Ethics

lam Encryption Export Rules," *Com-*

s, 2001), p. 306.
formationWeek (1 October 2001), pp.

6

Security and Cybercrime

Computer security problems have a long and complex history—the disruption of operations through viruses, worms, and logic bombs along with unauthorized access have plagued computer users for many years. These problems are not trivial and can cause serious economic harm. The infamous "ILoveYou" virus unleashed across the Web in 2000 is estimated to have cost about $11 billion. Denial of Service (DoS) attacks are one of the newer weapons deployed against commercial Web sites. These attacks overwhelm Web servers with fake requests from hijacked personal computers all over the world. As a result, real customers cannot access these sites and business is lost. Particular concerns have recently arisen about the growing threat of cyberterrorism. Digital assaults on the Internet infrastructure could have potentially devastating consequences.

There is also evidence that hacker attacks are on the rise. The Software Engineering Institute's CERT Coordination Center reported that attacks have grown from 6 in 1988 to 52,658 in 2001. The number of incidents reported to CERT in 2001 has almost doubled from what was reported in 2000 and increased steadily in the last five years.[1] While some of this may be due to greater public awareness of security breaches, the trend is still quite alarming.

Most companies recognize that for purely pragmatic reasons their business demands careful attention to security issues. But it should not be overlooked that there is also a moral responsibility to ensure that systems are secure and that data is adequately protected. This responsibility stems from the fact that careless or shoddy security procedures could allow sensitive data to fall into the wrong hands and thereby cause considerable injury for the data subjects. For instance, if careless security allows intruders access to financial records or credit card numbers, innocent people could easily be victimized.

Yet despite persistent security breaches, security remains all too lax. A security study conducted by Cisco found vulnerabilities in each of the 33 sites examined by Cisco. The study further found that these vulnerabilities "could be traced to outdated software or lax system administration maintenance, not to inherent flaws in the systems."[2] Businesses are slowly learning that they must devote more resources to protecting their Web sites and networks.

Many security breaches are caused by hackers, and some hackers have insisted that most of their intrusive activities do no real harm and do not constitute a serious ethical transgression.[3] But is there any merit to this claim? Also, how do we measure the damage caused by such intruders? If no files or data have been stolen or corrupted, does this mean that the intrusion should be dismissed as insignificant?

The cases in this chapter will take into account all of these issues. They will explicitly consider the moral challenge of ensuring a secure environment along with questions about the gravity of unauthorized access and the appropriate penalties for those who are culpable of violating another's property rights.

Most experts agree that the biggest threat to information technology security is still from within the organization. Many troubling questions come to the surface in the first case of the chapter called "The Disgruntled Consultant." After an employee is terminated, he corrupts a system scheduled for immediate delivery to a major client. What is the company's responsibility for the actions of this rogue employee and is there some obligation to compensate the injured party?

In the next case, "Security Breach at IKON," a company must decide what to do when customer data is inadvertently exposed. Among other issues, this case raises the question of what constitutes "adequate" security for a commercial Web site.

The other four cases in this section shift away from this corporate focus and deal with the hacker phenomenon. In the hypothetical case entitled "A Harmless Prank" university officials must determine a fitting punishment for a clever but penitent student hacker. Electronic trespassing

is a serious offense and it's important to send a strong signal, but extenuating circumstances make it difficult to arrive at a just and fair decision.

Similar questions arise in a case called "Interview with a Hacker," which presents a view of this subculture through the eyes of one of its former members. He articulates the so-called "hacker ethic" that one can look around on the Internet but not destroy someone else's data. Other opinions are expressed in the interview about this culture and its norms of behavior.

The case about Craig Niedorf, a young man arrested for propagating a secret text file on the Internet, deals with the government's apparent overreaction to the misappropriation of sensitive information. How much power should the government have to curtail activities and set limits on the mysterious new frontiers of cyberspace? This case bears some similarity to "Piracy on the Internet" in Chapter 3, since it too deals with some key civil liberties issues.

Finally, "Hacktivism" considers whether hacking can be morally justified as a form of civil disobedience. In this case a political activist faces criminal charges for defacing the Web site of a power company but argues that he acted to protest this company's questionable environmental policies.

Case 6.1 The Disgruntled Consultant

Donald Chase had just celebrated his tenth anniversary at TTI Consulting when he received the bad news. Due to declining revenues and a shrinking customer base he was one of seven consultants who was being dismissed. His boss, Dr. Phillip Bluestein, informed Chase at 11:00 A.M. on Tuesday that his services were no longer needed. Dr. Bluestein had usually been rather abrupt in his dealings with subordinates, and unfortunately this situation was no different. Chase was told to pack his things and clear out of the building by noon.

Crestfallen, Chase returned to his small office on the third floor of the TTI building. He struggled to suppress his anger and resentment. He had given his heart and soul to this company during the last 10 years and felt betrayed by this sudden dismissal. These feelings were perhaps accentuated because he had just recently completed a major project for one of TTI's established clients, the Northwest Commerce Bank. He had worked long hours and weekends to finish its complex cash management application on schedule. Chase had completed this sophisticated

program only several days ago, and during a brief internal demo he had received considerable praise from upper management including Dr. Bluestein. Managers at Northwest were eagerly awaiting delivery since they estimated that this new system would save the bank about $60,000 a month thanks to more efficient cash management.

However, at the time of Chase's dismissal the application had not yet been delivered to the client. It remained on Chase's IBM PC which was linked to the company's extensive client/server network. Chase kept the only backup copy of this system in his brief case; this had enabled him to work on the application at home at his convenience.

As Chase began packing his belongings, Dr. Bluestein appeared at the doorway. They briefly discussed the Commerce Bank application, and Chase pointed out to Bluestein how the application could be accessed on his PC. This discussion was followed by a cursory overview of the programs that comprised this system. It appeared to Chase that Bluestein wanted to make sure that everything was in tact for the system's imminent delivery to Commerce Bank. Bluestein remained with Chase as he finished packing a few boxes of books and other materials. Chase then put only a few additional items in his brief case and left his office followed by Bluestein He did not return the backup copy of the Commerce Bank system. After saying goodbye to a few friends, Chase left the building and drove home.

Upon his return home Chase decided to seek revenge on his ungrateful employer. He used his PC to connect to the company computer system, entered his user ID and password, and accessed the only copy of the Commerce Bank application. He proceeded swiftly to disable several key programs by inserting some code that subverted the display of menu screens and corrupted data. Chase also had the presence of mind to cover his tracks by erasing the audit file that accompanied the program; thus there was no record of this unauthorized access to this application.

Executives at TTI were not aware of what had happened until two days later when an associate of Chase proceeded to do one final quality assurance test before final delivery of the program to the bank. When she logged in to the application, she quickly realized that it had been tampered with and called Dr. Bluestein who strongly suspected sabotage. He immediately and repeatedly called Chase's residence but there was no answer; also Chase's large severance check had already been cashed.

As Commerce Bank waited patiently for its cash management system, the company quickly launched an internal investigation. It was apparent that the layoffs represented a chaotic situation within TTI; as a result, there was inadequate communication between certain departments. For example, the company's security manager had not been in-

ing a brief internal demo he had
per management including Dr.
eagerly awaiting delivery since
uld save the bank about $60,000
anagement.
smissal the application had not
ined on Chase's IBM PC which
client/server network. Chase
n in his brief case; this had en-
nome at his convenience.
gings, Dr. Bluestein appeared at
e Commerce Bank application,
w the application could be ac-
lowed by a cursory overview of
m. It appeared to Chase that
ything was in tact for the sys-
Bank. Bluestein remained with
s of books and other materials.
ns in his brief case and left his
return the backup copy of the
odbye to a few friends, Chase

ed to seek revenge on his un-
nect to the company computer
and accessed the only copy of
eded swiftly to disable several
subverted the display of menu
l the presence of mind to cover
companied the program; thus
cess to this application.
what had happened until two
eeded to do one final quality
rogram to the bank. When she
ealized that it had been tam-
ongly suspected sabotage. He
s residence but there was no
had already been cashed.
for its cash management sys-
nternal investigation. It was
otic situation within TTI; as a
ion between certain depart-
y manager had not been in-

formed about the layoffs until the day after they had occurred. At that point user IDs and passwords for the discharged employees were revoked. However, this was much too late to save the Commerce Bank application from this deliberate act of sabotage. When asked by the executive vice president about this communication failure, the human resources manager informed her that his department had never coordinated layoffs and dismissals with the security manager. "We've never had the sense in this company that we should lock the gates and put up barricades when people leave," he said; "Our employees are trusted colleagues even after they've been let go."

As the investigation continued, Dr. Bluestein faced a difficult decision about how he would deal with his contact at the Commerce Bank who was eagerly awaiting the cash management program that was now overdue. Chase was an especially clever and adept programmer and consequently Bluestein estimated that it would take at least several weeks to unearth the bugs and fix the system properly. Also, all of the other consultants were assigned to high-priority projects, so there might be some delay in getting started on this work.

Bluestein wondered what he should tell the people at Commerce. Should he be candid about the company's untimely security lapse? Commerce was one of TTI's most security-conscious customers, and hence this revelation might jeopardize lucrative future contracts. But Commerce had been told last week that the project was finished and that they would receive it right on time. How, then, could he explain what could have gone wrong to delay delivery by several weeks and maybe longer? Also, Bluestein wondered about the corporation's legal and moral responsibility for what had happened. Chase was clearly the main culprit here, but to what extent was the corporation also liable for his transgression? And if the company were liable, should it make some restitution to its customer whose business was adversely affected because of this mishap? Bluestein began sorting through all these questions as he stared at the pink phone messages in front of him.

Case 6.2 Security Breach at IKON[4]

Chester Davis was not looking forward to an emergency meeting of the Information Technology (IT) staff. It was just about 9:00 A.M. when he entered the third-floor conference room and the meeting was just about to get underway. He poured some coffee and took one of the

few remaining seats around the walnut conference table. He gazed at the putty-colored walls and pulled out his notes relating to today's topic: a gaping security hole at the company's Web site.

Davis worked in the IT department of a specialty clothing store called IKON. It was founded in 1988 and enjoyed an excellent reputation among young, upscale consumers. IKON had 227 stores located throughout the east and southeast with projected 2002 sales of $650 million. But despite IKON's success and profitability, the company lagged behind in the area of electronic commerce.

IKON had waited until 1999 before embarking on a project to build a B2C (business to consumer) Web site where customers could place orders or obtain product information and catalogs. Finally, in early 2000 the company's Web site was made available to much fanfare and even critical acclaim—the Web site team invested heavily in aesthetics and the site stood out among competitors' plainer looking sites. Unfortunately, less attention was paid to the Web site's security.

Brian Dobson, the associate VP for information technology, was the Web site development team's leader and Davis was in charge of security issues. Davis recalled a conversation with Dobson about the security planned for the Web site. At their initial planning meeting Dobson had laid out his views on security:

> Security should not be a big deal for a project like this. Just make sure that the application is restricted to authorized users and that the network is reasonably secure. Nothing too fancy, Chester, because we just don't have the time or the funding.

But Davis had been insistent that more needed to be done.

> I'm afraid that I can't agree with you, Brian. I have developed a comprehensive security plan with a good deal of emphasis on network security and detection measures. My plan calls for a managed firewall, intrusion detection,[5] authentication through passwords, and antivirus services. I also think that we should do vulnerability assessment, a periodic probing of the system to reveal any weaknesses. Also, my plan calls for ongoing security testing as new applications or servers are added to make sure that security holes have not opened up. Finally I think it would be prudent to subscribe to a security intelligence service that will notify us of potential threats or newly uncovered vulnerabilities in systems or hardware.

Dobson picked up the security specs and associated cost estimates from a pile of folders on his desk. He studied them for a few minutes and then said,

I've just been looking over these specs, and I think that the level of security which you are proposing is unnecessary. It's overkill. Also, let me point out, that nobody higher up at IKON is pushing for this kind of security. It doesn't seem to be a big deal for them. We obviously need a firewall, authentication, and virus protection, but let's knock off the intrusion detection. This would require heavy IT resources to be able to differentiate between normal traffic and an intrusion. Also, we'll do a full security audit before we launch, but we do not have the resources to continue testing for security breaches. Finally, I am not going to authorize a subscription to some security intelligence service—it's too expensive.

Davis raised some further objections but to no avail, and Dobson's security scheme was adopted.

It was now a year and a half later as the IT team assembled to discuss a major security breach at the IKON Web site. Dobson revealed that thousands of customer files on the Web site had somehow become exposed. A customer, who reported the security breach, was requesting a catalog and received an error message. That message showed him the way to the IKON database where he was able to peruse the names, addresses, phone numbers, e-mail addresses, and in some cases the credit card numbers of IKON's on-line customers. That database included over 100,000 names. No one yet knew the exact cause of the breach, how long it had existed, or whether other customers had accessed this data. Dobson had called in an outside security consultant and her initial assessment was that a series of changes recently undertaken by IKON may have led to the problem. The Web site had recently gotten a new "look" and links to several new partners had been added; a new server was also added to the configuration for load balancing. A security patch was quickly developed to provide a temporary fix for the problem.

As the meeting came to an end, Dobson turned to his team for some advice. He had a meeting scheduled for that afternoon with the company's chief operating officer to review the damage. The company had to decide whether or not to tell its customers about the security breach, since their personal data may have been exposed to hackers. What would such a revelation do to IKON's credibility? How should customers be informed about this? What might IKON say to allay their concerns about the prospect of future problems? IT also needed to develop a plan so that the probability of this happening again in the future would be minimized. Someone suggested that outsourcing security might be the answer.

Davis was pretty silent during the meeting, but he was surprised at Dobson's final comment that this incident should not reflect on the work of the development team which had incorporated "adequate" security

procedures into the Web site design. As Dobson saw it, this security breach was just an unavoidable fluke.

Case 6.3 A Harmless Prank

Steven Mackey was a junior and a computer science major at Riverview State College, a moderate-size four-year college located in the Midwest. He had worked with computers since childhood and he chose to attend Riverview because of its excellent computer science department. He consistently received good grades and he was highly regarded by the department and its faculty. During this second semester of his junior year he was learning two new computer languages, C++ and JAVA, and he was taking a difficult course on compilers.

Steven was also known among his friends and fellow computer science students as a typical "hacker." He enjoyed traversing through the Internet, especially at night, and he sometimes boasted about his ability to crack codes and break into computer systems that he had not been authorized to use. Some of the other students in the computer science department admired Steven's antics; in their eyes these transgressions merely confirmed his technical expertise. Steven's exploits were also well known around other circles of the campus, but since he had not tampered with any university systems he was never reprimanded by faculty or administrators.

One late evening in April just three weeks before Riverview's final exams, Steven and his girlfriend decided to see if they could tap into the administrative network at Riverview. This network included the files of the administrators at Chauncey Hall who were responsible for managing the financial affairs of the university. Many of these files contained confidential data about university finances or personnel matters. Steven was most interested in the payroll file which included the salaries of all Riverview employees, including the faculty. He was not interested so much in looking at those salaries but in demonstrating his exceptional ability by cracking the passwords to this file. His interest in doing this was stimulated by one of his professors who mentioned that he had helped design the security system for this file and that he considered it virtually impregnable. Steven construed this boasting as a challenge to the class, while others seemed to pay little attention to this remark.

But Steven was intrigued and excited about this challenge. He worked for four and a half hours to achieve this objective. It was rela-

tively easy to tap into the university network since its security was rather weak. But the payroll file did prove to be another matter. Steven ran algorithms used to crack passwords, but they kept failing. Eventually, however, through sheer ingenuity and persistence he broke the code and gained access to the file. He was so elated that he didn't even bother to look at any of the salaries or the other information maintained there. By now he was so exhausted that he simply logged off the computer and went to sleep.

The next day the system administrator found evidence that there had been an unauthorized entry into the IBM mainframe's CICS system at 2:36 A.M. She also detected that the payroll file had been accessed, but that no individual records had been read. University officials and campus police were notified immediately, and they were quickly able to trace this intrusion to Stephen's computer. No one was surprised that Stephen was the culprit, given his penchant for this sort of activity.

Stephen was summoned before the dean of students, Dr. Lillian Green, who confronted him with the overwhelming evidence. In his defense Stephen sheepishly claimed that this was a harmless incident, "just a prank," which merely disproved his professor's contention that the payroll file was "virtually impregnable." He claimed that gaining entry to a supposedly secure system was both a hobby and a challenge. Indeed, Stephen argued, he had done the university a favor by exposing the vulnerability of this file which was hitherto thought to be so secure. Furthemore, he pointed out that he did not look at any of the payroll data, and finally, he gave to the dean some specific instructions on how to buttress security for the administrative network. He said he had been formulating these recommendations since the morning after his break-in.

Dean Green became less hostile as the meeting proceeded since she saw that Steven was not a mean or especially devious person. Moreover, she appreciated his candor and sincerity. Prior to the meeting with Stephen she had reviewed his academic record and ascertained that he had a 3.4 grade point average and that he had not been subject to any disciplinary actions during his enrollment at Riverview. Given this and Stephen's contriteness, she was inclined to be somewhat lenient with him.

Nevertheless, this unfortunate incident was not viewed so benignly by college administrators who were furious over the break-in. Also, whatever sanctions were imposed on Stephen would be construed as an important signal from the dean's office. There was some apprehension that others might try to mimic Stephen's exploits.

After Stephen completed this explanation of his actions, he apologized and promised not to try this again. Dean Green thanked him for

his cooperation and honesty, but she also pointed out that this was a serious offense that the university could not take lightly. She told him that her assistant would call him tomorrow to set up a second appointment. At that time she would discuss the university's decision regarding an appropriate penalty for his actions.

Later that day in the faculty dining room she discussed the young man's plight with a small group of administrators and faculty members. Some of her colleagues felt that a stern lecture and a warning to Stephen were sufficient. But others felt that a more severe punishment was in order, perhaps even suspension for a semester. One person said that he would have no qualms expelling a student for doing this. Such a bold action would send a clear message to other "hackers" on campus that this sort of antisocial and deviant behavior would not be tolerated. The dean listened carefully to this advice as she tried to decide how the university should deal with "on-line offenders" such as Stephen.

Case 6.4 Interview with a Hacker

> hacker n. . . . [depracated] A malicious meddler who tries to discover sensitive information by poking around.[6]

In February 1995 the author interviewed Ed Jones (fictitious name), a professional computer programmer who also describes himself as a "hacker." Mr. Jones is a 28-year-old college graduate who was often described as a computer "genius" as far back as the eighth grade. During his high school and college days he worked with computers incessantly. In the following interview he is asked some pointed and specific questions about his experiences and his overall philosophy of computers, the Internet, and many other topics.

The interview has been edited and condensed by the author.

***Question*: Mr. Jones, how would you describe a hacker today?**

When most of us on the net use the term "hacker," we're simply referring to a person who enjoys programming, a person who enjoys solving computer problems and puzzles. Hackers love to focus intently on a problem—it's called being in hack mode and it's almost a mystical experience for some of us. For most hackers their lives revolve around a computer and their community is the electronic network.