# Weekly test

1. Describe a hypothetical situation in which the action you would take is not legal, but it is ethical. Describe a hypothetical situation where the action you would take is legal, but not ethical.

2. It can be difficult for a large organization to act ethically consistently across all facets of its business. Identify a recent example of a usually ethical company acting in an unethical manner.

3. Should software piracy within the boundaries of third-world countries be tolerated to allow these countries an opportunity to move more quickly into the information age? Why or why not?

4. Do you think that ethics training can really be effective in changing the behavior of employees? Why or why not?

5. As part of your company’s annual performance review process, each employee must identify three coworkers to be interviewed by his manager to get a perspective on the employee’s overall work performance. Your friend has offered to give you a glowing performance review if you agree to do the same for him. Truth be told, your friend is not a very dependable worker, and his work is often below minimum standards. However, he is a good friend, and you would hate to upset him. What would you do?

6. While mingling with neighbors at a party, you mention that you are responsible for evaluating bids for a large computer software contract. A few days later, you receive a lunch invitation from one of your neighbors who also attended the party. Over appetizers, the conversation turns to the contract you are managing. Your neighbor seems remarkably well informed about the bidding process and likely bidders. You volunteer information about the potential value of the contract and briefly outline the criteria your firm will use to select the winner. At the end of the lunch, your neighbor surprises you by revealing that he is a consultant for several companies in the computer software market. Later that day, your mind is racing. Did you reveal information that could provide a supplier with a competitive advantage in the bidding process? What are the potential business risks and ethical issues in this situation? Should you report the conversation to someone? If so, whom should you talk to, and what would you say?

7. You are a recent graduate of a well-respected business school, but you are having trouble getting a job. You worked with a professional résumé service to develop a well-written résumé and placed it on several Web sites; you also sent it directly to contacts at a dozen companies. So far, you have not even had an invitation for an interview. You know that one of your shortcomings is that you have no real job experience to speak of. You are considering beefing up your résumé by exaggerating the extent of the class project you worked on for a few weeks at your brother-in-law’s small consulting firm. You could reword the résumé to make it sound as if you were actually employed and that your responsibilities were greater than they actually were. What would you do?

8. You have just completed a grueling 10-day business trip calling on two dozen accounts up and down the West Coast. There were even business meetings combined with social events late into the night and on the weekends. On the flight back home at the end of this marathon, you are tired and feeling as if you have not seen your family for a month. As you work on completing your expense report, you say to yourself, “The company does not pay me enough for the work that I do.” For more than a few moments, you think about padding your expense report to make up for all the extra hours and time away from your family. Would it be okay to add “extra expenses” to compensate for the hardship of the trip?

**9. IBM–A Front-Runner in Sustainability**

During the 1970s, IBM produced mainframe computers, adding machines, typewriters, and telephone routing systems—much of the advanced information technology of the time. The company was one of the largest corporations in the world and ranked seventh in the 1976 Fortune 500 list of largest U.S. corporations. However, IBM’s component manufacturing processes produced large amounts of benzene-based materials that are carcinogenic. In an effort to take the lead in corporate responsibility, IBM established one of the first environmental programs of its kind in 1971.

The company implemented a three-pronged program that attempted to track waste from creation to disposal, to reduce IBM’s reliance on toxic chemicals, and to reduce the amount of toxic waste released during the manufacturing process. IBM incrementally reduced toxic waste by 220,500 tons from 1987 to 2011, a dramatic achievement. IBM has been able to accomplish this, in part, by recycling 44 percent of the hazardous chemicals used in its manufacturing processes. The company has also changed manufacturing processes to eliminate or reduce the use of hazardous materials.

Throughout the late twentieth century, IBM was an industry leader in its efforts to address a variety of environmental issues. For example, in the 1980s, scientists noticed a hole in the ozone layer of the stratosphere over Antarctica that protects the earth from harmful ultraviolet radiation. In response, IBM worked to reduce its use of ozone-depleting chemicals, such as chlorofluorocarbons, and in 1989, IBM led the IT world in its reduction of such chemicals.

Today, the company has expanded its initiative beyond toxic waste management. Its programs now seek to reduce energy use, conserve water resources, create energy efficient products, spearhead safety in the use of nanotechnology, and combat climate change. IBM has also focused on the use of environmentally preferable substances and materials, and it continues to work to reduce or eliminate its reliance on heavy metals and carcinogens. The company reduced greenhouse gas emissions in 2011 by 3.2 percent.

IBM works with the International Organization for Standardization (ISO) to create international standards for toxic and nontoxic waste reduction, water purification, efficient energy utilization, and waste emissions. In many cases, IBM helped ISO to develop a specific standard and then became the first company to demonstrate compliance with that standard. In 2011, IBM became the first corporation to meet ISO standards on energy management systems. The practice of meeting sustainability standards helps IBM maintain market share because the European Union, the United States, and other countries often give preference in awarding contracts to companies that have ISO certification. Maintaining market share is more challenging for IBM than it was in the company’s early days because many companies now compete with IBM. Samsung, HewlettPackard, Nippon Telephone and Telegraph, Apple, Dell, and other companies have crowded the market. By 2012, IBM had dropped to 19 on the Fortune 500 list.

Leveraging ISO certification helps IBM in its efforts to maintain market share and increase its revenue. In fact, the company has found that corporate responsibility has given it a better bottom line. During 2011, IBM spent $114.5 million on its environmental initiatives. During the same period, savings from environmental policies totaled at least $139 million. Company reports indicate that in each of the past 20 years, the savings from its sustainability and environmental stewardship programs have exceeded the costs.

IBM also has an expansive community and corporate citizenship program. For instance, the company has a program to match employees with community service needs. Over 220,000 IBM employees and retirees have participated in this volunteer program in areas such as education, economic development, health care, disaster relief, and environmental programs. IBM also provides employees to serve as teachers for inner city schools throughout the world. The company continues to pay its employees as they work in the schools. Finally, the company utilizes its technology in cities worldwide to help struggling governments find solutions to problems with traffic, emergency services, and infrastructure.

As a company, IBM has set up a steering committee and working group to draft goals and implement CSR strategies. IBM built an electronic meeting platform called Jams, which facilitates online brainstorming and engages a wide range of stakeholders. Since 2001, this platform has not only facilitated the collaboration of 300,000 IBM employees from all over the world, but it has also brought thousands of people from government agencies, nonprofits, corporations, and educational institutions together to identify and address the world’s greatest challenges. IBM has been a front-runner in environmental stewardship, and the IT giant has set challenging goals for itself in other areas of CSR.

a. Present three strong arguments that IBM might have used to justify the start of its sustainability programs in the 1970s.

b. What major goals has IBM achieved in environmental stewardship?

c. How might IBM leverage its leadership in sustainability to maintain its competitiveness in the IT market?

**10.** **Ethical and Business Setbacks for Nokia**

On the morning of September 5, 2012, Nokia staged a press conference in New York City to announce the official launch of its new Windows 8 smartphones, the Lumia 920 and 820. The event focused heavily on the phone’s PureView camera technology. Videos played at the press conference and online emphasized the phone’s stabilizing technology. One advertisement in particular extolled the steadiness of the smartphone’s camera with a video showing a woman bicycling by a riverbank in Helsinki, supposedly shot on a Lumia 920 by a young man bicycling beside the woman. However, the online tech magazine The Verge decided to take a closer look at the video, and while examining it, a researcher for the magazine noticed a reflection in a window of a trailer behind the woman on the bike. The reflection showed a young man not on a bicycle, but rather in a van—holding a large camera. Further investigation revealed that the shot was taken by a steadicam, a professional motion picture camera, held by a cameraman in the van. By 4:30 p.m. Eastern time, the word was out. And by 8:00 p.m. the same day, Nokia had updated the video with a disclaimer and issued a formal apology.

Five days after the Lumia advertisement fiasco, Nokia announced that it would conduct an ethics review of the incident. “What we understand to date is that it was nobody’s intention to mislead, but there was poor judgment in the decision not to use a disclaimer,” Nokia spokesperson Susan Sheehan said. She refused to identify the company responsible for producing the advertisement and stated that Nokia would conduct its investigation “quickly, fairly and privately.” The company quickly concluded its investigation, but has not revealed the results of its investigation, other than to acknowledge that “poor judgment” was used. Nor has Nokia not made public any ethics initiative or punitive measures taken as a result of the false advertisement.

Nokia is one of the world’s largest mobile phone manufacturers. It has a 120-year history of worker- and community-centered operations, and a sterling reputation for environmental consciousness. Its corporate manifesto, “The Nokia Way,” emphasizes people-centered decision making in a network of equals. The camera fiasco, however, was the latest in a string of ethical and business setbacks that have set the giant corporation reeling.

Nokia announced in 2007 that it was moving production from its facility in Bochum, Germany, to the relatively low-wage environment of Romania. A consumer backlash ensued. The company was eventually required to pay 60 million Euros ($93 million) back to the German state for subsidies paid to the company for locating its facilities in Germany. In addition, a boycott was organized by German trade unions, and several cabinet ministers publicly changed to other brands of cell phones. Nokia saw its share of the German smartphone market drop from 70 percent to 50 percent between the factory closure announcement and the end of 2009. Ironically, Nokia’s 2011 decision to close the Romanian facility and move manufacturing to Asia met with similar reactions in Romania.

In 2008, Nokia Siemens Networks, a joint venture between Nokia and Siemens AG, reportedly provided Iran’s monopoly telecom company with technology that allowed it to intercept the Internet communications of its citizens to an unprecedented degree. The technology enables the Iranian government to monitor voice calls, text messaging, instant messages, and Web traffic. Nokia officials insisted that the system constituted “a standard architecture that the world’s governments use for lawful intercept” and added that the company had refused to sell the technology to the governments of Burma and China. However, in June 2009, the emerging pro-democracy movement in Iran organized a boycott of Nokia devices and messaging services. Finally, on June 2, 2010, Nokia Siemens Networks held a press conference to apologize for the role its technology played in the brutal crackdown on Iranian demonstrators the year before. In late 2011, Nokia-Siemens Networks announced that it would begin to reduce its business commitments in Iran and would no longer take on any new business with Iranian customers.

In 2009, the company strongly supported a law in its native Finland allowing for corporations to monitor the electronic correspondence of its workers. While the protection of trade secrets is a legitimate corporate goal, and similar activities are allowed in many European Union countries, Finnish culture is strongly in favor of privacy and the right to confidentiality. The campaign did little to reassure workers that the Nokia commitment to trust and open decision making was going to continue.

The last several years have also been a time of unprecedented financial upheaval for Nokia. Since 2009, Nokia has lost over a third of its revenues, downsized its workforce by about 25 percent, and seen its market capitalization drop by over $100 billion. While the Lumia line of smartphones continues to be the market leader in Europe, Nokia’s share of the U.S. market has dropped to less than one percent. The public’s response to Nokia’s poor ethical decisions has cost the company heavily. The question remains whether Nokia will learn from its current troubles and adapt quickly enough to satisfy its customers, shareholders, and other stakeholders.

a. Were Nokia’s leaders acting unethically when they moved their facilities from Germany to Romania and from Romania to Asia, or was this a legitimate business decision to reduce costs and improve profits? How does this decision compare with Nokia’s actions in Iran?

b. Why did Nokia’s customer base in Europe and Iran react to the company’s decisions by withdrawing patronage? Do customers always respond to unethical decisions in this way?

c. How difficult is it to ensure ethical decision making in a business that is organized as a “network of equals”? How does this impact accountability? Does this explain why Nokia kept the investigation secret?

**11. Is There a Place for Ethics in IT?**

On March 15, 2005, Michael Schrage published an article in CIO magazine entitled “Ethics, Schmethics,” which stirred up a great deal of controversy in the IT community. In the article, Schrage proposed that CIOs (chief information officers) “should stop trying to do the ‘right thing’ when implementing IT and focus instead on getting their implementations right.” Schrage argued that ethics had become a buzzword, just like quality in the 1980s; he asserted that the demand for ethical behavior interferes with business efficiency.

In the article, Schrage provided a few scenarios to back up his opinion. In one such example, a company is developing a customer relationship management (CRM) system, and the staff is working very hard to meet the deadline. The company plans to outsource the maintenance and support of the CRM system once it is developed, meaning that there is a good chance that two-thirds of the IT staff will be laid off. Would you disclose this information? Schrage answered, “I don’t think so.”

In another scenario, Schrage asked readers if they would consider deliberately withholding important information from their boss if they knew that its disclosure would provoke his or her immediate counterproductive intervention in an important project. Schrage said he would withhold it. Business involves competing values, he argued, and trade-offs must be made to keep business operations from becoming paralyzed.

Schrage was hit with a barrage of responses accusing him of being dishonorable, shortsighted, and lazy. Other feedback provided new perspectives on his scenarios that Schrage had not considered in his article. For example, an IT manager at Boise State University argued that doing the right thing is good for business. Not disclosing layoffs, she argued, is a trick that only works once. Remaining employees will no longer trust the company and may pursue jobs where they can feel more secure. New job applicants will think twice before joining a company with a reputation for exploiting employees. Other readers responded to that scenario by suggesting that the company could try to maintain loyalty by offering incentives for those who stayed or by providing job-placement services to departing employees.

Addressing the second scenario, another reader, Dewey, suggested that not giving the boss important information could backfire on the employee: “What if your boss finds out the truth? What if you were wrong and the boss could have helped? Once your boss knows that you lied once, will he believe you the next time?”

Another reader had actually worked under an unproductive, reactive, meddling boss. Based on his experience, he suggested speaking to the boss about the problem at an appropriate time and place. In addition, the reader explained that as situations arose that required him to convey important information that might elicit interference, he developed action plans and made firm presentations to his boss. The boss, the reader assured Schrage, will adapt.

Some readers argued that CIOs must consider the company’s long-term needs rather than just the current needs of a specific project. Others argued that engaging in unethical behavior, even for the best of purposes, crosses a line that eventually leads to more serious transgressions. Some readers suspected that Schrage had published the article to provoke outrage. Another reader agreed with Schrage, arguing that ethics has to “take a back seat to budgets and schedules” in a large organization. This reader explained, “At the end of the day, IT is business.”

a. Discuss how a CIO might handle Schrage’s scenarios using the suggested process for ethical decision making presented in this chapter.

b. Discuss the possible short-term losses and long-term gains in implementing ethical solutions for each of Schrage’s scenarios.

c. Must businesses choose between good ethics and financial benefits? Explain your answer using Schrage’s scenarios as examples.

d. What do you think Schrage means when he says that CIOs “should stop trying to do the ‘right thing’ when implementing IT and focus instead on getting their implementations right”? Do you agree?

12. Draft a legitimate-looking phishing email that would strongly tempt its recipients to click on a link to a Web site or open an email attachment.

13. What is the difference between industrial spying and the gathering of competitive intelligence? Is the use of competitive intelligence ethical or unethical? Why?

14. How would you distinguish between a hacktivist and a cyberterrorist? Should the use of hacktivists by a country against enemy organizations be considered an act of war? Why or why not? How about the use of cyberterrorists?

15. You are the CFO of a midsized manufacturing firm. You have heard nothing but positive comments about the new CIO you hired three months ago. As you watch her outline what needs to be done to improve the firm’s computer security, you are impressed with her energy, enthusiasm, and presentation skills. However, your jaw drops when she states that the total cost of the computer security improvements will be $300,000. This seems like a lot of money for security, given that your firm has had no major incident. Several other items in the budget will either have to be dropped or trimmed back to accommodate this project. In addition, the $300,000 is above your spending authorization and will require approval by the CEO. This will force you to defend the expenditure, and you are not sure how to do this. You wonder if this much spending on security is really required. How can you sort out what really needs to be done without appearing to be micromanaging or discouraging the new CIO? How do you proceed?

16. It appears that someone is using your firm’s corporate directory—which includes job titles and email addresses—to contact senior managers and directors via email. The email requests that the recipient click on a URL, which leads to a Web site that looks as if it were designed by your Human Resources organization. Once at this phony Website, the employees are asked to confirm the bank and account number to be used for electronic deposit of their annual bonus check. You are a member of IT security for the firm. What can you do?

17. You are a member of the application development organization for a small but rapidly growing software company that produces patient billing applications for doctors’ offices. During work on the next release of your firm’s first and only software product, you discover a small programming glitch in the current release that could pose a security risk to users. The probability of the problem being discovered is low, but, if it is exposed, the potential impact on your firm’s 100 or so customers could be substantial: Hackers could access private patient data and change billing records. The problem will be corrected in the next release, scheduled to come out in three months, but you are concerned about what should be done for the users of the current release. The problem has come at the worst possible time. The firm is currently seeking approval for a $10 million loan to raise enough cash to continue operations until revenue from the sales of its just-released product offsets expenses. In addition, the effort to develop and distribute the patch, to communicate with users, and to deal with any fallout will place a major drain on your small development staff, delaying the next software release by at least two months. You have your regularly scheduled quarterly meeting with the manager of application development this afternoon; what will you say about this problem?

**18. Defending Against Distributed Denial-of-Service Attacks**

A DDoS attack can easily cost an organization tens of thousands of dollars per minute in lost revenue and worker productivity. In addition, in the fallout from such an attack, an organization may find its customers switching to competitors due to a loss of confidence resulting from the bad publicity. Financial and travel service firms and various e-commerce Web sites are frequent targets of DDoS attacks.

During the fall of 2012, powerful DDoS attacks were directed at the Web servers of several major U.S. banks. The DDoS attack directed 65 Gbps of data traffic at each bank server—the network equivalent of an F5 hurricane—effectively making the server inaccessible to customers. The attack repeated itself at one bank after another. Over the course of a few weeks, Bank of America, Capital One, JPMorgan Chase, PNC Financial Services, Regions Financial, Sun Trust, US Bank, and Wells Fargo were all hit. Particularly alarming is that the banks were not able to completely fend off the attacks—the attackers simply stopped on their own to avoid being identified. The parties responsible for these attacks have not been positively identified, but suspects include Hamas, an Islamic group called the Izz ad-Din Al-Qassam Cyber Fighters, the hacktivist group Anonymous, cybercriminals based in Eastern Europe, and hackers in Saudi Arabia and Iran.

SpaFinder is a spa and wellness company that sells spa, wellness, and beauty gift cards and rewards programs that draw millions of clients to its global network of spas, fitness studios, and wellness practitioners. A recent DDoS attack hit SpaFinder’s 24/7 call center, making it impossible for customers to access the Web site to view content, make purchases, redeem gift certificates, or spend rewards points. SpaFinder’s Web hosting service was unable to deal with the attack. In desperation, SpaFinder technical support people contacted a DDoS mitigation service company that was able to get their site back up and running in less than 24 hours.

DDoS mitigation service organizations monitor clients’ network equipment for signs of a DDoS attack. If such an attack is detected, all traffic is rerouted from the client Web site to the service provider over a dedicated high-speed network link for traffic “scrubbing.” This process allows the service provider to use powerful servers to inspect the data traffic for anomalies. All legitimate traffic is forwarded back to the customer for routine processing; all attack traffic is dropped.

In addition to contracting with a DDoS mitigation service provider, security experts recommend that organizations (1) develop and practice a standard operating procedure to follow in the event of a DDoS attack; (2) maintain contact information for their ISP and hosting providers that includes names and phone numbers for whoever should be contacted during a DDoS attack and what information they will need; and (3) prioritize network services to identify what services could be turned off or blocked if needed to limit the effects of the attack.

a. Outline a quantitative approach for justifying the use of a DDoS mitigation service to protect an e-commerce company such as SpaFinder. Can you identify any nonfinancial reasons to subscribe to a DDoS mitigation service? If so, what are they?

b. Identify three potential kinds of DDoS attackers of an e-commerce company such as SpaFinder. What would be the motive for each of these attackers?

c. Do research on the Web to find three DDoS mitigation service providers. How are their services similar? How are they different? Which DDoS service provider do you think is the best?

**19. Anonymous and Social Hacktivism**

The popular conception of hackers is one of young men sitting in dark basement rooms for hours upon end, surrounded by empty takeout containers: alone and unaffiliated. Individual hackers rarely influence history, the actions of large corporations, or the governments of the world—unless they can somehow work together and form a collective. The hacktivist group Anonymous seems to have achieved this goal.

The group’s beginnings can be traced back to 2003, when individual hackers began posting proposals for collective action on an Internet forum called 4-chan, a simple image-based bulletin board where anyone can post comments and share images—and one of the least regulated parts of the Internet in the early 2000s. At first, the idea was the adoption of a decentralized online community that could act anonymously, but in a coordinated manner. Group actions were usually aligned toward some nebulous goal, with the primary focus being on the members’ own entertainment. For example, Anonymous members hacked the copy-protect codes of DVDs and video games and posted them online. This action enabled other hackers to disable the copy protection and copy these products for free. As the movement grew, some members began to see the potential for greater social and political activity, and social “hacktivism” was born.

Anonymous has no leader or formal decision-making mechanism. “Anyone who wants to can be Anonymous and work toward a set of goals…” a member of Anonymous explained. “We have this agenda that we all agree on and we all coordinate and act, but all act independently toward it, without any want for recognition. We just want to get something that we feel is important done…”

Anonymous’ first move toward a political action came in the form of a distributed denial-of-service (DDoS) attack on the Church of Scientology in 2008. The church had made an attempt to remove an interview with Tom Cruise, a famous church member, from the Internet. The church felt the video injured its image. It succeeded in removing the video from YouTube and other Web sites, but Anonymous posted the video on the Gawker Website. The effort gave Anonymous a sense of the power it could harness.

As the movement grew, Anonymous expanded its targets and attracted media attention. After the Website WikiLeaks, which relied on donations to support its operations, released large collections of classified American military documents and diplomatic cables, PayPal, MasterCard, and Bank of America announced that they would no longer process donations to WikiLeaks. This action threatened to put the WikiLeaks Website out of business. In response, Anonymous launched major DDoS attacks on the Web sites of these financial companies.

In 2012, Anonymous published the names and credit card information of the subscribers to a newsletter published by the international security think tank, Stratfor, which Anonymous viewed as a reactionary force both online and in the real world. Stratfor customer credit cards were used to make over $500,000 in fraudulent donations to various charities. Also in 2012, Anonymous attacked the regime of Syrian president Bashar al-Assad. In this instance, Anonymous went beyond DDoS attacks on government sites and actually set up satellite transmission stations in all the major cities across Syria to serve as independent media centers in anticipation of the Syrian government’s efforts to cut off its citizens from the Internet.

In response to the suicide of Internet activist Aaron Swartz in early 2013, Anonymous briefly corrupted the Web site of the U.S. Sentencing Commission and threatened to release sensitive information concerning the U.S. Department of Justice. Anonymous blamed the justice system for Swartz’s suicide, claiming that prosecutors were pursuing “highly disproportionate sentencing” in cases against some of its members and others, like Swartz, who championed open access to online documents. Swartz was facing federal charges that he stole millions of online documents and could have served up to 35 years in prison.

The group’s strategy of using DDoS attacks and publishing personal information is illegal and has exposed numerous members of the collective to police inquiry and legal problems. The Interpol international policing body has been particularly active in its pursuit of Anonymous members. In early 2012, as part of Interpol’s efforts, 25 Anonymous members were arrested in four different countries. Furthermore, an influential member of the collective, known online as “Sabu,” was recently outed as an FBI informant. After participating in the Stratfor hack, Sabu gave information to the FBI leading to the arrest of several Anonymous senior members. However, after the revelation that one of their own had cooperated with the FBI’s efforts against the group, one member posted the following: “Don’t you get it by now? #Anonymous is an idea. #Anonymous is a movement. It will keep growing, adapting and evolving, no matter what.”

a. If you had an opportunity to join Anonymous, would you? Why, or why not?

b. Would you say that Anonymous’ actions in support of WikiLeaks were legal? Were these actions ethical? What about their actions to set up satellite transmission stations across Syria?

c. How serious of a threat does Anonymous pose to organizational and government Websites?

**20. Computer Forensics**

On September 8, 2009, 25-year-old airport limousine driver and former coffee cart vendor Najibullah Zazi rented a car and drove from Denver to New York City. His car was laden with explosives and bomb-building materials. According to the Department of Justice, Zazi’s target was the New York City subway system. It is believed Zazi was planning to work with other operatives over the weekend and detonate the bomb the following week. However, after learning he was under investigation, Zazi dumped the evidence and fled back to Denver. On September 19, the FBI arrested him on charges of willfully making false statements to the FBI. Computer forensics investigators with the FBI found bomb-making instructions and Internet searches for hydrochloric acid on Zazi’s laptop computer. Investigators also processed video surveillance of Zazi buying large quantities of bomb-making materials at a beauty supply store. Zazi had also emailed himself detailed notes on constructing explosives during an Al Qaeda training session on constructing explosives that he had attended in Afghanistan in 2008. In February 2010, Zazi pled guilty to conspiracy to use weapons of mass destruction against persons or property in the United States, conspiracy to commit murder in a foreign country, and providing material support to Al Qaeda.

In November 2007, a 900-foot-long container ship traveling through dense fog struck the Bay Bridge in San Francisco Bay. Approximately 58,000 gallons of fuel oil seeped through the 100-foot gash in the hull into the water. Over 2,500 birds died during the spill, and wildlife experts estimated that a total of 20,000 perished as a result of the long-term chemical effects of oil exposure. Prosecutors alleged that the captain had failed to use radar and positional fixes or other official navigation aids. However, the crime extended beyond the captain’s negligence. Computer forensics investigators found that computer navigational charts had been doctored after the crash, and falsified records, such as passage planning checklists, had been created on ship computers after the crash. The captain was eventually sentenced to 10 months in federal prison after pleading guilty to violating the Clean Water Act and the Migratory Bird Treaty Act. In 2009, the ship’s management company, Fleet Management Company Ltd., agreed to pay $10 million in compensation for violating the Oil Pollution Act of 1990. These two high-profile cases illustrate the central role computer forensics investigators are playing in criminal investigations today. These investigators are at work in both criminal and civil cases exploring everything from murder, kidnapping, and robbery to money laundering and fraud to public corruption, intellectual property theft, and destruction of property by disgruntled employees. Even parties to divorce cases are now making use of computer forensics experts to uncover evidence of infidelity or locate joint funds that have been hidden by one of the spouses.

Yet perhaps the greatest promise of this fast-developing field of investigation is its potential for preventing crime. On November 18, 2010, police arrested a Florida college student, Daniel Alexander Shana, who had posted on Facebook his plans for carrying out a Columbine High School–type massacre to target people who he felt had bullied him. He boasted that he had purchased a semiautomatic pistol and had registered for a firearms license. Students viewing his Facebook posts reported them to authorities.70 Computer forensics investigators found that he had viewed videos on Columbine and looked into how to purchase weapons and carry out murder.

As the role of computer forensics has expanded in criminal and civil investigations, the number of jobs available in the fields has grown. The Bureau of Labor Statistics predicts that employment in the field of private detectives and investigators in general will grow by 22 percent between 2008 and 2018. To meet this demand, a number of universities have begun offering undergraduate and graduate degrees in computer forensics. Computer forensics investigators not only analyze, recover, and present data for use as evidence, but also recover emails, passwords, and encrypted or erased data. They must detect intrusions and probe them. Hence, computer forensics investigators require specialized hardware and software, and they must master specific methods and techniques. That said, the Bureau of Labor Statistics advises that a degree in computer science or accounting is more helpful than a degree in criminal justice.

Most computer forensics professionals enter the field by getting a job with a law enforcement agency and receiving training while on the job. In addition, universities also offer certificates in computer forensics for those already working in the field, and professional organizations host seminars where people interested in the field can gain expertise. Professionals already working in the field can complete a certificate through an online program.

Once computer forensics professionals gain sufficient on-the-job experience, they frequently branch out into the private sector. Licensing requirements vary from state to state, and certification requirements vary from one professional organization to another. The Bureau of Labor Statistics reported that the median salary for private detectives and investigators in 2010 was $42,870. Although the bureau did not track salary information specifically for a computer forensics investigator, professionals in specialized fields are often able to demand higher compensation.

Most importantly, the Bureau of Labor Statistics reported that job competition in this area is keen. With high-profile cases such as the New York subway bomber and television shows romanticizing the role of computer forensics investigators, it’s no wonder people are flocking to the field. Yet even if computer forensics isn’t as powerful or glamorous as it appears on TV, the field is becoming more critical to criminal investigation, and increasing expertise will be required as cybercriminals develop more sophisticated means of attack.

a. What role did computer forensics play in the high-profile cases of the New York subway bomber and the San Francisco Bay oil spill?

b. Why might computer forensics be more effective at preventing crimes than other forms of criminal investigation?

c. In addition to computer-related training, what other education and background would be ideal for someone who wants to make a career in computer forensics?