

16.6: Security Issues in Electronic Communication

Learning Objective

1. Identify and discuss challenges faced by companies engaged in e-commerce.

E-commerce has presented businesses with opportunities undreamt of only a couple of decades ago. But it also has introduced some unprecedented challenges. For one thing, companies must now earmark more than 5 percent of their annual IT budgets for protecting themselves against disrupted operations and theft due to computer crime and sabotage (Alexander, 2011). The costs resulting from cyber crimes—criminal activity done using computers or the Internet—are substantial and increasing at an alarming rate. A 2010 study of forty-five large U.S. companies revealed that the median cost of cybercrime for the companies in the study was \$3.8 million a year (Ponemon, 2010). And some cybercrimes involve viruses that can spread rapidly from computer to computer creating enormous damage. It's estimated, for example, that damage to 50,000 personal computers and corporate networks from the so-called Blaster worm in August 2003 totaled \$2 billion, including \$1.2 billion paid by Microsoft to correct the problem (Shukovsky, 2011). The battle against technology crime is near the top of the FBI's list of priorities, behind only the war against terrorism and espionage (Alexander, 2011). In addition to protecting their own operations from computer crime, companies engaged in e-commerce must clear another hurdle: they must convince consumers that it's safe to buy things over the Internet—that credit-card numbers, passwords, and other personal information are protected from theft or misuse. In this section, we'll explore some of these challenges and describe a number of the efforts being made to meet them.

16.6: Security Issues in Electronic Communication is shared under a [CC BY 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

- [15.6: Security Issues in Electronic Communication](#) is licensed [CC BY-NC-SA 4.0](#).