Contra Costa County California

"Best Practices" Information Security Program

Information Security Advisory Committee
January 2004

Page intentionally left blank

Contributing Authors to County Information Security Program "Best Practices"

Departmental Information Security Advisory Committee members for Contra Costa County

Special Thanks to CCISDA Information Security Forum Members for the insight and forethought for working toward a common goal of securing county government systems and assets

Table of Contents

Page intentionally left blank

Executive Summary

Introduction

In light of the horrific events of September 11, 2001, the Federal Government is rallying federal, state and local governments, as well as private industry, to 'harden' their information systems. These systems must be protected from terrorists and the pervasive increases in both foreign and domestic Internet attacks (denial of service, Trojan horses, worms, viruses, hackers, etc.). The mission-critical systems that protect our communities and provide invaluable services are under attack. They are subject to being circumvented and destroyed and must be appropriately protected. An opportunity exists for county governments to answer a vital call to action for the survivability of these assets and services. Formal information security programs with executive support must be developed, budgeted and implemented. Without executive sponsorship and support of a formal information security program, the many services that counties provide, especially those focused on the preservation of life safety, health, and social assistance, will remain at risk, and may be adversely affected or denied by the successful penetration of our information systems. The existing threats and vulnerabilities to county information systems include, but are not limited to, telecommunications, information systems, networks, and facilities.

As Richard (Dick) Clarke, special advisor to the White House on Cyberspace Security, stated at a Critical Infrastructure conference in Austin, Texas on February 12th, 2002, we can guarantee the following:

1) We will have enemies, as we are a dominant force in the world;
2) These enemies will be smart;
3) They will use our technology against us;
4) Our infrastructures are fragile (not robust);
5) Society is interdependent, including our economy;
6) Proactive government actions can enable us to deal with these threats.

Mr. Clarke further said that:

1) We must look at how our economy works, understand it (e.g., the computers behind it), and harden them;
2) We need to ensure remediation by investing in both Information Technology and Information Security;
3) These technologies and information security programs must be robust, designed with and maintain redundancies, allow for degradation, and provide resilient restoration.
4) We must share information between all levels of government and the private sectors.

This document outlines an Information Security Program based upon industry and governmental proven "best practices," and designed for adoption by Contra Costa County and any other of the California Counties accepting the above-noted challenges. This program was developed under the leadership of the Contra Costa County CISO through the County's Information Security Advisory Committee and the California County's Information Services Directors Association (CCISDA) Information Security Forum (ISF) to discuss, define and develop the recommendations made in this document and model those proven to be best practices. The CCISDA ISF was establish by our CISO and consists of information security professionals employed by counties across California.

The approach used to develop this document was to review and discuss the aforementioned "best practices" in information security and technology and apply those practices to county governmental environments. This paper provides guidance and direction aimed at the survivability of county information and vital life safety systems. This will be accomplished without the removal or degradation of civil liberties and rights to privacy.

Content

This document is divided into six sections as follows:

1) **Executive Summary** – This section outlines the intended use and structure of this document.
2) **Best Practices Information Security Program, an Executive Perspective** – This section outlines the motivations for developing a Best Practices Program, the benefits of implementing a Best Practices Program, how a Best Practices program should be implemented, and the components of a Best Practices Information Security Program.
3) **Exhibit 1** – This exhibit provides detailed information on each component of the Best Practices Information Security Program.
4) **Exhibit 2** – This exhibit provides a sample Information Security Program.
5) **Exhibit 3** - This exhibit defines the International Information System Security Certification Consortium, Inc. (ISC2) Common Body of Knowledge (CBK).
6) **References** – This section lists references used in the development of this program.

Recommendations

We are encouraged to adopt information security best practices. Because this document is based on best practices and written by county staff and the CCISDA ISF, it can provide a firm foundation for establishing an effective information security program in any county. We acknowledge in advance that many counties are adopting these "Best Practices" now or are in the process of doing so. Many other counties will adopt this program through a modified version, based upon their size and resource limitations. However, it is expected that every California County could benefit directly from this document, and could implement this program to protect its information systems and ensure continuity of government services.

It is recommended that Contra Costa County implement this Best Practices Information Security Program through a Board of Supervisors (BOS) resolution. We have a moral and legal responsibility to do so.

Best Practices Information Security Program, an Executive Perspective

Introduction

One of the most important assets of a county government is its information, and the Board of Supervisors, County Administrator, and Department Heads have legal obligations to make certain that such information is managed within the frameworks prescribed by law and regulation. The value and criticality of these informational assets require the implementation of a formal Information Security Program to meet these legal and moral responsibilities. Major goals of the Information Security Program are to enhance the productivity of the government organization and the quality of life of its constituents, as well as ensure the protection and preservation of lives and systems. This is accomplished by maintaining the integrity, confidentiality and availability of the county's informational assets.

As a county government, we are a unique business entity. This is evident when one considers the threats that government now faces (e.g., cyberspace terrorism, bio-terrorism, day-to-day hackers, unauthorized intrusions, virus attacks, etc.), the diversity of the operations of its agencies, the various governing laws and statutes, multiple sources of funding, and the interaction between elected and appointed officials throughout government. This uniqueness requires a correspondingly unique Information Security Program, one that is tailored to a local county government. The informational assets of a county government include all data, in any form, and all data systems located anywhere within the county. The diversity of these assets, and the foreign and domestic threats to them, further complicate the task of information security. The threat to one asset may be integrity, the threat to another may be confidentiality, and to yet another may be availability. Consider, for example, what could occur if medical patient data or criminal records from the District Attorney, Sheriff, or Probation offices were accessed and unauthorized modifications were made? Lives could be lost or criminals released into the public. What if our 911 systems were disrupted or taken down? Again, life safety issues are at stake. It becomes apparent that a breach in the security of some of these informational assets could have catastrophic consequences; lives could be lost and lawsuits would inevitably result.

One of the greatest challenges within information security is that there are no guarantees. It has often been said that for a computer to be completely secure, it should left in its box – and sealed. The task is to build an Information Security Program established on business rules and reasonable security measures (layering), with an underlying acceptance of risk to assure a "good-faith effort" is achieved. A "good-faith effort" is a legal term described in the U.S. Federal Sentencing Guidelines and becomes an essential indicator of an organization's level of effort and concern as well as the adequacy of its security programs. Implementing the Best Practices Information Security Program outlined in this document will not only help absolve the county and senior management from potential liability by demonstrating a "good-faith effort," but will effectively, through threat avoidance, provide a level of security that will enhance the productivity of the government organization and the quality of life of its constituents.

Another unique aspect of being a county government is the ability – or necessity – to share information with other local county governments. In some instances, this interconnectivity exists for the benefit of increased productivity. In others, law mandates it. What threat does this pose to our system and resources? As the saying goes, a chain is only as strong as its weakest link. Security embraces that same analogy. For example, if one county's network is secure, but is interconnected with another county's network that is vulnerable (i.e., the weak link), then both counties are vulnerable. Historically, attackers will first penetrate the weak network and then "hop" through the interconnection to the secure network. Because counties have to connect with each other and other levels of government, what can be

done? A level of confidence or trust must be established between each entity. For one county to connect to another, it is necessary to trust that the other county is secure. With all counties adopting the Best Practices Information Security Program, this level of trust or confidence can be achieved.

The Program

This Best Practices Information Security Program is compiled from information gathered from the International Organization for Standardization's (ISO) Code of Practice for Information Security Management (ISO17799), State and Federal Statutes, input from the County Information Security Advisory Committee (ISAC), and the CCISDA's Information Security Forum members' expertise and experience, the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), the Generally Accepted Systems Security Principles (GASSP), and other references as listed in the References section found at the end of this document.

This program provides the foundation for an information security program for Contra Costa County. It outlines industry-proven components that constitute a comprehensive Information Security Program. A program that does not include these components will have gaps where the program can fail. Information security, like any other program, requires the support of senior management as a major success factor. This support is required because, by nature of its work, information security is a business activity that crosses departmental lines, chains of command and agency boundaries. Because of this fact, it is important that this program be supported by executive sponsorship through a Board of Supervisors resolution. This will not only contribute to compliance, but will provide the necessary budgetary funds to implement components of the program.

The general components of this program are:

1) Chief Information Security Officer, CISO
2) Information Security Advisory Committee, ISAC
3) Information Security Policies
4) Information Security Awareness Training and Education
5) Information Identification and Classification
6) Information Risk Assessment
7) Implementation of Information Security Controls
8) Monitor Effectiveness and Assurance
9) Business Continuity and Disaster Recovery

These components are briefly explained below. For a more detailed description, see Exhibit 1 and the in-depth analyses that follow it.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is the key to the development and enforcement of a comprehensive Information Security Program (ISP). This position will ensure the development of countywide policies and assist departments in the development of procedures for adherence to the ISP. Without this individual physically inserted into the management process, an information security program will neither be implemented nor be enforceable, and upper management will not be able to provide for the protection of its information assets. As the ISP is a countywide program, and not an IT program, the CISO must have direct access to the CAO/CEO regardless of where he/she reports administratively. Ideally, the CISO would report administratively to the CAO/CEO of the county as well to make sure that this countywide program obtains full countywide buy-in, and is not subject to departmental budget constraints or cutbacks. Currently, the CISO reports administratively through the County's CIO.

Information Security Advisory Committee (ISAC)

The Information Security Advisory Committee, comprising departmental representatives, in conjunction with the Chief Information Security Officer, will review and update the Information Security Program and Policies as necessary. The ISAC sees that the policies enable county departments to accomplish their objectives. Often, compliance with security policies is lacking because the policies would prevent an organization from performing its duties. The input of the Information Security Advisory Committee keeps the policies and business goals in line. Policies will be implemented at a much faster pace because of cross-departmental involvement. Advisory committee members will also act as the security champion for their respective departments. Departmental representatives will work with departmental managers to assure that files and databases have designated owners, coordinate requests for user IDs and data access, and participate in the development of agency specific information security policies and procedures.

Information Security Policies

The policy objectives are set forth in an Information Security Policy statement, which is the cornerstone of any effective program for managing and controlling an organization's information assets. Policies are the high-level guidance or vision directing the organization. The statement establishes the basic philosophy of the county and determines the functional areas where controls must be established. Implemented by management to provide information, control and direction, the Information Security Program establishes policies used to support the development of the subsequent security program. A good information security program policy statement must do a number of things:

1) Identify informational assets;
2) Define who is responsible for classifying and valuing information assets and who must comply;
3) Describe the role of employees in the protection and recovery of information; and
4) Provide for monitoring and enforcement.

"What is protected"

The Information Security Policy statement should describe what information should be protected, as well as the extent of allowable distribution. Responsibilities should address all levels of the departmental structure, stating who is responsible for complying with the policy and who is responsible for making sure that the classifying policies are enforced. Each employee's security role should be

spelled out; the consequences of non-compliance must be linked to those roles and attendant responsibilities.

"How is it enforced"

Monitoring and enforcement address when the policy becomes effective, conditions under which the policy is enforced, and how it will be monitored. For instance, does it apply only for a specific group of employees while working in the department's facilities, or does it apply to employees on travel or in the field. Normally, background on the need for a policy is also incorporated.

"Keep it simple"

The policy statement should be short, easy to read, and not incorporate technical terms. It must also be unambiguous, so that no one can be exempted from the requirements. One method of achieving accountability is to incorporate an employee acceptance page at the end of the document that must be signed and returned to appropriate management personnel. This form could also become an annual requirement delivered as part of annual security awareness training.

"Protect people as well as data"

Don't forget that people can make or break a policy.

1) Guard against -- and remove from unnecessary temptation -- inappropriate data to which employees might be exposed while fulfilling job responsibilities.
2) Make management aware of the need for information security, and see to its participation in the development and implementation of security policies.
3) Protect sensitive or confidential data, including public information.
4) Provide protection from acts that would cause malfunctions, errors and omissions, inaccuracies, unauthorized disclosures or destruction of data.
5) Determine that controls and procedures are in places that allow immediate detection and countermeasure implementation for information threats.
6) Protect management from charges of fault in the event of information compromise.
7) Guarantee the ability of the county to survive business interruptions and to function adequately thereafter.
8) Demonstrate 'due diligence' in handling county-controlled information.

Information Security Awareness Training and Education

Training is an essential part of a responsible employee's use of computing assets. The means of developing employee understanding and/or recognition of such responsibilities vary. User/employee security awareness training is one of the most common means available to achieve recognition of responsibility and computing asset worth. Each county department should require personnel to sign an agreement that includes the protection of computing assets as a condition of employment. In addition, another recognized means of communicating security awareness is the use of security login banners, which are displayed whenever a user logs onto any county computer. Without some guidance at the user level regarding appropriate protective measures and actions, the best conceived information security plans would not cover everything that can happen.

Information Identification and Classification

The Information Security Program must incorporate standards and procedures by which information resources are managed and accessed. These standards identify and classify the information collected and maintained by the information owner, based on that information's content, sensitivity and importance. An identification methodology is used to categorize information content into distinguishable categories. (Medical Records, Project Data, Fiscal Budget, Fiscal Annual Report) These categories then facilitate subsequent classification.

A classification scheme is used to determine adequate and appropriate procedures and their associated access controls for information protection and distribution. Access control must be consistent with the classified value of the information resources to be protected and the severity of the threat to them.

An identification methodology and classification scheme must be represented in accordance with this Information Security Program.

Information Risk Assessment

It is very important that management be able to quantify the benefits of an Information Security Program as a function of costs. These benefit vs. cost tradeoffs are essential in justifying an Information Security Program. In order to formalize this analysis process, certain concepts must be considered:

- A business risk is anything that could potentially harm the operation, assets, or profitability of the organization;
- Risk analysis is a formal process of determining the worth of computing assets, identifying vulnerabilities by discovering where threats/exposures could occur, then determining how much potential harm could be caused if the identified vulnerabilities are exploited;
- For all vulnerabilities identified, the risk analysis produces a cost vs. benefit analysis to determine if the cost to implement fixes or increase protection is justified by the cost of the asset's loss. Thus, information security policies and risk go hand in hand: policies are needed to reduce risk, and risk analysis is used to justify security policies.

Implementation of Information Security Controls

If management and employees understand their respective responsibilities for protecting computer data, it follows that they must also recognize the problems they face in developing and implementing an information security program.

"Management's role"

Management has the ultimate responsibility for implementing an information security program based on an assessment of business risk (cost/benefit tradeoff) and an information system (IS) security risk assessment. All levels of management, including the Board of Supervisors, CAO/CEOs and Department Heads, must be involved and held accountable that the program is understood and properly implemented. Management must understand that it may be legally responsible for the integrity of governmental data assets just as with other assets of the county.

"Employee's role"

Employees must recognize that the government data on their computers is both valuable and vulnerable. They must understand their (legal) responsibilities regarding the unauthorized release of sensitive data. Note that sensitive data means data that requires protection due to the risk and magnitude of loss or harm that could result from unavailability, disclosure, alteration, or destruction.

"Everyone in the county has an important security role"

The following summary relates responsibilities for various management levels within the County:

- Board of Supervisors - To protect and provide for continuity of the county.
- Elected Officials and Department Heads - To protect and achieve prosperity of the departments under their control.
- Managers - To maintain information as a strategic asset.
- Chief Information Security Officer - To guarantee that written information security policies are developed and implemented.
- Internal Information Systems Auditor - To determine that information security policies are followed.
- System Administrators, Technicians and Installers - To oversee configuration of technology assets to handle information in a secure manner.
- Users - Ultimate responsibility for appropriate use of county-controlled informational assets.

Notice, in the above list, that "operational information security" is not a direct concern of upper management, but the protection of information assets certainly is.

Monitor Effectiveness and Assurance

The county must be able to assess the measures that have been implemented within the Information Security Program and must determine that security goals of the enterprise are being met. This component defines how this is accomplished. Information collected from processes that measure effectiveness and assurance enable the county to identify value in implemented security measures. This information needs to be "independently" reviewed and evaluated. This is referred to as "separation of duties." Separation of duties is extremely important in monitoring effectiveness and assurance of information security. Staff responsible for administration of a process should not be responsible for evaluating how effectively it protects the county.

Business Continuity and Disaster Recovery

Contingency Plans (Business Continuity Plans) differ from Disaster Recovery Plans (Operational Recovery Plans) in that contingency plans address the business side (facilities, personnel, procedures, forms, day-to-day supplies) of departments, whereas the disaster recovery plans dwell more toward recovery of Information Technology assets (computers, storage, electronic communications and data). This aspect of an information security plan is based on the realization that if a man-made or natural disaster occurs, the county (department) must be able to resume its critical processing. It requires the identification of those applications critical to survival, e.g., storage of the related operating systems, operator instructions, utilities, programs, and data in an off-site storage facility. The most crucial aspect of these programs is testing the plans using the designated alternate processing sites. Many a disaster recovery plan has failed because it was never tested, and when it was needed, no one knew what to do.

Conclusion

Like any other countywide program, executive sponsorship and support are essential for this program's success. The Information Security Program outlined in this document can be used by us as a foundation for our efforts in providing availability, integrity and confidentiality of all county controlled assets, both logical (e.g., computers) and physical (e.g., building, personnel, hardcopy). This program is based upon industry and governmental 'best practices' and has been developed by a security forum sanctioned by the California Counties Information Services Directors Association and tailored for use by the County's Information Security Advisory Committee. The need for an Information Security Program based upon 'best practices' is required so that we can, using standards, build and maintain both effective and efficient methods to safeguard assets under county control. Each component outlined above is required for the program to meet those standards. Furthermore, adoption of this best practices program will allow our County, as well as both State and Federal agencies that are mandated by law to share informational assets with each other, to comply with published standards in Information Security. We are now in a position to adopt these standards in a proactive manner, to deal with newly recognized threats to the United States on Homeland Security efforts, internal and external threats, as well as ongoing threats from foreign countries, including viruses and Trojans (malicious software) that place information systems at risk daily.

Exhibit 1: Information Security Program Components

Following is a detailed explanation of the components that constitute the Best Practices Information Security Program.

AREAS	DESCRIPTION
Chief Information Security Officer	Defines roles and responsibilities for a countywide Information Security Officer.
Information Security Advisory Committee	Defines roles and responsibilities for a countywide Information Security Advisory Committee.
Information Security Policies	Recommends an approach to developing and managing information security policies. Suggests areas where information security policies should be written.
Information Security Awareness, Training, and Education	Recommends an approach to developing and managing information security awareness, training and education programs. Suggests minimum requirements and delivery methods.
Information Identification and Classification	Recommends identifying and classifying information assets. Suggests identification methodology and classification scheme.
Information Risk Management	Recommends an approach to managing risk to information. Suggests methods for analyzing and managing risk as well as assessing vulnerabilities and threats.
Implementing Information Security Controls	Recommends implementing information security controls. Suggests information security controls to implement.
Monitoring Effectiveness and Assurance	Recommends testing information security controls. Suggests methods for testing information security controls.
Business Continuity and Disaster Recovery Planning	Recommends development of business continuity and disaster recovery plans. Suggests minimum requirements.

Chief Information Security Officer (CISO)

Definition

Under general direction from the CAO, and reporting through the County CIO, the CISO plans, organizes and directs the countywide Information Security Program, including security awareness training, risk assessment, business impact analysis, disaster recovery, and business resumption. The CISO also performs other duties as required.

Distinguishing Characteristics

The incumbent in this single position class receives general program direction from the County Administrator or other County Executive (e.g., CIO) and is responsible for the day-to-day management of the countywide information security function. The incumbent may exercise direct supervision over assigned staff.

CISO Management Responsibilities

- Develops, secures approval, establishes, implements and maintains a countywide information security program;
- Develops, coordinates and maintains policies and provides guidance in Local Area Network (LAN), Wide Area Network (WAN), mainframe and desktop information security issues;
- Researches and recommends centralized written manuals and procedures regarding security controls;
- Acts as the countywide central point of contact for information technology related security incidents or violations;
- Assists information technology staff and others (e.g., law enforcement, auditors, etc.) to investigate information technology related security incidents or violations, maintaining records and writing reports;
- Conducts security risk assessments and business impact analyses of county departments to determine that a comprehensive countywide business resumption plan has been developed;
- Acts as a consultant to all county information technology organizations in the review of security policies, computer operations, data communications security, system development and logical access controls;
- Develops, promotes and presents security awareness training and education to all levels of the county organization structure on an ongoing basis;
- Develops and directs risk assessment activities regarding security;
- Interviews, selects, trains and evaluates assigned staff;
- Assists in the preparation of departmental budgets, as well as strategic and tactical plans, so that adequate resources are made available to implement information security controls;
- Makes verbal and written presentations to the county Board of Supervisors, County Administrator, County Elected Officials, Chief Information Officer, and agency and department executives;
- Plans, prioritizes, delegates and reviews the work of assigned project staff; establishes schedules and methods for achieving project goals and objectives; reviews work products and makes corrections; and coordinates staff training and development efforts;

- Establishes and chairs a countywide Information Security Advisory Committee for discussion and dissemination of information security and related programs;
- Drafts and maintains countywide information security policy in concert with the ISAC for executive management review and approval;
- Assists in the coordination and testing of department information technology disaster recovery and business continuity plans;
- May act as the prime manager in directing activities of all staff assigned to large-scale information technology security development and maintenance projects;
- May coordinate vendor activities, write and evaluate proposals and negotiate contracts for information technology security related equipment and services.

Knowledge, Skills and Abilities

Knowledge of:

- Principles and methods used in the analysis and development of information security;
- Systems and procedures;
- Currently accepted information security standards, guidelines and theories;
- Advanced computer technology;
- Principles of management and supervision;
- Information technology equipment operation, capacity and capability.

Ability to:

- Analyze and interpret complex data;
- Effectively supervise subordinate personnel and motivate and direct the work of others;
- Prepare and present effective, clear and concise reports and correspondence;
- Identify and recommend information security needs for the county;
- Analyze and assess policies and operational needs and make appropriate recommendations;
- Administer countywide goals, objectives and procedures;
- Analyze problems and identify alternative solutions;
- Deal effectively and harmoniously with county executives, department and assigned staff, customers and the general public

Conclusion

In conclusion, the CISO position is instrumental for the successful implementation of the County Information Security Program.

Information Security Advisory Committee

Introduction

The Information Security Advisory Committee (ISAC), comprising departmental representatives, in conjunction with the Chief Information Security Officer, will review and update the Information Security Program and associated policies as necessary. The ISAC ensures that the policies enable county departments to accomplish their objectives. Often, compliance with security policies is lacking because the policies would prevent an organization from performing its duties. The input of the ISAC keeps the policies and business goals in line. Policies are also implemented at a much faster pace because of cross-departmental involvement. ISAC members will also act as security champions for their respective departments. Departmental representatives will work with departmental managers, so that files and databases have designated owners. They will also coordinate requests for user IDs and data access, and participate in the development of agency specific information security policies and procedures.

Information Security Representatives

Under the general direction of the department, an Information Security Representative (ISR) is the designated member of the department on the ISAC. The ISR is responsible for overseeing and administering the department Information Security Program, Disaster Recovery Program, Risk Assessment Program, Security Awareness Program, and the Business Continuity Program (including business impact analysis) in coordination with the Chief Information Security Officer and countywide security policies and programs. These programs encompass all departmental sensitive systems - manual and automated, physical and logical (computerized) for which the department has administrative responsibility. It includes the policies, procedures, guidelines and safeguards that are required to protect information, confidentiality and privacy rights, as well as the integrity, auditability, and controllability of these information systems. The ISR has overall responsibility for the enhancement, implementation, monitoring and enforcement of the program and is further responsible for investigating all alleged information security violations. The ISR may direct a professional support staff, when required, to meet the departmental responsibilities.

Specific Job Assignments

Administration

- Overall responsibility over the department's Business Continuity Program: although this is a countywide endeavor, the ISR is responsible for their department's program;
- Oversight responsibility for the following operational areas: operating systems, teleprocessing monitors, support software, communications networks, capacity planning, data management, database management systems, and general functions;
- Analyze legislation, and federal, state, and county mandates for their effect on departments and countywide security policies;
- Review and approve: data and stock inventories, risk analysis (Risk Assessment Program) of data and assets, the adequacy of implemented safeguards, system documentation dealing with personal/confidential data, and the extent of compliance with security standards and procedures;

- Provide input into the development of countywide and departmental security policies, procedures and guidelines and implement security counter measures through the ISAC;
- Develop an ongoing program to inform department staff who collect, maintain or disclose information of their responsibility to enact published safeguards;
- Prepare reports regarding security activities in the department, as may be required by the Department Head, CISO and others;
- Meet and confer with high-level information security personnel from other counties, states, corporations and agencies regarding matters affecting security policy and procedures.

Reviewing

- Secure and maintain the confidentiality and integrity of sensitive data owned by the department by reviewing and approving, through a formal system development life cycle process, all security considerations for department automated and manual environments;
- Provide for the recoverability of department systems and assets by the development, implementation and maintenance of appropriate disaster recovery plans with department information technology staff and the CISO;
- Secure department compliance with all provisions of California Civil Code, Division 3, Part 4, Title 1-8, Chapter 709 (Information Practices Act of 1977), as required by Article 5, Section 1798.21 and other legal provisions as required by law and a conducive business environment;
- Work with internal and external auditors and analyze departmental-automated environments on an ongoing basis to identify risks arising from changes in those environments, with particular emphasis on changes and risks in teleprocessing components.

Planning

- Provide advice and assistance to management in making formal recommendations relative to safeguarding data, operations, and other assets;
- Work with appropriate bodies on the development and approval of statutes, regulations, and policies addressing security, including following appropriate legislation;
- Oversee the development of automated tools to support the auditing and monitoring of the automated information environment as required by the dynamic nature of those environments;
- Research and evaluate new and existing information security technology to identify methods for reducing risks that exist now or may arise in the future.

Operation

- Protect the department's sensitive resources against misuse, abuse and unauthorized use by establishing who, what, and how an individual may access and use the informational resources of the department;
- Investigate the authenticity of reported security violations, initiate corrective action and direct the implementation of additional security measures as warranted;
- Review the functions performed by the department to protect the data, confidentiality and privacy rights, and ensure the integrity, auditability, and controllability of the information systems.

Supervision Received

The ISR receives direction from and reports directly to the highest authority practical within the department. The authority will make certain that the ISR is sufficiently aware of department goals and policies to support staff through project activities and management actions.

Administrative Responsibility

The ISR is responsible for all information security related management functions in the maintenance of effective department policies and procedures and organizational structure and staffing, and represents the department as it relates to information security issues to the CISO and others.

Daily Contacts

The ISR can have contact with all levels of departmental management, representatives from other county departments, the CISO, representatives from other counties within the state, representatives from state and federal government agencies, and with contracted vendors and consultants.

Actions and Consequences

The ISR exercises judgment in making decisions affecting all security aspects of the department. Failure to use good judgment in handling sensitive and confidential material could result in release of information to unauthorized persons in violation of the Government Code, union contract agreement or department and county policies. Failure to perform the duties of this position could jeopardize the security and integrity of the department that is contrary to the image goal the department is striving to achieve.

Other Information

The ISR must have knowledge of the countywide Information Security Program (and all encompassing programs), the Information Practices Act of 1977 and computers, networks, and operations, and use of program languages, database management, job control languages, utilities and systems analysis methodologies commonly used in the department. Other duties not specifically stated might be assigned to meet operational needs.

Conclusion

In the course of policy development, the Information Security Representatives, through the ISAC, provide the vital bridge between the end-user community and technology personnel tasked with the implementation of security policies.

A county's security policies can be considered a set of "living documents" that must change rapidly to respond to the evolving security threats and changing data distribution topologies. Implementation of the Information Security Advisory Committee provides for the rapid creation and maintenance of these security policies, and as these policies now "belong" to all users there is much less communal resistance to change and implementation, while facilitating the enabling (and not hindering) of business objectives.

Page intentionally left blank

Information Security Policies

Introduction

Information Security policies should be written to apply to all employees, both permanent and temporary, and all contractors, consultants, vendors, interns, volunteers and others who use the resources that are either owned or leased by the county. Policies can address both general and specific issues, but they should be tailored to those people who will be held responsible for compliance.

Counties and their departments should adopt commonly accepted IT security policies since they directly reflect concurrence among information security professionals. Further, commonly accepted policies should be adopted without change because not to do so could introduce unforeseen risks. Counties and their departments can use commonly accepted IT security policies as a reference in developing their own policies, provided a thorough risk analysis is conducted.

Today's information technology offers improved communication, but also increases vulnerability. Critical information is distributed across different systems, consisting of various combinations of hardware, software and networks. Network interconnections offer users the ability to communicate and share data with any other connected user anywhere in the world. This capability also allows any other user to retrieve information, sometimes in inappropriate ways.

Information security policies must address both technical and non-technical means of communicating information. Information technology has diversified over the years, but requirements for information-handling have remained relatively consistent. People need to communicate via voice, video, paper, images, and data.

Technology allows us to communicate information in many ways, including telephone, radio, television, facsimile, and computers. Because information must be protected in whatever form it takes, it is also important to consider security-related issues with paper, surface mail and even presentations at public conferences. People are increasingly dependent on information technology, so it is important to protect technology from misuse. However, information security must also address non-technical methods of handling information.

Purpose

There are at least four major reasons for implementing information security policies. First, policies set the stage for appropriate behavior and awareness of acceptable business practices. Second, they help staff operate information-handling systems in a secure manner. Third, they assist administrators and developers in the implementation and configuration of secure information-handling systems. Fourth, they provide managers a means for determining whether new requirements are adhered to, or necessitate a change in, current policy.

Specifically, information security policies should:

- Provide a common understanding of information security terms;
- Define the roles and responsibilities of staff responsible for information security;
- Create a reference for commonly accepted information security policies and practices;
- Establish criteria for assessing the security capabilities of information handling systems;
- Define processes for adding, modifying, and deleting information security policies and practices.

Roles

Information security policies should be written for the intended audience. In general, policy writers should consider five audiences: executives, managers, administrators, developers and users. **Executive level policies** define what will be established and which part of an organization will be responsible for managing it. **Management level policies** define what an information handling system does and who is allowed access. **Administrator level policies** explain how an information handling system should be configured. **Developer level policies** define policies for the design and construction of information handling systems. And **user-level policies** explain how an information handling system should or should not be used.

Types

Policies should be tailored to address specific issues and activities. For each of the types shown here, consider what the policy is supposed to encapsulate.

- Usage policies define what is allowable and how it will be enforced. They explain user roles and responsibilities, limits on administrator access, and other restrictions related to usage.
- Control policies define what is secured and who is responsible. They identify what should be done to prevent unauthorized access to systems, programs, and data.
- Service policies define system management, technical support, etc. They identify what should be done to control software versions, system configurations and data integrity.
- Legal policies define the use of copyrights, trademarks, logos, hyperlinks, etc. They also identify applicable federal, state and local laws.
- Content policies define what can be published, uploaded or downloaded. They define ownership and who is accountable for content.
- Design policies define requirements for design, development and acquisition. They prescribe security reviews for specified processes.

Areas

Information security policies should be cataloged in one of several areas:

Information Architecture

These policies describe the information-handling systems employed by the county. They identify which information-handling systems are mission critical, whether they should be backed up or not, and the associated restoration priority. They can also include or refer to standards for hardware, software, network and other components, but specific procedures for acquiring, configuring, and maintaining resources should be defined elsewhere. These policies are intended for managers as well as system and network administrators.

General Information Protection

These policies define what should be protected and how people can determine if protection is needed. They outline the protective measures that should be employed (even for non-technical communication) and state the roles and responsibilities of staff in providing protection.

Managerial Security

These policies define information ownership, information security functions within the organization, and criteria for conducting personnel background investigations. They also define processes for assessing risk, implementing policy and responding to incidents. These policies are intended for managers, but might be of interest to system and network administrators as well as staff.

Physical Security

These policies define how to control physical access to information handling systems. They define controlled areas, key management, identification badges, visitor handling, facility requirements, and the roles and responsibilities of security guards as well as authorized staff.

Logical Security

These policies define how to control logical access to information. They address user IDs, passwords, the login process, activity tracking logs, configuration management and other topics. These policies are intended primarily to help system and network administrators manage information handling systems, but the users might want to know some elements, such as the limit for guessing a forgotten password.

Technical Security

These policies define how to control technical access to information. They describe general precautions for, and acceptable use of, e-mail, the Internet, intranets, telephones, electronic storage media, and other systems available to users. They also discuss specific technical measures such as the use of anti-virus software, encryption and other mechanisms.

Procedural Security

These policies recommend how to acquire, configure, maintain, and otherwise manage specific types of resources. For example, "hardening" a web server could refer to the manufacturer's recommended procedure, but the organization might include additional precautions that the manufacturer's procedure does not fully address. Procedural security policies can be very detailed. For example, there may be a need to explain why and how JavaScript should be disabled. Procedural security policies could also be very general. For example, all malfunctions should be reported to a Help Desk. In any case, procedural security policies explain what to do.

Domains

Policy writers should also consider different domains of operation. Within an organization, one department may need stricter controls than another. For example, policies for a law enforcement organization might be different than those for a training organization. Within an enterprise, one information handling system might apply different controls than another. For example, policies intended for mainframes may be different than policies for web servers.

Construction

With policy development, the following general questions should be addressed clearly and concisely:

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- On which laws/regulations (if any) is the policy based?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information assets must be protected?
- Who is the information owner (best source for shared information)?
- Who is the custodian of the information?
- Who decides who reads, creates, modifies, stores, distributes, or deletes the data?
- What are information users required to do to safeguard the data?
- How should security breaches and violations be reported? And how often?
- What is the effective date and expiration date of the policy?

Chief Information Officers (CIOs) will absorb these recommendations as appropriate, and communicate the results into a meaningful governance policy that fits the enterprise.

Related Documents

Wherever possible, policies should refer to original sources. For example, a policy on "hardening" web servers should refer to the manufacturer's documentation in case a new vulnerability is discovered that changes the recommendation. Existing laws, regulations and agreements must not be superceded by policies unless exceptions are allowed.

The following sources are highly recommended for helping develop information security policies:

- ISO 17799.
- "Common Body of Knowledge" International Information Systems Security Certification Consortium, Inc. 2001.
- Charles Cresson Wood. "Information Security Policies made Easy" Baseline Software. 1997. ISBN 1-881585-01-8.

Conclusion

The first step in establishing an effective Information Security Program is to document the policies for protecting information. Policies provide guidance for users, administrators and managers to protect information. They also help explain how to operate information-handling systems in a secure manner. As much as possible, policies should provide consistent protection across different scenarios. Policies should explain the process for change so that current practices can be improved. Documenting information security policies provides a focal point for resolving information handling issues, helps coordinate inter-department security efforts, and improves the overall security posture of the enterprise and the organization it supports.

Information Security Awareness, Training and Education

Introduction

Outlines the basic user security training and awareness requirements in the context of County Information Security Best Practices.

The Need for Security Awareness Training

For any set of policies to work, the target audience must be aware of it and understand it. The following Security Training and Awareness Program has been developed to help achieve these objectives. By necessity, this section of the Security Best Practices document is "general" in nature as every department must custom develop its program according to its own social culture and data systems topologies.

The term "security awareness" may be considered the daily "moment-by-moment" awareness level, while the term "security training" relates to the basic training all employees need to build their basic security skills. Security awareness is partially a by-product of training, but it also is the result of environmental factors. The elements that help develop information security awareness are treated separately in the Information Security Awareness Elements section.

What is Expected and by whom

The level of security awareness, security training, and corresponding responsibilities varies with County employee job function and department. Roles and responsibilities for each audience should be clearly communicated in this training.

Information Security Awareness Elements

While security training is a clear concept, the concept of security awareness is a bit more ethereal. It deals with the level of security consciousness. Therefore, we are talking about various "reminders" or "visual cues" that can be used to help users think security.

Following are some basic elements needed to increase security awareness:

- Pre-Login "Splash Screen" with usage warning. Must point to the county's Fair Usage documentation;
- Weekly security updates and notices;
- Institute security-centric contests for logos, mottos, etc.;
- Purchase pre-packaged security training materials (hard copy, web, or combo);
- Provide for in-house classroom training.

Basic Information Security Training Elements

The bulk of county employees will need only the minimum level of security training containing the following:

- Incorporate basic security training for all new hires, ideally before a new hire sits down to do his or her job;

- Include in the training curriculum "social engineering" techniques that hackers use to gather information;
- All employees must attend security policy training classes every two years;
- All employees must be tested for basic security awareness every year;
- Explain to employees that while their departments are the "owners" of the data, they need to assist the Information Systems department in its safekeeping;
- Explain to employees the difference between "public" records and the need to keep information "confidential";
- State reasons why specific policies are needed;
- Describe what is covered by the policies;
- Define policy contacts;
- Define user's responsibilities;
- Define how violations will be handled;
- Balance protection with productivity.

Advanced Information Security Training Elements

Information security personnel, Information Technology employees and certain other employees with access to sensitive information require advanced information security training in addition to the basic training above. The type of advanced training depends on the employees' roles and responsibilities.

Further Guidance

Another perspective on training breaks down the different categories according to the following three generalized classifications:

- Management
- Technicians
- End-users

All of these have different responsibilities that must be emphasized in the training. The management training module should discuss what information security is, what the county policies are, what the risks are, what we are doing to mitigate those risks, what management's role and responsibilities are, what it should be concerned about, and what members of management need to do in their daily activities. The technicians' training needs to identify risks, what the county policies are, what technicians need to be concerned with from a technical perspective, what kinds of practices they need to follow to sustain security, what the procedures are for administering, managing and maintaining the technology, what actions they need to take to identify problems, resolve them, and escalate problems that they cannot resolve. The end users need to be aware of applicable policies and procedures, where to get more information, and where to turn for help.

Conclusion

The success or failure of any set of security policies is directly related to the level of security awareness and security training in the employee population. A combination of clearly written policies, employee training, and security awareness activities will increase the overall level of information security effectiveness throughout the county.

Sample Information Security Awareness Training Outline

An Information Security Awareness Training Program must take into consideration all persons with the potential of coming into contact with county-controlled informational assets. This includes the custodians to executive management. Everyone will, in the course of a job, come into contact with a variety of information in many forms, and must have a thorough understanding of how this information should be managed, including certified destruction, recycling, or "holding in confidence" for a minimal amount of time (could be legal mandate). The Information Security Awareness Training Program will use multiple medias (e.g., electronic, posters, video, audio, banners, post-it notes) for this purpose.

Objectives:

- Create multimedia presentation specific to county business units;
- Use as stand-alone (Computer Based Training) or as classroom presentation;
- Give new employees information that they will find helpful in protecting informational assets;
- Raise awareness of county policies, departmental procedures and individual's responsibilities;
- Give direction about where – and from whom - to get additional information.
- Intended audiences
    - New employees
    - Employee "refresher" training

Contents:

1. Department Introduction
    a. Departmental Purpose and Objectives
    b. Departmental Charter and Mission Statement
    c. Key management personnel and the responsible roles
    d. Position in county organizational structure
    e. Relationship and interface with other business units
2. County Policies
    a. Board orders and CAO policies
    b. Relationship between policies
    c. Specific policies all users need to know
        i. County Information Systems – Management and Use
        ii. Acceptable Use of County Controlled Data/Information
        iii. Telecommunications – Management and Use
    d. Reasons and justifications for these policies
    e. Explain Information Security objectives covered in policies
        i. Confidentiality
        ii. Integrity
        iii. Availability
3. Department-specific sensitive, confidential, or restricted information
    a. List of information handled, generated, and stored by the department
    b. Must address both paper-based and electronic information

4. Department Procedures
    a. Procedures – To Be Developed
    b. Specific to the CAO and Department Head's objectives
    c. Needs to address handling, storage, and destruction of information
    d. Departmental policies if more stringent than county policies
5. Whom to contact or where to go for additional information
    a. Define with whom the employee needs to interface
        i. Supervisor, Manager, or Departmental Personnel Management Officer
        ii. Departmental Information Security Representative (ISR)
        iii. Personnel Assistant or Help Desk
    b. Define where the employee can obtain more information
        i. County Internet site (for official documents)
        ii. Intranet site (CAO Administrative Manual, Department Web site)
        iii. Departmental Procedures Manual
6. Whom to contact if issues or incidents arise
    a. Supervisor, Manager or Departmental Personnel Management Officer
    b. Departmental Information Security Representative (ISR)
    c. Chief Information Security Officer
    d. County Internal Affairs
    e. Personnel Assistant or Help Desk

Information Identification and Classification

Introduction

The Information Security Program must incorporate standards and procedures by which information resources are managed and accessed. These standards identify and classify the information collected and maintained by the information owner, based on that information's content, sensitivity and importance.

An identification methodology is used to categorize information content into distinguishable categories (Medical Records, Project Data, Fiscal Budget, Fiscal Annual Report). These categories then facilitate subsequent classification.

A classification scheme is used to determine adequate and appropriate procedures, and their associated access controls for information protection and distribution. Access control must be consistent with the classified value of the information resources to be protected and the severity of the threat to them.

Information Identification Methodology

Before information can be protected through a classification scheme, the following must first be understood: what the information is; where the information is; and why the information is important. These sub-elements are critical to the identification process, eventual information classification, and other processes such as Risk Assessments.

Information owners must develop standards by which categorization of information content can be accomplished. These standards must easily guide users in determining into which category their information falls.

Sub-elements are critical to Information Identification:

- Content: What is contained within the information (e.g., SSN#, medical info, project data, financials)?;
- Location: Where is the information located (system and/or physical location)?;
- Purpose: What purpose does the information serve (e.g., some information may be part of a larger information store)?

Classification Scheme

Once information is identified and categorized, classifications can be applied to enable applying appropriate access control and distribution of the information. The following key elements should be addressed, in combination or individually, when developing a classification scheme.

Security Classification

Classifications, which define how information is accessed, maintained, and distributed, must be established. These levels of classification further detail all associated protection measures as well as penalties for breach of access or unauthorized disclosure.

Classifications and their respective security measures must be consistent with the categories they protect as well as county, state, and federal guidelines and regulations.

Eligibility for Classification

All information can be placed into classifications that determine adequate and appropriate procedures and their associated access controls for information protection and distribution. However, some categories of information may be non-eligible for higher or more secure classification based on county, state, and/or federal guidelines and regulations. Standards or guidelines based on the previously identified categories must be developed showing eligibility for classification.

Original Classification

Original classification uses reasoned judgment and definitions of established classifications to determine which level of classification is to be applied. Guidelines shall be developed to detail original classification.

Duration of Classification

At the time of original classification, the original classifier must make a decision about the length of time the information shall require the protection of security classification.

Guidelines specific to duration of classification, and consistent with county, state, and/or federal guidelines and regulations, must likewise be developed.

Identification and Communication of Classification

Original classification must effectively be communicated to persons who will be in possession of the information. Also important to this aspect is ensuring that the information contains the proper marking and or warnings to reflect the classification.

Classification Access

Also important are the roles or persons who are allowed to view or interact with the information.

Consistency

Guidelines specific to classification access must be consistent with county, state, and/or federal guidelines and regulations. Any standards, guidelines or regulations developed for the identification and classification of information must not discard county, state or federal guidelines or regulations.

Conclusion

To achieve the most cost-effective information security controls, a county must identify and classify its information. County resources can then be most effectively utilized to prohibit sensitive information from unauthorized use.

Information Risk Management

Introduction

Risk is defined as, "the possibility of suffering harm or loss; danger," and "to expose to a chance of loss or damage; hazard." It is clear from these definitions that risk involves a probability of the outcome of an event turning for the worse.

As individuals, some level of risk is involved in almost everything we do. Risk is inherent to such things as crossing the street, investing in the stock market, driving to work, accepting a job, and playing a sport. We naturally take risks because we know that there may be some level of return involved. When we cross the street, we may get to where we want to go. When we invest in the stock market, drive to work, or accept a job, we may realize financial returns. When we play a sport, we may experience recreation, exercise, competition, and stress relief.

When we do something that involves risk, we consciously or unconsciously calculate what is involved in taking the risk. In some cases, if the risk is too great, we may decide to forego the return altogether. Crossing a busy freeway to get to where we want to go is something many of us would not do. In other cases, we study the risk carefully and we ask ourselves questions that allow us to come to a decision. We may try to see if the risk can be transferred in some way, as with purchasing insurance. We may also look at ways of mitigating the risk – are there smarter, less risky ways of approaching something? Is there anything that can be done to decrease the risk? Internally, we identify, analyze, and make a decision to accept or forego the risk. In other words, we are our own risk managers.

Like individuals, almost every organization that seeks some type of return must manage the risk that is associated with those returns. County departments that ignore risk or fail to transfer or mitigate risks have a good chance of failing. In these cases, the department may face legal penalties or, in extreme cases, people's lives may be endangered. Therefore, it becomes the responsibility of the department to manage its own risk to be successful. The key enabler to managing risk is to hire people who clearly understand how to identify risk, how to analyze risk, how to weigh the risk against numerous factors, how to transfer or mitigate the risk, and how to make well-informed decisions.

One of the most important risk factors for a department is how it manages information. Departments rely on information – knowledge derived from study, experience, or instruction. For example, information can include business strategies, ideas, research, financial and legal agreements, employee information, and overall financial figures. Above all, information enables decisions – decisions that can be made by the right people in order to build more success.

Information is central to the county's existence – it must be successfully managed. Only selected people should see some information, such as strategic communications, payroll information and personnel reviews, for example. There is risk if sensitive information is not kept confidential; if it leaks, it can cause harm to the county or to people within and outside the county. There is risk if information is not maintained to ensure its integrity; if it is permanently destroyed, weeks, months, or years of effort can be lost, ultimately affecting the county's outlook and reputation. There is risk in not ensuring the availability of information; if people cannot access vital information, decisions may not be able to be made or the wrong decisions may be made or customers may not be able to use the expected service.

This document outlines the general process for managing information risk – how to identify, analyze, and ultimately make well-informed decisions that will more than likely contribute to the success of the county business.

Managing Risk for Information

Risk management, in the context of information, is the identification, analysis, and management of events that have some probability of compromising the confidentiality, integrity, and availability of valued information assets. The primary goal of this type of risk management is to minimize or eliminate the chance of valued assets being exploited or damaged.

An information asset is any entity or system that is capable of containing or transferring information that is vital to the business. This can include a computer, a terminal, a file, a physical letter or contract, a white board, a user account, a paycheck, an e-mail communication, a service or program, communication media, and even people or a conversation between people.

There are inherent risks involved in containing and transferring information. Information is subject to intentional and unintentional actions by other people or systems. If information is confidential, there may be unauthorized people who want to see it, such as competitors or internal employees. People may try to break into the devices containing the information or try to intercept it as it is transferred. People may also receive confidential information unknowingly and completely by accident. Information breaches like these can seriously hurt the county. Furthermore, information and systems that compute and display information can be maliciously or accidentally damaged.

It is up to the county to manage these risks so that the desired returns can be realized. But how does a county go about managing these risks?

To manage information risk, an organization needs to:

1) Create an Information Risk Management group or committee;
2) Identify information assets, and the general value of each;
3) Identify the threats to each asset based on confidentiality, integrity, and availability;
4) Analyze the risk to each and all assets based on an acceptable risk model;
5) Analyze how to manage identified risk for each asset – accept, transfer, or mitigate the risk;
6) Continue to manage risk by reiterating this process continuously.

Create an Information Risk Management Group

Information risk management is always ongoing effort. Although it is possible to assess and manage risk at only one point in time, the assessment and actions taken may become obsolete over time due to the dynamics of systems, people, and information. New threats emerge every day on a worldwide scale for specific systems. A hacker attacking one company on one side of the globe may reveal a weakness (or a threat) that exists in all other companies, which ultimately increases risk to these companies. The county must have the capability to continually identify emerging threats that affect the systems in use, measure this new risk, and then react accordingly.

Because of this dynamic behavior, it is imperative that an Information Risk Management (IRM) group is established to periodically assess and manage risk within the organization. The main mission of this group is to first assess current risk to the organization using this process, and then to establish a periodic re-assessment schedule so that risk is continually managed. This group should consist of:

- People who understand, or can quickly develop an understanding of how the organization is structured, who the leading decision-makers are and the organization's strategic goals;
- People that understand information systems in detail, how these systems can be exploited, and how to identify, develop, and implement countermeasures to these threats;
- People that can interface with the leaders who can make decisions on how to manage identified risk.

Identifying Information Assets

The IRM group must first understand the department's vital information assets, a general value of each asset, and how it contributes to the overall business goals. An information asset can mean many different things to a department, depending on what that department is trying to accomplish. Information assets usually include proprietary information, critical processes, mission-critical systems, payroll information, research, strategic decisions, customer interfaces, financial data, and internal tools and source code. Information assets are vital to keeping the organization profitable and competitive. Some processes or services may be so vital and mission-critical that, if compromised, they may cause injuries (or worse) to people. Therefore, at the extreme end, vital assets also may be vital to keeping people alive.

What a department identifies as an information asset is completely up to the department itself. A single computer or an entire product line can be considered an asset, depending on who in the department is consulted. For the best results in measuring risk, information assets should be broken-down as much as possible. If a department is given an information asset, that asset should be broken into the systems and sub-systems that manage the information, the processes and procedures that people use, and the devices used to transfer, calculate, and present the information asset.

To identify the information assets and their related values within an organization, the IRM group must perform interviews with key people within the department, starting with top management and continuing down to technical staff. The IRM group must:

- Interview leaders within the organization. These people are ultimately responsible for keeping the organization running and should fully understand what the true, vital assets are (at least at a general level). These people should also have the ability to assign some type of value to each asset.
- Interview financial leaders within the department to understand critical assets from a cost perspective.
- Interview managers responsible for critical services or products and understand what is critical within their department/group. What systems are involved in managing the information?
- Interview technicians and engineers who are responsible for critical data, processes, or systems.

Ideally, each identified asset should be assigned a dollar value. This value can then be used to express risk in terms of total costs to the organization, which is a very clear and direct way of communicating to upper management and enables high-level decision-making. In some cases, deriving value is not possible because value cannot be assigned to some assets (such as people). If this is the case, the value should at least be expressed in general levels that make sense to the organization – very high, high, medium, etc. These levels should be well defined and able to be communicated to - and understood by - the organization.

Overall, the purpose in identifying vital assets is to enable the management of higher-priority risks first – the risks that can be the most damaging to the department.

Identifying Threats to Assets

A threat is a negatively impacting event that has some probability of occurring. A threat to an information asset is an event that may occur intentionally, accidentally, or naturally, and that has a probability of damaging or compromising the information. The damage depends on the type of information asset involved, but usually affects the confidentiality, integrity, and/or availability of the asset. The end-result of this damage is the degraded ability (or complete inability) of the organization to achieve its objectives.

Examples of threats to information assets include, but not are limited to:

- Internal threats (i.e., malicious or uneducated employees);
- Mobile threats (i.e., attackers who steal remote systems which, in turn, provide access to information);
- Physical threats (i.e., attackers who steal computers or enter server rooms, file cabinets, or offices);
- Natural threats (i.e., electrical outages, hardware failures, fire, floods, and earthquakes);
- Network threats (i.e., attackers who try to compromise systems exposed on a public network or try to spoof or imitate remote systems);
- Social threats (i.e., attackers who try to fool employees into revealing information);
- Viruses, worms, and Trojan horses (i.e., code that may damage, reveal, or capture information).

Threats to information assets must be identified at as many levels as possible. Collectively, the IRM group needs to have a thorough understanding of threats and how their outcomes can affect information. This group must develop a full understanding of the information assets and their values to the department. This group will need to understand how these information assets are stored, used, and transferred. This will involve a thorough understanding of the systems used, such as computers, operating systems, security subsystems, physical storage, network media and devices, phone systems, transmission protocols, and the related vulnerabilities that exist for these systems. This group will also need to understand higher-level processes, applications, and policies – how do employees use the information?

The combination of understanding the values of information assets, where these assets exist, and how these assets can be exploited will enable the IRM group to identify the true risk to the department, which is explored in the next section.

Analyzing Risk to Information Assets

Risk to an organization for a given asset can be provided in the most general form using the following equation:

Risk = (Probability of a threat occurring against an asset) x (Value of asset)

In other words, the higher the probability of a threat occurring and affecting an asset and the higher the value of that asset, the higher the risk. If a threat has little or no chance of occurring (which is the best case scenario), or if the value of the asset has no worth, then the risk is either very low or zero. Since information assets within a department most likely hold some level of value, risk management becomes a process of reducing the probability of threats from occurring.

Total risk to a department is the aggregation of all risks to all information assets, and can be calculated using a specific model, added together, or averaged, depending on how the quantified risk is to be communicated.

Selecting a Risk Model

In order to quantify risk in some fashion, the IRM group will need to develop a method of measuring risk so that this information can be communicated to the county or department leaders. Ultimately, these leaders need to understand:

- What is the total (aggregated) risk to the county or department?
- What information assets are at most risk and what can happen to these assets and the county or department if compromised or damaged?

The best way to quantify risk is to develop some type of risk model that expresses the quantity of risk involved for each asset. There are many models that have been developed to measure different kinds of risk. Some models involve detailed mathematical and statistical analysis to provide exact measurements. Other models are general and simplistic. Selecting a model (or models) that fits the needs of the county or department will be the task of the IRM group.

A more detailed model is provided below:

$$Risk = \frac{Threat}{Countermeasures} \times \frac{Vulnerability}{Precautions} \times \frac{Damage}{Lessons} \times \frac{Value}{Effort}$$

Where:

- Threat is a method, means or goal of attack;
- Countermeasures are the steps taken to prevent a threat from carrying out an attack;
- Vulnerability is the exposure of an individual or object to attack, even if countermeasures are employed;
- Precautions are the steps applied to reducing vulnerability;
- Damage is the cost realized in the aftermath of an attack;
- Lessons are positive values realized as a result of an attack; perhaps unrecognized before an attack;
- Value is the cost of implementing the capability that is at risk;
- Effort is the amount of effort to protect value.

The outcome of any risk analysis using some model will be a numerical representation of the risk that is associated with each information asset or an aggregated value for all assets. This can be communicated in cost or in relative ranking, or in both. For example, it can be determined that the department has $3,000,000 of assets at risk consisting of 28 separate assets that can be threatened in 430 different ways. Another example can include a department defined risk ranking on a scale from 1 to 5, with the example of 15 assets having a risk of 5, 10 assets having a risk of 4, 7 assets having a risk of 3, and so on.

While effort can be quantified as the cost of implementing countermeasures, taking precautions, and applying lessons learned, value cannot be easily quantified if human life is at risk.

Summarizing and Communicating Risk

Once risk has been measured for each information asset, and for the department as a whole, this information will need to be summarized and communicated so that decisions on how to manage this risk can be made. The IRM group will need to prepare these reports and present this information to the county or department decision-makers. These leaders will want to understand risk in terms of costs to the county or in terms of pre-defined levels.

Managing Risk

Once the risk to vital assets has been measured, a decision must be made on how to manage that risk. Managing the risk involves making a decision on how to approach the risk, including analysis of the costs involved in each approach. There are three approaches to managing risk - accepting the risk, transferring the risk, or mitigating the risk.

Accepting the Risk

An organization may choose to simply accept risk under these scenarios:

- This risk is considered low (i.e., the value of an asset is low and the probability of threats affecting the asset are acceptable).
- The cost of accepting the risk is found to be lower than the cost of transferring or mitigating the risk.

If the cost of accepting the risk is high or more than the cost of transferal or mitigation, then the organization should not accept the risk. The organization should then look at transferring or mitigating the risk.

Transferring the Risk

When the risk is transferred, the risk is shared with a third party in part or in whole. This is typically seen in the use of insurance. Third party insurance organizations, for a fee, agree to accept the risk and compensate the information owner for the full damage of a particular, given risk. In some cases, transferring risk may not be available – there may be no third-party entity that will insure the risk. In other cases, the risk may be too high and too costly to insure. In this case, the county or department must either mitigate the risk or accept the risk.

Mitigating the Risk

When a risk is high for a particular asset, and the risk cannot be transferred (i.e., not practical or cost-effective), then the risk should be mitigated in part or in full. The mitigation process is the process of identifying the most probable threats to a given asset and identifying, researching, or developing an acceptable countermeasure to that threat.

In some cases, mitigating the risk can be fast and inexpensive (sometimes free). Information systems suppliers may provide free security patches, and may even provide mechanisms that perform automatic updates to these systems. Applying security updates or bug fixes may simply involve the time and skills of the internal staff.

In other cases, mitigating risk can be very expensive. For example, if buildings housing computers that contain vital information are at risk to natural disasters, the department may have to consider moving to a different location or providing redundancy by adding buildings.

There may be different levels of countermeasures that can be applied to one threat that may only reduce the risk to an acceptable level to the department. There may be certain aspects of a threat that can be reduced by implementing countermeasures, and some other aspects that may be covered by transferring the risk. Taking the example of the development of a new building – costs may be incurred to purchase new, redundant hardware while insurance may be purchased to cover the building itself.

When processes are identified to incorporate threats, this may involve restructuring the process and re-training the people involved.

Assessment Tools, Auditing, and Policy Management

Throughout this process, the IRM group should examine leveraging tools (software, procedural, etc.) for helping in the assessment and management of risk. These tools, if applied and used properly, will usually speed-up the assessment process, or ease the management process. Freeware and shareware-based tools are available for multiple types of systems (although great care should be taken when using these tools, and support is typically limited). Tools that can be purchased, such as dedicated information risk management systems, are available and usually offer greater reliability and much-needed support services. Examples include tools that help identify and inventory information assets, assess security configurations, measure performance and availability, and implement "emergency" patches quickly.

Auditing tools are often available or integrated within systems that contain or transfer information assets. The IRM group should consider installing and enabling these tools to help manage risk continually. Although not a replacement for risk management, these tools can help to identify events that compromise the confidentiality, integrity, and availability of information assets.

Policy management tools also may be available or integrated into systems. Unlike auditing, which enables the identification of possible compromise, policies typically allow the prevention of possible compromise. Policy management tools can limit what people do or see on systems. For example, a user policy can be enforced to allow certain users access to only the programs they need to use, and prevent access to other programs, enforcing confidentiality. Some policy management tools can see that certain people or processes receive maximum bandwidth to critical systems, such as with Quality of Service, enforcing availability. Other policies help in sending data in a highly reliable format, enforcing integrity.

Tools, auditing systems, and policy enforcement systems can greatly ease and speed the assessment and management process.

Conclusion

Risk management must be fully understood by any department that seeks long-term success. Information risk management includes the identification, assessment, and management of information assets – assets that contain or transfer vital information on which the department depends. Proper risk management ensures that confidential information is not breached, data integrity is retained, and information and service availability is provided.

Assess information risks by first creating an Information Risk Management (IRM) group that takes responsibility for assessing and managing risk not only on a one-time snapshot basis, but on a continual basis as well. To assess risk, this group needs to identify the vital information assets within a department. Once these assets are fully understood, the group will need to identify any threats that can compromise their confidentiality, integrity, and availability. Risk to each asset can then be measured. Generally, the more valuable an information asset is to the department, and the higher probability threats are to occur against this asset, the more risk is involved. To provide a more detailed risk assessment, advanced models may also need to be used.

Once risk to the department's information assets is understood and measured, this assessment must be communicated to upper management so that decisions on how to manage the risks can be made. Managing risk involves the acceptance, transferal, or mitigation of the risk. In any case, detailed cost/benefit analysis must be used to determine exactly how to manage the risk.

Accepting risk should only occur if the risk is low or the cost of transferring or mitigating the risk is too high. Transferring the risk involves using a third party insurance entity to transfer the risk in part or in full. Mitigating the risk involves countering the risk - and the threats involved - with solutions. These solutions can either be third party-supplied or internally developed.

Also important is the use of tools, auditing, and policies. Tools can be used to help assess risk, as with dedicated information risk management systems. Some tools can also help mitigate risk for the longer-term. Auditing allows the department to identify over time the possible threats and risks to a department and allows future risk assessment and management. Policies enable a department to define how to prevent the exploitation of information assets and how to discipline those people who do compromise the information. Policies, whether procedural-based, or system based, should be used to minimize risk.

By following this general process, a department can be much smarter when making decisions, not only benefiting the profits of the department, but also benefiting everyone involved.

Implementing Information Security Controls

Introduction

Implementing security controls focuses on the generalized mechanisms that control access to data and resources. Here we consider: design constraints, third-party software and system evaluation, general evaluation guidelines, in-house software and system development, operating system upgrades and patches, and relating these complex issues while maintaining synchronization within accepted business constraints. Further consideration is given to Risk Assessment, with an emphasis on county-related issues. Please note, however, that Risk Assessment is handled in detail in the Information Risk Management section. Consideration is given to the relationship between usability and functionality, as well as social acceptability of various control mechanisms.

Design Constraints

Information security products that are selected should be easy to use, administer and audit. If all essential functional requirements can be met, security products that have been evaluated by county, state, or federal government computer security centers are preferred over products that have not been evaluated.

New information security products must be on the market for at least one year before being considered for use on county systems. Within the confines of cost-justification, information security controls must be selected and designed in such manner that reliance on a common mechanism is minimized. If a common mechanism, such as a PBX telephone switch, is used, its failure or unavailability may have a serious effect on overall security. For example, if a single node on a network is the sole provider of gateway-style access control services, then the unavailability of this one node might mean that the whole network is unavailable. This policy instructs systems designers and other technical staff to avoid such vulnerable designs.

For all business application systems, systems designers and developers must consider security from the beginning of the systems design process through implementation as a production system. Designers and developers must minimize the impact on user productivity and support resources. Information must be protected consistently, regardless of media, storage location, system or process used to handle information.

Whenever feasible and cost-effective, system developers should rely on system services for security functionality, rather than incorporating such functionality into applications. Examples of system services include operating systems, network operating systems, database management systems, access control packages, front-end processors, firewalls, gateways, and routers.

To take advantage of security improvements, the most recent version of a computer operating system should be obtained and installed after being thoroughly tested. If obtaining the complete operating system is not cost-effective, then any and all software patches that close security vulnerabilities should be obtained and installed.

The security of a computer system that handles sensitive information must not be dependent on the security of a computer system that handles non-sensitive information. Using wholly independent security systems for each computer system is not required, and in fact not preferred; but systems that handle sensitive information should be partitioned from systems that do not. For example, a given user's password to enter criminal justice information systems should be different than the password for accessing the Internet. Information owners make the final determination of whether or not to participate in a security system that provides "single sign-on" capabilities.

Business Constraints

To assure compliance with information security standards, hardware and software selected for county use should undergo a review by the departmental Information Security Representative (ISR). The CISO may be involved on a consultation basis if desired. Managers may not authorize the download and testing of trial version software without first obtaining approval from the departmental or centralized Information Technology unit, and this software must remain isolated from production software.

County information systems should employ information security standards typical of state, county and local government organizations. At the very least, all county information systems must include standard controls found in organizations in similar circumstances. Beyond this, the unique risks faced by the county must be addressed with customized solutions.

To keep costs down and to facilitate systems development, commercially available information security solutions are preferred over "in-house" solutions. Exceptions to this policy must only be made when the cost-effectiveness of an in-house solution has been clearly analyzed, documented, and approved by the CISO.

Information systems security controls must be enforceable prior to being adopted as a part of standard operating procedure. For a control to be enforceable, it must be possible for managers to clearly determine whether:

- The control effectively performs a required security function; and
- Authorized personnel actually comply with and use the control.

Risk Assessments

Production information systems must be evaluated by the departmental ISR to determine the minimum set of controls required to reduce risk to an acceptable level. Risk assessments for critical information systems and production applications must be performed at least once every two years. All major enhancements, upgrades, conversions, and related changes associated with these systems or applications must be preceded by a risk assessment. For every risk, management must make a specific decision about whether risk will be accepted, mitigated, transferred or eliminated.

In the absence of management approval, staff must consistently observe county information technology security policies. Exceptions will be permitted only when the ISR has signed a risk acceptance memorandum. Such a memorandum must document both the risk and actions that must be taken to mitigate that risk.

Agreements between the county and third parties who access county information systems must include a special clause. This clause must allow the county to review third-party controls, policies and procedures that protect county information stored or processed by that third party. The clause must also specify the ways in which county information will be protected. Third parties should be advised that if they present an unacceptable risk and refuse to improve their information security controls, policies and procedures, then the ISR has no alternative but to deny access by that third party.

Conclusion

Using commercially available security controls is the desired method to determine that appropriate controls are in place to monitor that informational assets remain secure at the risk level assumed by management. Using these commercial tools allows a more rapid deployment and ongoing maintenance to guarantee current technological changes are being implemented in enhanced versions of the security controls mechanisms. Properly implemented information security controls reap significant benefits by providing rapid deployment and ease in maintenance, validating systems integrity and availability and allowing proper information classification and information retention schedules.

Page intentionally left blank

Monitoring Effectiveness and Assurance

Introduction

The county must be able to monitor the measures that have been implemented within the Information Security Program and must determine that security goals of the enterprise are met. This section defines how this is accomplished. Information collected from processes that measure effectiveness and assurance enable the county to identify value in implemented security measures.

Security is something that everyone needs. We need it in our personal as well as professional lives. When our personal security is threatened, it is natural for us to reflect on events that occurred. Did we handle it well, maybe something didn't go quite right and we need to think about what to do next time. If we managed to escape without harm, it makes us feel secure and proud that we were effective in dealing with the situation. This provides "proof" that we were prepared enough to fend off a threat. Daily, we get into cars and feel assured that the air bag will deploy if we get into a collision. We are assured of the effectiveness of this device because manufacturers provide us with proof that it works and we are provided with evidence that drivers escaped injury when these devices were deployed.

Although they seem very different, threats that affect our personal security have much in common with threats that affect the security of information in the county. These risks take form as threats to county information. Both types of threats need protective measures and a process for identifying how effective the security measures are. In the county, there are electronic guardians that stand watch twenty-four hours a day, protecting sensitive county information. The most familiar of these electronic watchdogs is "anti-virus software" that is installed on county computers. We know it is there, but how do we know it is doing a good job? How many threats were actually stopped? How many threats went unnoticed? Were county business activities disrupted? There are more complicated preventative devices such as firewalls and intrusion detection systems, but the idea is the same. After deploying security measures, processes must be established to gather information about how well those security measures are performing. After the information is collected, it needs to be "independently" reviewed and evaluated. This is referred to as "separation of duties." Separation of duty is extremely important in monitoring effectiveness and assurance of information security. Staff responsible for administration of a process should not be responsible for evaluating how effectively it protects the county.

How to Measure Effectiveness and Assurance

Some of the ways that information security effectiveness and assurance can be measured are: best practices, benchmarking, surveys, penetration tests, vulnerability assessments and audits of automated and procedural processes.

Best Practices

Industry standard best practices are used in identifying ways to minimize the risks to county informational assets. Best practices identify new measures to be implemented or can be used in comparing to existing measures.

Benchmarking

Before a security measure is put in place, initial problems are identified and measured to enable a basis for comparison in the future. This process of establishing a "starting point" is called benchmarking. Some examples of the information collected in benchmarking is: help desk logs, staff incident reports, server logon activity, record access logs, Intrusion Detection System reports and Virus Management System reports.

Surveys

Existing manual and automated processes cannot identify all issues. That is where a survey becomes useful, to identify and address undocumented events, problems and issues.

Penetration Tests

Penetration tests are used to determine if existing security controls effectively protect internal networks, systems, applications and associated information from unauthorized users. Can a malicious user penetrate your defenses and gain unauthorized access to your systems?

Vulnerability Assessments

Vulnerability assessments seek to identify vulnerabilities that could be exploited by an unauthorized user to negatively impact the confidentiality, integrity and/or availability of your information. After someone breaks in, what can they do?

Audits of automated and procedural controls

It is important that procedures are followed. It is also important that these procedures effectively accomplish their goals.

Conclusion

Threats to county information resources are very real and must be dealt with like any other threat. Protective measures must be implemented and processes installed to determine that the intended function is being performed. Monitoring effectiveness and assurance is an integral part of a good Information Security Program, enabling the county to demonstrate value and provide reassurance.

Business Continuity and Disaster Recovery Planning

Introduction

This section outlines basic business continuity and disaster recovery planning requirements in the context of County Information Security Best Practices.

The Need for Business Continuity and Disaster Recovery Planning

Government does not have the option to fold under the stress of a disaster. All government agencies need to be prepared to deal with business disruptions and have a plan to resume business processes.

Three reasons for creating a Business Continuity and Disaster Recovery Plan are to:

- Develop documented strategies for the recovery of key systems;
- Alert personnel and management to possibility of disasters, making them more aware of those within their abilities to minimize or eliminate;
- Provide a framework to organize the business resumption process.

Business Continuity Planning (BCP) and Disaster Recover Planning (DRP) address preservation of business in the face of major disruptions. While many of the components of both of these are similar, they have a different focus. BCP is focused on maintaining business operations to reduce the overall impact of the disaster, even without automated systems. DRP is focused on getting back to normal operations. Thus BCP can be seen as more of an enterprise-wide responsibility, while DRP can be seen as more of an information systems department responsibility.

BCP and DRP Elements

❑ Awareness and Discovery	❑ Bombings
❑ Contingency Planning Goals	❑ Explosions
❑ Statement of Importance	❑ Earthquakes
❑ Statement of Priorities	❑ Fires
❑ Statement of Organizational Responsibility	❑ Floods
❑ Statement of Urgency and Timing	❑ Power Outages
❑ Risk Assessment	❑ Other Utility Failures
❑ Vital Records Program	❑ Storms
❑ Emergency Response Guidelines	❑ Hardware/Software Failures
❑ Emergency Response Procedures	❑ Strikes
❑ Mitigation	❑ Testing Outages
❑ Preparation	❑ Hazard Material Spills
❑ Testing	❑ Employee Evacuation/Unavailability
❑ Information Security Breaches	❑ Malicious Software (Viruses, Trojans)
❑ Denial of Service Attacks	❑ Public Disturbance (Riots)

Conclusion

The Y2K event is an excellent example of BCP and DRP. Everyone involved with computerized systems had to prepare for the worst-case scenario: the systems just not working on January 1, 2000. Due to the planning, Y2K was largely a non-event, but the processes involved in preparing for that event can be used as a starting point in developing business continuity and disaster recovery plans for any conceivable event

Exhibit 2: Sample Information Security Program

Goals

Information is a valuable asset to any organization. It is an asset that must be readily accessible to those who use the information.

To maintain integrity, information must be safeguarded and protected from inappropriate modification or use. Information that is confidential or sensitive must be accessible only to those who have a legitimate need and right to know.

Information must be carefully safeguarded through clearly defined roles and responsibilities and well-founded risk management procedures that do not unduly restrict access and incorporate careful disaster recovery planning.

Information Security Awareness

All employees and contractors should be aware of the importance of safeguarding county-controlled information and should integrate responsible information practices in their daily routines. Awareness training will be the responsibility of each department.

Roles and Responsibilities

The Board of Supervisors is entrusted to ensure ongoing county services through program support, funding, sponsorship, and board resolution that will allow county departments the ability to perform the county's business.

The County Administrator may establish policies and procedures designed to safeguard county information and compliance through oversight and program audits.

Each county department is responsible for the development and implementation of information security policies and procedures. They are responsible for keeping employees informed of information security programs and conscious of the importance of protecting county-controlled information.

The County Chief Information Security Officer (CISO) is responsible for recommending information security policy and procedures, administration of the countywide Information Security Program, and overseeing compliance by county departments.

Under the Information Security Program, the Internal Information Systems Auditor is responsible for being an advisory member to the ISAC and, working with the CISO to see that the county's assets remain available, maintain integrity, and provide accountability.

County departments, as information owners, are responsible for identifying information as public, confidential and/or sensitive, assigning value to the asset, determining the protection necessary and managing the information accordingly. Information Technology units are responsible for the technical means, to the extent possible, of preserving the integrity and security of county-controlled information and fulfilling the duties of Information Custodian.

Every county employee is responsible for understanding the need for information security and for following the policies and procedures designed to safeguard county-controlled information.

Definitions

- Accountability - An audit trail(s) at the user, application and/or system level that verifies use of any computerized system (network, Personal Computer or other host computer) that will depict the time and date of an individual event.
- Access Administrators - The individual or group that connects information users to information as authorized by the information owner.
- Confidential Information - Information maintained by the county that is exempt from disclosure under the provisions of the California Public Records Act or other local, state or federal laws.
- Critical Application - An application that is so important that its loss or unavailability would have a significant impact on the continued operation of county program(s). This is usually an automated programming tool but may also be a manual process.
- Custodian - An employee or organizational unit that acts as a caretaker of an automated file or database.
- Information - Information includes records, files and databases, but also the information technology facilities, equipment and software used by the county.
- Information Integrity - The accuracy and completeness of information systems and the data contained therein.
- Information Owner - An organizational unit, typically a county department, that has the responsibility for the information contained within an automated file or database as defined by the department's mission or by law.
- Information User - An individual authorized by the information owner to view, change, disseminate or delete information.
- Information Security - The protection of information from unauthorized access modification, destruction or disclosure.
- Physical Security - The protection of information processing equipment, facilities and personnel from potentially harmful situations.
- Program Librarian - A person and/or software program responsible for automated application source program control.
- Public Information - Any information prepared, owned, used or retained by the county which is not specifically exempted from the disclosure requirements of the California Public Records Act or other local, state or federal laws.
- Risk Management - The process of taking actions to avoid risks or reduce risk to acceptable levels approved by management.
- Sensitive Information - Information that requires special precautions to protect it from unauthorized modification, deletion or disclosure.
- User ID – An identifying symbol or set of characters assigned to a specific information user to identify that individual to the information system.

Overall Information Technology Policy

The county will manage the use of information technology to support and ensure countywide planning and collaboration on systems for common services (i.e., networks) and functions. The county will build and maintain a secure, common, standards-based, countywide information technology infrastructure (e.g., access controls, monitoring, network design and deployment) for collaboration between departments and other governmental institutions. County departments will individually manage the use of information technology in support of their missions, goals, and objectives and for dissemination of information to the public.

Elements of Information Security

Each county department will provide for the integrity and security of its information assets by:

- Developing reasonable information security procedures and controls;
- Informing and training all employees regarding information security issues;
- Evaluating employee performance in adherence to security policies and procedures;
- Identifying by type, all automated files, data bases, and other information owned or possessed by the department;
- Identifying automated systems which allow dial-up communication access to critical applications or sensitive information; and,
- Auditing compliance with all facets of the information security program.

Responsibility for Information Assets

Each department of the county maintains ownership and responsibility of the automated files, databases, and other information used in its business activities. If more than one department uses the information, the designated owner is defined as the department that collects and maintains the data by law or mission and authorizes the use of that information.

Each department must designate an information manager or representative(s). Information managers are responsible for determining the value of the various assets, the proper classification of information (e.g., public, confidential, and sensitive) and for authorizing and overseeing the access to files, databases, and other information by users.

Access Protection

Several layers of security protect the county's automated files and databases. System security administrators are responsible for creating, changing and removing user IDs, authorizing access to files and monitoring system usage for all platforms where data resides.

Information users of automated information are individually responsible to keep their passwords confidential and secure. When necessary, specific group-use, read only, user IDs will be assigned by system security administrators. User IDs must not be shared between employees or between supervisors and managers and their subordinates or vendors.

For systems that require "electronic authorization," such as the payroll system, information users must either log on and personally perform the authorizations themselves or have a delegation of this function on file with the Information Manager.

Information users must not use another individual's user ID and/or password.

System security administrators must be notified when:

- Employees no longer need existing user IDs or access to specific files and databases;
- An employee transfers to another position within the county; or
- An employee leaves the employment of the county.

Similarly, access administrators must be notified when contract employees are reassigned or leave their assignment with the county.

Requests to add or delete data system access or to add or delete user IDs can be requested through hard copy or electronically (i.e. e-forms, when available). The request should be fully completed by the requestor and contain all relevant information to establish the desired access requirements for approval. When completed, the form must be sent to the system security administrator for implementation. When available, electronic signatures may be used to validate the e-form request.

Access to county computers is restricted to authorized persons only. Extreme care must be taken at all times to safeguard passwords. Employees are responsible at all times for protecting their passwords and should avoid leaving their terminals unattended while they are actively accessing county-controlled information. Passwords should be changed on a routine basis, but no less than quarterly. Passwords will be at least six characters in length and should not follow a pattern or closely correlate with the user ID. If a password is forgotten, access administrators will assist users with continued access.

Guidelines

Separation of Activities

For the integrity of county-controlled information, there must be a separation between development/maintenance activities and production activities. Production control activities (job submitters and reviewer of production jobs and their output) and computer operations personnel shall not have access to compiler, assembler, production source code or object codes. All changes to production applications must be approved through controlled release procedures established by each department. This includes both mainframe and desktop computerized platforms.

Production users will only be allowed to enter those parts of applications for which they are authorized. All software and hardware functions that allow access to other than authorized information will be disabled.

Production Source Programs

All production source programs shall reside in a special production directory or library. Authorization to retrieve copies of programs for modifications by a programmer; or to add, move, copy, update, or delete production source programs; add, change or delete production libraries is limited solely to the Program Librarian.

Production libraries must be backed up for recovery when needed. The most recent generation of the source program of the load module shall be kept in the current library. All older generations will be archived.

System Changes

All changes to production or test systems must be entered, approved and tracked in change control logs maintained by the departmental IT unit responsible for the given application or system. The departmental ISR may review these logs on a periodic basis.

System/applications changes must be reviewed and approved by multiple personnel (users, managers, applications supervisors/analysts, and programming staff) so that only thoroughly tested and approved changes are made to the production environments. System abnormal-end (abends) changes or hardware repair do not require advance review.

Dial Up Access

Information regarding access to the county's computer and communication systems is confidential. It must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards or otherwise made available. Telephone numbers for dial up access will be changed periodically and eliminated altogether where possible.

Advance approval is necessary to connect dial up modems to workstations or other networked equipment on a network. Additional user authentication systems may be required for dial up modem lines.

IT units, under the supervision of each department head, will be responsible for developing approved hardware, software and procedural mechanisms to safeguard the county's information assets without unduly restricting user access.

Computer File Transfers

Electronic file transfers to or from any county computer are restricted to authorized individuals using an approved file transfer mechanism. Confidential or sensitive information must be protected within the computer environment to which the information has been transferred.

Network Security

County departments maintain, either through a centralized information technology organization or independently, various networks (LAN/WAN). These network(s) connect users to the Internet and to various host computers. Each of these connections (e.g., routers, bridges, gateways, login prompt) is vulnerable to attack and must have reasonable security measures in place to protect them as well as the information stored on or transmitted through them.

Because the county maintains electronic information in many electronic forms, a common cryptography must be established to protect 'networked' data that is sensitive or confidential in nature. Once that 'standard' encryption process is established, it will be implemented throughout county departments, based upon the technology limits. Until such time as a standard is developed and implemented, electronic (e.g., e-mail, Internet, intranet) transfer of sensitive or confidential information is prohibited.

Risk Assessment

The information owners will periodically review physical facilities to determine potential risks to county-controlled information and suggest protective measures necessary to reduce risk to an acceptable level.

Each county department will develop plans for emergency response, backup operations and post-disaster recovery to assure operations can be resumed normally as soon as possible in the event of any type of disruption.

Documentation of software, hardware and communication networks shall be available both on-site and off-site. The IT units responsible for the custody of the applications/systems involved will strictly enforce schedules for file backups and off-site storage of backups.

IT departments will ensure system and sub-system backup and recovery documentation is complete prior to release to production. Emergency recovery exercises must be performed at least once a year as part of normal maintenance procedures by departmental IT.

Organizational Practices

Protection of the county's information assets can only be successfully achieved if all county employees, at every level, consistently follow the policies and procedures that have been developed as part of the overall Information Security Program.

Minimum Level of Security and Audit Trails

Each computerized platform, from a stand-alone personal computer to a network terminal/personal computer accessing mainframe information, must maintain a level of security and audit ability determined by the responsible department and as required by law or county statutes. Each terminal or monitor (LCD) must display a banner stating that access to or through that particular device is for authorized users only. In addition, the banner will state that monitoring of the actions taken at that device may be performed by the departmental or county IT.

Personal computers that contain sensitive or confidential information must be identified by the Information Owner and have an additional security layer that prevents unauthorized access to the PC's locally stored information (hard drive). Each departmental IT unit will provide consultation on the appropriate security layer.

Each networked host computer must contain a security layer(s) that provides discrete, 'need-to-know' security and provides access in a granular fashion (i.e., system, application, record or field level controls). The host computer security package, if applicable, must also provide adequate audit trails of system users entering, modifying, or exiting at the operating systems level. As an additional requirement, user applications (proprietary and user developed) must maintain accountability of individual users reading, modifying, or deleting data in those applications based upon the classification of the data accessed in those systems. The Information Owner will define the data classification and audit trails.

Employees

A new employee orientation seminar will include information on the Information Security Program. Ongoing efforts will be made to maintain employee awareness of the importance of information safeguards. Where possible, employee performance reviews should include adherence principles to their respective roles in the Information Security Program.

Desktop/Laptop Computers

The information maintained in desktop/laptop computers must be properly safeguarded. Files containing confidential and sensitive data should not be stored in a PC without appropriate security measures.
Installation of any system software or application obtained from user groups, bulletin boards or other information services must be performed only after obtaining the Information Manager's approval, virus scanning, and copyrights and licensing agreement.

Facilities

Each department will develop policies covering physical access to county-controlled information assets in accordance with the physical location of the department. Whenever possible, county departments are located in physically secured buildings. Access to these facilities may require badge authentication and/or visitor escort.

Within the buildings, computers (e.g., routers, PCs and mainframes) should only be placed in secure locations (not readily available to the public) with power sources, electrical surge protection devices and air conditioning systems (if applicable) which can function independently of regular utilities during an emergency and with fire prevention and detection devices.

Oversight

An Information Security Advisory Committee (ISAC), composed of departmental representatives, in conjunction with the CISO, will review and update the Information Security Program as necessary. Departmental representatives will work with departmental managers to determine that files and databases have designated owners, coordinate requests for user IDs and data access, and participate in the development of information security policies and procedures. The Internal Information Systems Auditor will see that the ISP is being followed and will be an advisory member on the ISAC.

Violations

If an information security violation is noticed, it should be reported to the appropriate supervisor, department head, and the CISO. A Security Incident Report may be required documenting the alleged violation. Depending on the seriousness of the alleged security violation(s), the employee may be subject to disciplinary or criminal action.

Exhibit 3: The Common Body of Knowledge

The Common Body of Knowledge (CBK) is a list of ten information systems security domains. An effective Information Security Program must address each of these domains described below:

DOMAIN	DESCRIPTION
1. Access Control Systems and Methodology	Methods of limiting, controlling and monitoring system access. Do you understand current industry and government techniques? Can you explain the risks, exposures and ultimate consequences of using or not using each technique?
2. Telecommunications & Network Security	What are the basic mechanisms on which networks work? A solid knowledge of TCP/IP is expected. How can transmissions be secured? How do firewalls, routers and other engines work?
3. Business Continuity & Disaster Recovery Planning	If a major disruption to normal business operations (flood? hurricane? earthquake, explosion, etc.) happened, would the business operations continue? How could they be recovered? What's the plan?
4. Security Management Practices	What are the organization's information assets and its policies for their protection? How are standards, procedures and policies managed? How is data classified, risks assessed and analyzed? What are the roles within an organization?
5. Security Architecture & Models	How are operating systems designed, implemented and monitored for security? What are the controls used?
6. Law, Investigations and Ethics	Current law, regulations, investigative measures. Evidence gathering. Has a crime been committed?
7. Application & Systems Development	What controls exist within software? What steps are taken during development to assure security? What about change control, date warehousing, program interfaces?
8. Cryptography	How does cryptography provide Integrity, authentication, confidentiality, non-repudiation? What algorithms are used to provide key distribution, digital signatures? How are attacks mounted?
9. Computer Operations Security	Controls for hardware, media and operators.
10. Physical Security	Biometric, lighting, locks, alarms, fences.

References

(ISC)^2 = International Information Systems Security Certifications Consortium, Inc.
http://www.isc2.org/

Network Security is a Mixed Environment by Dan Blacharski - IDG Books Worldwide

Business Continuity Planning briefing by Mark Nicolett, Gartner Inc., Feb. 2002
Study Guide, Business Continuity Planning Domain 8, Chris Hare, Nortel Networks Version 1.0 - March 1999 http://www.cccure.org/Documents/Domain_8.htm2.

Information Security Notes – final by Michael R. Overly, Esq., CISSP
http://server7.bluedomino.net/www/bdweb5234h/detectiondesintrus.com/public_html/Documents/Michael_Overly/outline_of_the_10_domains.doc

CISSP® CERTIFICATION COMMON BODY OF KNOWLEDGE STUDY GUIDE

Nat. Inst. of Standards and Technology's Computer Security Resource Center: http://csrc.nist.gov/

Nat. Inst. of Health Computer Security Awareness Training Web Page: http://irm.cit.nih.gov/sectrain/

SANS: Information Security Awareness:
http://www.sans.org/infosecFAQ/policy/infosec_awareness.htm

Iowa State Information Technology Dept's Security Awareness:
http://www.itd.state.ia.us/security/

Easyi Corporation: http://www.easyi.net

Irongate Inc. Security training videos: http://www.irongateinc.com/index.html

Interpact Security Awareness: http://www.security-aware.com/sat.html

Security Focus, social engineering examples: http://www.securityfocus.com/infocus/1527

CERT's Social engineering paper: http://www.cert.org/advisories/CA-1991-04.html

COBIT – Control Objectives for Information and Related Technologies – IT Governance Institute

Defense in Depth – The National Security Agency

The 60 Minute Network Security Guide – Systems and Network attack Center (SNAC) – The National Security Agency

Generally Accepted Systems Security Principles (GASSP)
http://web.mit.edu/security/www/gassp1.html

The Life Cycle of Security Managers by John O.D. Wyder, Auerbach Publications

Managing Risk in electronic Commerce by Carol A. Siegel, Auerbach Publications

Enforcing and Monitoring an Information Protection Program by Harry DeMaio, Handbook on

Information Security Management, Auerbach Publications

Implementing Integrated Risk Management by Will Ozier, Handbook on Information Security Management, Auerbach Publications

Computer Ethics by Peter S. Tippett, Handbook on Information Security Management, Auerbach Publications

The Information Security Grid by Timothy R. Stacey, Auerbach Publications

Federal Government's Chief Information Officers (CIO) Council. http://www.cio.gov/

Computer Fraud and Abuse Act of 1986 - Sec. 1030. - Fraud and related activity in connection with computers – http://www4.law.cornell.edu/uscode/18/1030.html

National Security Agency http://www.nsa.gov/

National Institute of Standards and Technology http://www.nist.gov/

California Government Code Section 11771 - http://www.leginfo.ca.gov/cgibin/waisgate?WAISdocID=54701419935+6+0+0&WAISaction=retrieve

California State Administrative Manual - SAM–INFORMATION TECHNOLOGY Security and Risk Management – Section 4840-4845 http://sam.dgs.ca.gov/sam.htm