**Physical Security Controls**

In February 2019, a former student at the College of St. Rose in Albany, New York, pleaded guilty to destroying 66 computers on its campus with a “USB killer” stick.

**1. The link below is to an article that discusses the “USB Killer” attack. InfoSecurity Magazine: USB Breach, Physical Security**

As you read through the article, pay special attention to how Vishwanath Akuthota carried out this attack.

**2. Answer the following questions regarding the attack itself:**

What is a "USB killer" stick?

* USB killer is a modified USB drive that can damage or destroy a device when you insert it into the device's USB port.

What is its *intended* use?

* A USB Killer is a USB drive that has been modified to deliver an electrical surge that can damage or destroy hardware when the altered thumb drive is inserted into a computer's USB port.

How did Vishwanath obtain it?

* The item, which has the appearance of a USB thumb drive, is available from a number of online merchants. The device was purchased by Vishwanath Akuthota, a former student at the College of St. Rose in Albany, from an online reseller, and he used it to wipe out 66 computers on the campus.

How was Vishwanath caught?

* Security cameras captured him taking a backpack with the "USB killer" stick and a key to the classroom where the machines were destroyed. He was caught as a result.

What are the steps the college (and other organisations) should take to mitigate the risk of something this occurring?

**3. Read the article below on the “USB condom” device.**

USB Condom

What are your thoughts regarding the efficacy of this device? Is this something that could (or should) be deployed in an enterprise? Why or why not?

The USB condom is a device that blocks the data pins in a USB port so that power can still pass through, but no data can be sent. The system is made to guard against "juice jacking," which refers to the act of using a charging station or USB port to steal data or install malware on a device. The USB condom is reasonably priced and available to buy online.

The USB condom may be helpful for preventing the possibility of juice jacking because its effectiveness in preventing data transfer appears to be legitimate. The device might not be useful for enterprise deployment, though, as staff members would have to carry around a USB condom and use it between their devices and any unknown USB ports or charging stations. To lower the risk of juice jacking, an enterprise may choose to offer secure charging stations or restrict the use of USB ports.