Chapter 7
Securing Information Systems

LEARNING TRACK 1: THE BOOMING JOB MARKET IN IT SECURITY

The technology industry has experienced its share of ups and downs over the last decade, from the initial dot-com boom to the dot-com bust, and back to the current rise of next-generation online businesses. One area of technology that has not been characterized by inconsistent levels of prosperity is information technology security.

As more and more bricks-and-mortar companies took their business online and relied on network and Internet technology for communications and productivity, protecting the business interests that run on these technologies became a priority. Even during the years when tech stocks were down and Internet startups were falling off the map, the security industry managed to grow. Boosting the industry even further was an increased focus on IT security after September 11, 2001, a focus that remains in effect today.

Following the 9/11 terrorist attacks, many companies took a closer look at their security requirements. Firms that specialized in providing network security services saw an increase in demand for enterprise security evaluations. The scope of a proper security strategy is wide and can include everything from suitable locks on entrance and storage room doors to intricate pass codes for access to network resources. Companies sought to insulate their physical infrastructures as well as their vital data from harm. Within a few years, however, many businesses were forced to scale back their security budgets as economic conditions turned unfavorable. The trend turned to hiring application or system specific experts with less of an eye toward security.

In 2007, the demand for qualified IT security workers reached levels that were reminiscent of the period directly following 9/11. A report released by the research firm Foote Partners stated that salaries for certified security technologists increased by two percent in the first half of the year. It had been more than a year since this group of workers had registered a measurable increase in compensation. The competition to hire systems administrators and database analysts who are highly skilled in technical disciplines and security techniques has reached a feverish pitch.

One force behind this renaissance in IT security was identity theft. The price of IT security became more palatable as the cost of security lapses grew. Companies like TJ Maxx, ChoicePoint, and CardSystems suffered significant economic and reputational losses when they failed to protect the credit card data of tens of millions of customers. Even the United States government sensed the urgency and instituted a commercial certification requirement for all IT workers and contractors at the Department of Defense.

To prevent attacks on their businesses, some companies are looking for IT security personnel with backgrounds in white-hat hacking and computer forensics, among other skills. Developing such skills is viewed as crucial for future chief security officers (CSOs) if they are going to defend their employers' business interests from cyber-attacks.

To support the development of such careers, EC-Council, a professional association for e-business and security professionals, has added a Master of Security Science program to its EC-Council University training curriculum. The program covers cyber-

law, disaster recovery, e-business security, IT security project management, as well as security for Linux, networks, programming, and wireless installations. The students in this master's program already possess undergraduate degrees in computer science or IT security. The University aims to create a new front line of CSOs and highly skilled security executives. The program requires only part-time study so that students can continue to log real-world experiences as they complete the degree.

EC-Council does not guarantee job placement. According to Stephen Northcutt, president of SANS Technology Institute, finding employment should not be a problem. SANS awards graduate degrees in information security under the authority of the Maryland Higher Education Commission. Regarding his organization and EC-Council, Northcutt says, "if we are both wildly successful, we will fulfill perhaps 1% of the market's true need."

Whereas most advanced IT degrees relegate security to the second tier of learning, EC-Council's program places security training at the forefront. For an IT worker, an education in ethical hacking provides great insight into the approach of criminal hackers. Jay Bavisi, the president of EC-Council, hopes to encourage more companies to create positions for well-armed CSOs. He preaches, "the benefit of having a CSO with a Master of Security Science degree is that you will bridge the digital divide between security executives and their technical teams."

Professional security certification is definitely high on the list for employers with IT security jobs to fill. One tool that hiring managers have at their disposal is the Certified Information Systems Security Professional (CISSP) exam, which is a six-hour maximum, multiple-choice test sponsored by the International Information Systems Security Certification Consortium (ISC)2, an industry group. (ISC)2 has established a matrix of security disciplines, which is called the Ten Domains of Security. The exam focuses on these ten domains.

TABLE 1 The Ten Domains of Security

Domain	Key Topics
Access Control Systems & Methodology	Preventive, detective, and corrective access control, identificatio, and authentication
Applications & Systems Development	Key security issues at each phase of the software development cycle.
Business Continuity Planning	Four phases of business continuity planning; disaster recovery planning.
Cryptography	Encryption: symmetrical and asymmetrical.
Law, Investigation, and Ethics	Comprehension of laws related to information security and computer crimes; code of ethics.
Operations Security	Implementing the appropriate controls for hardware, software, and other resources; auditing and monitoring; evaluating threats and vulnerabilities.
Physical Security	Identifying threats and vulnerabilities in the information system's environment; protecting the system from threats.
Security Architecture & Models	Configuring security for specific information systems; models: access control, inteigrity, and information flow.
Security Management Practices	Key concepts, controls, and definitions for security practices, including the confidentiality, integrity, and availability triad (CIA), risk analysis, classification of data, documentation, and awareness.
Telecommunications, Network, and Internet Security	Network structures, communication methods, data transport protocols, network and transmission security.

The prerequisites for applying to take the CISSP exam are stringent. To be eligible for the exam, applicants must commit to the (ISC)2 Code of Ethics and have at least five years of "direct full-time security professional work experience" in a minimum of two of the ten security domains. Applicants may reduce the work experience requirement by up to two years-one year for a four-year college degree or a master's degree in information security earned from a U.S. Center of National Excellence in Information Security (or regional equivalent); and one year for possessing another approved and relevant (ISC)2 certification.

The fee for the CISSP exam is $499 for early registration and $599 for standard registration (within 16 days of the exam). Passing scores generally fall in the 70%-80% range, and fewer than 8 percent of exam takers score above 85% due to the expanse of knowledge covered on the exam.

Once a candidate for certification passes the exam, he or she must have the application endorsed by a CISSP in good standing. If none is available, arrangements can be made for another professional with information systems knowledge to endorse the application based on familiarity with the applicant's professional experience. CISSP certification also has a continuing education requirement. Credentialed CISSPs must be recertified every three years, which can be accomplished through attending courses, seminars, and conferences, as well as through self study and a variety of other continuing education activities. Certification in good standing also requires an annual maintenance fee of $85.

(ISC)2 is not the only organization that provides information security certification that employers may value. The following table lists various organizations and the

TABLE 2 Security Certifications

ORGANIZATION	CERTIFICATIONS
CWNP	Wireless#, CWNA, CWNE, CWSP
Check Point	CCSA, CCSE, CCMSE
Cisco	CCSP
CompTIA	i-NET+, Security+
CIW	CIW Security Analyst
(ISC)^2	CISSP, SSCP
TruSecure	TISCA

certifications they offer that you may want to investigate as you embark on a career in information security:

In the field, and certification notwithstanding, Paul Pescitelli recommends that job applicants have competence in at least two of the ten domains. Moreover, a successful job applicant often must combine IT expertise as it relates to a particular job or employer with a deep comprehension of security technology and practices.

Of course, if you are in college or graduate school now, you are a number of years of study and work experience away from being able to pursue some of these certifications. What can you do now to set yourself on a good path if you are intent on pursuing a career in IT security? The school you attend and the courses in which you enroll can play a large part in the your future success. Consult Table 3 for a representative survey of educational institutions and the relevant degrees they offer.

As you can see, the options for pursuing a degree in information security are

TABLE 3 Example IT Degrees

Institution	Type	Degree
DeVry University	Undergraduate	Bachelor's degree in Business Administration with a major/concentration in Security Management
RIT	Undergraduate	Bachelor of Science in Information Security and Forensics
RIT	Graduate	Master of Science degree in Computer Security and Information Insurance
Colorado Technical University Online	Undergraduate	Bachelor of Science in Information Technology-Security
Penn State University	Undergraduate	Bachelor of Science in Security and Risk Analysis
Capella University	Graduate	Master of Science degree in Information Technology-Information Security Specialization
Boston University	Graduate	Master of Science in Computer Information Systems: Security; Master of Science in Computer Science: Security
DePaul University	Undergraduate	Bachelor of Science in Information Assurance and Security
DePaul University	Graduate	Master of Science in Computer, Information, and Network Security

quite diverse. If you are not currently able to redirect your education to an institution that offers an information security, you can start preparing now by examining the curriculum of your own school. Make it a priority to enroll in courses that are in concert with the typical curriculum of an information security degree program. Some typical courses you might consider are:

Introduction to System Administration
Introduction to Programming
Security Management
Network Fundamentals
Information System and Network Infrastructure Protection
Cyber Self Defense
Information Security Policies
Cryptography Authentication
Computer System Security
Network Forensics and Security

An information security curriculum may also contain courses in other disciplines such as English, Economics, Psychology, Accounting, and Statistics.

One of the greatest challenges for IT security professionals is a work force that has little regard for security. The market research firm Insight Express surveyed users of mobile technology to see how careful they are with their company-issued devices. 44 percent of respondents reported opening e-mail and file attachments from unfamiliar or suspicious senders. 33 percent had hijacked a neighbor's wireless connection or used a public hotspot with no knowledge of its security. 73 percent admitted to sometimes being unaware of security threats and best practices for working on mobile devices. And 28 percent "hardly ever" consider the risks of their activities. The survey also uncovered one truth about why workers have little regard for security issues: they feel that security is the IT department's responsibility, not their own.

The attitude of the work force goes a long way to explain why security has become part of a company's day to day operations instead of remaining an adjunct

position. All levels of IT workers must now have an understanding of security issues. Let's take a look at two of the people working in the IT security field, one just starting out, and one with a many years of experience:

Harold Toler, Software Engineer, Blue Ridge Networks

Education: 2000 graduate of West Virginia Institute of Technology
Degree: B.S. in electrical engineering
Long-range goals: Complete a master's degree in an IT security domain and make security his life's work
Current work focus: Developing software to enable mobile devices and PCs to link with embedded network security devices
Quote: "With secure communications, the goal is to share information. Yet the challenge is to limit information distribution to only authorized individuals."

Craig Shumard, Chief Information Security Officer, CIGNA Healthcare

Education: Bethany College, B.A., 1973
Experience: 25+ years with the company including stints as assistant vice president of process management, assistant vice president of International Systems, and Year 2000 audit director; CISO since 1999.
Responsibilities: Protecting the personal data of customers and employees, as well as 9,000 laptops, 22,000 desktops, thousands of applications, and 140 TB of stored data.
Challenge: Increasingly aggressive demands from customers and addressing their concerns about privacy and data security.
Accomplishments: Making information protection a core competency and a part of everyone's job.
Typical day: Eight meetings touching on everything from sales effectiveness to vetting a vendor and promoting diversity in the IT department.
Quote: "We're only as strong as our weakest link and the weakest link is the person who doesn't know what they're doing."

These are just two examples of where an IT security career may take you. The following table displays a sample of key security positions and their related salary ranges:

TABLE 3 Example IT Degrees

Position	2007 Salary Range	Change from 2006
Chief Security Officer	$97,500 - $141,100	+1.9%
Senior IT Auditor	$81,500 - $107,000	+3.4%
IT Auditor	$69,250 - $97,000	+3.1%
Data Security Analyst	$72,500 - $99,250	+2.2%
Systems Security Administrator	$70,500 - $99,750	+2.3%
Network Security Administrator	$69,750 - $98,500	+3.7%

If you are searching for a job in IT security, you may also want to search for variations of some of the above job titles, such as: IT Security Engineer, Information Security Specialist, IT Security Manager, Security Architect, and IT Security Consultant. Of course, job titles and salary ranges are only part of the story. You will also need to consider the responsibilities that accompany each of these jobs:

Chief Security Officer: The CSO is a high-level executive who reports directly to the CEO, CIO, COO, or CFO. The person in this position takes the lead on all matters

related to setting and implementing security standards for the company. The CSO is charged with protecting all of the company's physical and digital assets, as well as ensuring the safety of all employees. The CSO's domain is as wide as the enterprise because security is a critical issue in all departments. In this role, you would need to work with IT, human resources, communications, legal, and other departments to coordinate enterprise security. The CSO often takes the lead on business continuity planning, privacy, loss prevention, and fraud prevention decisions.

IT Auditor: The IT auditor typically participates in identifying, documenting, and evaluating a firm's financial and operational controls. He or she performs audits to ensure compliance with professional and governmental standards, such as Sarbanes-Oxley. The IT Auditor may also be the liaison between the company and external auditors. The job may also require testing and validating internal controls, as well as making recommendations to senior executives about security areas that need improvement.

Data Security Analyst: A data security analyst protects the firm's data from threats, such as theft, fraud, vandalism, and unauthorized access. This position supports applications, operating systems, networks, and more. It generally requires you to institute procedures for safeguarding information assets. As a data security analyst, you will also make recommendations to senior executives based on vulnerabilities and integrity issues that you have found.

Systems Security Administrator: The person in this position performs risk management tasks on a firm's computers and network. The duties of a systems security administrator include real-time monitoring of traffic, incident response and analysis, forensics, and configuring and administering firewalls. In this position, you may also design and implement security best practices and support hardware and software from a security perspective.

Network Security Administrator: A network security administrator establishes and implements authorization policies for access to company resources on the network by assigning permissions. In this position, you would install, configure, and maintain all of the components of the network, including routers, switches, and wireless devices. You may also take the lead on technical direction, project management, documentation, and troubleshooting as they relate to IT security and infrastructure.

The IT security job market promises to remain strong for years to come. There are about 300,000 workers in the information security field. That number is expected to rise by 36 percent looking out to 2014. In addition to the overwhelming need for the services the industry provides, security is not an industry that is easily exported to overseas contractors. While moving the work offshore may be more economical, it is significantly less effective because overseas workers are not accountable under local laws and business practices. It is also more difficult to rely on the security of remote infrastructures, especially because security technology and practices require constant updating to be successful in the face of new threats.

Sources: John Edwards, "Top Secret-Launching a Career in the Booming I.T. Security Industry," www.graduatingengineer.com, accessed on September 13, 2007; Larry Barrett, "I.T. Security Specialists See Salaries Rise in First Half," Baseline, July 9, 2007; Larry Greenemeier, "IT Careers: New Master's Degree Emphasizes Ethical Hacking," InformationWeek, July 19, 2007 and "Cigna's Craig Shumard: One Man's Security Mission," InformationWeek, May 12, 2007; Mary Brandel, "12 IT Skills That Employers Can't Say No To," Computerworld, July 11, 2007; Sharon Gaudin, "Mobile

Workers Think Security Is IT's Job, Study Reveals," InformationWeek, August 21, 2007; www.my-it-career.com, accessed on October 3, 2007; "Robert Half Technology 2007 Salary Guide," www.rht.com; and John Parkinson, "Live and Learn," CIO Insight, June 1, 2004.