Global Information Assurance Certification Paper

Brent Veenstra
Security Essentials Assignment Version 1.3

Maintaining Departmental Security in a Centralized Environment: Keeping things secure when you have to cooperate.

Abstract
Information Technology infrastructure in many state and county governments consist of a centralized IT resource, with departments in that government structure also having a departmental IT group responsible for operations. Maintaining a demonstrable security environment at the departmental and organizational level requires a coordinated effort to establish defense in depth, risk management and assignment of responsibilities. For these groups to work together providing information security requires an understanding of security concepts, an understanding of the information to be protected and agreed upon plans to protect these assets.

Introduction
Departmental entities in larger organizations have security needs that may not be met by the policies of the larger organization. As a departmental informational technology (IT) manager, you have the responsibility to ensure that your departmental information security needs are met. In many governmental structures departments are responsible for their own data systems supporting their business functions, but a centralized IT (ie state or county or city) department provides services across the entire organization. Services provided often include E-Mail, Wide-Area-Network Connectivity, Internet Connectivity and Web Services (to the public Internet). Other services, such as database hosting or backup may be available for departments to contract from the central IS.

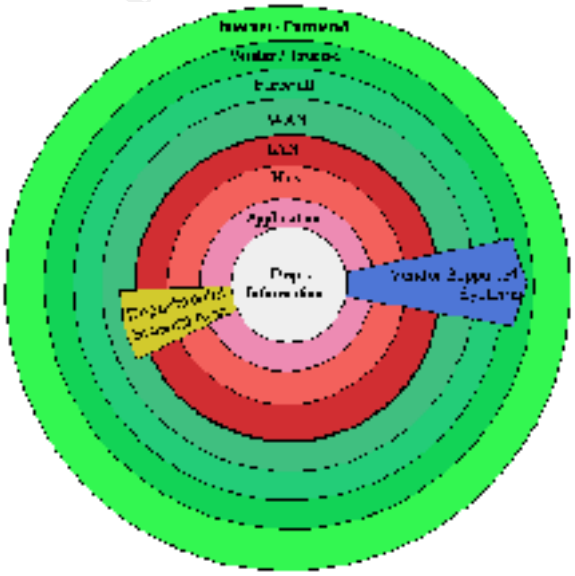
This paper will provide you with the insight needed for implementing a departmental Information Technology (IT) security plan, review relevant security issues you will need to be aware of and discuss some specific items to consider. Throughout this paper the following terms will be used to refer to business entities. *Organization* refers to the complete entity, such as a county or state. An organization is comprised of *departments*, where each department may have radically different business functions. For example, in a state organization, the health department and the transportation department have widely differing rules regarding security and privacy. *Central IT* will be used to refer to the department that provides infrastructure level technology to all departments, such as WAN support or E-Mail. *Departmental IT* refers to an IT group providing services in business support of a particular department. Additionally, departments may have their own internal business units with differing information security needs.

Security Concepts Overview

Information Security is one aspect of a larger umbrella which contains things like the business continuity plan, the communication (to the public) policies, disaster reporting plan, employee mobilization and other polices, that are part of the general business risk management. Ideally, departmental business continuity plans should be an extension of the organizational business continuity plans. This document will focus more specifically on developing an effective Information Security plan from a departmental viewpoint.

When implementing any departmental security initiatives, one often overlooked aspect is the need to be an excellent communicator and have a communications plan. Communication will need to take place at the departmental level – both with management to implement departmental policies and with users as policies are explained and put into force. Both users and management need to understand why IT security is important how these initiatives reduce risk to the department. Additional communication will need to take place between yourself and Central IT as you develop plans to implement your security needs across shared infrastructures. Departmental Policy needs will need to be communicated to the organizational security governance body, (which may or may not be Central IS) as you develop policies or modify the organizational policies to accommodate departmental needs. Communication with Central IT should occur on formal and informal levels to maintain and handle security issues. Communication of other security issues will occur between other departments and outside agencies that you share data or other services with.

To build a framework for discussion, I will layout a typical technical environment and from there develop the general concepts of risk management, layered defenses, security plan, policies and responsibilities.



Areas of Responsibility – Services Diagram
Layers of defense-in-depth approach

The diagram above shows a high-level layered view of services. In this layout, information is accessed by an application; the application runs on a host which is on a LAN (local area network), connected to a WAN (wide area network) which is behind a firewall. The firewall protects access to both trusted entities, which can be other vendors or business partners with which the organization has agreements, and the internet, which is untrusted. Additionally, vendor supported systems and central IT applications may cross all of these areas, at least from the perspective of departmental responsibility.
In this diagram, from a system administration perspective, the reddish colors are departmental responsibilities, the greenish colors are central IT responsibilities and blues are vendor responsibilities. The yellow 'departmental systems area' shows how even departmental systems span various areas of responsibility.

Implementing information security is taking steps to appropriately protect the confidentiality, integrity and availability of computer systems. Responsibility for security needs to be a visible role, assigned and incorporated into the job descriptions of appropriate staff. Keeping confidentiality refers to maintaining the privacy of the data or a system. If someone is able to access or view data without going through the security mechanisms in place, the confidentiality of the data or system can no longer be assured. Integrity refers to the unauthorized modification of data or systems. Availability refers to having a system (and data) available when authorized users expect it to be available.

One very important aspect of security to remember is that you cannot defend against all threats. Therefore you will need to determine what risks are acceptable, which are not acceptable, and which risks can be mitigated. This appropriate level of security allows your department to avoid spending $100,000 to protect data that would only cost $50,000 to recreate. These three dimensions of confidentiality, integrity, availability are elements that need be protected from a defensive perspective, and are the items that are attacked in a security breach.

Risk Management

Now that we have defined the components we are trying to protect, we can review how to go about determining to what degree our systems are at risk and how we can develop a security plan to defend against the risk of compromised confidentiality, integrity and availability.

Risk analysis is performed to determine where resources should be spent for a cost-effective approach to security. The three primary areas risk analysis addresses are determining what to protect, what to protect it from, and how to protect it. According to RFC2196 Standard information security threats include:

- Unauthorized access to systems, resources or information
- Unintended / unauthorized disclosure of information

- Denial of service (Fraser 5)

There are several commonly used methods to assess risk (Parmar 4.1.0.1). The two most common are qualitative, which estimates the probability of a particular threat occurring, using a ranking or scale (high, medium, low), and quantitative, which attempts to assign a dollar value over time to the threat; quantitative risk analysis can be very difficult to perform accurately. Since the purpose of risk assessment is to determine where to best invest security resources, a third option of using Best Practices is also available. Best Practices refers to using a list of IT security management recommendations, developed by a collaboration of organizations, which provide generally acceptable levels of risk mitigation. In general, using Best Practices as a starting point allows your security policy to benefit from the mistakes of other network administrators. In any given environment, there may be conflicting risk management recommendations, so you do need to evaluate and determine what is appropriate for your department. Some web sites for Best Practices listings and links are http://www.cert.org/security-improvement/ and http://www.caspr.org/references.php/ .

Once the risks are analyzed, a security approach needs to be developed to manage the risks. Risk management can be generalized into three approaches:

- Accept the risk and effectively do nothing
- Acknowledge the risk, mitigate and reduce exposure to the risk
- Transfer the risk (i.e. Insurance)

By understanding the risks that your department faces, and determining the level of effort your department is willing to expend to manage risk, you can develop an understanding of the how to judge the severity of an incident and the resources available to prevent or reduce exposure to a particular incident.

Defense in Depth

Managing Information Technology risk involves protecting your information from attack (compromised confidentiality, integrity, availability). An important aspect of managing this risk is to protect information in a series of layers. This concept is called defense in depth. Generally, the defense in depth concept is one of developing successive layers of security throughout all areas that risk can occur. The general concept is used in IT, nuclear power plants, the military and other areas. In IT, defense in depth can be portrayed as a series of circles, similar to a castle moat approach, with the information as the innermost circle, surrounded by the application providing access to the information, then the host providing access to the application and so forth out to the firewall. You are probably using this approach to some degree, assuming you use passwords for network access and a firewall for internet access. Review the responsibilities diagram in the Security Concepts Overview section. Each of these areas can be considered a potential area for defense to be applied.

For the defense in depth strategy to be effective three key aspects need to be addressed at each layer. These areas are People, Technology and Operations. The People aspect includes a commitment from upper management to security, followed by appropriate policies and procedures, training for administrators, security awareness by end users, and personal accountability. People need to understand why security is valued by the department before they can be expected to 'buy in' to the expectations set by the department. The Technology aspect involves a series of defensive strategies within each layer, such as auditing logins and activity, surveillance of use, or different technologies, such as internal firewalls at the network layer. Operational aspects are the day to day approaches to maintaining security. This includes maintaining and patching equipment, performing security assessments, reviewing logs, monitoring existing threats and recovering systems. By comprehensively addressing these three areas, your defensive layers will be supported, effective and understood.

By using a defense in depth approach, each risk that your department has identified can be addressed through a layered series of defenses, where each defense layer is supported by People, Technology and Operations. The trick is the get each potential layer of defense to be addressed by the appropriate department or the organizational structure. This is where the security plan and corresponding security policies fit it.

Security Plan

Now that you understand risk analysis and management through defense in depth for your department, how do you pull it all together? By developing a security plan, the issues identified through the risk analysis and how these issues are addressed at each layer in the defense in depth approach are documented.

Formally, the security plan is a comprehensive document designed to acknowledge the Information Technology risks faced by an organization, and then develop a framework to reduce these risks to an acceptable level. The organizational security plan should be a higher level architecture document into which specific policies can fit. The plan should provide general guidance, responsibility and incident handling procedures. Another element of a security plan is to define who (i.e. what department) is responsible for what systems. It is critical for a department to understand who is responsible for individual systems, for infrastructure systems and enforcement of both Central IT and departmental policies.

Review a copy of your organization's security plan. Does it exist? Does it cover the elements mentioned above? If not, consider initiating alterations through your governance structure or develop a departmental security plan that outlines your risks and how risks will be addressed.

The security plan and related policies should include the at least the following characteristics

- Implementable through system administration, policies and procedures.
- Enforceable, with security tools and supported with sanctions
- Defined areas of responsibility

Policies

When an acceptable organizational or departmental security plan is in place, then use it in conjunction with specific risks and the layered concept of defense in depth to develop policies. Policies are specific directives to all users about how to use departmental or organizational information. From an IT perspective, they can contain checklists of how to deal with a specific event, such as an intrusion, to ensure that legal evidence can be preserved. A variety of policies need to be developed to encompass a full defense of all the risks.

Here is a partial list of policies that should be under your security plan.

- A privacy policy, so users know what to expect from monitoring and other efforts.
- An access policy, outlining acceptable use, external connections, connecting new items to the network.
- An accountability policy, defining responsibilities of users, staff and management providing incident handling guidelines and audit capabilities.
- An authentication policy, establishing password policy and remote authentication methods.
- An availability statement, outlining users expectations for system availability (redundancy, recovery, operating hrs, maintenance windows).
- An IT system and network maintenance policy specifying how internal and external maintenance people are allowed to handle and access technology. Issues here include remote access for maintenance and outsourcing.
- A violations reporting policy.
- A physical security policy.

When you develop polices, there are two very important principles that need to be dealt with. First, policies need to be usable, that is, not so burdensome that users work around them. This is a balancing act, where the need for extensive security is balanced against the effective usability of the system. A recent example of this is the in FBI's automated case-support system (ACS), used to support sensitive case files, security was so difficult to configure when first installed that approximately 500 case files were not protected, compromising FBI informant operations. (Pincus 1)
Second, policies need to have ways to break them, at least for technical staff. This is where you have the opportunity to balance the need to keep the systems available with the need to strictly follow policy. Since you cannot predict all possible problems, you need to build flexibility into the policy that allows trusted staff to resolve a problem, then reconcile the solution with the policy afterwards.

Service Level Agreements

Armed with these policies, the next step is for you to develop methods for your central IT to utilize your polices when the layers they control touch your data.
I propose that if Organizational policies are not sufficient for your departmental security needs, Service Level Agreements (SLAs) are utilized to extend your departmental policies into areas managed by Central IS. While service level agreements sound like a high degree of formality for two entities within an organization, they serve the following purposes

- Clearly define goals of the department and organization
- Eases budgeting for security because the goals are defined
- Allows security to be more proactive and less reactive because a direction is defined
- Allows for differentiation between applications or tasks (Services Level Management 3)

By defining the expectations of the department and Central IS, many of the communications problems can be prevented, because the procedure is defined. Additionally, responsibilities of each group are clearly laid, with contact and documentation information. (Services Level Management 3) Service level agreements between the department and Central IT help establish that both parties are responsible for security issues.

While SLAs can provide many benefits, there are prerequisites that must be true in the organization (or at least in your department and Central IT) before the SLA approach will be effective. These include:

- A service oriented culture. The SLA makes improvements based on customer (your department) needs and perceptions.
- Customer / business initiatives must drive all IT security activities. IT needs to make sure that security efforts meet a business purpose, rather than a goal for the sake of a goal.
- Commitment to the SLA process and contract. This commitment must come from all individuals involved in the SLA as well as a commitment from management. (Services Level Management 30-31)

Remember that full communication, including management and user acceptance is critical. All departmental interactions with a centralized governance structure and a centralized IT, at least at a policy level, is going to involve some level of politics. Daniels and Spiker, in their book "Perspectives on Organizational Communication" remind us that organizations are "political structures that provide platform for the expression of individual interests and motives" (p84). Hence a fair understanding of all the security issues of the organization must be understood by the departmental security person so that the objectives and goals of these centralized political structures can be understood and worked with to accomplish the departmental security needs. Your

department will need to present a cooperative and collaborative front to develop a fully implemented security plan that will meet your risk tolerance.

Review of sample issues

As you develop SLAs within the organization, several specific topics need to be generally addressed. Depending on your particular department and centralized IT, these may be addressed using departmental policies, SLAs, or a combination of the two. The following is a list of some of the areas that your department may need to address when developing Service Level Agreements.

Data Ownership

The concept of data ownership comprises a set of responsibilities such as data definition, data modification, data viewing / use and custodian. Data ownership policy needs to identify ownership and who can exercise the responsibilities related to that ownership. Historically, IT has filled the role of data custodian, although IT may have filled other data ownership responsibilities in a de-facto manner.

The following are some questions you should answer as in relation to data ownership. Does the organization as a whole own the data? Does the department own the data or does a small group within the department own the data? What legal requirements restrict the data? This analysis may need to take place at a system-by-system level. Differing privacy and security requirements may exist for various systems' data, leading to a classification system where IT needs to support several degrees of security and policy within its' own department.

In a governmental organization, various departments may have very different legal requirements regarding the protection of data. For example, health and transportation are separate departments of a state government, but each has quite different sets of legislation regulating their client data and other business data.

Personnel Security

Communicate why the security policies exist and how they are used to protect departmental organization. Encourage users to reduce vulnerabilities by creating a heightened security awareness related to passwords and other data access protocols.

Physical Security

Review physical aspects of your departmental facilities. Beyond the basic security issues of building access and access to PC's, what about access to server and equipment rooms? In an existing facility, you may have departmental IT equipment, central IT equipment, telecom equipment all in the same room. What is a reasonable method of allowing access to the room, but not exposing your equipment to risk? Is it reasonable to expect staff at the site to know (or care) who is allowed in that room?

A second concern is laptops and other portable equipment. Laptops are at a high risk of being stolen or left behind. Do your data security requirements even allow certain data to reside on local laptop drives? What data classifications could be allowed on portable equipment?

Data Security
This category includes normal system administration tasks such as data backup, virus protection and intrusion detection. Develop policies that describe how these tasks will occur and are monitored (remember the enforceable aspect of a policy – you need to be able to monitor the results). If you have data residing on servers hosted by your Central IS, develop an appropriate SLA to meet your departmental policy.

If you utilize central IT services such as Web Hosting or database hosting, you will need to pull the actual administrators of your services into your departmental security policies and the SLA development. They need to be made aware of the legal liabilities surrounding the data, be given a contact for administrative changes such as changes in security and access rights. As the data owner, your department still retains the need to ensure the data is handled in a secure way in compliance with your departmental policies.

There may be agencies that your department shares data with. If your department does not own the data, and the data is residing on departmental servers, do you have a data sharing agreement specifying responsibilities at an IT level? What about at a business level?

Network Security
Many areas of the layered defense can be seen in this category. Does your department have a site or two where you actually share a LAN with other organizational departments? Does your data classification scheme specify that you need to be concerned about this? Does your NOS support packet encryption for file / print communication? What about mainframe connectivity or other TCP/IP connectivity?

At the WAN level, does organizational network allow for shared WAN traffic? Are you concerned if other departments see your packets as they move between your departmental sites?

Another area to consider is vendor and outside access. For any but the simplest departments, there is legitimate need for outside entities to access your network. These could be entities that you have a data sharing agreement with or vendors that need occasional access for support purposes. Your security plan should provide for ALL outside access to be routed through the organizational firewall, with assistance from centralized IT. Remember defense in depth, and use the depth that centralized IT is capable of providing. Putting in modem back doors and other methods around the main firewall is allowing non-monitored connections and increases exposure.

These same principles apply to telecommuting and access for employees to departmental resources from outside the network boundaries. Remember your data classification and develop a structure to protect appropriate data.

Conclusion

Departments in a larger organization have an obligation to ensure the confidentiality, integrity and availability of departmental information independently of organizational strategies. Performing risk analysis allows an understanding of possible options to handle IT security issues and develops a prioritized list of items to be defended against. The concepts of defense in depth allow a layered approach to set up a series of defenses protecting the information. At each area of the defense in depth approach people, technology and operations work in concert to provide a full-circle approach to defending against risks. By developing an architectural level security plan (preferably at an organizational level), then crafting policies specifically addressing items in the security plan, risks can be specifically mitigated. Where the security policies address defensive layers that are outside the direct control of the department, the security plan should be extended to other departments (including Central IT) through effective Service Level Agreements. Implementing this approach allows a departmental IT group to vigilantly maintain an appropriate security posture without directly controlling all areas where security could be compromised.

List of References

Benjamin, Yobie, "The Vigilant Enterprise, Part 2." Intelligent Enterprise.com. April 16, 2002 (2002):60.

Benson, Christopher "Security Planning." URL: http://www.microsoft.com/technet/security/bestprac/secplan.asp (22 Mar 2002)

Benson, Christopher "Security Strategies." URL: http://www.microsoft.com/technet/security/bestprac/secstrat.asp (22 Mar 2002)

Bernhom, Gerald; Bruhn, Mark and Cromwell, Dennis. "Security in a Client/Server Environtment." 1994. UR:http://www.educause.edu/ir/library/text/CEM9445.txt (1 Apr 2002)

Boyhan, Craig et al. "Fighting Cyber-crime with Risk Management Techniques." 2002. URL:http://www.ey.com/GLOBAL/gcr.nsf/International/Fighting_Cyber_Crime_-_Global_Thought_Center_-_Ernst_&_Young (1 Apr 2002)

Certicom. "An Introduction to Computer Security." (July 200) URL: http://www.certicom.com/research/wecc1.html (1 Apr 2002)\

Cheswick, William R. and Bellovin, Steven M. Firewalls and Internet Security: Repelling the Wily Hacker. Boston:Addison Wesley Professional, 1994. 197-234.

Daniels, Tom D. and Spiker, Barry K. Perspectives on Organizational Communication, 2nd Ed. Dubuque:Wm. C. Brown Publishers, 1991. 83-104.

Ernst & Young. "Computer Forensics Response versus reaction." 2001. URL: http://www.ey.com/global/vault.nsf/Australia/Computer_Forensics_Response_Versus_Reaction_0501/$file/E&YComputerForensicsResponseVersusReaction0501.pdf (1 Apr 2002)

Fraser, B. "RFC2196 - Site Security Handbook." Sept 1997. URL:http://www.faqs.org/rfcs/rfc2196.html (1 Apr 2002)

Galik, Dan. "Defense in Depth: Security for Network-Centric Warfare." 1998. URL:http://www.norfolk.navy.mil/chips/archives/98_apr/Galik.htm (1 Apr 2002)

Hart, Dennis N. "Data Ownership and Semiotics in Organizations, or 'Why They're Not Getting Their Hands on My Data!'" (2000) URL: http://www.cs.adfa.oz.au/research/imos/SemioticsPACIS2000.doc (19 Mar 2002)

Hobbs, W. John "Who Owns the Data?" (1990) URL: http://www.chryxus.com/V2N1.htm (19 Mar 2002)

Hulme, George V. "In Lockstep on Security." Informationweek.com. March 18, 2002 (2002):38-52.

Johnson, Johna. "Crafting Service Level Agreements that work." Network World March 25, 2002 (2002): 30

Kimball, Kathleen and Wall, Andrew. "How to Cathc Bad people Doing Bad Things: Network and Computer Security in Mobile, Distributed Environments" 4 Dec 1997. URL:http://www.educause.edu/ir/library/html/cnc9721/cnc9721.html (22 Mar 2002)

Langer, K. "Defense in depth: principle." URL: http://www.iaea.or.at/ns/nusafe/tutorial/design/defdep.htm (19 Mar 2002)

Management of Risks in Information Systems: Practices of Successful Organizations. March 1998. URL: http://www.itl.nist.gov/lab/bulletns/archives/mar98.htm (22 Mar 2002)

McClure, Stuart; Scambray, Joel and Kurtz, George. Hacking Exposed. New York:Osborne/McGraw Hill, 1999.

McKenny, Brian. "Defense in Depth." (Feb 2001) URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm (19 Mar 2002)

Microsoft Corp. "Security Threats." URL: http://www.microsoft.com/technet/security/bestprac/secthret.asp (22 Mar 2002)

MOREnet. "Best Practices in Internet Security." 2001. URL:http://www.more.net/security/best.html (1 Apr 2002)

Morris, Gary S. "Computer Security and the Law" (1990) UR:http://csrc.nist.gov/publications/secpubs/cslaw.txt (22 Mar 2002)

NSA. "Defense in Depth." URL:http://nsa2.www.conxion.com/support/guides/sd-1.pdf (19 Mar 2002)

Parmar, S.K. "An Introduction to Security." URL: http://downloads.securityfocus.com/library/index.html (22 Mar 2002)

Pincus, Walter "Hanssen betrayal exposed more that 50 FBI sources" URL: http://archives.seattletimes.nwsource.com/cgi-

bin/texis.cgi/web/vortex/display?slug=hanssen07&date=20020407&query=fbi (07 April 2002)

Rubin, Aviel D.; Geer, Daniel and Ranum, Marcus J. Web Security Sourcebook. New York:John Wiley & Sons, Inc, 1997.

Services Level Management: Best Practices White Paper. URL:http://www.cisco.com/warp/public/126/sla.htm (22 Mar 2002)

United States House of Representatives - Information Security Policy for Vendor Remote Access to the House Network. (Feb 4, 1998) URL: http://www.house.gov/cao-opp/PDFSolicitations/HISPOL_5.pdf (19 Mar 2002)

Waldon, Jeff. "Interagency Cooperation in Information Management: Why, Why Not, and some ideas on How." URL: http://fwie.fw.vt.edu/WWW/datashar.htm (19 Mar 2002)