Evolving Web Revolution & Security Measures

By MISUMI Ikuo

Recent Incidents

With mobile personal computers (PCs) and broadband communication networks used extensively in recent years, it has become possible for any user to acquire or exchange information globally through the Internet without any restraints on time or location. Individuals, corporations and other users can enjoy the benefits of such means as e-mail, electronic commerce and self-expressive weblogs. This is also true for people trying to abuse networks to acquire information.

On Sept. 25, Prime Minister Fukuda Yasuo's office posted an alert on its website against fake e-mails. According to media reports, the sender of a fake e-mail pretended that the prime minister sent it out to specific recipients. The e-mail reportedly discusses Japan's foreign policy matters in Asia. A file attached to the e-mail carried the title of mofa (short for the Ministry of Foreign Affairs). If the recipient clicks and opens the file, a text portion written in Japanese will be displayed. The recipient reads the text and closes it. Nothing happens at least on the surface.

If the file is opened, however, a malicious code planted in it begins functioning. The code leads the computer to connect up to a malicious website, against the will of its user. Then, the computer begins to download an offensive software program from the site. As a result, the computer takes on the offensive program, but the user is unaware. Usually, an anti-virus program that is frequently updated can detect an ill-intentioned code in its initial attack. But in many cases it cannot detect an offensive program once planted into the user's PC. Such an offensive program goes on functioning maliciously. For example, it steals information from the user's PC. Such an offense aimed at specific users, which has emerged in recent days, is called a "targeted attack."

Many computer users have come to take technological security measures such as using anti-virus software and firewall systems. But offenders try to exploit PC users' psychological weak points and invade their computers with such means as malware programs. Malicious assailants seek economic benefits by secretly stealing information. So they produce malware that cannot be detected easily by PC users. This will not lead to any major outbreak of network disturbance as seen in attacks by traditional computer viruses.

Measures against Usual Threats

The following two points must be taken into account to take effective information security measures. Those are defense against malicious attacks from outside and control against intentional or unintentional leaks of information from inside. At the same time, the size of an impact on corporations or individuals in the event of these incidents must be considered.

Among usual threats are malfunctioning of PCs caused by computer viruses, massive e-mail deliveries to other PCs, and unintentional deletion or disclosure of document files. Usually, a computer is infected with viruses that cause such phenomena when its user opens a file attached to an e-mail, browses Web pages or uses a file-swapping program. These problems will hit the computer immediately if there are weak points, or vulnerability, in the computer in terms of software security.

Nowadays, we can say the use of anti-virus software is spreading among PC users. Many users apparently buy anti-virus programs as well at the time of PC purchases. Users need to renew contracts with anti-virus software developers upon the expiration of a contract term to keep up with up-to-date information.

Meanwhile, computers with new operating systems automatically take on vulnerability-correcting programs to keep them in an up-to-date condition. The problem is that some users continue to use computers with old-fashioned operating systems whose maintenance service was terminated by software developers. This means that software vulnerability cannot be corrected. As a result, those computers face the above-mentioned threats.

Moreover, the use of a router with a built-in modem and personal firewall software is essential when connecting a computer to broadband networks. Notably, the latter is effective when mobile PC users connect to the Internet through wireless means or when spyware programs try maliciously to send information within a PC to the outside.

But more careful measures are necessary to cope with attempts that exploit PC users' psychological weak points, such as fraudulent "phishing" tactics, and new types of threats, as mentioned in the introductory part of this article, from malware programs that sneak through the firewall, sometimes fooling the user, and then into the computer system.

Measures against New Threats

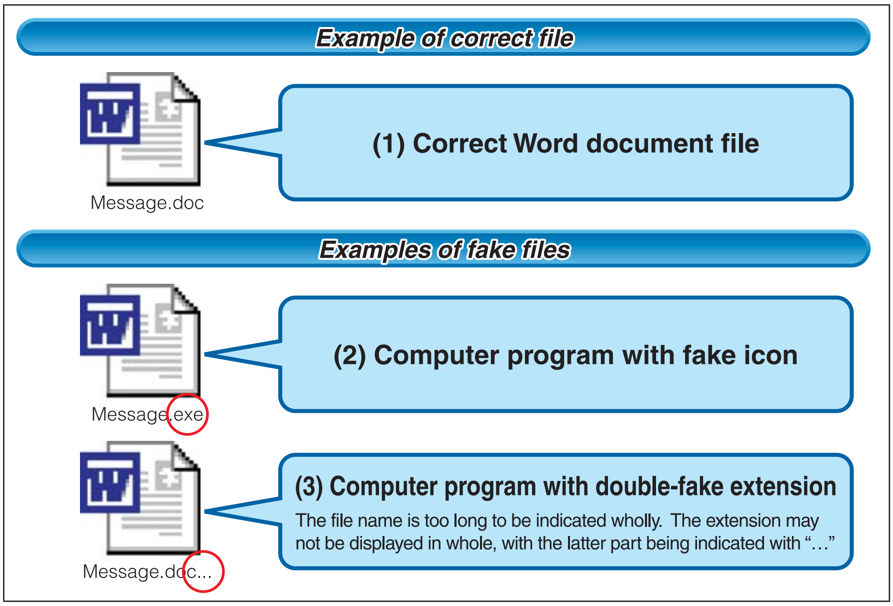
"Phishing" is a malicious activity. In a typical phishing attack, users are given a fake e-mail from a financial institution, tricked into a malicious website, and are swindled of their account numbers and security codes. This is a sophisticated form of fraud. The term phishing is a variant of fishing. A certain number of phishing cases have been reported in Japan recently. If a corporation's website contains vulnerability, it may be abused for phishing. Businesses therefore need to tighten security checks on their sites to keep them free of vulnerability. On the part of users, they should never input their personal information on a site to which they are guided after receiving a suspicious e-mail.

Against targeted attacks, users need to be fully careful and should not open a file attached to an e-mail unless they are sure it is safe to do so. Once users allow a malware program to begin functioning, a specialized and large-scale operation may be necessary to remove it. It can inflict massive damage on business activities in the case of a corporation. To prevent such a situation from hitting companies, they need, first of all, to promote anti-cyberattack education for their employees. In other words, employees need to check if e-mails, even though they are sent from their acquaintances, contain a malware program before opening them. A common method is to check if an attached file is a computer program disguised as a document file or spreadsheet. Even though the icon indicates that an attached file is a document or spreadsheet, it can be a fake in reality, as shown in *Chart 1*. Users need to always check if the extension following the file name and a dot indicate a computer program such as "exe." Some malware programs cover up the real nature of a file attached by inserting such extensions as ".doc" and ".txt" and placing ".exe" to the last part of the extension, making it likely for users to overlook it. Users are advised to know the existence of such an imitative deception and always pay careful attention.

Need to Tighten Security Governance

Information on organizations or individuals may sometimes be rewritten, leaked or lost not only by attacks from outside but by itself or insiders. Restaurant owners or chefs are thought to be paying close attention to keep secret the recipes of their specialties.

***Chart 1* Examples of fake files & how to distinguish between fake and genuine ones**


Example of correct file
Message.doc
(1) Correct Word document file
Examples of fake files
Message.exe
(2) Computer program with fake icon
Message.doc...
(3) Computer program with double-fake extension
The file name is too long to be indicated wholly. The extension may not be displayed in whole, with the latter part being indicated with "…"

Source : *Information-Technology Promotion Agency*

When a restaurant opens a branch, it must be paying even more careful attention to keep the recipes confidential.

It is also important for organizations to keep secret their business and technological information, which is the source of their profits. The first step for the heads of organizations and owners of information is to recognize the value of information. Next, they must consider impacts on their organizations in the event of damage done to their confidentiality, integrity and availability due to leakage or loss of the information. They must also consider probabilities of such a situation. They are also required to assess risks and then decide whether to avoid or accept these risks. Such work should be done by the heads of organizations.

It is also necessary to establish a system to make users properly handle information under policies and rules set by the heads of organizations. Third parties, not the owners or users, need to keep a log of information handling.

It is effectively impossible for the head of an organization to fully control in-house handling of information if the size of the organization is large. It is therefore important to establish an internal control system from the viewpoint of information security. The Ministry of Economy, Trade and Industry (METI) has since 2005 continued to publicize the need for strengthening information security governance in society. For example, METI has developed a benchmark tool that enables an organization to compare the level of its information security measures with those of others. The tool is open to the public at the Information-Technology Promotion Agency's website (http://www.ipa.go.jp/security/english/benchmark_system.html)*(Chart 2)*.

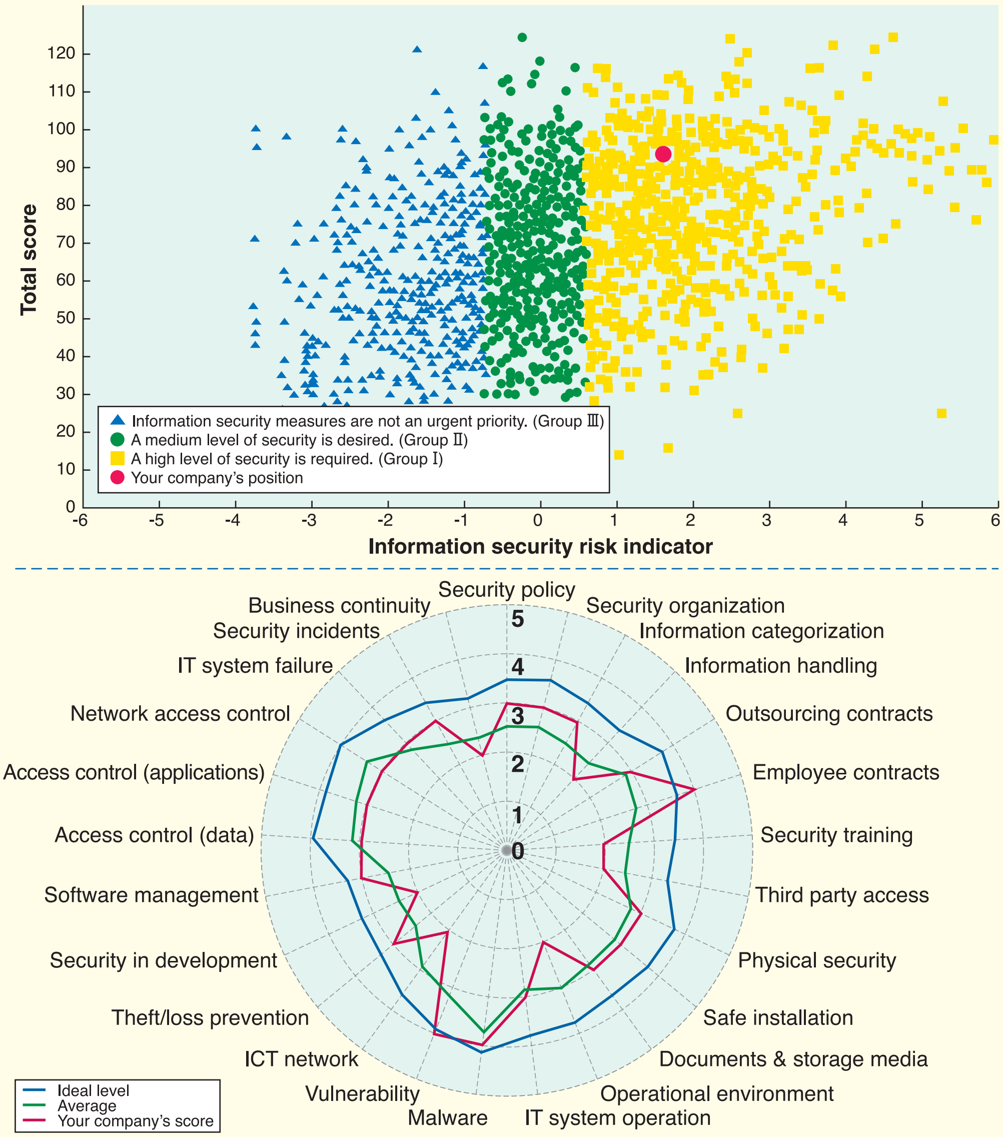
METI plans to conduct studies on laws and ordinances that should be followed when organizations take information security measures and introduce steps to improve their business continuity with the use of information technology (IT). METI plans to work out standards and manuals that will be needed in those cases. As these are considered useful documents for international organizations, METI is scheduled to strengthen efforts to introduce them to Asian countries.

Chart 2 Information Security Measures Benchmark

▶**25 items related to security measures**
(For important information assets such as information and information systems, they are categorized in accordance with their levels of importance, and are given scores based on such standards as whether they are properly managed according to the levels.)

▶**15 items regarding corporate profiles**
(Of business processes relating to main business, the level of dependence on the Internet and other aspects are given ratings).

▶**The above total of 40 items is checked.**



Source : *IPA (Information-technology Promotion Agency, Japan)*

Conclusion

This article looked into topics about recent information security situations. It took up simple examples of measures that are recommended for immediate implementation. However, risk levels differ by the size of a firm, its business field and the nature of information in the event of an information security incident. Needless to say, proper measures must be taken by organizations and individuals on a case-by-case basis.

At times, information security measures are regarded as a cost-raising factor. But information and communications technology has become essential in today's social and economic activities. Information produces fresh value added. Therefore, it should be recognized anew that important information should be properly managed, as in the case of cash being protected in a safe. JS

Misumi Ikuo is Director, Office of IT Security Policy, Commerce and Information Policy Bureau, METI. He has a Ph.D. from the University of Tokyo and a Claremont Graduate School MA in Management.