Security for the IoT Era

Rena Oi

Abstract

Internet of Things devices have enhanced the value of data collection by collecting more detailed and broader information. However, they have also increased the risk of data breaches and large-scale cyberattacks. While value associated with utilization is being realized, it is now necessary to change the way we treat and protect data.

Keywords: cyberattacks, stray IoT, personal data

1. Escalation of cyberattacks

The escalation of cyberattacks and the damage they cause know no boundaries. Today, the process that starts with these attacks and ends with the extortion of funds has been established as a business model. As criminal programs proliferate, more copycat offenders emerge, which requires the techniques and tools for defending systems against cyberattacks to be continuously strengthened. This vicious cycle is accelerating.

Data breaches are steadily increasing, and billions of individual user accounts are being leaked. This information includes account data of online services, email addresses, associated passwords, and sometimes secret questions and answers. This personal information is traded on the dark web, an Internet space accessible only by a special means. The damage is usually exposed two or three years after the fact. As a result, it is imperative to foster human resources that possess the skills to detect leak-seeking cyberattacks, deal with the ever-changing modus operandi, and continue to protect information. Because it is virtually impossible to completely prevent attacks, the promptness of detection and recovery is vital. Efforts are underway to use technology to disconnect the affected section from the network as soon as possible as well as to implement artificial intelligence (AI)-assisted automatic protection.

Ransomware damage also continues to spread. Ransomware, also called ransom-demanding malware, encrypts infected data in a computer to make it unusable and demands a ransom for decryption. It became common around 2013 and remains an effective means of attack. Cyberattackers purchase low-cost ransomware tools on the market, distribute them, and wait to obtain ransoms, repeating this *business*. It is difficult to control this crime except by improving the computer literacy of the public. The damage is expected to continue.

2. Increase in cyberthreats due to Internet of Things

In 2016, the Internet of Things (IoT) was much discussed as an element that makes cyberattacks more serious. IoT devices, which include surveillance cameras, network devices, video recorders, and electric meters, are powerless, stand-alone computers that are always connected to the Internet and therefore exposed to the risk of information breaches and takeovers. These devices tend to run for a long time with a widely known initial password. Cyberattackers look for these *stray* IoT devices on a daily basis, and upon finding one, exploit its vulnerability.

By the end of 2016, the number of stray IoTs in the world rose to hundreds of thousands. Cyberattackers organized them as a botnet, a group of bots working for cyberattackers, and used them in the largest DDoS (distributed denial of service) attacks in history. Huge numbers of packets were sent to specific websites in classic attacks intended to disable access to those sites and resulting in enormous damage where multiple online services were suspended. A variety of similar attacks ensued. As with other cybercrimes, the IoT botnet is probably already established as a

business and its use is on the rise.

The search for specific security measures to respond to IoT security threats is gathering speed. With the computer security knowledge already established for IoT, it will probably be possible to eliminate the vulnerability of IoT. However, the difficulty of dealing with the costs for such measures, combined with the lack of incentives for action, may present obstacles. The imposition of liability to IoT device manufacturers, and authenticating and labeling these devices to prevent the emergence of stray IoTs, is currently under discussion. In Japan, an IoT security guideline was published, and detailed measures are under review.

3. Rapid rise in quality and quantity of personal data due to IoT

The value of secured data, especially personal data that should be protected and kept intact, will be changing. Traditional personal data include data that users registered themselves and data obtained when users' behaviors on the Internet were recorded. In the future, personal data will include behavioral and biological information of individuals captured from the physical world by IoT devices. As the amount of information continues to increase, it is assumed that a dramatic improvement in analytical ability will determine more detailed attributes of individuals. Even today, personal data on the Internet such as clicking actions on a browser, postings on a social networking service, and products selected, are thoroughly collected. For example, the reason for the extremely accurate recommendations made for on-demand videos is the presence of a system that records and analyzes the user's viewing history, time, search history, pausing, fast-forwarding, and even scrolling actions when selecting a video.

In the future, more information will be added to the data on individual behaviors that are observed by IoTs in the physical world. For example, wearable devices will obtain heart rate, blood pressure, running distance, speed, and position information. Navigation systems will collect the driving area, speed, and vehicle condition. Security cameras will catch images of faces, which are automatically identified and analyzed. A system will record the rail stations where people get on and off a train, the duration of the ride, and the time it takes to change trains. As long as the user agrees, all this information will be attached to personal data, making personalization more robust.

However, additional data created through estimation by AI based on huge amounts of combined personal information could bring negative results and disadvantages. For example, if estimated data on personal details such as health condition, healthy life expectancy, and the possibility of illness in the future are created, all kinds of personalization could happen, from the presentation of certain drug advertisements to the control of advertisements soliciting for insurance policies or loans. This negative type of estimated data is produced before the individual realizes it, so it cannot be changed even if the information is wrong. This will cause disagreements if individuals have no way to alter the wrong information.

4. Status of security and information

As we face problems about the treatment of widely collected personal and estimated data, we can no longer avoid the key question of who owns the data. Currently, information about private citizens belongs to companies that collect and analyze that information. As a result, many countries require the agreement of private parties on the collection of their information and/or have legislation that governs the use of such information by

third parties.

Trials are underway to build a data trading market that promotes the fee-based distribution of valuable information. Meanwhile, there are services that use anonymization technology to process the collected personal data into forms that do not enable individuals to be identified so that the data can be used in marketing without approval. The GDPR (EU General Data Protection Regulation), which aims to protect particularly critical personal data, is expected to go into effect in May 2018. The time has come for companies to build specific plans to adhere to this framework.

Large companies, who hold a dominant position on the Internet, particularly in the area of information distribution by smartphones, have already established a system where individuals who provide personal data can control their own information. In addition, in an attempt to acquire the information on IoT devices, large companies are expanding their service menus. They are also providing a console where users themselves can configure the opt-ins broken down by types of information, the viewing of collected information, and the customization of advertisements. In other words, large companies are building a system to store information, while meeting the changes in the status of information.

It is possible to create an organization to counteract this oligopoly and to actively distribute information. However, it will be a long-term challenge to establish a business model where the new organization will acquire the trust needed to take care of large amounts of information and protect it. One of the first ideas may be data exchange markets for open data collected by IoT devices, which a public organization owns. Accumulating such experiences will lead to the next stage of dealing with valuable information, such as personal information, which generates more profit.

Rena Oi

Assistant Manager, Strategy Development Section, Research and Development Headquarters, NTT DATA Corporation.

She received a B.A. in sociology from Keio University, Tokyo, in 2008. After joining NTT DATA in 2008, she worked on the development of a customer contact system. She joined the NTT DATA Technology Foresight team in 2017.