MANAGING INFORMATION RISK

By Micho Schumann, Senior Manager, IT Advisory, KPMG

In the past, IT groups did not have to worry about laptop-related computer incidents because laptops were less in use. However, this trend is changing fast. There is an abundance of reports that 50 per cent of laptops have had security incidents of one kind or another.

In the recent past, IT groups did not have to worry about laptop-related computer incidents because laptops were less in use. However, this trend is changing fast. There is an abundance of reports that 50 per cent of laptops have had security incidents of one kind or another.

It is in this bleak truth that this article is rooted. If you are faced with the situation of having to manage computers, you should be prepared to cope with the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.

This model should enable employees to identify attacks on their devices as described above and to report access to unauthorised users.

In order to prevent a laptop from being lost or stolen, you should be able to identify the following:

- Laptop theft.
- Data corruption.
- Computer viruses.
- Data encryption.
- Data restoration.
- Data loss.
- Data manipulation.