Preface

This guide is intended to serve organizations’ owners, management-level officials and employees who are considering implementing information security controls from now.

For those who claim to be familiar with what is described in this guidance, it can be used as a reference material for reviewing their information security controls and for security education for their contractors or subsidiary organizations.

For questions or consultation about this guidance, please e-mail to: isec-info@ipa.go.jp

WHAT ARE INFORMATION SECURITY CONTROLS?

Organizations are surrounded by security threats. So they need to:

⚠️ reduce (or prevent) the risk of problems arising from those threats; and

⚠️ protect their information assets (e.g., information, devices/networks that manage such information), including:

✔️ protecting personally identifiable information and client/business information against those threats; and

✔️ protecting the organization’s facilities against those threats.

In other words …

Protect your client

⚠️ That is information security (control)

Information Assets
Information leakage is one of the most serious information security incidents, and other security incidents, such as the loss of availability of information systems or data destruction due to a computer virus infection may cause the loss of credibility from clients. Information security issues may lead to management risks and therefore, every organization should address them.

Implementing information security controls begins with risk assessment and based on the assessment results, organizations should develop security control criteria and implementation procedures. However, some organizations do not even know what to do. So, IPA developed this "Minimum Information Security Controls Guide for Organizations" to help organizations enhance their information security. Please feel free to make use of it.

**Information Security Self-Assessment for SMEs – It takes only 5 min.**

We developed 25 information security controls as minimum-required controls for organizations. By answering those questions and reading the associated explanations, organizations can achieve the following:

- Identifying what problems lie where;
- Selecting appropriate controls to address the identified problems; and
- Enhancing information security by implementing those controls.

### Classification of Questions

- **About Storage**
- **When Taking out Info.**
- **When Disposing of**
- **In the Office**
- **About PCs**
- **About Passwords**
- **About Virus Countermeasures**
- **About E-mails**
- **About Data Backup**
- **About Employees**
- **About Business Partners**
- **About Incident Responses**
- **About Rules**
# Contents / Checklist

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>About Storage</td>
<td>Does your organization establish rules to keep important information from being accessed by third parties? For example, are you requested to store documents containing such information in a locked cabinet without leaving them unattended on your desk?</td>
<td>7</td>
</tr>
<tr>
<td>No. 2</td>
<td>When Taking out Information</td>
<td>Does your organization establish rules to protect information taken out of the office against theft or loss? For example, are you requested to apply password-lock on your portable PC?</td>
<td>10</td>
</tr>
<tr>
<td>No. 3</td>
<td>When Disposing of (Papers etc)</td>
<td>Does your organization establish rules to securely dispose of media containing important information (such as paper, CD, etc.)? For example, are you requested to shred them so that the important information contained will not be disclosed?</td>
<td>13</td>
</tr>
<tr>
<td>No. 4</td>
<td>When Disposing of (Electronic Devices, Electronic Media etc)</td>
<td>Does your organization establish rules to securely dispose of PCs or storage media containing important information? For example, are you requested to erase the electronic data contained by using dedicated software or by asking a specialist for the erasure?</td>
<td>15</td>
</tr>
<tr>
<td>No. 5</td>
<td>In the Office</td>
<td>Does your organization establish rules to prevent unauthorized people from entering its office? For example, when you see a stranger in your office, are you requested to speak to him?</td>
<td>21</td>
</tr>
<tr>
<td>No. 6</td>
<td>In the Office</td>
<td>Does your organization establish rules to prevent theft? For example, when you leave your office, are you requested to store your portable PC and other equipment in a lockable drawer?</td>
<td>23</td>
</tr>
<tr>
<td>No. 7</td>
<td>In the Office</td>
<td>Does your organization establish process for office closing? For example, requesting the last leaver to lock the office and record his/her name and leaving date and time?</td>
<td>25</td>
</tr>
<tr>
<td>No. 8</td>
<td>About PCs</td>
<td>Does your organization establish rules to keep employees' software secure? For example, having employees apply Windows Update?</td>
<td>28</td>
</tr>
<tr>
<td>No.</td>
<td>About</td>
<td>Question</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>No. 9</td>
<td>About PCs</td>
<td>Does your organization prohibit the use of any software carrying a high risk of file leakage? For example, forbidding the installation of file-sharing software?</td>
<td>32</td>
</tr>
<tr>
<td>No. 10</td>
<td>About PCs</td>
<td>Does your organization establish rules to limit the use of privately-owned PCs for office works? For example, having an approval system in place for the use of such PCs at its office?</td>
<td>35</td>
</tr>
<tr>
<td>No. 11</td>
<td>About PCs</td>
<td>Does your organization establish rules to prevent unauthorized access to PCs? For example, are you requested to turn off your PC when you leave your office?</td>
<td>38</td>
</tr>
<tr>
<td>No. 12</td>
<td>About Passwords</td>
<td>Does your organization establish rules to set a hard-to-guess password? For example, are you requested to avoid using your name?</td>
<td>43</td>
</tr>
<tr>
<td>No. 13</td>
<td>About Passwords</td>
<td>Does your organization establish rules not to disclose passwords? For example, prohibiting written passwords from being left in public spaces?</td>
<td>43</td>
</tr>
<tr>
<td>No. 14</td>
<td>About Passwords</td>
<td>Does your organization establish rules to make passwords difficult to crack? For example, requesting login passwords to be changed on a regular basis?</td>
<td>43</td>
</tr>
<tr>
<td>No. 15</td>
<td>About Virus Countermeasures</td>
<td>Does your organization establish rules to protect PCs from virus infection via suspicious Websites or e-mails? For example, are you requested to install antivirus software on your PC?</td>
<td>49</td>
</tr>
<tr>
<td>No. 16</td>
<td>About Virus Countermeasures</td>
<td>Does your organization establish rules to keep your antivirus software’s virus definition files up-to-date? For example, are you requested to apply the automatic update of virus definition files?</td>
<td>58</td>
</tr>
<tr>
<td>No. 17</td>
<td>About E-mails</td>
<td>Does your organization establish rules not to send e-mails to wrong recipients? For example, are you requested to visually confirm the destination address prior to sending an e-mail?</td>
<td>64</td>
</tr>
<tr>
<td>No.</td>
<td>About</td>
<td>Question</td>
<td>Page</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>18</td>
<td>E-mails</td>
<td>Does your organization establish rules not to disclose e-mail addresses to third parties? For example, are you requested to use the &quot;BCC&quot; feature when sending an e-mail to multiple recipients who do not know each other's e-mail address?</td>
<td>67</td>
</tr>
<tr>
<td>19</td>
<td>E-mails</td>
<td>Does your organization establish rules to protect confidential information when transferred by e-mails? For example, are you requested to store such information in an attachment file with password protection?</td>
<td>70</td>
</tr>
<tr>
<td>20</td>
<td>Data Backup</td>
<td>Does your organization establish data backup rules not to lose important information in case of a breakdown or mis-operation? For example, are you requested to make backup copies of such information periodically?</td>
<td>78</td>
</tr>
<tr>
<td>21</td>
<td>Employees</td>
<td>Does your organization have employees protect confidentiality? For example, notifying its employees when hiring them that every employee is obliged not to disclose the organization's information assets?</td>
<td>83</td>
</tr>
<tr>
<td>22</td>
<td>Employees</td>
<td>Does your organization make its employees aware of the importance of information security? For example, providing periodic information security training or education?</td>
<td>85</td>
</tr>
<tr>
<td>23</td>
<td>Business Partners</td>
<td>Does your organization require its business partner(s) to protect confidentiality? For example, including nondisclosure clauses into its contractual agreement?</td>
<td>89</td>
</tr>
<tr>
<td>24</td>
<td>Incident Response</td>
<td>Does your organization prepare for security incidents? For example, having a procedure manual for responding to information leakage/loss/theft incidents?</td>
<td>93</td>
</tr>
<tr>
<td>25</td>
<td>Rules</td>
<td>Does your organization clarify its information security controls? For example, making the information security controls described in No.1 to No.24 organization rules?</td>
<td>96</td>
</tr>
</tbody>
</table>

**Total Score:**

FYI, each item is evaluated from 0 to 4 as follows: Implemented (4 points), partly implemented (2 points), not implemented/Not sure (0 point)
No. 1 About Storage
Does your organization establish rules to keep important information from being accessed by third parties? For example, are you requested to store documents containing such information in a locked cabinet without leaving them unattended on your desk?

No. 2 When Taking out Information
Does your organization establish rules to protect information taken out of the office against theft or loss? For example, are you requested to apply password-lock on your portable PC?

No. 3 When Disposing of (Papers etc)
Does your organization establish rules to securely dispose of media containing important information (such as paper, CD, etc.)? For example, are you requested to shred them so that the important information contained will not be disclosed?

No. 4 When Disposing of (Electronic Devices, Electronic Media etc)
Does your organization establish rules to securely dispose of PCs or storage media containing important information? For example, are you requested to erase the electronic data contained by using dedicated software or by asking a specialist for the erasure?
Information leakage incidents are mainly caused by mismanagement or mis-operations (see Figure 1.) This mismanagement includes ignorance and/or neglect of the information security controls established by the organization to manage information. On the other hand, mis-operations include careless mistakes (e.g., wrong transmission of enclosed documents, facsimiles, or e-mails.) Information leakage from paper documents seems to be most cases (See Figure 2.) In the case of paper-document-caused incidents, even trivial mistakes may lead to information leakage, the amount of the information leaked might be small, compared to USB- or PC-caused incidents.

For example, aren't you leaving any documents containing important information (i.e., information that should be protected from leakage) unattended on your desk in the office? Such documents might also be stolen or peeped by others. This may happen when you leave your desk for a moment or when you come home. To protect important information, do not leave any documents unattended on your desk and keep them in a lockable cabinet, so that third parties cannot access them.
Documents left unattended on your desk might be stolen by others. Accordingly, documents containing important information should be managed and protected properly **without being left unattended**, so that unauthorized people cannot see or alter them.

**Question**

Does your organization establish rules to keep important information from being accessed by third parties? For example, are you requested to store documents containing such information in a locked cabinet without leaving them unattended on your desk?

*Yes*: Implemented (4 points)
*Yes, but partly*: Partly implemented (2 points)
*No*: Not implemented (0 point)
**FIGURE 2: BREAKDOWN OF MEDIA/ROUTE OF INFORMATION LEAKAGE**

- **paper documents**: 1,117 cases (72%)
- **USB stick or other transportable storage media**: 144 cases (9%)
- **E-mails**: 108 cases (7%)
- **Internet**: 70 cases (5%)
- **PCs’ main bodies**: 58 cases (4%)
- **Others**: 30 cases (2%)
- **Unknown**: 12 cases (1%)
- **Total number of incidents**: 1,539

Information leakage from paper documents has significantly increased (to 72.6 percent), compared to a year ago (56 percent).

[Text: Fiscal 2009 Information Security Incident Survey Report Ver. 1.0 (JNSA)]
Without managing the take-out of information from an office is one of the major causes of information leakage incidents. If such information was accidentally left/lost or stolen outside, that would lead to an information leakage incident.

When you take out important information for a fieldwork or other tasks that are performed outside your organization, make it unreadable by others so that the leakage of such information is prevented in the event of loss or theft.

For paper media (e.g., documents), you need to implement the following measures to protect against loss or theft: not taking them out from your bag when you are outside your organization (except when absolutely necessary); keeping them in a file-binder/clear-file folder, etc.; keeping your bag close to your body (i.e., not leaving it on a vacant seat or an overhead-rack in a train or a bus); locking your bag; and staying awake while holding your bag.

Don't forget to take this bag with you ...!?
For electronic storage media such as USB stick, you can apply data-encryption, password-protection and/or anti-lost controls (e.g., attaching a large tag or a bell (so you will notice when you accidentally drop it), or a strap dangling it from your neck.) Apart from the above controls, if such media is put in your bag, you need to exercise the same controls as those applied to paper documents. It would be safe not to bring them to an alcoholic party.

When you take out a portable PC (e.g., notebook, netbook, Tablet) or smartphone or other mobile devices that contain important information, you need to implement certain controls to prevent the leakage of such information. This may include: using a hard-to-guess password (e.g., setting a login password, applying BIOS password lock*1), encrypting the internal hard disk drive or the information stored, and so on.

*1) BIOS password lock
This is a feature for locking a PC with a preset password during its start-up process, and can be applied on a motherboard basis. Although it can prevent your PC from being used by others, it does not lock its internal hard disk drive. So if the internal hard disk drive in your PC was taken out directly by a malicious entity, its contents could be retrieved. From the security aspect, it would be better to encrypt the entire hard disk drive.

As far as the taking out of information is concerned, you should first ask yourself "Is it OK if I take this information out of the office?" To prevent your organization's information from being taken out easily, the organization needs to implement strict controls over the taking out of information. They may
include: "those wanting to take out information must obtain permission from their superiors" or "keeping the record of information being taken out."

Another advantage for keeping such record is that: in case you lost the information you had taken out, the lost information could easily be identified and the incident handled in a timely manner. But the principal is: try not to cause such incidents.

Nowadays, many people use their mobile phone for business purposes, but they also contain important information (i.e., information that should be protected from leakage), don't they? So, we recommend that you apply security controls that come with your mobile phone (e.g., PIN lock) or that are provided by communication service providers (e.g., remote lock service) [NB: Remote lock service enables mobile phone users to remotely lock their phone in the event of loss or theft.]

Taking important information out of your organization might lead to an accidental theft or loss of such information. By taking proactive controls (e.g., password-protecting your mobile phone/PC or data files), you can prevent others from viewing the information stored in the event of loss or theft.

**Question**

Does your organization establish rules to protect information taken out of the office against theft or loss? For example, are you requested to apply password-lock on your portable PC?

*Yes:* Implemented (4 points)
*Yes, but partly:* Partly implemented (2 points)
*No:* Not implemented (0 point)
Shred important documents!!
When dissolving or incinerating them, make a written contract with a waste disposer!!
Manage the documents to be disposed of until they go out of your hand, and never leave them unattended!! If possible, keep them in a lockable cabinet …
General garbage buckets are dangerous (We don't know what may happen to those disposed!!)
Documents/data being taken out are at the highest risk!! Do not dispose of them anywhere easily.
Nowadays, media shredders that are capable of shredding CDs, DVDs, floppy disks, magneto optical discs, and even SD cards and USB sticks are showing up in the market.

(A Small Question)
"SD" in "SD card" is said to stand for "Secure Digital", but in what sense, is it secure? When I thought about it, I recalled that a regular-sized SD card has a switch to prevent an accidental erasure (i.e., overwriting.) So, is it secure in this sense? I know this feature is useful as it can prevent virus entry, but still …

Question
Does your organization establish rules to securely dispose of media containing important information (such as paper, CD, etc.)? For example, are you requested to shred them so that the important information contained will not be disclosed?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)

(A Small Question)
"SD" in "SD card" is said to stand for "Secure Digital", but in what sense, is it secure? When I thought about it, I recalled that a regular-sized SD card has a switch to prevent an accidental erasure (i.e., overwriting.) So, is it secure in this sense? I know this feature is useful as it can prevent virus entry, but still …
When you dispose of PCs, external hard disk drives, or external storage media (e.g., CDs, DVDs, floppy disks, magnet-optical disks, SD cards, USB sticks, magnetic tapes) that you have been using for your business, you need to properly erase the data (information) stored.

INERASABLE DATA?

Generally, when deleting files from these electronic devices, people would use the delete-file function. For example, when deleting a no-longer-required file on your PC's hard disk drive, you must have executed the delete-file function provided by the OS running on your PC.

However, this function does not delete the file itself but to remove its location information, physically leaving the file contents on that PC (although the file itself is not accessible) (NB: We are not talking about a garbage box here). This specification is intended to prolong devices' life or achieve superficial efficiency (including processing speed) (NB: This is not particularly-problematical in a normal usage environment.)

Superficially-deleted files like these can be restored to their original forms by using dedicated file-recovery software (unless the locations formerly occupied by those files are re-occupied by other files, in other words, unless overwriting is done.) In short, seemingly-nonexistent files
can be brought back to life by using file-recovery software (NB: It requires specialized operations in general.)

As a result, from a disposed PC's hard disk drive, floppy disks, magnet-optical disks, or flash memories (nonvolatile semiconductor memories) etc., the files (data) which are thought to have been deleted might be revived and leaked.

In particular, flash memories as typified by USB sticks or memory cards, which are inexpensive for their capacities and therefore used by many people, might hold data if used or operated without careful consideration.

ALTHOUGH THIS IS LIKE THE ICING ON THE CAKE …

[Risks Associated with Flash Memories]
Flash memories have excellent mobility and storage capacity, but when lent or borrowed among people, they pose a major risk.

There must be an occasion where USB sticks are lent or borrowed among friends/acquaintances, or even work colleagues or business partners, but this is a risky behavior. If a USB stick is rent to a person with malicious intent, even if its files (data) is deleted in advance with the delete-file function, they might be restored one way or another (NB: This is a problem that cannot be solved with general formatting (as with the delete-file function mentioned earlier) and it becomes more serious for flash memories that have a life issue described later.)

For example, if you lend your digital camera’s memory card to someone … What if a private photo that was taken in the past and deleted once is revived by the borrower and posted on the Internet without your permission? Images of showbiz celebrity are thought to be leaked in this way. This may develop into a troublesome problem in the future.

Furthermore, if a USB stick that was used once for data exchange with a client is used again with another client, the data exchanged with the former might be leaked to the latter if not deleted properly.
There are two ways to avoid this problem: one is, not to lend/borrow USB sticks; and the other is, to use a USB stick that is capable of automatic data encryption (hereafter referred to as encryption-enabled USB stick.) In the case of encrypted files (data), by changing their encryption keys, you can make them un-restorable even with file-recovery software (To put it the other way around, no one else can restore them even if they want to.) In that sense, if you are going to use a USB stick for business purpose, it is recommended to choose an encryption-enabled one. Note, however, that it requires proper controls and operations.

A LIFE ISSUE ASSOCIATED WITH FLASH MEMORIES
A flash memory (also known as nonvolatile semiconductor memory) contains countless switches. Information is recorded when their on-off state changes, but each switch has life-span in terms of how many times it can be opened/closed. For this reason, flash memories are designed to record data with the least number of opening/closing of those switches. And because they do not use the same switch in a row, the probability that an existing data in a location is overwritten with another data is low. But this means, it is more susceptible to file-restoration.

LET'S GET BACK TO THE SUBJECT
For information stored on PCs or storage media (e.g., CDs, USB sticks), even if you perform "file-deletion", it can still be retrieved by using file-recovery software. When you dispose of PCs/storage media containing important information, you need to erase such information by using dedicated erasure software, or to physically destroy them.

DISPOSAL PRECAUTION (2)

⚠️ Floppy disks should be broken down and their content cut with scissors!!
⚠️ CDs/DVDs should be physically destroyed!!
⚠️ For flash memories such USB sticks and PCs’ hard disk drives, it's not enough to delete the stored files!! Use data erasure software for the wipe-out or physically break and dump them!! You may choose to contract a specialist!!
⚠️ When you dispose of fax/copy machines, contract a specialist!!
⚠️ Be cautious when you dispose of digital cameras and mobile phones as well!!
Nowadays, floppy disks are rarely used, but you may still have them. In order to securely dispose of floppy disks without leaving room for information leakage, you need to make them unreadable. It is best to open their shutter and scratch the recording site, or to rip out their outer package and cut the recording site with scissors.

In the case of CDs and DVDs, a basic way is to break them up, but you may also shred them with a media shredder. Another, handier way is to scratch their surface so that they can no longer be read, but you need to be careful not to scratch the wrong side. Because people often misunderstand and may scratch the glossy surface, which is totally wrong. The glossy surface is thickly coated, so by polishing those scratches with a dedicated device, anyone can make it readable again. For this reason, you need to scratch the side on which a label is written (generally called "white label"). The underside of this label is the recording site, so by scratching it until you see its basic material (or until the other side is seen through), you can make it unreadable.

In the case of flash memories (e.g., USB sticks) or PCs' hard disk drives, even if you apply the delete-file function, their contents are not completely erased; so you need to use data erasure software to completely erase their contents or to break and dump them (e.g., boring that hard disk drive with a drill and dumping it.) In any of these cases, you may contract a specialist. However, care should be taken when selecting a specialist. If the specialist (or its erasure technique) is not satisfactory, the following incidents may occur:

A News Article Released in June 2009

- A U.S. Company's Classified Information Found in an Used Hard Disk Drive on Sale in Ghana
  - A journalist team looking into the world e-waste situation discovered an information security incident from a heap of garbage;
  - A U.S. company's classified documents (national defense information) were found;
  - An improper data erasure on the part of the waste disposer (contactor), followed by the theft and illicit sales of the PC components.

Meanwhile in JAPAN: A News Article Released in January 2010

- A Net-Auctioned PC Contained a Company's Client Information; A Man Arrested for Attempted Extortion
  - A net-auctioned PC's HDD contained a company's client information.
  - The winner attempted to blackmail the company into buying it.
When you dispose of fax/copy machines, you need to exercise caution. Nowadays, these machines are equipped with a built-in memory in which data to be sent as a fax or to be copied is stored temporarily to improve performance. However, this memory's contents might also be leaked due to improper disposal. So when you dispose of these machines, contract a specialist to have their memory contents erased completely.

For digital cameras and mobile phones, the same caution should be exercised in disposing of them. If you have no confidence in erasing the memory contents of your fax/copy machine, contract a specialist and never put it up for an auction.

**Question**

Does your organization establish rules to securely dispose of PCs or storage media containing important information? For example, are you requested to erase the electronic data contained by using dedicated software or by asking a specialist for the erasure?

- **Yes:** Implemented (4 points)
- **Yes, but partly:** Partly implemented (2 points)
- **No:** Not implemented (0 point)
In the Office …

No.5 In the office
Does your organization establish rules to prevent unauthorized people from entering its office? For example, when you see a stranger in your office, are you requested to speak to him?

No.6 In the office
Does your organization establish rules to prevent theft? For example, when you leave your office, are you requested to store your portable PC and other equipment in a lockable drawer?

No.7 In the office
Does your organization establish process for office closing? For example, requesting the last leaver to lock the office and record his/her name and leaving date and time?
THIS IS ABOUT OFFICE SECURITY

Do you prefer an office where anyone can easily enter? If you do, is it worth taking the risk that important information might be stolen?

People working in an office have to realize that, letting a stranger get into their office poses a serious security risk. No matter how well the office is organized, as long as it holds important information that needs to be protected from peeping or theft, it should have security controls in place.

Identifying visitors to your office is also an important task for your business. By taking such controls as asking visitors to record a visitor's note; receiving their business cards; or speaking to them, etc., you can prevent wrongful acts that might be carried out by anyone of them.

You should also be careful not to leave a visitor alone in your office (whether you know the person or not), as it might lead to an information leakage or theft. In such a situation, ask the visitor to go out with you.
Remember that the same cautions should be exercised with the contracted cleanup/maintenance workers entering your office. It's risky to leave them alone in your office. It is good to have an employee in your office observe their work.

The following people may also enter your office without feeling of strangeness.

- Cleanup workers
- Maintenance workers (e.g., for air-conditioning)
- Workers of delivery companies (e.g., door-to-door delivery service staff, dispatch riders)
- Salespeople (e.g., insurance agents) who are allowed to enter
- Firefighting-equipment inspectors
- And so forth.

But even for the people you are familiar with or who do not bring a feeling of strangeness, you should not let down your guard.

**In order to protect your organization’s important information against theft, it is necessary to prevent unauthorized people from entering its office. In particular, access to servers/book rooms/cashboxes areas should be strictly controlled.**

**Question**

Does your organization establish rules to prevent unauthorized people from entering its office? For example, when you see a stranger in your office, are you requested to speak to him?

- **Yes**: Implemented (4 points)
- **Yes, but partly**: Partly implemented (2 points)
- **No**: Not implemented (0 point)
"Locking an office after all the employees leave there": that goes without saying. On the other hand, it is also risky to leave easy-to-carry-away equipment or portable PCs on your desk in the office. If the office was accidentally left unlocked and burglarized, those left on your desk might well be carried away by the burglar.

In particular, portable PCs that focus on mobility (i.e., easy to carry) are susceptible to theft, and the important information stored on them is also at the risk of being leaked.

It's not limited to the night. We often hear about a portable PC stolen during the daytime while its user was away from the office for a while. It would be pain to store your portable PC in your desk or locker each time you leave your seat. That's why wire-lock is highly appreciated.

For a portable PC used in an office, you can wire-lock it with your desk, which is also one of anti-theft measures.

But, it may not work for during nighttime. A burglar who breaks into an office at night might easily break a system like wire-lock if not seen by others. By using so called "wire cutter", anyone can cut it off easily. So it is important to keep your portable PC and other equipment in a lockable desk-drawer/cabinet during nighttime, so they are not seen by others.
While portable PCs, mobile phones and USB memory sticks are easy to carry and convenient, they are at a high risk of being stolen. When you leave your office, store them in a lockable drawer.

Question

Does your organization establish rules to prevent theft? For example, when you leave your office, are you requested to store your portable PC and other equipment in a lockable drawer?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
"Locking an office after all the employees leave there": that goes without saying. But who should be responsible for locking the office? If it is not designated, it would be a problem. And if the office was accidentally left unlocked, it might allow a burglar to break in.

Is there any way to prevent employees from forgetting to lock their office?

One solution is: to keep the last leaver's record. By having the last leaver record the last leaver's note, the organization can remind its employees of the established office closing procedure and prevent them from forgetting to lock their office.

Then, what kind of information could be recorded in the last leaver's note? For example,

- **Date**
- **The last leaver’s name and leaving time**
- **Aren’t important documents left on desks?**
- **Are the PCs and their monitor turned off?**
- **Are the copy machines and shredders turned off?**
- **Are the lights turned off?**
- **Is the office locked?**
By keeping a record like this, the last leaver would be reminded of what they should do and act accordingly.

**Keeping the last leaver’s record** (his/her name and leaving date and time) would be helpful in raising employees’ awareness of locking their office when they leave last. Let’s implement lockup and recordkeeping.

**Questions**

*Does your organization establish process for office closing? For example, requesting the last leaver to lock the office and record his/her name and leaving date and time?*

- **Yes:** Implemented (4 points)
- **Yes, but partly:** Partly implemented (2 points)
- **No:** Not implemented (0 point)
No.8 About PCs
Does your organization establish rules to keep employees' software secure? For example, having employees apply Windows Update?

No.9 About PCs
Does your organization prohibit the use of any software carrying a high risk of file leakage? For example, forbidding the installation of file-sharing software?

No.10 About PCs
Does your organization establish rules to limit the use of privately-owned PCs for office works? For example, having an approval system in place for the use of such PCs at its office?

No.11 About PCs
Does your organization establish rules to prevent unauthorized access to PCs? For example, are you requested to turn off your PC when you leave your office?
Windows Update is a service provided by Microsoft. It regularly (once a month in general) provides Windows PC users with bug fixes and version upgrades for their operating systems (OS) and Microsoft-provided application software (Microsoft Office: Excel, Word, Internet Explorer, etc.) Security patches to solve security problems (i.e., program defect and problems in specifications) within the OS and Microsoft Office applications are provided via Windows updates. Since they are indispensable for the secure use of PCs, they should be applied promptly.

Other OS vendors than Microsoft also provide security patches on a regular basis or as-needed basis. These patches are also critical for PCs running a non-Windows OS, so users should apply them promptly.

In the field of information security, security problems presented here are called “security holes” or “vulnerabilities”. If such vulnerabilities are exploited, the PC might be taken over remotely by a malicious entity or it might be infected with a computer virus. Information on vulnerabilities is provided by OS/application vendors or distributors. IPA also provides vulnerability information through “JVN (Japan Vulnerability Notes: Vulnerability Information Portal Site)” (See <Reference Information>.)
These days, Microsoft and other OS/application vendors encourage users: to activate the automatic update of security patches (i.e., a program to eliminate OS/application vulnerabilities); or to use the one-touch (or one-click) update. By making these settings on your PC, you can use it more safely. So, it is recommended to check your OS/application’s settings as well as if they are kept up-to-date (JVN also provides a tool with which you can check if popular applications running on your PC are the latest versions (See <Reference Information>.)

🎉 JUST FOR THE STOCK OF YOUR KNOWLEDGE
(i): When is Windows update released?
Windows Update and Microsoft Update are released once a month on the second Tuesday in the U.S. time (NB: Release date in Japan may not be the second Wednesday depending on the month.) This may be a little information but it is good to remember that each localized version is released slightly after the release of the U.S. version.

(ii): Remote code execution?
In the case of Windows Update or Microsoft Update, you may see the expression "Remote Code Execution" in the vulnerability impact description. This means that a vulnerability in that PC might be exploited by a malicious program and disadvantages brought to its user. Because such malicious program is delivered from outside to the target PC, it is expressed as "Remote Code Execution". Examples of such malicious program include: the one that runs each time the user boots his PC; or the one that steals the user's important information. In the worst case, OS itself might be destroyed. This mechanism might also be used to exploit certain vulnerability in PCs and infect them with a virus. While English version uses the expression "Remote Code Execution", Japanese version uses "Code is executed remotely."
FIGURE: JAPAN VULNERABILITY NOTES: VULNERABILITY COUNTERMEASURE INFORMATION PORTAL SITE
If any security flaw (called “security hole” or “vulnerability”) was left un-remedied, your PC might be infected with a virus exploiting it. Always apply the latest security patches, or use the latest versions.

Question

Does your organization establish rules to keep employees’ software secure? For example, having employees apply Windows Update?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
The number of information leakage incidents arising from the use of file-sharing software is still high. Why such incidents occur? Originally, file-sharing software was developed by those wanting to share information across the Internet. To achieve the smooth sharing of information (files), various techniques are used in its development. However, in the case of software like this, non-originally-intended usages might be found out by a malicious user. As a result, a variety of malicious information (files) and copyright-protected files have come to be distributed freely. Among such malicious files is the one that distributes a variety of information (files) on the target PC to a network without permission. This is a computer virus called "exposure virus".

**FIGURE: INFORMATION LEAKAGE ARISING FROM THE USE OF FILE-SWAPPING SOFTWARE**
According to a survey, many malicious files are on such file-sharing network. These malicious files are designed to trick PC users into executing them, and if executed, their PCs are infected. On that score, file-sharing software is said to carry a high risk of information (file) leakage.

Installing and using such software on your business PC might lead to the infection of such exposure virus, for which your organization's sensitive information might be leaked over a network.

In the case of information leakage incidents involving file-sharing software, some are quite newsy and if introduced by mass-media, the leaked information might be distributed further.

Examples of newsy information if leakages are:

- Information on nuclear power plants
- The police investigation materials
- A bank's depositors' information
- Information on a hospital's patients' surgeries
- Sensitive information of the Self-Defense Force
- An online shopping site's clients' information
- A Stock Exchange's system information
- Information on an airport security
- A company's clients' information, etc.

<Reference Information>

To Prevent Information Leakages Arising from the Use of Winny
http://www.ipa.go.jp/security/topics/20060310_winny.html
(in Japanese)

Typical example of dangerous software (applications) to use within an organization includes, but not be limited to file-sharing software.

Non-guaranteed free software and privately-owned software are also unsafe because:
- Security updates for remedying vulnerabilities are not provided (i.e., not supported);
- A malicious program (e.g., fake antivirus software) that steals or destroys the information stored might be embedded.

So, do not install these dangerous software programs on your business PC. If, for some reason, you have to use your organization's important information on your home PC, make sure that such software is not installed. It's wrong to assume OK just because nothing wrong has happened before. It is important
to handle important information with care and not to leave room for a malicious code execution on your PC. This is a basic principle for not causing an incident.

If you are sharing a home PC with your family, even if you are certain that you are not using such high-risk software, anyone else in your family might be using it. Because that home PC is not under the control of your organization, you should discuss its usage with your family to avoid such problem. If you knew that anyone else in your family was using file-sharing software on that home PC, you should never use your organization’s important information on it.

The number of information leakage incidents arising from the use of file-sharing software is still high. Winny and Share are typical examples of high-risk programs

Question

Does your organization prohibit the use of any software carrying a high risk of file leakage? For example, forbidding the installation of file-sharing software?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
Aren't you using a privately-owned PC for internal operations? Typically, the operating environment of organization-supplied PCs is different from that of privately-owned ones.

For privately-owned PCs, the security controls defined by the organization might not be implemented. For example, the organization-defined security software might not be running on them; data encryption might not be applied; data backup might not be performed; or available e-mail systems might differ. Using a privately-owned PC for internal operations might lead to a non-predictable security incident.

In the case of a privately-owned PC, file-sharing software described in No.9 might be installed and used by anyone else in the user's family. Furthermore, if the business data used on that PC was left undeleted, it might be leaked some time in the future. Note that,

Privately-owned PCs are out of your organization's control.

To avoid these risks, organization-provided PCs must be used for internal operations.

In some cases, however, you may have to use your privately-owned PC for internal operations. In such cases, your organization needs to be aware of the use of such privately-owned PC and take necessary controls (e.g.
authorization for use) accordingly. Approved privately–owned PCs must have the security controls in place that are the same level as or a higher level than those implemented by organization-supplied PCs (especially controls against information leakage.) It is also necessary to define how to operate and use those PCs, as they might to be taken out of the organization with the organization's confidential information stored.

The following security controls that have already been explained may be necessary:

- Eliminate vulnerabilities in your OS and applications (No.8);
- Prohibit the use/installation of the applications that might adversely impact your business data or business processing itself (No.9);
- Use your security software properly (details are described in No.15 and No.16);
- Do not unnecessarily keep any business data in your PC, delete it promptly (completely, if possible) (No.4);
- Do not perform data-passing in an e-mail environment\(^2\)/remote-access environment\(^3\)/storage medium that is not provided by your organization;
- Implement appropriate security controls (especially against information leakage), including setting a login password to restrict access to your PC; encrypting important information stored, and so forth. (No.11 to No.14)

\(^2\) E-mail environment
As explained in No.9, it's not appropriate to use for internal operations privately-owned software and any software that are unrelated to your job. For example, for personal use, one may be using free e-mail service or his/her provider's e-mail environment. In the case of such e-mail environments, users might not know how the e-mails sent/ received are managed, and they cannot be assured that their e-mails were not intercepted on the way to the destination. This is because: they are not informed of who manages their e-mails on what mail server. Furthermore, setting an easy-to-guess credential might allow for spoofing by a malicious entity. Using an e-mail environment that is under your control or that your organization has contractual relationship with would lead to an improved security.

\(^3\) Remote-access environment
Nowadays, accessing an organization's IT environment via the Internet from a remote site has become feasible. Once a remote connection has been established, the PC in the remote site is able to use the organization's data and application environment and process such data without storing it locally. This remote connection environment enables secure use of an organization's IT environment from a remote site. But if the user's authentication infrastructure (including passwords), which is used each time a connection request is made, is not strong enough, it might allow for spoofing by a malicious entity.
Mobile Devices that Generate New Business Configuration?

Nowadays, various mobile devices including smart phones and other mobile phones and even media tablet (Apple's iPad) and electronic book readers (Amazon's Kindle) are used by many people in their business.

For example, to present information to a client on the spot; to make a presentation on a commercial product; or to collect information via the Internet in the field, etc.

If the organization's important data is processed via such devices, they must be provided by the organization. Meanwhile, if privately-owned mobile devices are going to be used for internal operations, (same as in the case of privately-owned PCs) they should be controlled by the organization (e.g., adopting registration system or approval system.)

Allowing for the use of privately-owned PCs for internal operations may make it difficult for the organization to achieve information security, since managing those PCs and organization-supplied PCs at the same level is usually difficult. The organization should make a clear distinction between privately-owned PCs and organization-supplied PCs, and prohibit their use for purposes other than the original intent.

Question

Does your organization establish rules to limit the use of privately-owned PCs for office works? For example, having an approval system in place for the use of such PCs at its office?

Yes: Implemented (4 points)
Yes, but partly:Partly implemented (2 points)
No: Not implemented (0 point)
When you work at a PC in your office or workplace, you are not always sitting in front of it, are you? You must have time to leave it for a while (e.g., lunch break and a little rest). At a time like this, leaving your PC logged in might allow anyone else to see or retrieve any information stored.

From information security point of view, it is risky to leave your PC unattended in the state in which anybody else can readily use it. Although it is possible that one PC is shared by multiple users ... What if it was used by an unauthorized person?

PCs require the same cautions as those for papers. An open window on your PC may contain important information; so, if you leave your PC in the state in which anybody else can readily use it, important information stored might be peeped or printed out, or unwanted operation performed (e.g., installation and execution of a malicious program.)

Please remember:
"When you leave your seat, lock your PC by applying computer lock!"

If your PC is running Microsoft Windows OS, you can easily apply the computer lock.
Use of the Computer Lock Function (For Windows XP)

Press [Ctrl + Alt + Delete] and click the [Lock the computer] button.

Or

Press [Windows key + L] for an instant lock.

"When you leave your PC, apply the computer lock so that others cannot use it" – this is also an important security control.

By doing so, you can prevent others from using your PC without your permission. You would have no intention of doubting your co-workers, but leaving your PC unattended might lead to information leakage. This control is particularly important for business offices and other facilities where any people might enter.

A screen-saver which has the password lock function is also useful, but it is better for PC users to use the computer lock function consciously. If you are apt to forget things, use computer lock and a password-protected screen-saver together.
In the case of Windows, to enable password protection for that screen-saver: right-click on the desktop and select [Property] from the pop-up menu, which opens the [Screen Property] screen, and then click the [Screen-Saver] tab and check the [Password protection] checkbox and click the [OK] button.

Regularly performing this operation would enhance the user's security consciousness.

PCs that are left to be used might also be used fraudulently by unauthorized people. To protect your PC against such fraudulent use, take appropriate controls (e.g., when you leave your seat, lock your PC.)

Question

Does your organization establish rules to prevent unauthorized access to PCs? For example, are you requested to turn off your PC when you leave your office?

Yes: Implemented (4 points)
Yes, but partly: Partially implemented (2 points)
No: Not implemented (0 point)
As in the case of PCs, when smart phones/mobile phones are not in use, it is recommended to security-lock them. If these devices are used for business purposes, the business-related important information might be stored on them. As a matter of course, they might contain client information (phone number, e-mail address, etc.) Therefore, it is important to protect them with authentication feature.

For mobile phones, you can apply PIN lock. For smart phones, there are many different authentication methods, so please refer to the manual for the model in use. Generally, smart phone users are encouraged to make settings in a way that password authentication (or other forms of authentication) is performed when the initial screen appears (or when you perform a flick.)

Some carriers and providers provide a remote security-lock service for mobile phones and mobile devices. By using this service, even if your mobile device is lost or stolen, you can prevent information leakage. For more information, please refer to the information provided by your carrier/provider.

Security-lock your mobile phone!!
No.12 About Passwords
Does your organization establish rules to set a hard-to-guess password? For example, are you requested to avoid using your name?

No.13 About Passwords
Does your organization establish rules not to disclose passwords? For example, prohibiting written passwords from being left in public spaces?

No.14 About Passwords
Does your organization establish rules to make passwords difficult to crack? For example, requesting login passwords to be changed on a regular basis?
No.12,13,14 About Passwords

- Does your organization establish rules to set a hard-to-guess password? For example, are you requested to avoid using your name?

- Does your organization establish rules not to disclose passwords? For example, prohibiting written passwords from being left in public spaces?

- Does your organization establish rules to make passwords difficult to crack? For example, requesting login passwords to be changed on a regular basis?

When a PC is booted, a login screen is displayed: it is a part of security control (NB: PCs running old version of Windows might not require login authentication.) This is an important security control already explained in "No.11 About PCs", However, if your user identifier (UID) and password that are used in login authentication become known by others, that information (also known as "account information" or "user information") might be exploited for "impersonation".

One PC might be used by multiple users and therefore, a unique UID is assigned to each user. But because UIDs are used only to distinguish individual users, they don't need to be a highly-complicated character string.

On the other hand, passwords are used to prove the identity of computer users. So they should be known only to their owner.
To avoid falling victim to "impersonation", make your password difficult for others (or other users) to guess.

Easy-to-guess (inappropriate) passwords are:

- not sufficiently long;
- using a word in a dictionary;
- identical with their corresponding UID;
- using information on oneself or one's family;
- using a proper noun;
- using a simple number/character sequence;
- using the same password as the one used in the past.

In an attack technique called "password cracking", a password of a small repertoire of characters (e.g., numeric characters only) or a short password consisting of a small number of characters can easily be cracked. For example, brute-force attack – an attack that tries every possible combination of characters until it breaks the code – can easily crack simple passwords like the ones noted above.

Let's think about a password consisting of six-digit numeric characters. In this case, the possible combination of numbers ranges from 000000 to 999999. So, the probability of this password being cracked is: one in a million (1/1000000, 1/10^6). In short, the password is cracked by trying up to one million different combinations of numbers. Then what about a password consisting of six-digit alphanumeric characters (lower-case alphabetical characters plus numeric characters)? While assignable values for numeric characters are "0" to "9" (i.e., ten different characters), those for lower-case alphabetical characters are "a" to "z" (i.e., twenty-six different characters.) So, the probability of this password being cracked is: 1/ (10+26)^6. In short, the password is cracked by trying up to 2,176,782,326 different combinations of characters.

In this way, by using different types of characters for your password, you can make it difficult to crack.

On the other hand, if you specify a nonsensical, complex word for your password, you might forget it. For this reason, you may opt to use a simple password (e.g., a word in a dictionary), but this is dangerous. If you use such a simple password, it can easily be cracked by the dictionary attack – an attack that tries every possible word in a dictionary until it breaks the password. Furthermore, an attacker who carries out this attack might create and use a dictionary that contains the words used frequently in the target region; so, watch out for it.

Then, what about using the name or nickname of yourself or your family members? Anyone who knows you or your family members can easily guess it, isn't it? Being like this, it wouldn't serve as a password.
So, use an appropriate password that meets the following requirements:

- Use the combination of upper- and lower-case alphabetical characters, numeric characters, and symbols;
- Use a long password (preferably, eight or more digits);
- Use a hard-to-guess, but easy-to-remember password.

Even if you set an appropriate password, if you use it for a long period or in a variety of contexts, it might be brought to the knowledge of someone else (e.g., by blurting out your password; or losing a paper on which you wrote down your password)

So, you need to implement the following controls to protect your password against theft:

- Change it regularly
- If you write it down on a paper, don't leave it unattended
- Do not store it on your machine
- Do not tell it to others

Password change intervals vary depending on the user, but three to six months are deemed reasonable in general.

You might write your password down on a paper in case you forget it. But in such case, keep it in a safe place (e.g., safety box) as you'd need it only when you forgot it.

Do not stick it on your PC's display.

This is like saying "Please feel free to use it."
You might store your password on your PC, but this is also a risky behavior. For example, if your PC was infected with spyware or other viruses that steals the information stored, your password might also be stolen.

Needless to say, if this happens, other information might also be stolen... Even if your PC is not infected with a computer virus, the files stored might be accessed by someone else. So, for the sake of safety, it is better not to store your password on your PC.

As a matter of course, don’t tell it to others. This is a basic principle.

THE THREAT OF IMPERSONATION IS:
Logs of a PC or a network contain the record on what was done by its user. So even if an illegal operation was performed by an impersonator, it would be logged as if done by the legitimate user, for which he might be sued for the malicious act.

*4) Brute-force attack
As the name indicates, this is an attack "by force" that tries every possible character string or word until it breaks the code. In fact, it simply tries every possible word in a dictionary or character string until it breaks the code, but depending on the performance of the computer used by the attacker, it might become an extremely-bothersome attack. So, it is risky for you to specify a word in a dictionary or a combination of simple characters for your password. You should also remember the existence of attackers’ dictionaries that contain commonly-used passwords. An example of frequently-used simple passwords is: "1234".
A user’s password for an Internet service is guessed and abused: such incident has been reported in large numbers. One of the major causes is that the user was using a simple password such as one’s name or date of birth. If your password is guessed by others, your PC might be used fraudulently by means of impersonation. To avoid this, use the combination of upper- and lower-case alphabetical characters, numeric characters and symbols for your password, and change it regularly.

Questions

Does your organization establish rules to set a hard-to-guess password? For example, are you requested to avoid using your name?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)

Does your organization establish rules not to disclose passwords? For example, prohibiting written passwords from being left in public spaces?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)

Does your organization establish rules to make passwords difficult to crack? For example, requesting login passwords to be changed on a regular basis?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
No.15 About Virus Countermeasures
Does your organization establish rules to protect PCs from virus infection via suspicious Websites or e-mails? For example, are you requested to install antivirus software on your PC?

No.16 About Virus Countermeasures
Does your organization establish rules to keep your antivirus software's virus definition files up-to-date? For example, are you requested to apply the automatic update of virus definition files?
Computer viruses are a major nuisance for computers and computer users. Computer viruses have been evolving along with the development of computers. While viruses for crime-for-pleasure were prevalent a decade ago, viruses for financial motive are prevalent in these days. (NB: Some of the latest viruses are not financially motivated, like the one that targeted at a nuclear facility in Iran.)

Note)
To facilitate the understanding of readers, the term "PC" is used to collectively mean personal computers, servers and networking equipment in the remainder of this section. All of these devices might be infected with computer viruses.

MANY DIFFERENT VIRUSES
Nowadays, there are many different forms of viruses such as spyware*5, exposure virus*6, scareware*7, ransomware*8, bot*9 and Trojan horse*10. Spyware steals the information stored on that PC; exposure virus exposes such information to the Internet; scareware (so called fraud virus) carries out an act of intimidation; ransomware covertly encrypts files and folders on a PC and demands a ransom; bot enables an attacker to remotely control that PC via the Internet (a network); and Trojan horse lurks in that PC and does bad things or installs a backdoor*11 which enables attackers to break into that PC via the Internet (a network.) Viruses have evolved into a hybrid virus that performs such a variety of activities
that does not fall into any category. Behind this background is the emergence of virus-development tools, with which anyone can easily create new viruses or subspecies by specifying functions they want to incorporate.

**MANY DIFFERENT INFECTION ROUTES**

- Via websites on the Internet (a network)
- Via e-mails
- Via external storage media such as USB sticks
- Via a direct attack over a network

Via the infection routes such as e-mails, websites on the Internet, Instant Messenger (IM), microblog (such as Twitter), SNS (such as mixi) and message board, computer viruses attempts to lure PC users into a virus-distribution site or to get them to click a link to a trappy website. PCs can be infected via: e-mail attachments, downloaded files (obtained via file-sharing software or from websites) and virus files.

**FIGURE: INFECTED VIA A TRAPPY WEBSITE**

**FIGURE: INFECTED VIA A VIRUS-CONTAINING E-MAIL**
Among the infection via e-mails, what is troubling in these days is: "targeted attack". Targeted attack takes a shot at a specific organization or individual via e-mails. A typical example is that: an attacker sends an e-mail whose text or subject contains a topic that seems relevant to the e-mail recipient's job, so that the recipient who is interested in it clicks its attached file. If the recipient opens that attached file, his PC is infected with the virus and the information stored might be leaked.

For more details on and countermeasures against targeted attack, as well as details on security controls for the secure use of the Internet and e-mails, please refer to the following materials:

- Countermeasure Guide Series
  - Guide for <Avoidance of Risks> When You Use the Internet
  - Guide for <Avoidance of Risks> When You Use Electronic Mails

- About Security Settings for E-mail Software (JPCERT/CC)
  [https://www.jpcert.or.jp/magazine/security/mail/index.html](https://www.jpcert.or.jp/magazine/security/mail/index.html) (in Japanese)

Furthermore, virus infections can be caused through the exploitation of the "Autorun" function of USB sticks or other external storage media, or a direct attack over the Internet (which is launched when the PC is connected to the Internet.) In the former case, a commonly-used function (process) is exploited and in the latter case, a vulnerability in the OS or applications (programs) running on that PC is exploited.
Among the incidents involving a direct attack over a network, well-known ones are the MSBlaster worm\textsuperscript{11} incident, which occurred in August 2003, and the Sasser worm incident, which occurred in May 2004. In both of these incidents, when the infected PC was connected to the Internet, it repeated shutdown process. The first shutdown was caused by a worm which got into that PC and subsequent shutdowns were caused by the worm's copies created through self-propagation. At this distance of time, this is a bit risible incident.

\begin{itemize}
  \item Information About the "W32/MSBlaster" Worm  
  \url{http://www.ipa.go.jp/security/topics/newvirus/msblaster.html} (in Japanese)
  \item Information About a Newly-Discovered Worm "W32/MSBlaster"  
  \url{http://www.ipa.go.jp/security/topics/newvirus/sasser.html} (in Japanese)
\end{itemize}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure.png}
\caption{INFECTION VIA A DIRECT ATTACK OVER A NETWORK}
\end{figure}

\textbf{ALTHOUGH THIS IS NOT ABOUT ANTIVIRUS SOFTWARE …}

As for the " Autorun" function of USB sticks or external storage media, a security patch for disabling this function was released by Microsoft. So it is recommended to apply it (i.e., apply Windows Update.)

To protect against such direct attack over a network, you can use firewall devices (feature) for your organization's network environment, broadband routers for privately-owned PCs employing broadband connection, or Windows firewall feature for Windows PCs.
ANTIVIRUS SOFTWARE

To prevent the invasion (infection) of various viruses into your PC through many different infection routes, it is essential to use an application called "antivirus software".

Antivirus software has virus definition files that describe characteristics of each virus, and by using them, it detects and cleans those viruses. Recent antivirus software employs new detection techniques such as heuristic scan and reputation technique, which is contributing to enhance the security of PCs. While heuristic scan is used to detect suspicious activities (behaviors) and deter virus activities, reputation technique is used to deter an access to suspect websites/e-mails by using public reputation information.

But there is also fake antivirus (security) software that causes a self-produced virus hoax, which is a type of scareware*. This sort of fake antivirus software serves for nothing, so watch out for it. When you select an antivirus software product, select generally-acknowledged reputable one! If you feel uncertain about selecting an appropriate product, you can chose from hot-selling commercial products at a computer shop, which is one of the safest options. You may ask advice of a specialist who has good deal of knowledge of security controls.

FYI, the following site contains information on antivirus software (security software):

- A List of Major Vaccine Vendors' Websites

Refer also to the following materials:

- Countermeasure Guide Series
  ✓ Countermeasures on Computer Virus
  ✓ Countermeasures on Spyware
  ✓ Countermeasures on Bots
*5) Spyware
Spyware is a virus that covertly invades (infects) the victim’s PC and records the information stored as well as operations performed by the user, and then transfer such information to an external party as needed. Among those that record users' operations is "keystroke logger" that records users' keyboard operation, which is a well-known tool. Internet reference record, which is also considered a history of users' operations, might be captured as well.

Spyware is thought to have been derived from so called adware which, for marketing over the Internet, displays information (such as commercial messages) or collects information (for the analysis of the user's preference.) Spyware is said to be a radical version of adware in terms of activities.

*6) Exposure Virus
A exposure virus causes information leakage via file-sharing software (e.g., Antinny virus) or covertly alters the victim's PC into an Internet website, so that the information stored is exposed to the Internet (e.g., Yamada virus.) These are also a type of spyware described above.

*7) Scareware
As indicated by the name, Scareware is a virus that scares the victims. It displays fake information such as "Your PC is infected with a virus" (i.e., self-produced virus hoax) and might also urge the PC user to purchase fake antivirus software.

*8) Ransomware
"Ransom" in "ransomware" refers to ransom money. Ransomware covertly encrypts specific files/folders on the target PC and demands a ransom by saying: "If you want to know the password to get them back, hand over your money!" In most cases, even if the user paid the money, the hostage (i.e., encrypted files/folders) would not be released (decrypted.) The same things as real-world crimes are happening in the virtual world of the Internet.
Bot

Bot is a program designed to infect PCs and then allow outsiders to remotely control them via a network (the Internet.) Once it invades the PC, it waits for commands from a command server (NB: Communication with the command server is done at certain intervals) and executes any of the preprogrammed processes as instructed. Because this behavior is similar to that of a robot, it is called "bot". A bot virus that infects recently-popularized smartphone has also been confirmed, so smartphone users need to watch out.

Examples of preprogrammed process are:

• Spam delivery (sending a flood of spams)
• Attacks such as DoS attack*12 (carrying out denial-of-service attack against a specific website)
• Network infection (gaining unauthorized access to a computer by exploiting its vulnerabilities and then infecting it)
• Network scan (collecting information on the target PCs for its infection or PCs having vulnerabilities)
• Version-upgrading of oneself or change of the command server
• Espionage activities (transferring the information stored in the infected PC to an external party)

A real threat of bots is: a group of bot-infected PCs might be under the control of a command server, forming a botnet. Botnet may consist of several hundred- to several hundred thousand-PCs, sending spams at the same time or carrying out a coordinated DDoS attack against a specific site. The larger the network, the greater the effectiveness of the attack.
**10) Trojan horses**

Do you know of a Greek mythology "Trojan horse"? This is a story about dummy horses being sent by a troop to its opponent, claiming to be a gift; inside the dummy horses, however, are soldiers who are ordered to attack the opponent's castle once they get into it. As in this story, Trojan horse type virus is a virus that lurks in the victim's PC and does various bad things as needed. Generally, it belongs in a different category than those of spyware, scareware, ransomware and does the following bad things:

- Installs a backdoor
  
  It installs a backdoor on the victim's PC so that the PC can remotely be controlled by an outsider via the Internet (network.) Through this backdoor, the outsider can break into that PC and perform various operations. It is a very dangerous situation.

- Downloads malicious programs
  
  It covertly downloads malicious programs from the Internet into the victim's PC and executes them.

- Collects information from the victim's PC
  
  It carries out so called spyware activities.

- Uses that PC as a steppingstone for an attack (e.g., relaying an attack)
  
  As with bots, it carries out an attack or works as a relay agent for an attack.

**11) Worm**

Unlike the "virus" in general and narrow sense that infects (parasitizes) other programs or files, worm is a self-contained program that is installed and executed on the victim's PC. It creates copies of itself and places them on the victim's PC (i.e., self-propagation.)

To distinguish it from a traditional, narrowly-defined "virus", it was given a distinct name (type) "worm". Because it does bad things on the victim's PC such as destructive activities and infection (self-propagation) while wriggling like worms, it is termed "worm".

In fact, this type of virus is most-easily created; so many different types and subspecies have emerged. The foregoing spyware and scareware as well as ransomware and bots are also said to be of this sort. This means that traditional viruses are waning.

Anybody who can write a program can create worm. Generally, since it requires PC users to activate it, it is masqueraded as a useful program for them or exploits their PCs' vulnerabilities to get it activated.

**12) DoS Attack**

Overloading networked computers through the exploitation of the characteristics of the Internet protocol is one of DoS attacks. If this is carried out by multiple agents against a single computer, the burden placed on that computer would be much greater. This type of DoS attack is called DDoS (Distributed Denial of Service) attack.

This attack is not necessarily carried out by an attacker himself (a human being.) For example, an attacker may, in advance, embed an attack program in multiple sites that are not the targets of the attack, and then launch a coordinated DoS attack from a remote site. This method is widely known.
The number of viruses that steal victims’ ID and password, or credit-card number is on the increase. Install **antivirus software** and watch out for an access to suspected websites and the receipt of suspicious e-mails.

**Question**

Does your organization establish rules to protect PCs from virus infection via suspicious Websites or e-mails? For example, are you requested to install antivirus software on your PC?

- **Yes:** Implemented (4 points)
- **Yes, but partly:** Partly implemented (2 points)
- **No:** Not implemented (0 point)
You may understand the usefulness of antivirus software. But there is one thing you should remember: just installing it doesn't produce sufficient effect.

Generally, antivirus software requires virus definition files, which describe characteristics of viruses, to detect them. These files are called "virus definition files" by McAfee and Symantec, and "pattern files" by TrendMicro. By using these files, antivirus software detects known viruses. Therefore, if your antivirus software's virus definition files are not kept up-to-date, your antivirus software cannot detect newly-emerged viruses. (NB: Some of the latest antivirus software employ heuristic (behaviors) scan, with which you can detect suspicious behaviors, or a cloud service that enables antivirus software to refer to the latest virus definition files on the Internet.)
For this reason, virus definition files need to be kept up-to-date.

These updated virus definition files are provided by antivirus software vendors and can be downloaded from the Internet, so users need to download them manually on an as-needed basis or automatically.

Generally, it is recommended to apply the "automatic update" feature that enables virus definition files to be updated automatically.

The figure below shows a setting screen for Symantec's AntiVirus Corporate Edition.

Setting methods vary depending on the antivirus software, but the "automatic update" feature is basically enabled by default. Check for your current settings by referring to the operation guide for your antivirus software. If the "automatic update" feature is not activated, it is recommended to activate it. Meanwhile, if you are not connecting your PC to the Internet all the time, you should also perform manual update to ensure your PC's security. For example, it is effective to manually update virus definition files whenever you boot your PC.

To make effective use of the antivirus software installed on your PC:

1. Configure your PC to automatically update virus definition files so that they are kept to up-to-date;
2. Antivirus software is good at detecting viruses at the border, so enable automatic protection (real-time protection) so that a virus infection is prevented;
3. There is no point in leaving the detected viruses on your PC, so configure your antivirus software to "clean the virus upon detecting it" (Information security beginners are encouraged to make this setting even though there is an issue of false positive. For those having a certain level of knowledge about information security, it would be more appropriate to configure their antivirus software to "quarantine the virus upon detecting it".)
When you buy a new PC, antivirus software may come bundled with it. But generally, such antivirus software is a trial version and is valid only for certain period of time. If you are using this type of trial antivirus software, upon reaching its expiration date, you can no longer update your antivirus software and its virus definition files. As a result, it loses effectiveness against new viruses, so, be careful. To address this problem, you need to purchase its right version or other products.

New computer viruses are being detected on a daily basis, so if you do not configure your antivirus software in a way that newly-emerging viruses are also included in its virus definition files, your PC might be infected with such viruses. Let’s check for the settings of your antivirus software and make sure that state-of-the-art virus countermeasures are being implemented!

Question
Does your organization establish rules to keep your antivirus software’s virus definition files up-to-date? For example, are you requested to apply the automatic update of virus definition files?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
FYI … MISCONCEPTION ABOUT ANTIVIRUS SOFTWARE

There seems to be many people who misunderstand about antivirus software. Because antivirus software is capable of detecting viruses through the virus scan and cleaning them, people often feel secure once they installed it. But this is a huge misconception.

For example, if a Trojan horse virus is detected on that PC, it is possible that the PC has already been infected with other viruses as well. And because antivirus software refers to its virus definition files and detect viruses, it cannot detect any viruses not included in them. In particular, if a Trojan horse virus infected that PC, it might download other viruses from the Internet, thus leading to the infection of those viruses.

One of the recently-emerged virus delivery techniques is sequential attack*13.
This is an attack that causes a large number of copies (or subspecies) of a virus to be downloaded onto the target PC, some of which are not detected by the antivirus software installed.

In this sequential attack, a Trojan horse virus called "downloader" attempts to enter the target PC and if the antivirus software fails to detect it, that PC can be infected with many other viruses. In short, if the downloader is detected through a virus scan, it is likely that the PC has already been infected with other viruses not included in its antivirus software's virus definition files. As time advances, those viruses might be included in the definition files, but until such time, PC users would not know what is being done by those viruses. This is a very dangerous situation.

Beyond that, although antivirus software can detect and clean viruses, it cannot restore the data or files altered or damaged by those viruses.

According to a highly-knowledgeable security researcher, in the above case, it is necessary to perform clean setup on that PC (i.e., resetting the PC to the factory default.)

It may be tough for general users to accept the recommendation of clean setup. But it should be remembered that antivirus software is not almighty and there is no justification for overconfidence, and that it can be used only for preventive purposes.

In the past, antivirus software was called "vaccine software", but vaccines are not cure-all medicines but prophylactic agents.

*13) Sequential attack
This is an attack that causes a large number of copies (or subspecies) of a virus to be downloaded onto the target PC via a network. So this is also called "continuous attack". In most cases, it leads to multiple virus infection and because no antivirus software can detect and clean all kinds of viruses, the PC that received this attack might fall into a prickly situation.
No.17 About E-mails
Does your organization establish rules not to send e-mails to wrong recipients? For example, are you requested to visually confirm the destination address prior to sending an e-mail?

No.18 About E-mails
Does your organization establish rules not to disclose e-mail addresses to third parties? For example, are you requested to use the "BCC" feature when sending an e-mail to multiple recipients who do not know each other's e-mail address?

No.19 About E-mails
Does your organization establish rules to protect confidential information when transferred by e-mails? For example, are you requested to store such information in an attachment file with password protection?
There are a number of information leakage incidents occurring due to the wrong transmission of an e-mail or a fax. If the recipient of such e-mail/fax was a good-hearted person, it might not lead to a problem. But since an e-mail/fax may contain personal information, if it was sent to a wrong address/number, it would lead to information leakage and the owner of the personal information would not be able to take it easy.

If you have tendency in making careless mistakes, you need to take steps to prevent wrong e-mail/fax transmission.

Basic principles are as follows:

FOR E-MAILS

🎉 Check the destination address prior to sending an e-mail

This is so called "visual confirmation". Before pressing the send button, check the destination address and the e-mail text for their consistency once more.

One of the good practices is to specify the destination address only after entering the e-mail text, with which you can confirm consistency between the destination address and the e-mail text.

When replying to an e-mail, the consistency between the return address and the e-mail text should be checked. For example, if the return address is a mailing list, that e-mail is sent to all the members in

Does your organization establish rules not to send e-mails to wrong recipients? For example, are you requested to visually confirm the destination address prior to sending an e-mail?
the mailing list. If you want to send an e-mail reply to specific persons, you need to specify their address on your own.

💡 **Configure your mailer in a way that you can confirm the destination address (and/or text) of an e-mail prior to sending it**

By doing so, you can check the consistency between the destination address and the e-mail text.

For example:

👉 For Microsoft's Outlook Express, disable the immediate sending option. By doing so, clicking on the [Send] button in the [Mail Creation] screen would only result in the e-mail being placed in the [Sent Mail] folder, and it would not be sent until the [Send and Receive] button is pressed. This would provide more opportunities for you to check again for the e-mail text.

👉 For Mozilla's Thunderbird, there is no function to disable immediate-sending, but you can use an add-on instead. If you use such add-on, you are prompted to check the e-mail text prior to sending it. Note that add-ons should be used on your own responsibility.

For more details, please refer to the following materials:

🔍 Countermeasure Guide Series
- Guide for <Avoidance of Risks> When You Use Electronic Mails

🔍 About Security Settings for E-mail Software (JPCERT/CC)
[https://www.jpcert.or.jp/magazine/security/mail/index.html](https://www.jpcert.or.jp/magazine/security/mail/index.html)
(in Japanese)

FOR FAX

👉 **Check for the recipient's fax number prior to sending a fax**

This is so called "visual confirmation". Before pressing the [Send] button, check the recipient's fax number and the text for their consistency once more. If you feel uneasy about it, it is good to ask other people to check them. In fact, some organizations have such fax transmission rule in place.

Further cautions should be exercised if the recipient's fax number is registered in the fax machine.
If the registered number is incorrect, it would lead to wrong transmission. Particular attention should be paid in the event of the changes in the recipients' fax number or the replacement of the fax machine.

When you got used to use a fax machine, you might make a careless mistake. Remember that careless mistakes could lead to information leakage and always perform operations with care.

There are a number of information leakage incidents occurring due to the wrong transmission of an e-mail or a fax. When you send an e-mail or a fax, check carefully the destination address/number.

Question

**Does your organization establish rules not to send e-mails to wrong recipients? For example, are you requested to visually confirm the destination address prior to sending an e-mail?**

- **Yes:** Implemented (4 points)
- **Yes, but partly:** Partly implemented (2 points)
- **No:** Not implemented (0 point)
These days, the number of e-mail address leakage incidents is on the increase, isn't it? After the Personal Information Protection Law was enacted, these incidents came to be treated as security-related information leakage incidents.

For example, the following incidents have been reported (some text is intentionally altered)

- Leakage of clients' e-mail addresses due to the wrong transmission of an e-mail (xyz real-estate Corp., Ltd.)
- Leakage of e-mail addresses due to the wrong transmission of an e-mail introducing a training workshop (xyz Prefecture)
- 678 addresses disclosed to the e-mail recipients due to the wrong transmission of an e-mail (xyz Create)
- Leakage of e-mail addresses during a campaign by the lyric search site "xyz"
- Leakage of e-mail addresses due to the wrong transmission of an e-mail (xyz City Center of Environmental Information)
- Leakage of e-mail addresses due to the wrong transmission of an e-mail magazine (xyz Prefecture)
- Leakage of e-mail addresses due to the wrong transmission of an e-mail (xyz Science)

These are the news found on the Internet during a two-month period, but there must be many other cases unreported.

Most of these security incidents were caused by misplacement of destination addresses.

Do you know the term "BCC"?
E-mail Terminology: "BCC (Blind Carbon Copy)"

When you send an e-mail to two or more people who do not know each other, you can use "BCC". In this case, each e-mail received does not show the other people's e-mail address.

On the other hand, if you use "To" or "CC (Carbon Copy)", all the addresses specified is shown along with the e-mail text.

In the case of Microsoft's Outlook Express, the [BCC] field is not shown by default. To make it appear:

- Start Outlook Express, open the [Message Creation] screen and select [View] -> [All Headers].

For other mailers, refer to the information provided by their vendor.

All the above-listed incidents were caused by the misplacement of destination addresses (i.e., not in the [BCC] field but the [To] or [CC] field.)

If those e-mail senders did not know about "BCC", "it could not be helped", but their organizations need to conduct adequate employee training on the use of e-mails. If such incidents were caused due to employee's negligence, it would be a serious problem. Remember that careless mistakes can lead to information leakage and always perform operations with care.

FYI …
If you search the Internet for "What is BCC", you can get various information concerning "BCC".

For more details on "BCC", please refer to the following material:

- Countermeasure Guide Series
  Guide for <Avoidance of Risks> When You Use Electronic Mails
Disclosing individuals’ e-mail address to others without consent is also an information leakage incident. When you send an e-mail to plural persons, check carefully where you placed the destination addresses.

Question

Does your organization establish rules not to disclose e-mail addresses to third parties? For example, are you requested to use the 'BCC' feature when sending an e-mail to multiple recipients who do not know each other’s e-mail address?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
As you know, information leakage incidents via an e-mail are occurring frequently. By using a little idea to protect the information contained in an e-mail, you can minimize damages caused by such incident.

For example, you can apply the following:

- **Encrypt the E-mail Text**
  
  Use a Public Key\(^{14}\)
  
  If the receiver of your e-mail is disclosing the public key, you can use it for encrypting your e-mail text. Note, however, the encrypted e-mail can only be decrypted using the associated private key the receiver has. In short, only the receiver can read the e-mail text. In general, free software PGP is used by people, but there is also commercial, encryption software that uses this technique. Because such software requires key management, it is not commonly used by people, though it does provide a reliable means to encrypt your e-mails.
But users are required to learn about the dedicated environment and key management and therefore, it may be a high bar for them.

**Use a Common Key**

If both the sender and the receiver of an e-mail have a common key for encryption, they can use it to encrypt their e-mails and send them each other. There is also commercial, encryption software that automatically generates a common key and the associated password at the time of encryption, so you may use it. For those who can afford the installation cost of such dedicated software, this may be a relatively-low bar.

**Password-Protect an E-mail Attachment and Send it**

When you send important information by e-mail, include it in a document file, password-protect the file, and attach it to that e-mail. Since a commonly-used word-processing tool or file compression/decompression tool has the password protection feature, it may be a relatively-low bar for people. Actual usage of such feature is described later.

**Store Your E-mail Text and Attachment file(s) on a Dedicated Server and then Send Temporal Access Rights (URL of the Dedicated Server; User ID and Password for Access) to the Receiver**

Separate your e-mail text and attachment files from other information on the mail server that controls (sends) e-mails, and store them on a dedicated information distribution server. Then, send the receiver temporal access right for those information (files) on this information distribution server (i.e., URL of the information distribution server; and user ID and password for access.) The receiver can retrieve necessary information using this access right.

Advantage of this technique is that even if you send information to a wrong receiver, by manipulating the information distribution server, you can prevent the receiver from accessing it. Furthermore, by checking the server's access history, you can see if that information was passed on to the intended person.

But building this operation environment incurs reasonable cost so it may be high bar for users.

As seen above, there are various ways to securely use e-mails. Here are explanations for one of the simplest and easiest ways to password-protect your e-mail attachment.
FYI, refer also to the following material:

Countermeasure Guide Series
http://www.ipa.go.jp/security/antivirus/shiori.htm
☑ Guide for <Avoidance of Risks> When You Use Electronic Mails

*14) Public key
This is a key used for encryption and it is used in combination with a private key which is generated as its key pair. Messages that are encrypted with a public key can only be decrypted with its associated private key. There is a similar key called "common key" but in the case of common key, messages are encrypted and decrypted with that same key and not pair keys.

How to Password-Protect Your E-mail Attachment and Send it

You may balk at the keyword "password-protection", but it can be done with simple operations, so let's apply it.

When you send important information by e-mail, do not write it in the e-mail text. Instead, include it in a document file, password-protect the file, and attach it to that e-mail. By doing so, you can ensure the security of that information. All that is left is to send that e-mail.

To encrypt document files, you can use: commercial, dedicated encryption tools; the encryption feature of commonly-used word-processing tools (Microsoft Office applications, etc.); or file compression/ decompression tools. Actual operations are described later.

Please note that;

Do not write the password to open the password-protected file in the body text of the e-mail to which the file is attached!!

You don't need a further explanation, do you? But there are some people who unthinkingly write such password. So be careful.

There are several ways to inform the receiver of such password, including:

🎉 Tell it to the receiver by telephone;
🎉 Agree with the receiver on which password to use before sending password-protected e-mail attachments;
Write it in another e-mail and send it some time later (Watch out for misdirection)

There are some mail servers (function) that automatically perform these operations. To realize this kind of environment, you need to have a dedicated environment including dedicated servers but it could incur reasonable cost. If you can afford the expense for the creation and operation of such environment, it would be worth considering installing them to prevent careless mistakes by e-mail users.

To Encrypt Microsoft Word 2003 Documents

Follow these steps, and password-protection is activated upon closing Word.
There are two types of passwords in WORD 2003: "password for read" and "password for write". For the above-mentioned purpose (for attachment files), set the "password for read".

When the e-mail receiver tries to open this Word document file, a window is displayed, prompting him/her to enter a password. Unless he/she enters a correct password, this file does not open.

When the e-mail receiver tries to open this Word document file, the above window is displayed, prompting him/her to enter a password.
To Encrypt Microsoft Word 2007 Documents

In the case of Word 2007, the words used for operator guidance are different from those of other versions, but by following these steps, you can have a password-protect file.

For other Microsoft Office applications such as Excel and PowerPoint, password protection is activated in the same manner.

For non-Microsoft word-processing tools or file compression/decompression tools, check their operation guide for password protection and apply it (if available.)

---

<table>
<thead>
<tr>
<th>1: The Office button</th>
</tr>
</thead>
<tbody>
<tr>
<td>2: Preparing for distribution</td>
</tr>
<tr>
<td>3: Document Encryption</td>
</tr>
<tr>
<td>4: Password</td>
</tr>
</tbody>
</table>
To Encrypt Microsoft Word 2010 Documents

When you send important information by e-mail, include it in a document file, *password-protect* the file, and attach it to that e-mail. Do not write the password in that e-mail and instead, inform the receiver of the password by another e-mail or telephone.

**Question**

Does your organization establish rules to protect confidential information when transferred by e-mails? For example, are you requested to store such information in an attachment file and with password protection?

**Yes:** Implemented (4 points)
**Yes, but partly:** Partly implemented (2 points)
**No:** Not implemented (0 point)
No.20 About Data Backup
Does your organization establish data backup rules not to lose important information in case of a breakdown or mis-operation? For example, are you requested to make backup copies of such information periodically?
With the evolution of information technology (IT) within organizations, a variety of information has come to be stored electronically. These electronic data may contain important information for corporate activities. What if these electronic data (contained in PCs, storage media, etc.) were rendered unusable for some reason?

Many people seem to believe that PCs or storage media within an organization would never go off. Certainly, they do not easily break down. But PCs can go off due to: a virus infection; fall from the desk to the floor; a beverage spilling over them; an end-of-life hard disk drive broken suddenly with an abnormal noise, and many other reasons.

Even worse case is the loss of these data due to users' careless mistakes or mis-operations (e.g., overwriting with other data.)
Data Backup Servers as a Fort of Last Resort

As mentioned in "Preface", "Information security controls are to protect information assets", data backup serves as a fort of last resort. In short, should any incident occur, it provides a means for data recovery … Even if incident itself cannot be prevented, data backup enables the organization to continue its business, while protecting its information assets.

Data backup is one of the import information security controls. However, if its operation and management is wrong, it might serve for nothing. There is no point in performing a useless backup.

Followings are precautions for data backup:

Precaution for Data Backup

- Perform a periodical backup
- Make sure that the backed-up data is restored
- Manage backup media (external storage media) safely so that the leakage (loss/theft) of data is prevented
- Delete backup copies that are no longer required

- Perform a Periodical Backup
Daily-updated information requires a periodical backup. If backup copies of such information are made only once a year, the information can only be restored to the state of a year ago at most. Being like this, the organization would not be able to continue its business. This is why a periodical backup tailored to the organization’s frequency of information update is required.

While this update frequency should be based on the manner and content of that business, backup methods also vary depending on the volume and structure of that information. For example, you may choose to make a full backup, a differential backup, or a partial backup (which is performed whenever the information is updated). Which one you should choose depends on the manner and content of your business as well as your backup environment (i.e., type or capacity of that storage medium, and repository, etc.)

If you want to prepare for an incorrect operation for daily update, you can adopt "generation management". This enables a series of backup copies to be managed as one generation and an appropriate generation (e.g., the latest, the previous, some generations before) to be restored. For example, let's think about a case: "I made an incorrect
update yesterday and yesterday's backup was performed after the update." In this case, if you had a backup copy of the day before yesterday, the information is restored to that point, sweeping the yesterday's incorrect update clean. This is not a matter of information security but operation. Still, this generation-based backup is effective and worth considering using it as a backup option.

Make Sure that the Backed-up Data is Restored
Even if you made backup copies of data, it would make no sense if you were unable to restore that data after an incident. To avoid this situation, you need to make sure periodically that the data is restored from any generation. And be careful not to damage current data during the checking of restoration.

Manage Backup Media (External Storage Media) Safely so that the Leakage (Loss/Theft) of data is Prevented
As described above, it is important that backed-up data be restored; however, it might not be restored due to the backup media (the ones on which you stored backup copies) being lost or damaged for some reason. In such cases, you cannot restore the data and therefore, the backup itself becomes meaningless. So it is important to manage your backup media safely.
It would be silly to let your backup media become the source of data leakage/flow. To avoid this, you need to perform secure management equivalent to that of original data. But this does not mean to manage backup copies in the same environment as that of original data (e.g., in another folder on the same hard disk drive, in the same locker, etc.) Managing them in the same environment might allow for a disruption or theft at the same timing. To put it simply, if you used a CD or DVD for your backup, keep them in a lockable cabinet in another secure room.

- **Delete Backup Copies that are no longer required**
  Over time, a backup copy may reach the point where it is no longer required. You may have to keep backup copies for several generations, but the backup copies that are too old to use for data restoration should be disposed of. When you dispose of backup media, follow the secure disposal steps described in "No.4 About Disposal". It would be silly to let discarded backup copies become the source of data leakage/flow.

(Reference: Microsoft)

- General Data Backup Method and Precaution

---

**Data stored on a PC might be lost due to a breakdown or mis-operation. By making backup copies on a regular basis, you can prepare for such incidents.**

**Question**

Does your organization establish data backup rules not to lose important information in case of a breakdown or mis-operation? For example, are you requested to make backup copies of such information periodically?

- **Yes**: Implemented (4 points)
- **Yes, but partly**: Partly implemented (2 points)
- **No**: Not implemented (0 point)
No.21 About Employees
Does your organization have employees protect confidentiality? For example, notifying its employees when hiring them that every employee is obliged not to disclose the organization's information assets?

No.22 About Employees
Does your organization make its employees aware of the importance of information security? For example, providing periodic information security training or education?

No.23 About Business Partners
Does your organization require its business partner(s) to protect confidentiality? For example, including nondisclosure clauses into its contractual agreement?
In general, an organization provides new employees with employee training before they start their job. In such occasions (and when screening for hire), the organization needs to inform them about confidentiality obligation - not disclosing corporate information and any information obtained through their job.

If the organization fails to inform its new employees about confidentiality obligation, it might lead to a serious information leakage/flow incident caused by them while they are on the job. In such cases, liability issues might arise, interfering with the organization’s incident response and post-incident controls.

For everybody, there is confidentiality obligation to conduct, and you might consider it "a matter of course", but this is a pitfall. An excuse "I didn't know that" would lead to a serious problem to the organization. This may be interpreted that the management failed to fulfill their responsibilities to its employees. Of course, employees must conduct confidentiality obligation in carrying out their business activities, but it is the responsibility of the management to inform them of such obligation. This is also the first step of security controls for organizations.

"Does your organization have employees protect confidentiality? For example, notifying its employees when hiring them that every employee is obliged not to disclose the organization's information assets?"
Generally, it is effective to get new employees to sign on the nondisclosure agreement of the organization when hiring them. Regardless of the method applied, it is important to clearly inform such obligation to its employees and to obtain a written consent.

In stead of trying to obtain detailed agreement at the time of employment, the organization can instruct its employees on as-needed basis how to handle the information that is related to or obtained through their job.

Points to remember are:

- Specify the subject of confidentiality obligation;
- Specify how to protect confidentiality (business rule, etc.);
- Specify disciplinary process for security bleach (work rule, etc.)

In short, it is important to specify what to protect and how.

**It is a matter of course that employees should conduct confidentiality obligation in accordance with the organization’s work rule and policies. However, the organization should also explicitly instruct its employees to do so, without leaving it as an unspoken rule.**

**Question**

Does your organization have employees protect confidentiality? For example, notifying its employees when hiring them that every employee is obliged not to disclose the organization’s information assets?

**Yes:** Implemented (4 points)
**Yes, but partly:** Partly implemented (2 points)
**No:** Not implemented (0 point)
Although this is not true of everybody, one might be steeped in lukewarm water of "habituation" if he had no security incident or problem for a long period of time.

Remember that this habituation might result in off-guard and eventually a security incident. This is why the organization needs to periodically train and educate its employee about information security.

- Security controls are becoming superficial at some organizations;
- Efforts to raise security awareness is required;
- For example, "chilling and startling", which is Heinrich's law, is useful for such purpose.

Why do you think a careless mistake happens? "I knew it, but I've done a mis-operation" or "I forget to confirm it": even such a trivial negligence can lead to a major incident. For example, a person who usually re-check the destination addresses of his e-mails may forget to confirm them just one time, leading to the misdirection and transmission of important information to a third party. This is an incident caused by a careless mistake.

If one gets used to do a thing, he may have a thought "So far, I've had no incident, so maybe I won't have it." This is what we often hear regarding traffic accidents. It sure is a serious problem.
Heinrich's law

"Behind one major accident are twenty-nine minor accidents. And behind those minor accidents are three-hundred events that did not lead up to an accident."

- This law was presented by Herbert William Heinrich in his research paper in 1929. Heinrich's law is considered a lesson learned from an industrial accident statistics.

To prevent one major accident, one needs to prevent twenty-nine minor accidents, which requires him to eliminate (reduce) the chances of three-hundred relevant events taking place.

In short, one must take such events as a foretaste of one major accident and take necessary steps to prevent such a major accident.

One solution is: sharing the information on an event that was caused by an employee with other employees, which would help prevent the occurrence of similar events (e.g., mis-operations, carless mistakes.)

This is the "chilling and startling" activity.
Chilling and Startling

- "Chilling and startling" events refers to the events that are abnormal but not leading up to an accident;
- Reporting/recording/sharing of such events would help prevent the occurrence of similar events (e.g., mis-operations, carless mistakes) and eventually the occurrence of major incidents;
- These activities (reporting/recording/sharing of such events) often become sloppy when employees get used to them. Such halfway records would not bring about good lessons, so caution should be exercised.
- Remember that, having employees report/record/share any discrepancies they noticed in their daily activities would help detect a sign of an accident.

Examples of "chilling and startling" events are as follows:

- I used a privately-owned medium for business purpose, which surprised a client;
- As I forgot to clean a whiteboard in a conference room, the subsequent user cautioned me;
- I almost forgot my bag on a net rack in a train;
- I was cautioned that my desk was messy;
- I left my luggage unattended in a distribution vehicle;
- I did inappropriate management of a device's operating instruction manual and it caused delay in the response to an incident;
- I left a printout unattended at a printer;
- I informed one’s personal mobile phone number to a third party without permission;
- I left the office with my locker unlocked.
It is effective to have "chilling and startling" events record what happened and **how such event could have been prevented**, and then share such information.

This sort of information (documents) can also be used for in-house information security education.

In *day-to-day work*, employees handle information, but they tend to get used to it and their awareness might get sloppy. It is important to **repeatedly** make them aware of the importance of information security.

**Question**

Does your organization make its employees aware of the importance of information security? For example, providing periodic information security training or education?

Yes: Implemented (4 points)

Yes, but partly: Partly implemented (2 points)

No: Not implemented (0 point)
An increasing number of information leakage incidents are occurring at outsourced organizations. As large organizations are strengthening their information security controls, information leakage incidents from them (except those caused intentionally and in-workers) are decreasing. However, the number of information leakage incident as a whole is not decreasing. This phenomenon ascribes to the fact that the number of information leakage incidents occurring at outsourced organizations is increasing.

Ideally, the outsourcer’s information security controls should be inherited by the outsourced organizations. But this is not working well.

In the past, an organization would outsource its business to another organization which was deemed reliable from the aspect of its commercial practice. But nowadays, many outsourcers expect (require) their outsourced organizations to implement adequate information security controls. In other words, implementing adequate information security controls is becoming a mandatory requirement for outsourced organizations.

In light of this situation, there is a mandate information security control that should be implemented by outsourcers. That is, specifying nondisclosure clauses in their contract agreement with outsourced organizations. In particular, if the information handled by their outsourced organizations contains personal information or corporate information, its criticality and confidentiality (in some cases how to manage it) must be communicated to them so that such
information is handled properly and protected from the leakage to an external party.

This would, in the event of incidents occurring at outsourced organizations, make clear who should be responsible for those incidents, in terms of executive responsibility and operation liability.

Particular attention should be paid to ensure that information security controls specified in the contractual agreements are communicated to all of their employees concerned. If the established contractual agreements turned out to be mere paper agreements, they would serve for nothing. Pursuing liability issues after the outbreak of an incident would cause a delay in the incident response and give an irreparable trouble to the owner of the leaked information (client or client enterprise.) If any information incident happens, it is important that all the people concerned work on the incident response in a timely and coordinated manner (No. 24 About Incident Responses.)

FYI: About Trade Secret

What would be important information (i.e., information that should be protected) for an organization? That is:

- Client information/personally identifiable information
- A variety of information entrusted by outsourcers
- An organization's technical/technological information and corporate strategy information including the organization-specific know-how
- Others: information which, if leaked, would cause a serious problem to the corporate activities (e.g., corporate secret/trade secret)

Here is an explanation of the term "trade secret" used in this document. A universal definition of "trade secret" is given in Unfair Competition Prevention Act\(^{15}\). In this document, it refers to an enterprise's important know-how (e.g., technical information) and classified sales-and-marketing information, which are not protected by copyrights or trademark rights but by Unfair Competition Prevention Act under the following conditions:

- Managed as confidential (confidentiality)
- Useful for the corporate activities (usability)
- Not a public knowledge (not in the public domain)
To put it simply, "information which is treated halfheartedly within an organization is not trade secret and therefore, it is not adequately protected." If trade secret is handled by the outsourcee, maintenance of confidentiality becomes particularly important.

*15) Unfair Competition Prevention Act
This law is intended at ensuring a fair competition among businesses as well as the precise implementation of relevant international agreements. It includes necessary steps for preventing an unfair competition and solving damage compensation issues and thus contributes to the sound development of the nation’s economy. The purpose of this law is to protect "trade secret" from theft, etc. and it was revised on April 30, 2009. The Websites below would be of help.

"Trade Secret Management Guideline (Revised Edition) - How to Manage a Business's Valuable Information -", which is listed on the third below, presents specific managerial approach for trade secret and therefore, it serves as a useful reference for information security measures.

Intellectual Property Policy/Unfair Competition Prevention (By METI)
(in Japanese)

Unfair Competition Prevention Act

Trade Secret Management Guideline (Revised Edition) - How to Manage a Business's Valuable Information -

---

**Question**

Does your organization require its business partner(s) to protect confidentiality? For example, including nondisclosure clauses into its contractual agreement?

---

**Yes:** Implemented (4 points)

**Yes, but partly:** Partly implemented (2 points)

**No:** Not implemented (0 point)
No.24 About Incident Response
Does your organization prepare for incidents? For example, having a procedure manual for responding to information leakage/loss/theft incidents?

No.25 About Rules
Does your organization clarify its information security controls? For example, making the information security controls described in No.1 to No.24 organization rules?
Even if the organization implements various information security controls, an information security incident could still occur one day. Nowadays, information security controls are required to cover both preventive actions (i.e., controls to prevent security incidents) and incident response (i.e., countermeasures against, and preparation for, such incidents.)

Information security incidents are not limited to information leakage. If a business making use of information (information systems) is discontinued due to earthquake, typhoon, flood, fire, etc., it is also an information security incident. Because such incident is unpredictable, if it really occurs, people concerned tend to get panics and have difficulty in minimizing the damage and restarting their business.

To address this problem, BCP (business continuity plan) and BCM (business continuity management) are required. Points for BCP and BCM are as follows:

⚠️ It's too late to take an action after the outbreak of an incident; so, preparation and simulation drill are required;
⚠️ If possible, prepare an incident response manual and clearly allocate responsibilities.

Preparation refers to: considering what incidents could happen, specifying and documenting response policy, process and procedure for those incidents,
as well as allocation of responsibilities. If the organization has this manual, it will not get panics in the event of such incident. It is also important to practice a simulation drill for incident responses (e.g., fire training.) It may help identify missing parts or deficiency in their incidents responses.

In simpler terms, it would be necessary for organizations to create an emergency telephone tree as well as procedures for confirming the safety of its employees in the event of a wide-scale disaster.

The Website below provides useful information on BCP at organizations.

Guideline for Making and Operating BCP for SMEs (Small and Medium Enterprise Agency)

As for information leakage incidents, the Website below provides useful information. These sites give a summary of what organizations should do if they caused an information leakage incident.

Points for Responding to Information Leakage Incidents
Without preparation, people tend to misbehave at security incidents, making the things worse. Considering other security incidents that have already been reported, prepare for those security incidents by assuming 'if the same things happened to my organization', and document necessary actions appropriate for your organization as well as those responsible for such actions.

Question
Does your organization prepare for security incidents? For example, having a procedure manual for responding to information leakage/loss/theft incidents?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
Organizations are encouraged to incorporate what is described in the above sections into their business rules. However, rules are not easy to formulate.

- Ambiguous rules that are too abstract would make no sense as it might produce different interpretations among employees (The organization needs to establish rules that are understood equally by everybody);
- Rules that are too strict to observe or that make employees feel irrelevant to them or that are not suited to their business content are useless (The organization needs to establish rules that can be followed by everybody);
- As business contents vary depending on the organization, so do rules for information security. An organization's rules might not work at another organization. The point is, each organization needs to establish rules that are well-suited to them.

No.25 About Rules

Does your organization clarify its information security controls? For example, making the information security controls described in No.1 to No.24 organization rules?

Ambiguous rules: NG
Rules that cannot be observed: need to be reviewed
Rules that are well-suited to the organization: OK
In this self diagnosis sheet, we used the form 'Does your organization…? For example …?': the former represents objective/purpose and the latter represents an example of controls. Without the former, it would be difficult for you to grasp its objective/purpose and without the latter, it would be difficult for you to implement those controls. For this, we need to present both objective/purpose and examples. As for the controls presented, organizations may need to tailor them on an as-needed basis.

Question

Does your organization clarify its information security controls? For example, making the information security controls described in No.1 to No.24 organization rules?

Yes: Implemented (4 points)
Yes, but partly: Partly implemented (2 points)
No: Not implemented (0 point)
How did it go!?

- For people whose score is: 100 Points
  - Introductory levels of security controls are perfectly implemented. Let's consider advanced controls!
- For people whose score is: between 70 and 99 Points
  - Mostly OK, but some controls are not sufficient.
- For people whose score is: between 50 and 69 points
  - Many controls are not sufficient.
- For people whose score is: 49 points or less
  - It's no wonder that an incidents such as information leakage occurs sometime.

Lastly …

Don't worry about your score. This self-diagnosis is intended to help you identify deficiencies in your organization's information security controls, and not to encourage you to make comparisons with other organizations.

It would be valuable if you could identify any fundamental information security controls that are missing or that require an emergency improvement.

We hope that your organization achieves better information security by examining and implementing the current security controls in place, providing employees training, and reviewing its security rules based on the PDCA cycle, etc.

May 2011
<Key to succeeding with the implantation of information security (measures)>

PDCA Cycle

- Review the rules
- Establish rules
- Analyze the implementation records
- Operate in accordance with the rules

<Reference>

- Information Security Measures for SMEs
  [Link](http://www.ipa.go.jp/security/manager/know/sme-guide/) (in Japanese)
- A Security Tool Library for SMEs
  [Link](http://www.ipa.go.jp/security/manager/know/tool/) (in Japanese)
- Understand Information Security in 5 Minutes!
  [Link](http://www.ipa.go.jp/security/vuln/5mins_point/) (in Japanese)
- IPA Countermeasure Guide Series
- Introduction of Tools
  [Link](http://www.ipa.go.jp/security/tools/) (in Japanese)
Overview

"Understand Information Security in 5 Minutes!", which is mainly targeted at those working at SMEs, is a learning tool with which you can study information security through simulated experiences. Each topic takes only five minutes and should be familiar to you as it contains one frame of daily events at a workplace. Through the simulated experiences of various information security-related events, you can learn the correct ways to cope with them. Please feel free to use this tool for checking the implementation status of your security measures.

- To address a variety of information security needs of SMEs, this learning tool offers 105 learning topics; you can pick out what you want to learn.
- Each topic takes only five minutes. Through the pictures of reality, you would feel security issues as immediate problems.
Based on the 25 check items in the sheet for "Information Security Self-Assessment for SMEs It takes only 5 min.,” this tool is consisted of 105 learning topics by taking into account the combination of business types and duty positions.

By selecting topics based on your business type and duty position, you can learn the information security measures relevant to your business content.

Structure of Learning Topics

Even within the same learning topic, the story varies depending on the business type and the duty position.

The contents for CEOs were created based on the assumption that their role is to construct a framework for promoting information security within their companies. So, at the time of formulating security rules, relevant learning topics were bundled together into one group.

E.g., where e-mail-related rules are concerned, it would be more efficient for CEOs to learn the three e-mail-related topics at the same time (in this tool, there are three relevant topics.)
About the Learning Flow

Each topic begins with "Learning Content", followed by "Adoption", "Case Example", the description of "Intent of This Learning Topic", and "Correct Answers". Furthermore, "Assurance Test" to see if the user understand that learning content is also given.

When you are finish with all the topics registered, you can have the "Certificate" issued. If you register the learner's information (affiliation and name) in advance, that information is also included in your certificate. This certificate serves as evidence that you have gone through all the learning topics. So, feel free to make use of it at your organization.
System Requirements

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS</strong></td>
<td>Microsoft Windows XP SP3 or higher, or Microsoft Windows Vista SP2 or higher,</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>Intel (R) Pentium(R)4 3GHz or a processor that is equaling or surpassing it</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>512MB or more</td>
</tr>
<tr>
<td><strong>Hard Disk Drive</strong></td>
<td>Required free space: 690 MB (at a maximum)</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>65,536 colors (16 bit) or more, resolution: 1,024×768 pixels or higher</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td>Mouse Speaker that can reproduce sounds; headphone</td>
</tr>
<tr>
<td></td>
<td>Microsoft .NET Framework Ver. 2.0 SP2 or higher</td>
</tr>
<tr>
<td></td>
<td>Microsoft DirectX 3 or higher</td>
</tr>
<tr>
<td></td>
<td>Adobe Flash Player 9 or higher</td>
</tr>
<tr>
<td></td>
<td>Microsoft Internet Explorer 6 SP1 or I higher</td>
</tr>
</tbody>
</table>

(Note) You may need to install "Microsoft .NET Framework" and "Adobe Flash Player" by yourself depending on the PC in use. For information on how to download and install them, please refer to the information provided by their vendors.

About Usage

In order to use "Understand Information Security in 5 Minutes!," you need to download it into your computer. For more details on its usage, please refer to the Website below (in Japanese only).

"Understand Information Security in 5 Minutes!"
http://www.ipa.go.jp/security/vuln/5mins_point/ (in Japanese)

Where to Contact:
E-mail:5minis-point@ipa.go.jp (in Japanese, domestic only)

If you find any problems or anything unclear about "Understand Information Security in 5 Minutes!," feel free to contact us at the above address.
Bunkyo Green Court Center Office 16th Floors
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan 113-6591

URL    http://www.ipa.go.jp/security/

[Worry-Free Information Security Consultation Service]
URL    http://www.ipa.go.jp/security/anshin/
E-mail  anshin@ipa.go.jp