

Article from SIRS Discoverer Database; (ProQuest) Lexile:1170L

Cyber Sleuths

CAREER WORLD
(Vol. 34, No. 1)
Sept. 2005, pp. 6+

Copyright © Weekly Reader Corporation. September 2005. All rights reserved. Reprinted with permission.

Cyber Sleuths

By Carole Moore

- *Help wanted: Computer experts to purge hackers and other criminals from our digital systems*

Do you want to foil evil plots, hunt international criminals, and bring bad guys to justice? You don't need a big red S on your chest. Instead, become a cybersleuth and solve crimes like the computer crash that cost one travel company a small fortune.

[\(See picture, "Man Using a Computer."\)](#)

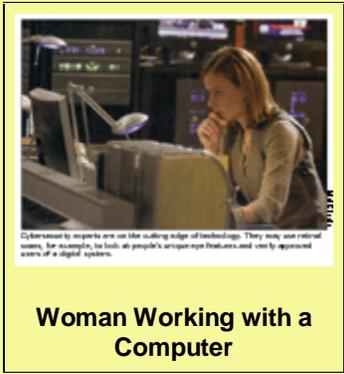
How long was the company's site off-line? Only two hours. How much money did the company lose? A whopping \$10,000 per minute. "A big virus outbreak literally brought down their Web page," says Scott Newman, head of the information technology program at Oklahoma State University at Okmulgee. "They couldn't communicate with the outside world." In the end, that break-in and the resulting lack of communication cost the company a cool \$1.2 million.



Cybersecurity problems such as that one keep the information security field hotter than a jar of jalapeno peppers. If you want to get in on the action, read on to see if cybersecurity is the right career for you.

A Wide-Open Field

Cybersecurity technicians go by various names, including information assurance specialists. They use their knowledge of encryption to secure information infrastructures. The work can involve anything from restoring hacked systems to chasing cyberterrorists. They work for private companies and government agencies worldwide and must stay current with brand-new technology.



Woman Working with a Computer

[\(See picture, "Woman Working with a Computer."\)](#)

Some entered the field because their employers needed cybersecurity and sent them for training. Others dove in as teenagers. For example, Christopher Klaus founded an Internet-based security firm when he was still in high school. The firm became a great success, and Klaus donated \$15 million to Georgia Tech University in 2000--not bad for a kid who once described himself as a "science nerd." Today, Klaus's company, Internet Security Systems, is a leader in the field of corporate cybersecurity.

Corporate security is only one slice of the cybersecurity pie. Lance Hawk, a Philadelphia-based computer forensics expert who trains investigators for law enforcement agencies, says the field is crammed with career choices. Hawk says the demand is high for specialties ranging from detecting and countering computer viruses, worms, "Trojan horses," and spyware to cracking cases of cyberfraud (using a computer to steal property or services).

"Right now [cybersecurity] is one of the top jobs in the FBI," Hawk says. Applicants usually must be 23 years old, but the need for experts in this area is so great that the Federal Bureau of Investigation is making exceptions to that requirement.

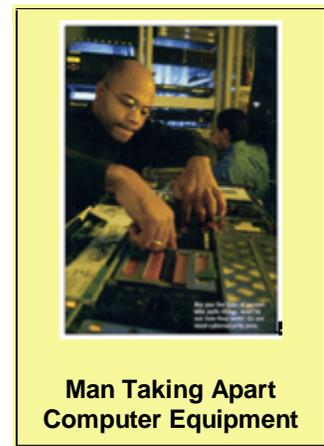
Hot, Hot, Hot...with Salaries to Match

The FBI isn't the only agency with this profession at the top of its most-wanted employee list. Almost every federal, state, and local government agency--including the U.S. armed forces--needs skilled cyberinvestigators. At some colleges, students interested in cybersecurity can apply for a program called Scholarship for Service (SFS), funded by the National Science Foundation. SFS pays for books and tuition and provides students with an allowance and a summer internship. In return, SFS recipients must work for the government for two years. (For more information, visit www.sfs.opm.gov.)

[\(See picture, "Man Taking Apart Computer Equipment."\)](#)

Martin Goslar of Phoenix, Ariz., is the principal analyst for E-PHD, a cybersecurity research and analysis company. Goslar says salaries for qualified, experienced cybersecurity analysts can range from \$70,000 to \$90,000 a year--with corporations paying their chief security officers even more. "This is a job that requires brains," Goslar says. "You need a logical, rational, mathematically oriented mind-set."

Oklahoma State's Newman says the best candidates for success in the field are those who not only enjoy technology but also respect its technical side. Individuals who simply like cruising the Internet probably won't find a home here. This field is for people who like to take the computer apart. "They're people who are curious, the ones who like to tinker with stuff and see how it works," Newman says. Indeed, security specialists learn to collect evidence from a computer by taking it apart and removing storage devices for analysis.



Man Taking Apart Computer Equipment

Science, Math, and Language

If you like a mental challenge, then this field may be for you. This highly demanding profession requires a solid education in a variety of areas. Hawk outlines minimum studies for students planning to enter the field: keyboarding, logic classes, investigative techniques, PowerPoint, and other

presentation methods. "Make sure you take all the science, math, and computer classes you can," Goslar advises.

As for education, he says, a community college can be a good place to begin. Many universities, including Oklahoma State University, provide degree programs in information assurance and forensics. Other schools offer information technology majors with course work in security. Some technicians complete postgraduate work.

Hawk adds, "Take a second language." The potential for dealing with international cases is strong in this field. "Spanish has helped me a million times," he says.

What else is a budding cybersecurity specialist expected to know? The answer may surprise you. "Ethics. It's so easy to cross the line from an ethical standpoint in this business," Hawk says. For example, in order to learn how to combat hackers, you need to know what hackers know--without using that information to break the law.

A World of Opportunity

Cybersecurity is one field where the possibilities truly are endless. When hotel heir Paris Hilton's cell phone address book was hacked and the contents disseminated on the Internet, cybersecurity technicians conducted the investigation.



Hilton, Paris: Talking on a Cellular Phone

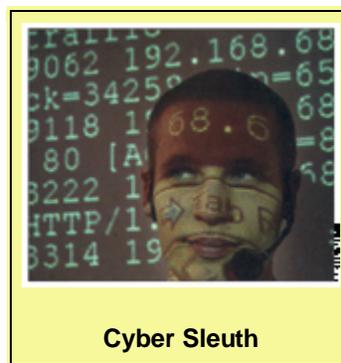
[\(See picture, "Hilton, Paris: Talking on a Cellular Phone."\)](#)

Think the field is limited to chasing hackers and rooting out new viruses? Not so. Some of the types of cases handled by cybersecurity pros include cybervandalism, theft of information, industrial espionage, cyberterrorism, financial fraud, unauthorized access by insiders, sabotage, spamming, spoofing, browser attacks, telecommunications eavesdropping, misleading HTMLs, online predators, cyberstalking, cyberextortion--to name a few.

[\(See picture, "Cyber Sleuth."\)](#)

Those who want to be their own bosses can also find a niche in this field. Charles "Buck" Fleming heads up a nonprofit agency called the Cyber Incident Detection and Data Analysis Center (CIDDAC), which bridges the gap between law enforcement and corporations.

The key to the agency's success is opportunity. "We saw a need and filled it," Fleming says. CIDDAC helps track down hackers while keeping the victims anonymous. Private companies, like banks, do not want anyone to know that someone has hacked into their databases. Law enforcement officers can't chase criminals without information. CIDDAC sets up a false portal that obscures a company's real portal. When a hacker breaks in, he or she doesn't get any information, but the information surrounding the break-in is passed to the appropriate law enforcement agency without letting the public know the company's identity.



Cyber Sleuth

As technology develops and becomes more complex, you may find and meet a particular need, as Fleming and Klaus did.

Dot-Com or Bust

Unlike the dot-com bust of the 1990s, when so many Internet-based businesses went belly-up and cost thousands of people their jobs, experts say the cybersecurity field will be around--and flourishing--for a long time.

Although many information technology jobs have been outsourced to India and other countries, few security positions have moved outside the United States. And because the needs of the cybersecurity field grow every day, the profession is not likely to become overcrowded soon.

Is Cybersecurity for You?

It might be, if you

- like math, science, and **computers**.
- want to know how **computers** work.
- want to continue your education after you find a job.
- can speak comfortably in front of others.
- have the patience to solve complicated puzzles.

Discuss

- Why is the cybersecurity field growing?
- What academic subjects do you think you should study to prepare for this field?
- Why, according to Lance Hawk, are ethics so important in this profession?

Do

Ask students to find newspaper and magazine articles that demonstrate cybersecurity professionals at work. In writing or as a class presentation, have students explain the problem and describe how the cybersecurity experts contributed (or were in the process of contributing) to the solution.

Resources

Cool Careers for Girls in Cybersecurity and National Safety, by Linda Thornburg (Impact, 2004), follows the career paths of 10 women in the information security field.

Students with a growing interest in computer technology can learn basic information about how viruses work, how the Internet works, how hard drives work--all at **computer.howstuffworks.com**.

More technologically advanced students with an interest in cybersecurity can visit **SecurityFocus.com**, a Web site that offers a peek into the field of information security and features job listings.

Another Web site for advanced students is **www.thei3p.org/news/today.html**, a daily news site from the Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College.