# Job description cyber security specialist term paper examples

Business, Company

Job Description: Cyber Security Specialist at ABC Ltd.

PART I: The JOB DESCRIPTION

1. Position Title: Cyber Security Officer (CSO)

Position Code Number: IT/CSO/001

Position summary

Under the department of IT, the CSO will head the cyber security division and will responsible for policy formulation and implementation, securing the company's network and management of all cyber security issues including the division's budget and staff training.

2. Job Structure

The CSO will be working for forty five hours a week. Extra time worked will be regarded as overtime and will be compensated at a premium. The CSO will enjoy all working time related benefits such as annual leave and sick off days as stipulated in the job contract but will be expected to be available on short notice at all times to handle urgent job related issues.

The CSO will report to the Information & technology manager, and will work closely with the company General Security Manager, the IT department staff, the governance and policy formulation team, the Training Manager, and the Head of Software development and maintenance (University of Albany, 2009). In addition to this internal relationship, the CSO will cooperate with the relevant law enforcement agencies and hardware and software supplies.

3. Essential Functions

Policy Development - the CSO will cooperate with the governance and policy formulation team to develop cyber security policies aimed at ensuring security of the company’s network, hardware, and data. These policies will cover mode of training for network users, network security and emergency procedures and tests, disaster recovery/contingency plan, cyber attack incident reporting and response, risk assessment and compliance with required standards (University of Albany, 2009).

Education and Training – the CSO will develop a cyber security curriculum and coordinate the training of company staff on security of the company’s network. The training will be continual and will cover the precautions the workers should take to ensure integrity of the network and data. The CSO will also train end users of new security software and hardware (Newman, 2009).

Risk assessment and incident prevention – Risk assessment will involve analyzing all internal and external risk factors and recommending on how to minimize or eliminate them. This will require occasional ethical hacking of the company’s network to determine vulnerabilities. Incident prevention will mainly ensure that the company’s network is protected security software and hardware relevant to the risks identified during risk assessment (Newman, 2009). Such software will include; internet filters, antivirus and backup software while the security hardware will include physical firewall devices and routers.

4. Duties and Responsibilities

The CSO will be responsible for Installing, testing, commissioning, and maintaining security software, implementing the policy on cyber security including training the company staff on cyber security, maintaining and modifying the company's data as needed to incorporate new software, correct errors and change access status and encrypting all data transmissions (Newman, 2009). The CSO will also conduct security tests by ethical hacking to determine vulnerabilities. Other duties of the CSO will be; Preventing accidental or unauthorized modification, and corruption of data in the company network so as to maintain the integrity of the company's data. Reviewing violation of cyber security procedures and processes with an aim of preventing future violation and ensuring proper network ethics among the uses.

Responding to and reporting all cyber security incidents according to the laid down procedures.

Updating personal knowledge on the latest cyber security trends, threats and countermeasures with an aim of keeping the company's cyber security policy updated.
Monitoring internet use and firewall activity so as to identify cyber security bleaches and collect data for use in legal address of cyber attacks.

Develop and implement disaster recovery plans such as data backup and business continuity plans after cyber security incidents.

Minimize network down-time during security operations by planning to conduct them when the network is not under heavy use.

Serve as the company’s compliance officer in regards to state and federal information security policies and laws.

Advising the procurement division on all purchases regarding IT security devices and software.

Managing the cyber security divisions’ budget.

Perform related work as required.

5. Position Qualifications

Education - The CSO will have Bachelors degree in a computer related field such as Information Technology, Computer science, computer engineering, or software engineering. An advanced degree is preferred.

Experience – Minimum five years experience in information technology and security. The CSO will be experienced in computer programming, network security applications and hardware, development and implementation of cyber security policy and training. Excellent project management, written and oral communication skills and a demonstrated ability to work with diverse groups of people is required (University of Albany, 2010).

6. Skills and Abilities

The CSO will have the following technical and functional skills (Virginia State career guide, year);

Computer programming in various languages and for different applications.

Multi-platform computer application and maintenance of in-house software.

Project management skills.

Effective written and oral communications aimed at diverse groups of

people.

Adapting different equipments and technologies to meet user needs.

Using mathematics, logic and reasoning to identify the best strategies and solutions.

Listening, taking time to understand points and asking relevant questions.

Skills to conduct an investigation or audit computer usage and collect relevant evidence for use in legal address for cyber attacks.

The CSO will display the following abilities (Virginia State career guide, year);

Recognizing problems by discovering when things are wrong or when things are likely to go wrong.

Finding relationships by combining seemingly unrelated events and information.

Generating many ideas about a problem during brainstorming sessions.

Communicating ideas clearly and effectively so that other people can understand.

Apply procedures to specific problems so as to come up with logic solutions.

Arrange events in chronologic order or in any other given rule.

See fine details in an event and recognize their implications.

The CSO will also require knowledge in the following areas (Virginia State career guide, year);

Computer hardware, software, electronic equipment, embedded systems, including application and programming.

Business management principles involved in strategic planning, resource allocation and business modeling.

Relevant State and Federal policies and regulations on information management and cyber security.

Data backup schemes, checking integrity of backups, and encryption of data transmissions.

Network redundancy and disaster preparedness.

7. Certification and licensing

The CSO will have professional certification in a computer security course; Certified Information Systems Auditor (CISA) is preferred. In addition the CSO will be a member of relevant professional association such as, Information Systems Audit and Control Association (ISACA). Persons meeting the position qualifications including skills, knowledge and abilities but are not certified in professional computer security can hold the position of CSO after demonstrating that they are in the process of getting relevant professional certification.

8. Physical Demand

The CSO position requires walking, standing, climbing, bending, kneeling, crawling, pulling, pushing, reaching and handling. Ability to lift and carry items weighing up to fifty pounds is desired but reasonable accommodations may be made to enable people with disabilities to perform the essential tasks (Virginia Beach city public schools, 2009).

9. Work Environment

The CSO will be based in the IT department and will head the Cyber Security Division. The position is mainly office based but protective clothing including dust coats, hand gloves, goggles, and heavy boots will be required for visits

to the data center and sever room. Formal and decent clothing is expected in the office. The position also demands site visits, seminars and executive meetings with the CSO handling presentations on cyber security. In the event cyber attacks, the CSO will be expected to cooperate fully with all internal and external interested parties such as; internal commissions of inquiry, security software vendors, insurance companies, federal and state investigators.

10. Statement of Understanding

This job description for the CSO position at ABC Ltd is liable to review in keeping with company, state and federal policy changes. The duties and responsibilities of the CSO can hence be changed to align with business necessities and industry standards and this call for a flexible approach to the position.

11. Entry-Level Salary

The Entry level salary for the CSO position at ABC Ltd is $68, 000 - $ 80, 000 depending on experience and education.

PART II: What is the Outlook (in the short-term) for this Occupation?

Employment outlook of cyber security specialists is projected to increase much faster than the average of all occupations with good job prospects for those with a bachelor’s degree and relevant experience (Labor department: Labor statistics, 2010). This is a result of the continued expansion and sophistication of electronic data processing systems in many settings such as Government, business, telecommunication, and health care.

Implementing and upgrading this computer systems and safeguarding them requires new techniques to detect attacks and discover vulnerabilities (Singhal 2007). This has increased the demand for knowledgeable people in the field of cyber security. Hispanics Engineer & IT reports that Maryland-Based SafeNet Inc, which provides security consultancy services to government agencies and private businesses, could only fill 4 out of 100 openings for cyber security consultants in recent a recruitment drive (2011).

# PART III CONCLUSION

Human resource management has evolved and developed new technologies. This includes human capital programs such as; compensation, succession planning, training and development. There is a need for solid understanding of the jobs performed and job documentation has proved as an efficient tool for this (). A well written job description is based on competency and can serve as a basis of control in both the hiring and the performance evaluation process. Undertaking this project on job description has helped clarify on the importance of a job description such as; improving organizational order, defining expectations, determining compensation plans, communicating a companies needs to the job market so as to attracting qualified people who can fit in.

The Editors. (2011). " Top Employers in Cyber Security: Hot Jobs in a Super-Cool Sector," Hispanic Engineer & IT, 26(1), p53-55.

Labor Department, Labor statistics. (2010). Occupational Outlook Handbook, Washington, DC:

Government Printing Office.

Marder-Clack, M. (2008). The Job Description Handbook: Everything you need to write

effective job descriptions- and avoid legal pitfalls. Berkeley, CA: Nolo’s Human Resource Essentials.

Newman, R. (2009). Computer Security: Protecting Digital Resources. Burlington, MA: Jones

& Bartlett Learning.

Singhal, A. (2007). Data Warehousing and Data Mining Techniques for Cyber Security, New

York, NY: Springer.

UIC Human Resource. (2009). Writing Effective Job Descriptions. Retrieved on 25 May 2012,

May 2012, from < shr. ucsc. edu/forms/forms/shr-1274. pdf >

Virginia Beach City Public Schools. (2009). Computer Security Specialist: Job Description.

Retrieved on 25 May 2012, from