Cyber

Laptop Security

Laptops are vital tools frequently used by many businesses. Along with other handheld devices, they typically are not used in a fixed, securable location, and thus additional measures are needed to protect them.

Security Procedures for Corporations[1]

- A formal security policy detailing end-user responsibility for securing the devices and the data they contain is essential. Devices should never be left unattended.
- Cable locks and docking stations should be used only when the device is left in a secure location, for short periods.
- These security methods are easily compromised and higher security options should be used when leaving a laptop in an office overnight (locked in storage area, file cabinet, etc.)

Travel Procedures

- Travel procedures should address common high-risk situations:
  - Avoid storage in automobiles.
  - Do not leave devices unattended in hotel rooms; secure them in safes or a locked suitcase.
  - Airport security areas, check-in counters, baggage claim, restrooms, food courts and curbside pick-up areas are all high-risk areas for theft of portable devices.
- Potential losses associated with exposure of sensitive data on stolen laptops can be greater than the cost of replacing the stolen equipment. According to IBM, the average cost of a data breach in 2019 is almost 4 billion USD. [2]

Take additional steps to mitigate losses related to data breaches associated with the theft of data storage devices and media.

Remote Protection

Protecting information on laptops can be more important than the physical computer. Setting up remote data deletion software can help prevent increased losses. Installing device trackers can also help with tracing the physical device, but it is important to stay cautious and report the incident to the police.

Cloud Software

Using secure, password-protected cloud software to store data can help protect valuable corporate information from being accessed from the physical device.

Removable Storage

Carefully evaluate the need for the storage of sensitive information on any type of portable device or removable media. In many cases, the need for storing information on these difficult-to-secure devices is not worth the benefit given today's threat environment. If it is determined that storage on portable devices or removable media is absolutely necessary, this data must be protected. Data encryption, the process of making data inaccessible without access to a secret key, is a useful way to protect confidential information.[3]

Resources for encryption of stored data:

Microsoft Transparent Data Encryption (TDE)

TrueCrypt

For more information, visit cnacanada.ca.

1 ITProToday (2016) Retrieved from https://www.itprotoday.com/business-resources/how-prevent-laptop-theft-and-what-do-when-it-happens
2 IBM (2019) Retrieved from https://www.ibm.com/security/data-breach
3 DigitalGaurdian (2019) Retrieved from https://digitalguardian.com/blog/what-data-encryption