GIAC ENTERPRISES

Network Access
Security Policies and Procedures

Prepared for:

SANS Certification - GIAC Information Security Offcier (GISO)
Version 1.1 (December 12, 2001)
by
Haldis R. Toppel
March, 2002

Table of Contents

Assignment 1

Describe GIAC Enterprises

The Organization
The Network Infrastructure
The Business

The Organization

GIAC Enterprises, a Service Bureau
GIAC Enterprises provides central and distributed Information Technology (IT) services to the City of Willowby, an imaginary municipality, referred to as the "City." The IT functions of the City were previously supported by its central IT organization and have been outsourced to GIAC Enterprises one year ago. GIAC's services and expenditures are contractually agreed upon and funded by the City. The contract between GIAC and the City is renewable annually. The property and building occupied by GIAC is owned by the City and leased by GIAC for the fee of $1 per year.

GIAC serves no other customers. It is the sole provider of central IT services to the City and provides consulting services as well as technical support for the distributed processing needs within the various, semi-autonomous City Departments. GIAC also manages the City's radio and microwave tower (antenna) facilities atop Mount Sans which provides radio, micro wave and remote data communication capabilities to the Police and Fire Departments as well as wireless communication capabilities for various City-internal access needs. The GIAC central processing facilities are located within the city limits of the municipality.

GIAC and City Responsibilities and Authority Structure
GIAC Enterprises is governed by the City's Information Technology Committee (ITC). Members of this committee are City Council Members, representatives from the Mayor's Office, and technical advisors from the public and private sectors. The committee directs, controls, and reviews the City's technology direction, acquisition, project management and implementation, and major contractual and budgetary decisions. ITC audits and enforces the City's policies and procedures. Processes and IT installations, serving the needs of a specific City department are budgeted, managed and maintained by each department individually.

GIAC, with assistance and direction from ITC, acts as coordinating entity for departmental IT issues which affect the City business beyond departmental boundaries or that have City-wide impact. GIAC's role is to make technology recommendations to the City's departments and to ITC. It is ITC's role to formulate, mandate and enforce IT decisions with extended or city-wide fiscal, operational, or administrative impact or on issues which require review or interpretation of existing laws, policies, contracts, directives or other mandates. ITC enforces IT decisions, procedures, policies, and the City's Administrative Code. The Audit Bureau of the City's Controller's Office audits compliance by GIAC and the City departments with existing policies, procedures, and the City's Administrative Code.

City Business Supported by GIAC Enterprises
The information technology in support of the City's municipal business requirements are supported by GIAC Enterprises in a manner as if GIAC were an integral City Department. Each of the City's Departments are autonomous and independent entities similar to private industry's wholly owned subsidiaries. The City's business details are outlined in the section below titled "The Business." With the exception of Human Resources (Personnel) and Payroll processing, all other business function provided as a central service to the Departments are optional. Such

optional services include but are not limited to access to the City's central Geographic Information System data base and software and access to cost accounting/labor distribution capabilities as an integral part of the City's timekeeping/payroll system.

GIAC Budget and Charge-back

GIAC operates on a charge-back system, where operating and development costs are charged and paid for by department(s) benefiting from the services. GIAC also has an independent annual budget to cover expenses for shared resources and technology upgrades or improvements which are independent of the services provided, but enhance the overall operational and cost efficiency of the City's technology support. Such shared services could include but are not limited to upgrades and expansions of the network infrastructure, shared server hardware or peripherals, and upgrades of operating systems or compilers, disaster preparedness, security procedures and audits, etc.

The Network Infrastructure

Most of the larger applications supported by GIAC are processed centrally and may be accessed from remote locations via the Departmental Private Networks. Such applications may be those shared by all Departments such as payroll or personnel functions or they may include custom applications developed and owned by City Department. Other applications or functions are processed and maintained by the City's semi-autonomous departments at their local sites. In its main processing center, GIAC houses a large mainframe-type processor, commonly referred to as the City's central processor or enterprise server, a server farm which consists of several smaller servers supporting departmental or distributed applications, large disk and tape storage and retrieval facilities, large database and file servers, high-volume/speed print and post processing services, and the City's central network control and distribution center.

The City departments, operating at various locations throughout the City, maintain their own Private Network(s). They may operate and support a multitude of servers, terminals, and miscellaneous IT equipment and peripherals in support of department-specific business functions. While some departmental LANs/WANs are standalone installations, most have connectivity to the City's network infrastructure. This connectivity may provide transaction processing in support of the applications, database, file and print services via the central enterprise server or provide access to major applications such as payroll or accounting business. Some applications operate one or more servers located in the server farm, others use the enterprise server for processing resources or data sharing.

The servers located in the server farm are administered by the user departments, but monitored, and serviced by GIAC personnel. This includes disaster preparedness backup and recovery services, periodic maintenance, and a secure access and climate controlled physical environment. In some cases, and to a limited degree, monitoring or interaction with the application is performed by GIAC personnel.

Some City departments operate solely from within their offices, other departments such as the Parks Department or the Police Department operate to a large extent from field offices or mobile units. City employees, approved vendors and contract/consulting firms have dial-up access to the City's network infrastructure and the ability to provide or retrieve authorized information, may access approved data storage volumes, and/or have access to e-mail services.

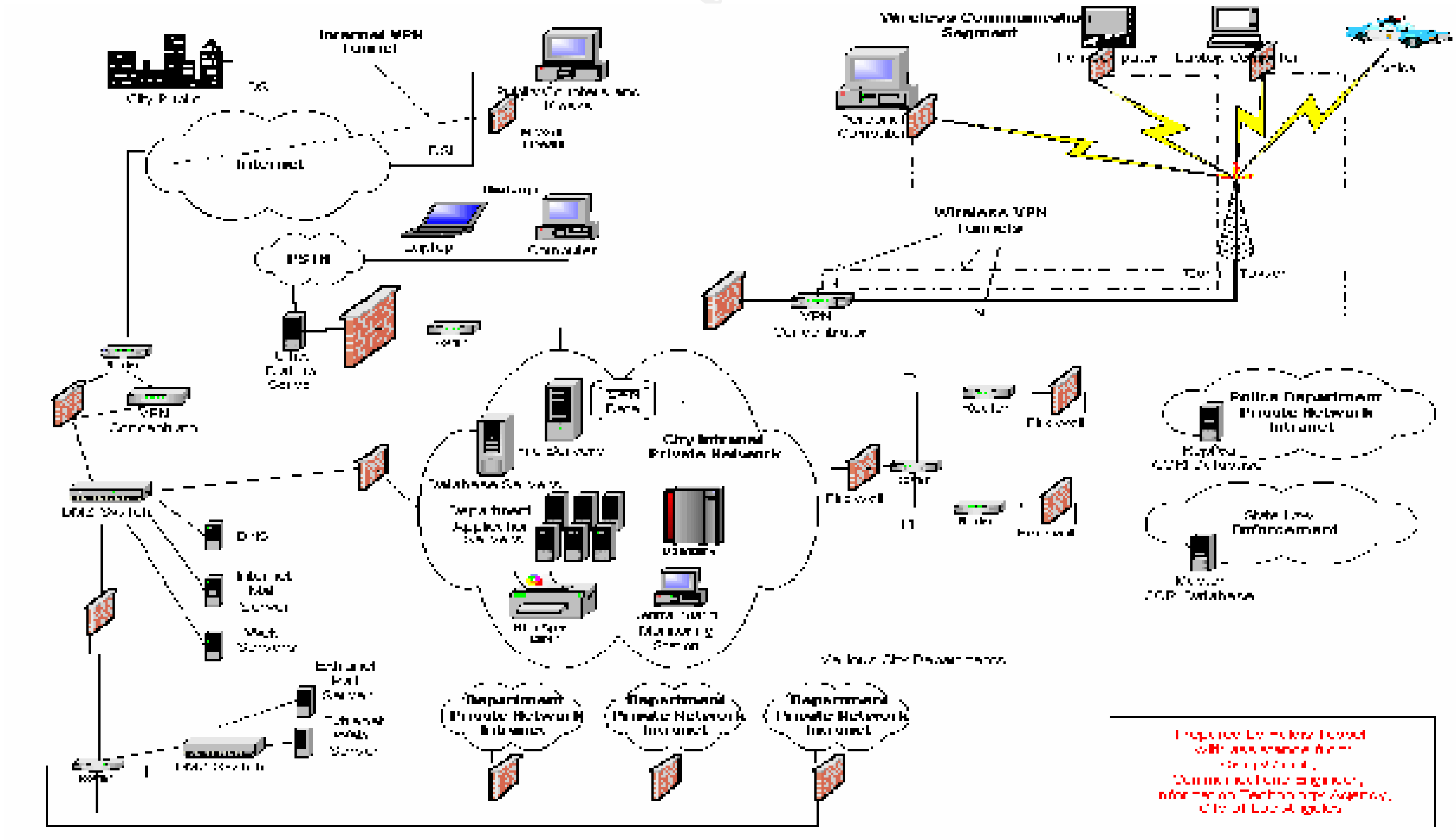
The public has access to select City information via the Internet or from kiosks or PCs located at public counters such as the Building and Safety Department. Access to City-internal information is not available to the public.

Wireless access to the City's network infrastructure is limited to transmissions of non-sensitive data and requires routing through a Virtual Private Network (VPN) for maximum intrusion protection.

The City's communication tower is equipped with various antennae and supports both the wireless communication needs and Police and Fire Departments' voice communication.

Due to its extensive interconnectivity with the City Departments and the public, it is GIAC's policy to control and protect access to the City's Intranet (private network) with a firewall at each entry point. It is also a strong recommendation for all City Departments to provide their own firewall access control into the departmental private network, controls that are designed to address department-specific requirements and rules and prevent access into departmental networks from inside the City or from the outside.

City of Willowby
Conceptual Network Diagram



The Business

GIAC provides a reliable, safe, and secure technology platform and network infrastructure in support of the various City Departments' information technology needs.

The City conducts its business through independent and semi-autonomous departments that typically operate and administer the majority of their own applications and their own departmental Private Networks. However, an estimated 80% of all departmental, technology-based services require access to the City's Intranet (private network) and consequently support from GIAC. It can be said that GIAC's most significant role in addition to application and general technology support is in the support, design, maintenance, and safekeeping of the City's network infrastructure.

Some of the major business entities include:

- the Fire Department,
- Police Department,
- General Services Department
- Radio Communications Department
- Public Parks Department,
- Animal Regulations Department
- Street Maintenance Department,
- Automotive Fleet Services and Maintenance Department,
- City Controller's Office,
- Finance Department
- Property and Geographic Services Department,
- Health Care and Ambulance Services,
- Purchasing Department,
- City's Libraries
- Building and Safety Department
- Public Housing
- City Attorney's Office,
- various City Council Offices
- Mayor's Office.

In the course of its business the City provides public services to its citizens, including public safety services such as highly sensitive police and fire protection, and less sensitive activities such as street maintenance, public park and library services, etc. The various City Departments share information via the City's internal private network.

Via its public WEB site and through kiosks and PCs located at various public locations the City provides select and public information to its citizens such as tax and property information, job openings, information on pending or active RFP/RFBs, Council Member constituent services, civil emergency alerts, and more. Public access is prevented from entering into the City's private network by firewalls and other measures and is limited to public data.

Authenticated dial-in access to the City's Intranet is granted to authorized City personnel and contractors via a Citrix MetaFrame XP client setup.

Wireless communications capabilities are currently provided for non-sensitive data transmissions such as mobile geographic location monitoring of parking enforcement vehicles, as well as police, fire, and ambulance vehicles. Another typical application is the Recreation and Parks Department's Emergency Neighborhood Response and Evacuation (ENRY) program which makes requests and provides inventories for emergency supplies such as food, blankets or portable toilets during natural or man-made disasters as part of the City's disaster preparedness program. Considering the current state of technology, wireless access to the City's Intranet is considered high risk and severely limited.

GIAC's roles and responsibilities are detailed in the City of Willowby Administrative Code[1]:as follows:

> GIAC has been contracted as a proactive, highly skilled firm to lead the City in its efforts to design, acquire and implement cost effective, quality information technology systems, networks and equipment which will assist City departments in providing efficient and effective customer-driven service to the public.
>
> GIAC has the authority and responsibility for planning, designing, implementing, operating and coordinating the City's information technology systems and networks, either directly or by oversight of these activities when carried out by other departments. In addition, GIAC, upon written request, is authorized to provide Information Technology System services to organizations authorized to occupy premises owned by or under the control of the City, and/or organizations providing or requiring Information Technology System services if the General Manager of the department finds and determines that the requested service is to be in the interest of the City.
>
> GIAC has the power and duty to supervise, control, manage, design, develop and administer Information Technology Systems to provide optimum utilization of equipment, devices and systems commensurate with sound, economic, managerial, and systems design practices.
>
> GIAC services shall include, but not be limited to the examination and approval of plans for the construction of new public buildings and the remodeling of existing public facilities or leased facilities for City use, when such construction or remodeling affects the City's network architecture or adversely affects the physical or logical security requirements and installations for systems under the jurisdiction of the City.

GIAC's Security Directives are detailed in the City of Willowby Administrative Code which states[2]:

> Each department or office of the City utilizing any service employing the information technology equipment under the jurisdiction of GIAC, shall have control over the information supplied to and received from such equipment as each such department or office finds necessary to conduct its own affairs.

[1] Excerpts from the City of Willowby Administrative Code, Chapter 26 – Adapted from: City Administrative Code. Los Angeles: City of Los Angeles, 2001. Division 22, Chapter 26, Sections 640-652

[2] Excerpts from the Willowby City Administrative Code, Chapter 26 – Adapted from: City Administrative Code. Los Angeles: City of Los Angeles, 2001. Division 22, Chapter 26, Sections 640-652

> The General Manager of any department having control of any information to be processed or accessed by GIAC directly or via the GIAC controlled Wide Area Network (WAN), which the respective General Manager determines is confidential, shall notify the General Manager of GIAC in writing of the existence and confidential nature of such information, and shall specify with particularity the information which is to be treated as confidential.
>
> Notwithstanding the security requirements identified to GIAC by all other City Departments, Offices, or approved entities, the Police Department and its associated agencies require additional attention and consideration due to the sensitive nature of the information placed into the custody of GIAC and the interaction and exposure to State, Federal, and other Law Enforcement agencies.
>
> The General Manager of GIAC shall consider the confidential nature of information placed into its custody or to which access is provided via the City's Wide Area Network, and shall take such measures as are required to maintain the security of such information. During the period of time such information or access is under control of GIAC, it shall have sole responsibility for the maintenance of the security of such information. A breach of security shall be a misdemeanor.

The Police Department requirements which govern the access and processing of law enforcement data are detailed in the Police Department/GIAC Enterprises Management Control Agreement (PG-MCA). The agreement is intended to guarantee the high priority of service and security needed by the Police Department and associated law enforcement agencies to ensure the public's safety and welfare. The PG-MCA places special emphasis on Criminal Offender Record Information (CORI). The PG-MCA[3] states:

> Both GIAC and the Police Department acknowledge the necessity of compliance with Title 28 DFR, Part 20, and the State's statutes and administrative regulations concerning access to and dissemination and security of CORI."
>
> GIAC shall provide continuous physical, logical and/or electronic security to preclude unauthorized access or use of hardware, firmware, and/or software facilities used to facilitate exchange or storage of CORI, and switching (sending over the network) of messages for the criminal justice community as well as secure network access to law enforcement agencies. Such physical security shall include all areas occupied by GIAC.
>
> GIAC shall maintain an electronic system which shall alert the City's Office of Security of any unauthorized intrusion into any GIAC offices which contain CORI data or which have access to CORI data. The Security Services staff of the Office of Security shall be requested to notify the Police Department's Information Resources Division (IRD) staff of any such intrusion. GIAC shall implement appropriate secure measures so that workstations in the GIAC offices will be secure from unauthorized access.

[3] Excerpts from the Police Department/GIAC Enterprises Management Control Agreement (PG-MCA), – Adapted from: Los Angeles Management Control Agreement (MCA). Los Angeles: City of Los Angeles, 2000.

Assignment 2

Define Security Policies – Areas of Risk

Introduction
Security Goals and Objectives
Primary Concerns – Risk Categories
Areas of Risk
Select Security Policies

Introduction

In defining security policies and procedures, GIAC Enterprises acknowledges that certain constraints will not allow the removal of all risks to the City's technology resources. The policies and procedures strive to protect the City from reasonable risks of unauthorized or malicious access or damage to the City's and its business partners' physical and logical technology and data/information resources, and denial of service attacks. Cost and resource constraints as well as timely and functional access to the City's business applications and systems will have to be taken into consideration when determining the appropriate and acceptable extent of risk mitigation and security implementation.

In its risk assessment/management procedures, GIAC uses the formula: "Risk = Value x Threat x Vulnerability"[4]. A reduction in threat, vulnerability or value will result in a reduction of risk. In the development of its security policies GIAC focuses primarily on the reduction of threat and/or vulnerability to assess risks and improve the City's IT security.

Security Goals and Objectives

The objectives for GIAC's business security measures can be summarized in three major categories:

1. Protection of the City's data privacy, confidentiality, and integrity;
2. Availability of City services to its citizens through reliable availability of, and access to computerized systems, applications, and data/information.
3. Prevention of the use of the City's information technology resources for unauthorized, illegal, or unethical purposes.

While item 3 above may not directly affect the security of data and systems, unauthorized and or illegal/immoral use of the City's information technology constitutes a misuse of public resources, could dilute the public's trust and may expose the City to liability lawsuits, especially in cases where fraud is committed.

Its is GIAC's goal to support the security objectives by:

1. maintaining a safe, secure, and reliable network infrastructure free of unauthorized logical intrusions for the efficient transport of data/information among the various entities within the City and between the City and its citizens.
2. establishing and maintaining a reliable, safe and secure physical operating environment free of unauthorized physical intrusions for the protection of GIAC's personnel, the City's network infrastructure, and the processing and support of centralized and departmental applications and data;
3. providing a reliable, safe, and secure repository and support structure for centralized and departmental hardware, software, and data/information placed into the custody of GIAC;
4. assuring the continued and reliable operation and availability of applications, systems and data/information managed and operated by GIAC or placed into the custody of GIAC.

[4] Fried, Stephen. SANS Security Leadership, Part 1. SANS Institute, 2001. 1.9.

Primary Concerns - Risk Categories

In order to achieve the security goals and objectives, GIAC is focusing on three primary risk categories for the purpose of risk assessment. These categories/concerns are used as initial guidelines to evaluate the security of the operation and status of GIAC's physical and logical environments, GIAC's activities, the effectiveness of policies and procedures, and the general validity of established security measures. Other concerns may emerge as systems and procedures are evaluated or as technologies or methodologies evolve, and they are incorporated into the risk assessment process as needed.

Applicable contractual arrangements, and federal, state, or municipal laws, directives or mandates are considered minimum standards for acceptable risk levels. In the absence of contracts, laws, directives or mandates, the minimum acceptable risk levels are based on "industry best practices." GIAC recognizes that an assessment and acceptance of "industry best practices" is subjective in nature and driven by innovative or evolutionary changes in the information technology industry. GIAC also recognizes that effective security measures must be continually assessed to keep up with, and preferably stay ahead of the industry's progress, innovation and change. GIAC relies on its technical staff to make a concerted and on-going effort to observe, research, and study emerging technical issues/procedures, and evaluate "best practices" which could affect the City's existing security measures and to make recommendations for improvements as necessary.

While GIAC consistently strives to operate with due diligence to uphold a secure and reliable operation, an independent security consulting firm is contracted annually to review and assess security risks and minimum standards. This firm is also expected to make recommendations for improvements and remedial actions.

The thee categories of primary concern for risk assessment focus on data/information security and business continuation with emphasis on public safety services:

1. risk of physical intrusion, destruction of GIAC facilities, compromised GIAC employee safety;
2. risk of logical intrusion from inside and outside the City into the City's Intranet; compromised data privacy, confidentiality, integrity; introduction of viruses and/or denial of service attacks, unauthorized use of City resources;
3. risk of the introduction of "weak links" into the City network architecture which might make the private network of one City Department vulnerable to intrusion from another City Department and from external sources, posing threats to the departmental data privacy and integrity, exposure to viruses, denial-of-service attacks and unauthorized use of City resources.

Summary of Security Assessment

Through a process of observations, and interviews with senior City management and technical staff, GIAC has identified areas which clearly exceed minimum security standards as well as areas with serious deficiencies and vulnerabilities which pose a considerable risk to GIAC's and the City's security in one or more of the three risk categories listed above . Areas which meet standards or have only minimal deficiencies are not listed. No priority is implied in the list.

Areas Which Clearly Exceed Minimum Standards

1. Screening and background checks for new employees and contract personnel.
2. User ID and password management and use.
3. Dial-up access.
4. Public access via the Internet.
5. Network activity logging and intrusion detection (except radio communication/microwave).

Areas With Significant Deficiencies

The concerns, risks, and consequences are detailed below. GIAC has prepared recommendations for steps to be taken to mitigate the risks. Cost and resource requirements are not included but have been considered when alternative security options were evaluated. Estimates will be prepared upon request and prior to final acceptance and approval of the recommendations by ITC.

1. GIAC Physical Security;
2. Access to the Radio Communication/Microwave Facilities
3. Police Network Architecture
4. Wireless Network Access,
5. Security Awareness for GIAC and City Employees.

Areas of Risk

1. GIAC Physical Security

Areas of Concern:
Malicious destruction or damage from intruding individuals into the City's central technology operations center at GIAC has the potential to severely disrupt or disable the City's business by threatening the safety of employees and by rendering hardware, software, and/or the network inoperative or inaccessible. This section does not cover destruction from natural disasters or acts of war. Such threats are addressed in the "Disaster Preparedness/Recovery and Business Resumption Planning" manual.

Threats or Risks:
The GIAC facility is the central processing site for City-wide, shared, or numerous distributed applications, the common point of access for the interconnectivity of the various City Departments, and the central network distribution site.

As a public sector entity, the City and its operating units are subject to potential civil unrest or terrorist attacks and vandalism, as well as attacks from disgruntled employee. While it will be costly to recover or replace technology and lost data/information (qualitative risks), the potential loss of life through the disruption of City services and the public's confidence in the City's ability to manage its business (qualitative risks) warrant significant considerations.

The GIAC facilities are located in the center of a expansive parking lot. A large sign at the entrance to the parking lot reads: *GIAC - City of Willowby Information Services Center*. GIAC employees, City employees and a significant number of employees from an adjacent high-rise building use the parking lot and are issued parking permits at a nominal fee. The parking lot is surrounded by 12 inch high cement barriers and accessible through a card-controlled wooden lift gate which is easily and frequently broken, allowing unchecked access to the parking lot by the public.

A guard is stationed in the entrance hall to the GIAC facilities. GIAC and City employees sign in, visitors are escorted by GIAC employees. No identifying badges are used for access to the facilities or worn by the employees.

The open parking lot and the lack of positive authentication for employees and visitors via badge access create opportunities for unauthorized intruders to go unnoticed. The large public sign, indicating a City operating unit may attract unwelcome attention to the facilities.

Consequences of Vulnerability:
In the event that an intruder successfully enters the facilities and causes a disruption of the City's business functions at GIAC, applications/information processing could be interrupted.

Network communications between City departments and the CIAC center as well as between various City departments could be unavailable. The most significant initial impact could be on the public safety services, such as police, fire, and ambulance dispatch and information tracking. Lives of City workers and/or citizens could be at risk. Police officers in the field may not have access to criminal or vehicle information to make safe decisions on imminent actions, putting officers at risk or allowing criminals to escape apprehension. Firefighters may not have access to information about hazardous material located in burning buildings, thereby putting their lives and health at risk in fighting fires.

Disruption of financial services could significantly delay payroll and other payments to City employees as well as the payments or collections of funds from the citizens and/or the City's business partners. This could cause financial hardships not only for the City government and its employees but also for the City at large.

Finally, the absence or delay of needed services and expected services, such as building and safety permits, street maintenance, animal control, scheduling of City park facilities, library checkout and return, etc. could severely undermine the confidence of the constituent population in its elected City Officials and in the ability of the City to govern effectively.

Recommendations:
Item (1) below is designed to reduce risk by reducing threat; items (2), (3), and (4) are designed to reduce risks by reducing vulnerability.

1. Remove wording which identifies GIAC as a City business function from the GIAC sign at the entrance to the parking lot, and from letter heads and business cards. This will reduce visibility and the threat of becoming a target especially during civil unrest or terrorist actions.
2. Create a Defense in Depth environment by adding a perimeter fence around the parking lot, placing a guard at the parking lot entrance, and adding batch access to the entrance door of the GIAC facilities. The cost of these security measures can be recovered by a small increase in the monthly parking fees collected from non-GIAC employees (the parking fees are currently 30% lower than for nearby parking lots).
3. Several City departments have recently implemented a new smart-card security access system which uses fingerprint biometrics for positive authentication and which is tied to the City's personnel and payroll system for up-to-the-minute employee status information. This system could be used for GIAC access, limiting initial costs to the installation of one card reader and the issuance of the smart cards. An extension of this system may be considered in the future for authentication of users to gain logical access to the Cities technology systems.
4. Mandate that badges be worn visibly at all times, issue visitors' badges.

2. Access to the Radio Communication/Microwave Facilities

Areas of Concern:
The City's radio and microwave antennas are located in a remote area at the top of Mount Sans near the outskirts of the City. The facilities are not manned or guarded and visited infrequently by GIAC technical staff for maintenance or upgrade of communication/network equipment or software. A number of hiking trails and a dirt road provide access to the adjacent park and the antenna site. The facilities are surrounded by a 10 ft chain-link fence and a gate locked with a chain and key. The chain-link fence can be easily scaled, the lock and chain easily broken. Due to the remoteness of the site, an intruder will not be immediately detected and would most likely escape quick apprehension.

As result of 9/11-related evaluations of the City of Willowby's physical and logical security and vulnerability, the City's communication antenna site was discovered as the "forgotten" facility. While GSD is responsible for the maintenance and security of all other City facilities, the antenna site is not included.

Security challenges involving the protection of the Sans communication tower differ significantly from the challenges of protecting the central GIAC facility due to the remote and isolated location of the tower site, its unattended status, and the exposure of a considerable portion of its physical communication components without the protective cover of a solid, surrounding structure.

Threats or Risks:
Mount Sans is designated as a City Park and visited by many hikers and outdoor enthusiasts. The area of Mount Sans is also occasionally used for gatherings of groups involved with illegal activities (Gangs) or individuals involved in the use or trade of drugs. This necessitates law enforcement activities and could potentially provoke retaliatory actions by criminal elements.

Physical intrusion into the antenna facility may not only lead to potential sabotage, but could also lead to logical intrusion into the network, an act that could go largely un-noticed for some time under current conditions. Physical or logical intrusion is not continually monitored for this segment of the City's network architechture. This could compromise data and network security.

The antenna site at Mount Sans constitutes a single point of failure in the City's voice and wireless data communication systems. Full redundancy is not feasible.

Consequences of Vulnerability:
The antenna's vulnerability is of special interest since the Mount Sans communication tower facility plays a significant role as an integral part of the City's network and communication infrastructure. Several of the wireless applications were designed to be activated during natural or manmade civil emergencies and will not be operable if the antenna site or the communication link is inoperable. This affects, among others, the Recreation and Parks

Emergency Neighborhood Response and Evacuation (ENRY) program in its effort to request, inventory or distribute emergency supplies and equipment. When isolated segments of the City's network infrastructure may be inoperable during disasters or emergencies, procedural and technical provisions have been made to allow select voice communication capabilities as well as mobile wireless applications to act as backup to the customary data communications. Conversely, when voice communication is disrupted, data communications can be activated in emergency vehicles equipped with the appropriate technology, such as police and fire mobile units. Information available via the wireless geographic locator applications in emergency vehicles can also provide significant assistance during emergency dispatch operations. These capabilities may not be available in case of an antenna disruption.

The impact on public safety applications and actions could be significant when a partial network failure is combined with a failure of the communication tower facility.

Recommendations:

1. At the GIAC central operations facility, provide remote physical and logical intrusion detection capabilities for the Sans communications tower installation to allow for 24x7 monitoring of actions or intrusions.
5. Develop policies and procedures for incidence response including instructions for a potential controlled or emergency shutdown of the communication link if logical or physical intrusion is detected.
6. Place the communication tower site under the jurisdiction of GSD for the maintenance and security protection of the physical facility.
7. Install a "scale-safe" top onto the chain link fence.
8. Provide a secure gate structure with "in-ground" anchors for the gate locking mechanism.
9. Add 24x7 armed protection with a Police mobile unit (Police car) and at least two Police Officers at the antenna site to provide crime/sabotage deterrent and prevention.

3. Police Network Architecture

Areas of Concern:
The City's Police department information system private network is linked to the State law-enforcement network, and via that network, has access to federal and world-wide law-enforcement agencies. The Police Department's private network is also linked with the City's private network for data sharing and processing of resource intensive applications. Access to the State's network is granted only with the provision that the Police Department and the City assures strict adherence to the State's "Outside Agency Network Access" (OANA) policies, procedures, and guidelines. OANA is designed to prevent intrusions into the State's law-enforcement information system and, by association, into federal and word-wide systems.

Threats or Risks:
The City's Police department operates in a semi-autonomous mode and designs, installs, and supports most of its departmental information and network systems. While the technical expertise within the department's IT workforce is extensive, the network design and implementation approach requires close management and coordination with the City-wide network architecture to prevent the inadvertent introduction of vulnerabilities into the Police department's network and its connectivity with the City and the State.

As old technologies change and new technologies are introduced, the implementation of a single "weak link" change into the network could compromise the whole and could provide a sophisticated or highly motivated intruder with access to restricted systems.

While many of the State's network policies and procedures may parallel the City's own, they are not under the City's control and jurisdiction. They are also addressing the protection of data and information that is not under the control and jurisdiction of the City. Adjustments and recoveries from a breach of security are more difficult to manage and may become publicly visible, magnifying the consequences and drawing extensive criticism.

Consequences of Vulnerability:
Most law-enforcement data/information is highly confidential and sensitive. Access to certain data/information violates various privacy acts. Denial-of-service attacks or destruction or modification of data could severely impact the involved law-enforcement agencies' ability to conduct the necessary business/activities. Disclosure of law-enforcement plans or actions could compromise activities and the security of the operation and of law-enforcement personnel.

Since access to the State's law-enforcement network is contractual and governed by adherence to OANA's policies, procedures and guidelines, a breach of security or a failure of an audit by the State will have the immediate consequence of severing access to the State's network and information systems. It could also severely affect the State's confidence in the City's ability to manage it's contractual obligations and adversely influence future inter-agency agreements with the State.

In the event that the Police department's network-link with the State is not available, important information and valuable data can no longer be accessed or exchanged. This will not only deprive the City of needed law-enforcement information, but also prevent such information to be cross-linked with other law-enforcement systems for broader resolution by the City as well as other agencies.

Recommendations:

1. GIAC and the City's Police Department should develop a cooperative, pro-active technical review process of the agencies' network architecture requirements, implementations and modifications with focus on Police Department business and security needs and general City network security issues as well as compliance with OANA requirements and the City's policies and procedures. The Police Department should take responsibility to protect data and processes activities within its own private network; GIAC should provide protection for the City's network infrastructure from intrusion via the Police private network, as well as intrusion from the City's network infrastructure into the Police private network. This technical review process should result in a written agreement of proposed architecture and implementation, signed by both the CIO of the Police Department and the GIAC General Manager.
2. Every effort should be made by both agencies to come to a mutually agreeable resolution through consultations, information exchange, and the pursuit of available and reasonable alternatives. In case a common agreement can not be reached, a formal Technology Impact Analysis (TIA) Report (including a full risk assessment analysis) should be prepared by GIAC and submitted to the Police Department's CIO for consideration. The TIA report should then be submitted to the City's Information Technology Committee (ITC) for final resolution, if a Police/GIAC agreement can not be reached.
3. Actions which require a network architecture review by both GIAC and the Police Department and may result in the preparation of a TIA report should include;
   - new, replaced, or substantially modified Police applications,
   - changes in the network access to the City's network infrastructure,
   - major changes or additions to the Police Department's or the City's network infrastructure,
   - additions or modifications of Police applications or activities which result in noticeable increase in the City's infrastructure traffic,
   - physical relocations of components of the existing Police network infrastructure.

4. Wireless Network Access.

Areas of Concern

The Gartner Group states in a Research Note titled "Deploying Safe Wireless networks[5]:"

> Because today's wireless LANs use radio frequency signals in the 2.5 GHz range to carry network traffic, they are vulnerable to eavesdropping by anyone with a PC and a wireless NIC or inexpensive frequency scanner. To be 802.11b-compliant, wireless NICSs have to implement full promiscuous mode, which allow the NIC to monitor all network traffic. An attacker can also use the NIC to attempt to inject network traffic or spoof legitimate users. WLANs are also vulnerable to denial-of-service attacks, in which an AP receiver is jammed so that it can not receive legitimate traffic.

"Without protective measures, accessing data packets sent over a wireless link into a network is relatively easy and can be achieved with inexpensive technology. "WLANs can provide high convenience for users at the cost of significant disruption to the IS organization. Deploying WLANs without carefully building in security will provide lucrative entry points for hackers and cybercriminals"[5]

In the recent past, various City Departments have purchased equipment and have implemented wireless access applications without review or approval by GIAC. While a Department may inadvertently compromise its own data and network security with the wireless access, the larger implications of facilitating inadvertent access to the City's internal network infrastructure via the Department's private network must be considered.

Threats or Risks

A hacker may gain access to sensitive information/data sent over the wireless network link. This poses a privacy risk and could result in compromised integrity of Departmental or City data.

A hacker may also gain access to addressing and authentication information by intercepting the data packets. This will allow spoofing or intrusion into the Departmental and the City network, may negate firewall protection and user authentication and will make the City's network infrastructure vulnerable to viruses and denial-of-service attacks.

Consequences of Vulnerability

In the event that a hacker successfully intercepts confidential data over the wireless link, data security and confidentially and integrity could be seriously compromised. The City is exposed to the risk of lawsuits and loss of confidence by the public in the ability to protect the rights of Citizens and the ability to conduct City business reliably.

[5] Pescatore, J., Dunlaney, K., Egan, R., Girard, J., Reynolds, M. "Deploying Safe Wireless LANs." Gartner Decision Framework, DF-13-8250 Research Note 5 July 2001: 1.

An intruder, who successfully enters (spoofs) into the Department's or the City's network architecture, could potentially gain access to confidential information/data at any City site connected to the network. Access to the entire City network could also allow for the introduction of viruses or a denial-of-service attack with the potential of shutting down part or all of the City's business functions. Network communications between City departments and the GIAC center may become unavailable. The most significant initial impact could be on the public safety services, such as police, fire, and ambulance dispatch and information tracking. Lives of City workers and/or citizens could be at risk. Police officers in the field may not have access to criminal or vehicle information to make safe decisions on imminent actions, putting them at risk or allowing criminals to escape apprehension. Firefighters may not have access to hazardous material information in burning buildings, putting their lives at risk in fighting fires.

Recommendations

1. As the wireless technology matures and becomes more available it is imperative that the City develops and maintains a well-researched and up-to-date wireless access policy. This will enable the City's Departments to plan and implement the appropriate wireless systems in a safe and reliable fashion in order to protect not only the departmental information/data and operation, but to also prevent intrusions and damage to networks and systems City-wide.

2. Improvements in the state of the art in wireless security are often followed by counter-measures developed in the hacker community. At this time, wireless access policies should adopt a continued conservative approach in the use of wireless communication. Until sufficient access protection and security can be assured the following restrictions should be included in the wireless access policies:
   - Disallow all wireless connectivity to the City's network which requires that sensitive data be sent over the wireless link.
   - Disallow all wireless connectivity to the City's network unless the application requirements and the network design have been reviewed and approved by the Office of Security with the goal to assure data and network security within the Departmental private network and the City-wide network.

3. The wireless access policy should provide a high degree of flexibility and should be reviewed and revised as advances in encryption and other security measures, procedures and technologies become available or as new risks become known either through experience or research, or through developments in the hacker community.

5. Security Awareness for GIAC Employees

Areas of Concern:
Technology alone can not entirely provide the needed security for a large, complex and changing organization, such as the City. Security awareness is a people issue. It is ultimately the individual employee who understands the security policies and procedures, and who applies the intent to the every day processes, who truly guards the organization's information resources. Such knowledge and understanding needs to be acquired by every new GIAC employee, contractors, agents, or designees. Awareness needs to be heightened through education. However, security knowledge and awareness can get diluted over time without a recurring awareness program, and complacency can set in. The careless sharing of a password, the entry of a stranger through a secured entry door behind a well meaning and courteous employee, the thoughtless installation of an inexpensive wireless port at some remote office PC, all can compromise the most sophisticated technical security measures. The favorite hacker practice of "Social Engineering," a process, by which a hacker extracts security information from an accommodating employee through apparently harmless conversations, can be avoided with heightened security awareness.

The Gartner Group, in its "First Take" research notes states: "[Security] breaches. are common and often result from a lack of security awareness on the part of a well-intentioned IT security staff.[6]" COBRA risk consultants state: "Enterprises that do not have a security policy should develop one. Those that do have a policy should verify that employees understand and comply with it.[7]" Handing a new employee the GIAC security policies is not enough. A program is needed to assure that the employee has read the policies, understands them, and is willing to comply with them. A follow-up assurance program is needed at regular intervals to verify that policies continue to be followed and understood and that new ones are integrated in the existing knowledge base.

Currently, the City does not have a formal security awareness program for existing employees. The security awareness program for new employees is limited to the new employee's signature on a non-disclosure agreement. No verification is conducted that the employee actually read the statement or understood it. While new or amended security policies are distributed among all employees, no process is in place to verify that all employees have actually read and understood the policies.

[6] Hunter, R., Malik, W. "Power Station Incident Should Generate Further Security Awareness." Gartner FT-13-9552 Research Note. 18 June 2001. URL: http://www3.gartner.com/Init Search: FT-13-9552. (30 Jan. 2002)

[7] COBRA Risk Consultants. "The New Era in Security Risk Management." WEB home page. URL: http://www.ca-systems.zetnet.co.uk/risk.htm (30 Jan. 2002**)**

Threats or Risks:

The lack of employee security awareness poses as much of a risk to the City as any potential breach of security. An imposter or terrorist may gain access to the physical facilities and cause damage. Sharing of passwords or other personal authentication information may gain a hacker access to the City's information/data and the network infrastructure. As technologies change, the unintended implementation of a single "weak link" into the network could provide an intruder with access to sensitive information/data sent over the network.

Consequences of Vulnerability

Unauthorized access to sensitive information/data poses a privacy risk and could result in compromised integrity of the data. A hacker may also gain access to addressing and authentication information. This will allow spoofing or intrusion into the network, may negate firewall protection and user authentication and will make the City's network infrastructure vulnerable to virus attacks and denial-of-service attacks.

In the event that a hacker successfully intercepts confidential data, the data security and confidentially and integrity could be seriously compromised. The City is exposed to the risk of lawsuits and loss of confidence by the public in the ability to protect the rights of Citizens and the ability to conduct City business reliably.

A successful intruder, who enters (spoofs) into the City's network architecture, could potentially gain access to confidential information/data at any City site connected to the network. Access to the City network could also allow for the introduction of viruses or a denial-of-service attack with the potential of shutting down part or all of the City's business functions. Network communications between City departments and the CIAC center cold be unavailable.

In the event that an intruder successfully enters the facilities and causes a disruption of the City's business functions at GIAC, applications/information processing will be interrupted. Network communications between City departments and the CIAC center will be unavailable. Damage to the facilities, the installed technology, the loss of data and the cost of recovery could be considerable.

The most significant initial impact of malicious intrusion into the GIAC facilities or the City's network will be on the public safety services, such as police, fire, and ambulance dispatch and information tracking. Lives of City workers and/or citizens will be at risk. Police officers in the field will not have access to criminal or vehicle information to make safe decisions on imminent actions, putting them at risk or allowing criminals to escape apprehension. Firefighters will not have access to hazardous material information in burning buildings, putting their lives at risk in fighting fires.

Disruption of financial services could significantly delay payroll and other payments to City employees as well as the payments or collections of fund from the citizens and/or the City's business partners. This could cause financial hardship not only for the City government and its employees but also for the City at large.

Finally, the absence or delay of the needed services and expected services, such as building and safety permits, street maintenance, animal control, scheduling of City park facilities, library checkout and return, etc. could severely undermine the confidence of the constituent population in its elected City Officials and in the ability of the City to govern effectively.

Recommendations:

1. Develop and implement a security training and awareness program for new GIAC employees, contractors, agents, or designees including a briefing on existing policies and procedures, an awareness and defense to the "Social Engineering" process, a question and answer session, and a quiz to validate understanding.

2. Develop and implement an annual recurrent security training and awareness program for existing GIAC employees, contractors, agents, or designees. This program should include changes in policies and procedures, continued awareness and defense against the "Social Engineering" process, a question and answer session, and a quiz to validate understanding.

3. At regular intervals distribute pamphlets, flyers, notes, or newsletter alerts as frequent reminders and updates to enhance and support security awareness among GIAC staff.

Select Security Policies

1. GIAC Enterprises Physical Security Policy

Purpose

This policy intents to ensure a safe working environment for people and to protect the City's Information Technology resources, data and information from unauthorized access, damage, or dissemination in order to ensure resource and information confidentiality, integrity and availability.

Background

This policy is intended to guarantee the high priority of security and services needed by City Departments and associated agencies that are served by GIAC Enterprises, to ensure the public's privacy, safety and welfare. The policy addresses requirements and mandates set forth in the City of Willowby Administrative Code, Chapter 26, the Police Department/GIAC Enterprises Management Control Agreement (PG-MCA), any security agreements between GIAC Enterprises and the City Departments, or other authorized agencies, as well as any other applicable laws, directives, privacy acts, or mandates such as Health Insurance Portability and Privacy Accountability (HIPPA) and Family Education Right to Privacy Act (FERPA).

Scope

This policy is limited to physical security aspects which affect facilities occupied by personnel, technology resources, and data/information placed into the custody of GIAC Enterprises or under the control and management of GIAC Enterprises, or accessible via the GIAC Enterprises controlled City network infrastructure. Excluded from this policy are facilities, resources and data/information under the control of City Departments.

Policy Statement

Physical access to GIAC Enterprises' technology, facilities, and data/information is governed by the following principle:

> The authorization for use or access has been granted, AND
> a job-related, or service-related need to know or use exists.

It shall be a misdemeanor for any person to violate, or attempt to violate this policy or in aiding or abetting in its violation either purposely or through negligence. This includes any unauthorized tampering, modification or interference with existing security measures.

"It shall be a misdemeanor for any person to tamper with, change, alter, destroy, or use Information Technology resources or data/information, or use, disclose or make known in any manner data/information, except to a duly authorized representative of the department supplying such information. This includes the content or nature of any such confidential information while it is in the custody of GIAC Enterprises for processing, or any such information which is originated or accessed by GIAC Enterprises without the express consent of the General Manager of the department supplying the information, except in accordance with programs for processing the data/information which have been approved by the General Manager of GIAC Enterprises."[8]

<u>Responsibility</u>

The responsibilities for physical security are detailed in the City of Willowby Administrative Code[8] as follows:

> The GIAC Enterprises General Manager shall enforce all GIAC Enterprises policies and procedures. The General Manager of GIAC Enterprises shall consider the confidential nature of information placed into its custody or to which access is provided via the City's network architecture, and shall take such measures as are required to maintain the confidentiality, integrity, and availability for such information. During the period of time such information or access is under the control of GIAC Enterprises, it shall have sole responsibility for the maintenance of the security and availability of such information and the network architecture which provides access to the information.
>
> The General Manager of GIAC Enterprises has the sole authority to approve the installation or removal/modifications of GIAC Enterprises' physical security measures. .
>
> GIAC Enterprises shall provide continuous physical, security to preclude injury to staff or damage to technology resources and data/information as well as unauthorized access or use of hardware, firmware, and/or software facilities used to facilitate exchange, or used for storage of confidential data/information. Such physical security shall include all City-owned and leased facilities occupied or used by GIAC Enterprises.
>
> GIAC Enterprises services shall include, but not be limited to the review and acceptance of plans for the construction of new public buildings and the remodeling of existing public facilities or leased facilities for City use, when such construction or remodeling affects the physical security requirements and installations for systems and networks under the jurisdiction of GIAC Enterprises.
>
> GIAC Enterprises shall comply with all other restrictions, such as applicable regulations, laws, directives, privacy acts, or City mandates. GIAC Enterprises shall monitor the maintenance of its facilities, information systems and the network architecture to ensure protection of the information technology resources and data/information confidentiality, integrity, and availability.

[8] Excerpts from the City of Willowby Administrative Code, Chapter 26 – Adapted from: <u>City Administrative Code</u>. Los Angeles: City of Los Angeles, 2001. Division 22, Chapter 26, Sections 640-652

Action

In case of a breach of security, it shall be the responsibility of the General Manager of GIAC Enterprises to take the appropriate preventive and disciplinary actions and report any breach of security to ITC.

All GIAC Enterprises employees, contractors, agents, or designees using the City's computing environment, resources, facilities or data/information under the jurisdiction of GIAC Enterprises, are responsible for:

- understanding, supporting, and complying with all applicable and related GIAC Enterprises Security Program policies, standards and guidelines.
- understanding their respective roles and obligations regarding physical security requirements,
- actively safeguarding the GIAC Enterprises resources and the confidentiality and integrity of data/information entrusted to them at all times,

2. Wireless Network Access Policy

Purpose
This policy is intended to protect the City's information resources from unauthorized access to data/information or to the City's network infrastructure via wireless segments connected to the City's network.

Background
Unauthorized and malicious access to the City's network infrastructure could compromise the data/information security, privacy, and integrity, could inject a damaging virus, or could initiate a denial-of-service attack, potentially shutting down or damaging some or all of the City's critical and life-saving support systems.

"Wireless network technology is viewed as an inexpensive alternative to wired network installations and it provides greater flexibility for access options and choice of equipment. Flexibility and open-ended technology creates increased opportunities and risks for intrusion. "The Wireless Equivalent Privacy (WEP) encryption algorithm, which is at the heart of the 802.11 standard, has been shown to be susceptible to hack attacks using statistical analysis and other know techniques."[9] Currently available encryption "could be compromised in between 15 and 45 minutes. Even if attackers didn't break code, they could cause denial-of-service problems."[9]

Scope
This policy addresses wireless connectivity to the City's network that is under the control of GIAC Enterprises or to devices (PCs, servers, etc.) that have access to the City's network infrastructure. Connectivity to departmental standalone systems is addressed separately.

Policy Statement
Wireless communication with the City's network infrastructure is prohibited if it requires that sensitive, confidential, private data, or data protected by laws or mandates is sent over the wireless link.

Wireless access to the City's network infrastructure is prohibited unless the application requirements and the network design has been reviewed and approved by GIAC' General Manager to meet current access and security standards. The review will address both the risks to the application and its data to be transmitted over the wireless segment, and the risk of intrusion into the City's network infrastructure.

Approval to connect a wireless segment to the City's network infrastructure shall not be unreasonably withheld. Permission to install a wireless link to the City's network infrastructure

[9] Moad, Jeff, Cottam, Bob. "Olympics Benching Wireless LAN Plans." e-Week. 21 January 2002. URL: http://www.eweek.com/article/0,3658,s%253D701%2526a%253D21479,00.asp (22 Jan. 2002)

will be granted if the architecture of technology, processes, and application design can assure that the operation and security of the City and its departments will not be compromised.

For wireless access to the City's network infrastructure to be granted, the following minimum requirements must be met:

- The highest level of available default WEP encryption must be used.
- The unique MAC (Media Access Control) address on the NIC (Network Interface Card) of the hand-held device must be checked and authorized. Where MAC address tracking cannot be implemented, a Virtual Private Network (VPN) will be required.
- Wireless devices must be equipped with virus protection software and a personal firewall.
- Access to the City's network must be via a City De-Militarized Zone (DMZ) providing firewall protection between the access point and the City's network.
- User authentication will be, at a minimum, user-id and unique password. More sophisticated authentication may be required.

Responsibility

The GIAC General Manager shall approve all new wireless installations as well as modifications to existing installations. The Manager of the Office of Security shall prepare a written report and recommendation of the technical approach to wireless connectivity to the City network infrastructure, including risks to the application and/or to other City systems, for review and approval by the GIAC General Manager. The project manager responsible for the implementation of the wireless connectivity project shall present a written proposal to the manager of the Office of Security, detailing the project requirements, the sensitivity of data, and the technical approach to the wireless connectivity.

GIAC's technical staff in cooperation with the Office of Security shall review the technical foundation of the requirements, assess feasibility and security of the proposed implementation plan using currents standards, technology, and information, and make alternative recommendations if needed. As additional factors, capabilities or functionalities become available GIAC's technical staff will review the status of acceptable security solutions and technology. When new security issues become known which pose a significant threat to the application or the City, GIAC will advise the affected user Departments and coordinate remedial measures.

Action

A violation of this policy will result in the removal of the wireless access to the City's network. A violation may also result in the removal of the violating Department's access to the City's network until the Department's network security has been reviewed by GIAC and it can be established that the City's network architecture is adequately protected from unauthorized intrusions.

3. Security Awareness for GIAC and City Employees Policy

Purpose:
The purpose of the security awareness program is to ensure that GIAC employees, contractors, agents, or designees participate in the physical and logical protection of the City's information resources across multiple computing platforms and the network. Information security involves five major functions: physical and logical access control, identification and authentication, data confidentiality, data integrity and non-repudiation and systems and data availability.

Background:
The protection of the City's information resources is of utmost importance to assure the continued ability to deliver the required services and information to the citizens of Willowby. While technology and procedures have been implemented to guard against many risks of physical and logical intrusion and malicious activities, employee awareness and vigilance are of equal importance to detect, prevent and guard against breaches of security or the introduction of "weak links" in the chain of security procedures or provisions.

Scope:
This policy is intended to assure that all GIAC employees, contractors, agents, or designees conduct themselves and plan their actions in accordance with the practices and intent of the established general physical and logical GIAC security policies and procedures as well as those policies and procedures specifically applicable to their area of responsibility to:

- ensure the availability and integrity of information resources entrusted to the care of GIAC or accessible by GIAC,
- maintain a secure operating environment for personnel and technology,
- support current and emerging business practices within a secured environment.

All new and existing GIAC employees, contractors, agents, or designees will be provided with appropriate security awareness training. This will assure that they are equipped with the necessary knowledge and awareness to comply with the directives and intent of the applicable security policies and procedures as well as the vigilance to detect and act in response to unusual or suspicious events or behavior.

Policy Statement:

1. Prior to being granted security privileges, new GIAC employees, contractors, agents, or designees:
   - shall be provided with written copies of GIAC's general policies and procedures and all policies and procedures applicable to their specific area of responsibility and/or duty;
   - shall participate in an introductory security awareness course;
   - shall pass a written test designed to assure understanding of the course content and intent of the applicable policies and procedures.
   - shall sign a written statement that the GIAC policies and procedures and security practices have been read, are understood, and that the individual is prepared to support and comply with the requirements.

2. Within (+-) 30 days of their annual anniversary date, all current GIAC employees, contractors, agents, or designees:
    - shall participate in a recurrent security awareness course;
    - shall pass a written test designed to assure understanding of the course content and intent of the applicable and current policies and procedures.
    - shall sign a written statement that the current GIAC policies and procedures and security practices have been read, are understood, and that the individual is prepared to support and comply with the requirement.
3. Throughout the year, new and updated policies and procedures shall be provided to GIAC employees, contractors, agents, or designees as applicable; notes, updates and reminders shall be distributed.

Responsibility:
The Director of Personnel is responsible for the development, implementation and administration of the security awareness program and to ensure the inclusion of all applicable personnel. The Manager of the Office of Security is responsible for providing the pertinent information on policies and procedures, best business practices, and updated industry information and to monitor the effectiveness of the security awareness program. Each of GIAC's managers is responsible for monitoring and assuring that their staff has received the security awareness training applicable to the specific area of responsibility or duty and to support and monitor their staff's participation and compliance with the security awareness program.

It is the responsibility of all participants in the security awareness to understand, support, and comply with the GIAC security directive and with their respective roles and obligations regarding physical and/or logical security requirements. All users of the City's computing environment, resources, or facilities are responsible for safeguarding the confidentiality and integrity of information entrusted to them at all times and to understand, support, and comply with all applicable and related Security Program policies, standards, and guidelines. The manager entrusted with the information, information resource, and/or facility is responsible for reviewing and monitoring compliance with the GIAC Security Program's policy, standards, and guidelines.

Action:
No security privileges shall be granted to new GIAC employees, contractors, agents, or designees unless requirement 1 of the security awareness policy is met. Failure to meet this requirement within 30 days of employment could result in termination.

Failure to meet requirement 2 of the security awareness policy 30 days past the annual anniversary date will result in the revocation of all security privileges and may result in termination.

Assignment 3

Define a Security Procedure

GIAC Enterprises Physical Security Procedure

GIAC Enterprises Physical Security Procedure

What actions are needed

The perimeter and offices of GIAC Enterprises must be monitored and protected, and individuals authenticated, to prevent unauthorized access and/or intrusion, injury to personnel, or damage to facilities, resources and/or sensitive City information/data. Installation and maintenance of a perimeter fence, a parking lot gate with attendant, access to the facilities only via personal badges and badge readers, and wearing of personal and visitors badges will provide access control and an acceptable level of authentication of personnel on the premises.

Why actions are important

The facilities of GIAC Enterprises are frequently visited by a multitude of technical and management personnel from many City departments as well as vendors and contract support/maintenance personnel. They are often not personally known to staff and therefore not easily distinguished from potentially malicious or dangerous intruders. Positive authentication of City/GIAC and visiting personnel is needed to allow early and proactive measures in case of a breach of security.

A secure perimeter for the GIAC facilities and personnel authentication will ensure the delivery of services needed by City Departments and associated agencies that are served by GIAC Enterprises. Delivery of City services provides privacy, safety and welfare to its citizens. Sensitivity to the need to protect public sector facilities has heightened since the 9/11 terrorist events.

Who is responsible for carrying out actions

The manager of the GIAC Office of Security has the responsibility for planning, designing, implementing, operating and coordinating the physical security measures for the GIAC facility perimeter and access security. The Manager of the Office of Security reports to the General Manager of GIAC Enterprises.

The installation and maintenance of the badge readers is the responsibility of GIAC Enterprises. The GIAC Enterprises Facilities Manager is responsible to monitor the compliance with policies and procedures and with established security measures and report breach of security to the GIAC Manager of Security and the GIAC General Manager. The GIAC Enterprises General Manager must approve requests for exemptions to the installation of badge readers or the 24/7 closure policy.

The manager of the City's Personnel Office and the manager of the GIAC personnel office are responsible for the up-to-date maintenance of their respective personnel files used to establish, modify or revoke badge access to the GIAC facilities.

All GIAC Enterprises managers entrusted with the information, information resource, and/or facility are responsible for reviewing and monitoring compliance with the GIAC Enterprises physical Security Program's policy, standards and guidelines, to maintain a secure environment, and to immediately report any breach of security or an apparent weakness in GIAC Enterprises' physical security to the GIAC Enterprises Office of Security, and the GIAC Enterprises General Manager.

GSD is responsible for the installation and maintenance of the GIAC facility perimeter fence. GSD is responsible for the installation and maintenance of the access gate to the GIAC parking lot. GSD is responsible for hiring and managing the parking lot attendants and the facility guards and monitor the guards' availability and diligence.

In case of a breach of security, the City's Personnel Department shall carry out disciplinary personnel actions for City personnel; The GIAC personnel manager shall carry out disciplinary actions for GIAC personnel.

When and/or where are actions taken

The perimeter fence is to be constructed immediately and maintained in good working condition and free of defects or damage.

The GIAC sign is to be removed immediately and is to be replaced with a generic sign which only indicates the name GIAC without indicating a City affiliation.

The parking lot gate at the entrance to the parking lot is to be attended by a parking lot attendant 24 hrs. a day, 7 days a week.

Individuals without valid parking permits may not enter the parking lot.

A security guard at the entrance to the GIAC facilities is to be present 24 hrs a day, 7 days a week.

Entrance into the GIAC facility is limited to City and GIAC employees, and contractors or consultants with valid identification badges, or visitors which are escorted by an individual with a valid identification badge.

How are actions monitored/audited for desired effect

GSD periodically patrols the perimeter fences and evaluates the proper functionality of the entrance gate into the GIAC parking lot.

GSD regularly monitors the presents and diligence of the parking lot attendants and the security guards in the GIAC facilities.

The Office of Security periodically monitors and audits the personnel data provided to authenticate only current and active employees

The Office of Security periodically monitors and audits the functionality and proper settings of the GIAC badge readers.

Procedures, Actions, and Incident Response

Perimeter Fence:

A security office shall periodically check the perimeter fence, at least twice daily, for signs of break-in, damage, or intrusion. Any damage or wear shall be reported to the GIAC Office of Security immediately. The Office of Security will notify GSD with a request for repair. GSD shall respond to the call with remedial actions within two (2) hours.

Facilities Management:

The City's General Services Department (GSD) shall manage all leases for facilities occupied by GIAC Enterprises staff or equipment. In managing the GIAC facilities, GSD shall incorporate into contracts the GIAC Enterprises physical security requirements and the installation of GIAC Enterprises required security measures. In the event that permit processes, building safety or fire codes or any other applicable mandates or laws require modifications to the GIAC Enterprises security measures, GSD shall coordinate in the most expeditious time frame such changes to meet the GIAC Enterprises security requirements and pursue the necessary funding (if needed) to make the modifications or to find alternate facilities.

Parking Lot:

Regular parking permits shall only be issued to GIAC or City employees, contractors or consultants and employees of business with parking contracts with the City. No other individual may receive or use a regular parking permit. Parking permits may only be used by the person to which the permit was issued. Providing such a permit to another individual or allowing such a permit to be used by another individual will result in the confiscation of the permit either temporarily or permanently.

Vendors or other visitors must be pre-approved by the office of security at least 30 minutes prior to arrival and such approval shall be communicated to the parking lot attendant via telephone by the Office of Security. The parking lot attendant issues the temporary parking permit to the visitor. The visitor's name and drivers license number must be provided to the parking lot attendant; the attendant will verify the authorization to enter the parking lot by checking the driver's license. The temporary parking pass must be clearly displayed on the inside of the front windshield of the vehicle.

A security officer shall periodically, at least twice daily, check the cars in the parking lot to verify that a valid parking pass is displayed on the rearview mirror or on the windshield of all vehicles.

Security Guard:

All City owned or leased buildings occupied by GIAC Enterprises staff shall have entry of all personnel to the building controlled and monitored by security personnel at all times. The security guard checks identification badges and issues visitors' badges to approved visitors. The security guard assures that a visitor is escorted by an individual who carries a City or GIAC identification badge and signs the visitor entry log for the visitor.

The Security personnel is to report any unusual or suspicious activities immediately to the GIAC Office of Security and notify the City law enforcement agency where this may be warranted. A panic button in the form of a silent alarm is installed at the desk of the Security Officer and will alert the Office of Security as well as law enforcement of an incident in progress.

The Security Officer shall maintain a log of all visitors and their escorts which contains the visitor's name, the escort's name, the time of entry and the time of departure, and the person or department the to be visited.

Identification Badges, Visitors' Badges:

An identification badge or visitor's badge must be worn in clear view at all times. Any GIAC employee, who observes a person without a visible GIAC badge or visitor badge shall report such an observation immediately to the Office of Security. The Office of Security shall, with the assistance of a security guard, escort the individual without an identification badge or visitor's badge out of the building. A GIAC or City employee, contractor or consultant, who willfully or carelessly does not wear an identification badge visible at all times inside the GIAC facilities may lose all security privileges and may be subject to disciplinary actions, including termination.

Vendors or other visitors must be pre-approved by the office of security at least 30 minutes prior to arrival and such approval shall be communicated to the security officer via telephone by the Office of Security. The visitor will be issued a temporary visitor's badge by the security guard. The visitor's name and drivers license number must be provided to the security guard. The security guard will verify the authorization to enter the building by checking the driver's license. The temporary visitor badge is only valid for the day it is issued but may be used for multiple entries that day, provided that the visitor is accompanied by an escort for each entry. The visitor's badge must be visibly worn at all times while within the GIAC facilities. The visitor's badge lists the name of the visitor, the name of the escort, the current date and the initial time of entry, and the person or office to be visited.

An authorized City employee or contractor must accompany (escort) visitors through the GIAC Enterprises facilities. That accompanying person will be held responsible for any security breaches committed by the visitor.

A badge access master file is maintained by the Office of Security. This file is automatically linked to the City and GIAC personnel files and updated when a newly hired or contracted person is added to the workforce, or modified when the person's status changes.

For an individual to receive badge entry authorization, the manager responsible for the person submits a badge authorization form to the Office of Security. This form indicates, in addition to the person's name and employee ID number, the authorized facilities for which access should be granted, and the authorized hours and/or days of access. The necessary level of access security for the identification badges will be approved by the GIAC Enterprises General Manager via the Badge Access Form

The Office of Security issues the personal identification badges. The authorized person brings the approved badge access form to the Office of Security. Two pictures will be taken, one to be laminated onto the identification badge, the other retained by the Office of Security for future reference. In addition to the picture, the badge contains the persons name and the City or GIAC employee identification number.

Access to GIAC facilities will be temporarily revoked and reassigned upon loss or theft of badge or employee's change of duties as part of the Notice of Assignment process. Access will be revoked upon termination. Access shall be temporarily revoked for an individual at the direction of the GIAC General Manager or the responsible manager while that individual is under investigation of a potentially serious breach of security. Ongoing monitoring of granted badge access authorities will be the responsibility of the manager of each City employee or contractor.

Access to GIAC Enterprises facilities via personal security badges shall be based on the principle of "Least Privilege." Access to facilities and time of access via badges shall be granted only to those individuals that need such access to perform the assigned duties in support of City business, be limited to the needed locations and during the needed hours. Formal city badges shall only be issued to City and GIAC employees, contractors and consultants; others will receive temporary visitor's badges.

A lost or stolen badge must be reported immediately to the Office of Security. Any misuse of a lost badge is the employees responsibility. A badge reported lost or stolen will be deactivated immediately and a new badge will be issued to the employee or contractor.

Badge Readers:

Access to all GIAC Enterprises offices, storage facilities, or network and wiring closets shall be secured via a badge reader at the door(s), except doors specifically excluded from such requirements. The doors equipped with badge readers are to remain locked at all times, 24 hours a day, 7 days a week (24/7), allowing access to the facilities only to properly authorized individuals via their personal badges.

The Office of Security shall monitor all badge reader activities and report to the General Manager of GIAC Enterprises any unauthorized attempt to access the facilities through any door equipped with a badge reader either with a badge, or key, or any other means, and report any incidents where a door was held open for more than 20 seconds.

GIAC Office of Security shall monitor access via the installed badge readers and provide written information to the GIAC General Manager upon request about the following:

- Identify the individual who was issued the badge used in the attempt to access the reader (door/facility);
- Identify date and time of access;

- Indicate if the access was within or outside the authorized parameters (badge not authorized, location not authorized, time frame not authorized);
- Indicate if the door has been opened by means other than an approved badge
- Indicate if door held open for an extended period of time;
- Maintain an automated warning system of unauthorized, unapproved, or inappropriate (i.e. door held open) access to GIAC Enterprises facilities and notify the GIAC Enterprises General Manager, the Assistant General Manager of Public Safety, the Office of Security, and the GIAC Enterprises Facilities Management Office as soon as practical of any unauthorized access attempts.

Emergency requirements to disable or modify physical security measures or any component failures must be communicated immediately to the GIAC Enterprises General Manager and the Office of Security. Conditions must be returned to the original, approved status as soon as practical. Such emergency actions could be, but are not limited to, the result of a fire in the building, or could be the result of construction activities.

Incident Response:

In case of a breach of security, which may include but is not limited to, successful unauthorized access to a facility or theft of City or personal property, the manager responsible for the business conducted at the compromised facility shall notify via e-mail or any other available means, the GIAC Enterprises General Manager, and the Office of Security as soon as possible but no later than one working day after the incident has occurred. The Manager shall prepare a written Incident Report within three working days and assist the Manager of the Office of Security with the follow-up investigation. The incident report shall include:

1. the location, date and time of the incident,
2. the detailed and researched assessment of risk to City security,
3. in case of theft, the description of the property and its value,
4. a detailed and researched description of the incident,
5. a detailed and researched assessment of any contributing factors to the incident,
6. detailed and researched assessments and recommendations on how the incident can be avoided or prevented in the future.

The Office of Security will coordinate the follow-up investigation with GIAC Enterprises' management and affected or involved outside Departments or Agencies, the filing of police reports if this is warranted, and the implementation of preventive measures.

Bibliography

COBRA Risk Consultants. "The New Era in Security Risk Management." WEB Home Page. URL: http://www.ca-systems.zetnet.co.uk/risk.htm (30 Jan. 2002)

Fried, Stephen. SANS Security Leadership, Part 1. SANS Institute, 2001. 1.9.

Hunter, R., Malik, W. "Power Station Incident Should Generate Further Security Awareness." Gartner First Take FT-13-9552 Research Note. 18 June 2001. URL: http://www3.gartner.com/Init Search: FT-13-9552. (30 Jan. 2002)

Moad, Jeff, Cottam, Bob. "Olympics Benching Wireless LAN Plans." e-Week. 21 January 2002. URL: http://www.eweek.com/article/0,3658,s%253D701%2526a%253D21479,00.asp (22 Jan. 2002)

Pescatore, J., Dunlaney, K., Egan, R., Girard, J., Reynolds, M. "Deploying Safe Wireless LANs." Gartner Decision Framework, DF-13-8250 Research Note 5 July 2001: 1.

Imaginary City of Willowby Bibiliography

Willowby City Administrative Code*

Los Angeles City Administrative Code*. Los Angeles: City of Los Angeles, 2001. Division 22, Chapter 26, Sections 640-652

Police Department/GIAC Enterprises Management Control Agreement (PG-MCA)**

Los Angeles Management Control Agreement (MCA)** Los Angeles: City of Los Angeles, 2000.

*Note: The Willowby City Administrative Code referenced in this report is an imaginary document designed for the imaginary City of Willowby. References to this document were adapted from the Los Angeles City Administrative Code.

** Note: The Police Department/GIAC Enterprises Management Control Agreement (PG-MCA) referenced in this report is an imaginary document designed for the imaginary City of Willowby. References to this document were adapted from the Los Angeles City Management Control Agreement (MCA).

END OF REPORT