Endpoint Security

An endpoint device generally refers to any electronic device with information storage capability and is connected to a computer network, including desktop computers, notebooks, smartphones, portable electronic storage devices, etc.

Endpoint security is the security measures used to safeguard endpoint devices and the stored information against security threats. It aims to:

- implement the latest security policies on all endpoints;
- identify, control and manage the use of removable devices;
- prevent the copying of information to unauthorised electronic storage devices;
- Enforce encryption when information is transferred to electronic storage devices;
- provide detailed audit records; and
- prevent introduction of malicious code, such as computer virus, into the corporate network via any endpoint device.

Endpoint Security Measures

As the types of endpoint devices are ever increasing and their usage continuously expanding, common computer security measures, such as anti-virus software and personal firewalls, are no longer sufficient to protect these devices and the stored information. For better protection, it is necessary to adopt endpoint security solutions integrated with different technologies.

Data Encryption

When information is being transferred to removable devices, it will automatically be converted into non-readable or meaningless data. This enhances the confidentiality of the information.

Port Control

With proper endpoint security requirements and regulations, an endpoint user will be authorised or forbidden to use different ports of the endpoint device. For example, the endpoint user is prohibited from connecting to any removable device via a USB port.

Device Control

There are different types of endpoint devices, such as portable electronic storage devices, CD/DVD writers and Portable Digital Assistants (PDAs). Each endpoint device has its own unique device identity number. Device control is used to authorise the use of endpoint device by registering its device identity number.

Application Control

Application control restricts any use of unauthorised applications on an endpoint device. This can prevent users from accidentally installing or executing applications that are not authorised by the computer owner, for example, downloading freeware from the Internet.

Endpoint security measures can protect each endpoint device from intruders' attacks and reduce the risk of data leakage. Meanwhile, organisations should provide staff education to enhance their awareness of information security and remind them not to download any files, such as application software or software updates, from suspicious website.

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk