Airport Chief Information Security Officer (1404)
Task List (2015)

I. Advising

1. Advises the entire department on all cyber security issues through daily threat assessments in order to ensure maximum security of all department information and technology assets.

2. Provides advice and guidance to non-technical managers and staff within the department on systems such as applications, network, utility, Supervisory Control and Data Acquisition (SCADA), and on any new technological advancements.

3. Advises law enforcement on cyber security issues and threats such as potential nation-state attacks, insider threats and anonymous attacks, and on response and mitigation strategies.

4. Advises management on the threat environment, mitigation requirements, and the steps needed to secure and protect the departmental technology environment from potential cyber threats, including Distributed Denial of Service (DDoS) and other common attack methods.

II. Design

5. Designs network infrastructure with layers of security using best practices for cyber security and network architecture based on standards published by the Information Systems Security Certification Consortium, Escal Institute Of Advanced Technologies, Inc., and the National Institute of Standards and Technology.

6. Performs in-depth security reviews on any new implementation of internet website services using a host of cyber security tools such as tools that detect cross site scripting and Structured Query Language (SQL) injection.

7. Designs daily intelligence reporting on new vulnerabilities and threats as they occur, and disseminates to the Information Technology community.

III. Development

8. Develops up-to-date security policies, standards, and guidelines by adopting best practices as found in other organizations and industries by working closely with other airports and city organizations.

9. Develops testing procedures for security devices using industry standard tools and protocols such as those developed through Fire-eye, Symantec, and other leading manufacturers.

10. Develops incident response procedures using standards found in International Organization for Standardization (ISO) 27032 in order to be prepared in the event of a security breach.

11. Develops mandatory computer-based or in-class training in the area of cyber security that employees must complete prior to utilizing departmental assets.

12. Develops a program to advise employees on social engineering threats including phishing, dumpster diving, spoofing, spamming, and password protection.

IV. Implementation

13. Implements Cyber Security Awareness training programs for all employees, contractors, and approved system users to increase awareness of cyber risks such as spoofing, phishing and other social engineering threats.

14. Implements an information security management framework based on payment card industry security standards and the National Institute of Standards and Technology.

15. Implements risk management programs to assess the risk level of the Enterprise network infrastructure, and updates the program as the technology environment evolves.

16. Implements Business Continuity Planning to identify all the critical assets of the Enterprise Network in order to ensure the department's ability to return to normal operations following any cyber-related incident.

V. Operation

17. Publishes up-to-date security policies, standards, and guidelines which adhere to cyber security best practices as well as the City of Los Angeles Charter regulations and rules, including all major federal cybersecurity frameworks and standards.

18. Disseminates latest security threats to all Information Technology administrators and managers within the department in a non-technical manner which can be understood by all departmental stakeholders.

19. Oversees dissemination of security policies and best practices such as those published by security organizations including International Information Systems Security Certification Consortium, Escal Institute Of Advanced Technologies, Inc., and federal organizations such as the National Institute of Standards and Technology.

20. Performs incident response procedures, including computer forensics, threat mitigation techniques, and recovery of attacked systems in the event of a security threat affecting the department.

21. Performs incident escalation to outside entities such as the City's Information Technology departments, Federal Bureau of Investigation, City of Los Angeles Airport police, and Los Angeles Police Department by disseminating sensitive and confidential information describing the threat.

22. Coordinates the work of staff to responds to any security alerts from the Multistate Information Sharing and Analysis Center (MS-ISAC) by taking action to protect the department's assets from all known cyber threats.

23. Integrates security incident events occurring within the department with the City of Los Angeles Cyber Security Command Center.

VI. Maintenance

24. Ensures all critical Information Technology devices (e.g., work stations, servers, routers) have the latest security patches in order to prevent any intrusion to the device.

25. Performs routine on-site checkups to ensure that all security software and hardware support maintenance from vendors are up-to-date.

26. Liaises with vendors, legal, and purchasing departments to establish service contracts and agreements that comply with security requirements.

VII. Risk Management

27. Performs risk auditing of critical infrastructure systems such as routers, firewall, domain name server, active directory, and Virtual Party Network (VPN) remote device by developing automated scripts which continually monitor the department's Information Technology environment.

28. Performs risk auditing of critical business application systems such as payroll application, Enterprise Resource Planning (ERP) application, video management system, and access control system by conducting penetration tests and using a variety of software products designed to scan applications and detect vulnerabilities.

29. Performs external auditing of the internet infrastructure by conducting penetration testing and vulnerability scanning in order to determine infrastructure security strength and to identify any weaknesses.

30. Enlists third party vendors such as external cyber security experts and consultants to perform security assessment of the department.

31. Assesses potential risks of new software implementation to the department by conducting penetration testing and vulnerability scanning.

VIII. Management/Supervision

32. Calculates costs and benefits involved in the procurement of hardware, software, or hardware maintenance agreements in order to determine the cost effectiveness of different projects and to provide justifications for budget requests.

33. Determines the prioritization of cyber security projects within the department by considering factors such as impact on users, the department, and the City, the resources and staffing needed for different projects, and communicates prioritization to staff and supervisors.

34. Decides which subordinate team, section or staff member should be assigned responsibility for particular projects.

35. Informs staff through individual and group meetings and memos of their assignments and the relevant history behind specific projects.

36. Directs subordinates to develop plans for the accomplishment of projects, reviews the plan for appropriateness of time and staffing allotted, and approves or disapproves of plans.

37. Coordinates meetings with supervisors and forms committees between sections or departments in order to solve problems and coordinate work between work groups.

38. Decides what the sequence of tasks and projects within section will be and directs subordinates to carry out that sequence in order to best coordinate the section’s work.