Global Information Assurance Certification Paper

Recruiting for your Computer Security Vacancy

Terry Wimsatt
January 29, 2001

Introduction

If we learned anything from "Y2K," it was the importance of computer security. Organizations, large and small, have come to realize the need to protect their computer resources. In a "2000 Computer Crime and Security Survey," ninety percent of the survey respondents stated that they had detected computer security breaches in the past year. This was the fifth annual survey conducted by the Computer Security Institute (CSI) in partnership with the Computer Intrusion Squad of the San Francisco Federal Bureau of Investigations (FBI). The survey was their combined effort to determine the scope of computer crimes in the United States as well as raise security awareness. The survey generated 643 individual responses from computer security practitioners in various U.S. corporations, government agencies, financial institutions, medical institutions and universities, and included the following findings:

25% reported detection of system penetration from outside their agencies

27% reported detection of denial of service attacks

79% reported detection of employee Internet access abuse

85% reported detection of computer viruses

Patrice Rapalus, CSI Director, made the following statement regarding the results of this survey:

> *"The trends the CSI/FBI survey has highlighted over the years are disturbing. Cyber crimes and other information security breaches are widespread and diverse. Ninety percent of respondents reported attacks. Furthermore, such incidents can result in serious damages. The 273 organizations that were able to quantify their losses reported a total of $265,589,940. Clearly, more must be done in terms of adherence to sound practices, deployment of sophisticated technologies, and* ***most importantly adequate staffing and training of information security practitioners in both the private sector and government.****"*

Role and Responsibilities

So, why am I sharing these alarming statistics? I want to reinforce the importance of establishing computer security within your organization. Security is a vital part of an organization's daily operations; it's not just a luxury anymore. While employees are

responsible for computer security at a very basic level within their organization, additional security responsibilities are always present and must be managed. The three main objectives of computer security are:

- **Confidentiality** – preventing the deliberate or accidental disclosure of sensitive automated information.

- **Integrity** – protecting automated information from deliberate or accidental corruption.

- **Availability** – protecting automated information resources from deliberate or accidental actions that would prevent availability to users.

Computer security is responsible for identifying system vulnerabilities and possible threats and then applying the necessary safeguards (both technical and administrative) to minimize those vulnerabilities and defend against potential attacks. In addition, other responsibilities of computer security include (but not limited to):

- Developing and administering the agency's security program, including recommending and implementing security policies and procedures.

- Developing, implementing and managing security awareness and training for agency users.

- Providing advice and assistance to various organizational personnel (technical and non-technical) in identifying security requirements for the different automated systems including security considerations in application development, implementation, operation and maintenance.

- Performing risk assessments and identifying potential security risks that may arise.

- Communicating security issues and concerns to agency management staff.

- Investigating security incidences and taking appropriate actions.

- Evaluating and recommending security products and solutions.

Remember that the role of computer security is not to physically secure every network device or every new automated project; nor is it to stand over the shoulder of every agency employee that goes online. The role is to establish a baseline of security standards, policies, and awareness programs, then delegate the security functions to other information systems staff and agency managers. The computer security professional or team should then ensure everything is working properly by performing regularly scheduled audits.

Recruitment and Retention

Now that we have established the value of a strong computer security program in your organization, where do you begin? Where do you go to find a qualified security professional, let alone several, if needed to build a team? Do you recruit outside of your agency or within? How do you decide how many security professionals are needed for your organization's computer security team? What qualifications do you look for? Should you consider outsourcing your computer security program to a managed security services provider? These are all options worth considering.

First, determine how many computer security professionals are needed for your organization. Small organizations should have a least one employee fully dedicated to computer security. Larger organizations should consider a team of employees working collaboratively in their computer security efforts. Very large organizations that are spread out geographically may need a security professional at each major work site.

Because of the drastic shortage in qualified computer security professionals, many organizations look within their own agency when filling their security positions. There are definite benefits in hiring candidates who already know the company's business. In a recent roundtable discussion featured in Information Security Magazine, David Foote, managing partner and research director of Foote Partners LLC, made a statement:

> *"Having IT skills, or security skills, is no longer enough. Companies want people who are just as savvy in business as they are in technology. The goal is to hire people who understand the business and know what it takes to guard against security breaches."*

The jury is still out when it comes to deciding the ideal qualifications different organizations are looking for when recruiting for a computer security professional. The desired skill set and educational background varies greatly from agency to agency. In fact, this was the main topic for a panel discussion held at the Computer Security Institute's 25th annual conference in Chicago, IL, on November 1998. Many skills and backgrounds were highlighted during this discussion – all with good reasoning behind them. Major skills discussed were:

- **Technical expertise** – the ability to understand and communicate the technical aspects of computer security. Because information technology is constantly changing, candidates may not be skilled in every technical area. For that reason, you must determine the specific technical skills needed for your organization.

- **Communication skills** – the ability to verbally communicate technology-related issues and security-related issues to every level of the organization (end-users, IT staff, managers, vendors, contractors, etc.). Written communication skills are also important for writing security-related policies, standards and awareness documents.

- **Presentation skills** – the ability to present security awareness programs and training to all levels of the organization.

- **Influence skills** – the ability to influence people, as well as build collaborative relationships, to overcome the negative attitudes toward security.

- **Mediation skills** – the ability to bring people with competing objectives together and reach appropriate compromises toward final solutions. Equally important is the ability to take a stand when needed, even when it's unpopular.

- **Management or business skills** – the ability to manage teams, manage multiple projects or problems, convey ideas and effectively bring security solutions to individual lines of business. Organizations find an understanding of their mission-critical business perspective a real asset.

- **Political skills –** the ability to work with diverse groups (in and outside the organization) and communicate security issues and needs. Often it is the ability to persuade management into supporting ideas, providing additional funding, changing policies, etc., to ensure a solid computer security program.

In addition to the skills addressed above, you should consider what educational background and/or certifications you want in your recruiting criteria. Because computer security is a multi-disciplinary field, a degree in computer science may not be the only one to consider. While a background in computer science is helpful, computer security also involves aspects of human resources, law, management, and communication. The educational requirements may differ from agency to agency depending on specific organizational needs and the particular job you are filling.

Certifications, while useful, should not always be the determining factor for choosing your final candidate. Certifications can give credence to a candidate's level of knowledge and expertise and can be helpful in deciding between two equally qualified candidates -- one with a certification versus one without. However, be careful of accepting a certification alone as evidence of knowledge and skills. Not all certifications are created equal and while many are highly regarded by employers today, others have become devalued, as they have become easier to obtain. For a list of certifications in this field, go to www.sans.org/infosecFAQ/how_to.htm, and review "Appendix C: Certifications for IT Security Professionals" in "How to Become a Bona Fide IT Security Professional" written by Anita Dodson.

Once you determine the duties and qualifications for your computer security vacancy, you must decide where you want to focus your recruiting efforts. Again, you may decide to look within your own organization if the skills and qualifications desired relate more to the business side of security (setting and implementing policies, security awareness, etc.). Finding an internal candidate who possesses most of the skills discussed above and a basic knowledge of information technology, then cultivating that knowledge, can work

well in many cases. Recruiting outside the agency can bring more diverse backgrounds and skill sets; but again, you must determine what you are looking for before deciding how and where to advertise your vacancy.

Recruitment and retention is of great importance these days due to the tight labor market. While there may be a shortage of qualified computer security professionals in the job market today, it is a rapidly growing field and you must be willing to pay the price. Security was traditionally a low-skilled and low paying function of an organization. Due to increasing vulnerabilities and threats to automated systems worldwide, this field is increasing in vitality and demand. Because of demand, wages must be competitive in today's security job market. SANS Institute released a 2000 Security Salary Survey that includes current market salary information for the security field. The survey can be found at http://www.sans.org/newlook/publications/salary2000.htm.

In addition to salary, other important retention factors are vacation time, employee benefits (i.e., insurance, retirement planning, etc.), training and tuition reimbursement, position growth, and promotional opportunities. You must determine what your organization can offer the successful candidate, then highlight those benefits in your recruiting announcement to make your vacancy stand out among competing job opportunities.

Another option you may want to consider is outsourcing your computer security program to a managed security services (MSS) provider, but be aware that these companies are fairly new to the industry and still evolving. While you should require fewer internal security professionals when outsourcing, some in-house staff is still needed to coordinate and monitor the computer security efforts with the MSS and manage the remaining security obligations within your organization.

Conclusion

As with any job recruitment, you will find the process much easier if you are prepared. Have an accurate job description ready prior to advertising your vacancy. This will help identify the specific job criteria and the skills you are looking for in candidates. This will also help you decide where to focus your recruitment efforts. Determine the salary range your organization is willing to pay remembering that candidates with extensive experience, formal training, and college degrees command higher salaries then candidates who have received their training on-the-job. When creating your interview panel, don't limit panel members to IT staff, but also include colleagues and staff from other functional departments within the organization. Finally, always insist on a background check as a condition of employment to ensure the integrity of the candidate you hire for the job.

Resources

"Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey." 22 March

2000. URL: http://www.gocsi.com/prelea_000321.htm (23 Jan. 2001).

"The Computer Security Handbook of CIT." URL: http://www.cit.nih.gov/security/handbook.html (23 Jan. 2001).

Radcliff, Deborah. "The ABCs of Security Team Building." 25 October 2000. URL: http://computerworld.com/cwi/story/0,1199,NAV65-663_STO52862_NLTs,00.html (22 Jan. 2001)

Information Security Magazine. "Infosec Job Market Flies." January 2001. URL: http://www.infosecuritymag.com/articles/january01/features.shtml (23 Jan. 2001).

"CSI Roundtable: Infosec Career Path." February 1999. URL: http://www.gocsi.com/inforound.htm (22 Jan. 2001).

Dodson, Anita. "How to Become a Bona Fide IT Security Professional." 30 October 2000. URL: http://www.sans.org/infosecFAQ/how_to.htm (03 Jan. 2001).

"SANS 2000 Salary Survey Summary." URL: http://www.sans.org/newlook/publications/salary2000.htm (25 Jan. 2001)

Thibodeau, Patrick. "Survey: Above All Else, IT Workers Need Challenge – Recruitment, Retention Methods Called 'Paramount'." 15 January 2001. URL: http://www.computerworld.com/cwi/stories/0,1199,NAV47-68-84-88-94_STO56335_TOPHiring,00.html (18 Jan. 2001).

Goslar, Martin. "Hiring Security Professional – It's Not (Just) About the Money." 8 January 2001. URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2672023,00.html (22 Jan. 2001).