3.2.2 Hardware Security Facts

This lesson covers the topic of hardware security measures.

Hardware Security Measures

The following table describes several recommended hardware security measures.

Security Measure	Description
Door locks	The first line of defense in protecting computer systems is to control access to the location where the computers are located. ▪ Many businesses use cubicles, which leave computers in plain sight and easily accessible to anyone. Controlling access to the building is critical to prevent unauthorized people from gaining access to computers. ▪ Place critical or sensitive devices in a locked room. For good physical security, implement the following protections. ▪ Keep doors to the rooms locked as much as possible, especially when the rooms are not in use. ▪ Use keypads or card readers to control room access. ▪ Do not leave the door ajar to adjust the temperature inside the room.
Hardware locks	Hardware locks prevent the theft of computers or components. ▪ Keep servers and other devices inside locked cabinets or locked rooms. ▪ Bolt or chain workstations to desks or other stationary objects to prevent theft. ▪ Lock cases to prevent opening up devices and removing components, such as memory and hard drives. ▪ For laptops, use removable cable locks when computers are left unattended in public areas. You can also use motion detectors that sound an alarm when a laptop is moved.
Access cards	Access cards can be used to secure a facility, room, or cabinet. ▪ Barcode readers require a barcode to be scanned using infrared technology. ▪ Magnetic stripe readers require that a card be swiped. ▪ Proximity card readers transmit a low radio frequency (RF). When a card is within a certain distance, the card uses the RF signal to transmit the code to the reader.
Secure data destruction	Data is an important resource for any organization. All digital data and paper data should be protected. Any paperwork containing sensitive information should be securely destroyed. The following are some of the options for secure data destruction: ▪ Burning ▪ Shredding ▪ Pulping ▪ Pulverizing ▪ Degaussing ▪ Third-party solutions

Checkout policy	A checkout policy ensures that hardware does not leave the organization's premises without a manager's approval. Checkout policies can include the following details: ▪ Acceptable use is limited to business-specific activities on the device. ▪ A listing of software that is installed on the device. ▪ Characteristics of the hardware such as the serial number, make, and model number. ▪ A rule that borrowers must not install software on the devices. ▪ A rule that returning the device should be within a reasonable or defined period. ▪ A rule that liability is placed on the borrower for the device's physical safety.