Read the following and answer the questions below it.

Hacker Hunters

Hacker hunters are the new breed of crime fighter. They employ the same methodology used to fight organized crime in the 1980s—informants and the cyberworld equivalent of wiretaps. Daniel Larking, a 20-year veteran who runs the FBI’s Internet Crime Complaint Center, taps online service providers to help track down criminal hackers. Leads supplied by the FBI and eBay helped Romanian police round up 11 members of a gang that set up fake eBay accounts and auctioned off cell phones, laptops, and cameras they never intended to deliver. The FBI unleashed Operation Firewall, targeting the ShadowCrew, a gang whose members were schooled in identity theft, bank account pillage, and selling illegal goods on the Internet. ShadowCrew’s 4,000 gang members lived in a dozen countries and across the United States. For months, agents had been watching their every move through a clandestine gateway into their website, shadowcrew.com . One member turned informant and called a group meeting, ensuring the members would be at home on their computers during a certain time, when the Secret Service issued orders to move in on the gang. The move was synchronized around the globe to prevent gang members from warning each other via instant messages. Twenty-eight gang members in eight states and six countries were arrested, most still at their computers. Authorities seized dozens of computers and found 1.7 million credit card numbers and more than 18 million email accounts.

ShadowCrew’s Operations

The alleged ringleaders of ShadowCrew included Andres Mantovani, 23, a part-time community college student in Arizona, and David Appleyard, 45, a former New Jersey mortgage broker. Mantovani and Appleyard allegedly were administrators in charge of running the website and recruiting members. The site created a marketplace for more than 4,000 gang members who bought and sold hot information and merchandise. The website was open for business 24 hours a day, but since most of the members held jobs, the busiest time was from 10 p.m. to 2 a.m. on Sundays. Hundreds of gang members would meet online to trade credit card information, passports, and even equipment to make fake identity documents. Platinum credit cards cost more than gold ones, and discounts were offered for package deals. One member known as “Scarface” sold 115,695 stolen credit card numbers in a single trade. Overall, the gang made more than $4 million in credit card purchases over two years. ShadowCrew was equivalent to an eBay for the underworld. The site even posted crime tips on how to use stolen credit cards and fake IDs at big retailers. The gang stole credit card numbers and other valuable information through clever tricks. One of the favorites was sending millions of phishing emails—messages that appeared to be from legitimate companies such as Yahoo!—designed to steal passwords and credit card numbers. The gang also hacked into corporate databases to steal account data. According to sources familiar with the investigation, the gang cracked the networks of 12 unidentified companies that were not even aware their systems had been breached.

Police Operations

Brian Nagel, an assistant director at the Secret Service, coordinated the effort to track the ShadowCrew. Allies included Britain’s national high-tech crimes unit, the Royal Canadian Mounted Police, and the Bulgarian Interior Ministry. Authorities turned one of the high ranking members of the gang into a snitch and had the man help the Secret Service set up a new electronic doorway for ShadowCrew members to enter their website. The snitch spread the word that the new gateway was a more secure way to the website. It was the first-ever tap of a private computer network. “We became shadowcrew.com ,” Nagel said. Mantovani and Appleyard were slated for trial. Authorities anticipated making additional arrests

Questions

1. What types of technology could big retailers use to prevent identity thieves from purchasing merchandise?

2. What can organizations do to protect themselves from hackers looking to steal account data?

3. Authorities frequently tap online service providers to track down hackers. Do you think it is ethical for authorities to tap an online service provider and read people’s email? Why or why not?

4. Do you think it was ethical for authorities to use one of the high-ranking officials to trap other gang members? Why or why not?

5. In a team, research the Internet and find the best ways to protect yourself from identity theft.

UPS Invests $1 Billion to Go Green

United Parcel Service (UPS) will make about $1 billion in technology investments to improve the efficiency of its operations, with the goal of cutting billions more from its costs over the long term. One of its main goals is to improve the speed and efficiency of its delivery operations. To achieve that, UPS is equipping its vans with sensors that allow it to collect data about things such as fuel consumption, chosen routes, and how much time its engines spend idling. Reducing fuel consumption will help UPS not only to cut costs, but also to be more environmentally responsible. A big portion of the company’s costs comes from transporting packages by air. In fact, UPS is the world’s ninth-largest airline, so it is trying to conserve aircraft fuel as well by lowering flight speeds and better planning to avoid duplication of routes. But a lot of fuel is also burned by its trucks, and the sensors being implemented there could save the company millions of dollars. UPS is installing about 200 sensors in its vehicles—in the brakes, engine box, and on the exterior—to collect data and pinpoint opportunities where drivers can adjust their driving to maximize fuel efficiency. The company wants to reduce idle time of its delivery trucks, as each hour spent idling burns about a gallon of fuel. The company is also installing equipment to track the routes drivers take to deliver packages. Every morning the drivers are briefed on the data captured by the sensors and how they could drive differently to save fuel. UPS wants to optimize the number of times a vehicle has to start, stop, reverse, turn, or back up.

Green Data Center The company is also investing in more efficient cooling technologies at its two data centers, which are in Mahwah, New Jersey, and Alpharetta, Georgia. During the winter, the company can shut off its chiller equipment and use outside air for cooling. The Alpharetta data center has a 650,000-gallon water tank outside for cooling and a heat exchanger to faster dissipate the heat captured in the fluid. The water flows in a circular motion around the data center, cooling the equipment, and the heat exchanger helps lower the temperature of the hot exhaust water more quickly. UPS is also investing in faster server processors, allowing it to consolidate existing servers through virtualization. That helps lower energy costs and also reduces the physical footprint of its servers. And the company has been consolidating smaller server rooms that were scattered around the world. These changes are saving UPS around $400,000 each year.15

Questions

1. Why do you think UPS is embracing sustainable technologies?

2. How is UPS developing a sustainable MIS infrastructure?

3. What business benefits will UPS gain from virtualization?

4. What role does each characteristics of an agile MIS infrastructure play in helping UPS to operate its business?

5. How could UPS benefit from cloud or grid computing?

6. What types of ethical issues might UPS encounter with the tracking technology it has placed in its trucks?

7. What types of security issues might UPS encounter with the tracking technology it has placed in its trucks?