

For details, please refer to "Points of Security Measures in Telework Security Guidelines (4th Edition)" (Ministry of Internal Affairs and Communications).[2]

1 Ministry of Internal Affairs and Communications "Telework Security Guidelines (4th Edition)" (https://www.soumu.go.jp/main_content/000545372.pdf), page 4 (Japanese only)

2 https://www.soumu.go.jp/main_content/000532482.pdf (Japanese only)

Protection of Trade Secrets under the Unfair Competition Prevention Act

Each company should review its information handling rules in connection with telework arrangements to confirm that it requires: permission for employees when they take documents and recorded media containing confidential information outside of the company; labeling of confidential information with "confidential" or "in-house only"; and setting IDs and passwords.[3]

The Unfair Competition Prevention Act (hereinafter referred to as the "Law") categorizes and prohibits acts that impair fair competition between businesses, including the unauthorized acquisition, use, and disclosure of trade secrets.

Article 2, paragraph 6 of the Law defines trade secrets as the following:[4]

1. "controlled as a secret" (hereinafter referred to as the "Confidentiality Control Requirement")
2. "production methods, sales methods or any other technical or operational information useful for business activities"
3. "things that are not publicly known."

Trade secrets are protected under civil and criminal law, including the availability to seek an injunction to stop unauthorized use or disclosure.

Of the above three requirements, the most important issue in relation to telework security is the Confidentiality Control Requirement. The purposes of the Confidentiality Control Requirement are "preventing individuals who have come into contact with the trade secret from being wrongly accused, ensuring employees' predictability, and preserving economic stability, by clarifying the information controlled as a secret by the company."[5] Therefore, in order for the Confidentiality Control Requirement to be satisfied, a company must clearly make its employees aware of its intention to keep the information confidential.[6]

Due to the inherent difficulty in preventing duplication and delivery to third parties of paper media, which are made more difficult in connection with telework, companies should consider promoting the use of paperless practices to address such risks.[7]

Regarding Cross-border Trade Secret Infringement Cases

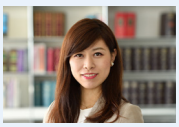
Nowadays, it is common for trade secrets to be managed by servers or branch offices located outside of Japan. In such cases, when filing actions seeking injunctions or other actions for damages, it important to keep in mind that governing law and jurisdiction can become key issues.

Authors

Mörk Murdock
Partner, Tokyo
E mork.murdock@squirepb.com

Brett Gilbert
Senior Associate, Tokyo
E brett.gilbert@squirepb.com

Yuichiro Yasutomo
Associate, Tokyo
E yuichiro.yasutomo@squirepb.com



Shoko Okubo
Associate, Tokyo
E shoko.okubo@squirepb.com

3 Ministry of Economy, Trade and Industry Intellectual Property Policy Office "Points of secret information management during telework (Q&A commentary)" (https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf), page 2 (Japanese only)
4 A full English definition of trade secret would be "2) technical or sales information useful for production methods, sales methods, and other business activities 3) that is not publicly known, 1) that is managed as a secret."
5 Ministry of Economy, Trade and Industry "Business Secret Management Guidelines" (https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf), page 5 (Japanese only)
6 "Guidelines for Management of Trade Secrets", page 6
7 Foreword "Points of secret information management during telework (Q&A commentary)", page 4