Global Information Assurance Certification Paper

GISO - Basic Practical Assignment Version 1.3 (February 7, 2003)
Assignments 1-4

Avoiding Disaster: Business Continuity Challenges at a Small Non-Profit Organization

Jeffrey M. Stanton

8/12/2003

Abstract:

GIAC Enterprises is a small non-profit organization that serves the professional needs of approximately 4500 academics and practitioners. With a permanent staff of only ten and a single systems administrator, GIAC has many operational tasks related to an online bookstore, a large annual conference, a media referral service, and a variety of other information resources. Although GIAC has avoided any major information systems disasters, a number of recent, minor problems have underscored the need for more formalization of policies and procedures, particularly with respect to ensuring that critical files could be restored in case of loss or damage to the organization's file server. The present GISO practical assignment describes GIAC's operations, identifies risks related to current vulnerabilities and threats, revises an extant disaster recovery policy to suit GIAC's needs, and derives a backup rotation and offsite storage procedure that addresses responsibilities defined in that policy.

GISO - Basic Practical Assignment Version 1.3
Assignment 1 – Describe GIAC Enterprises

Description of GIAC Enterprises

GIAC Enterprises (hereafter referred to simply as GIAC) is a 401c3 non-profit corporation, in existence for 26 years, and focused on promoting education, research, and professional practice for approximately 4500 academic and practitioner members. Most of the members are Ph.D. or master's level professionals employed in large U.S. firms and institutions of higher education, although an increasing number of members are also employed in international settings.

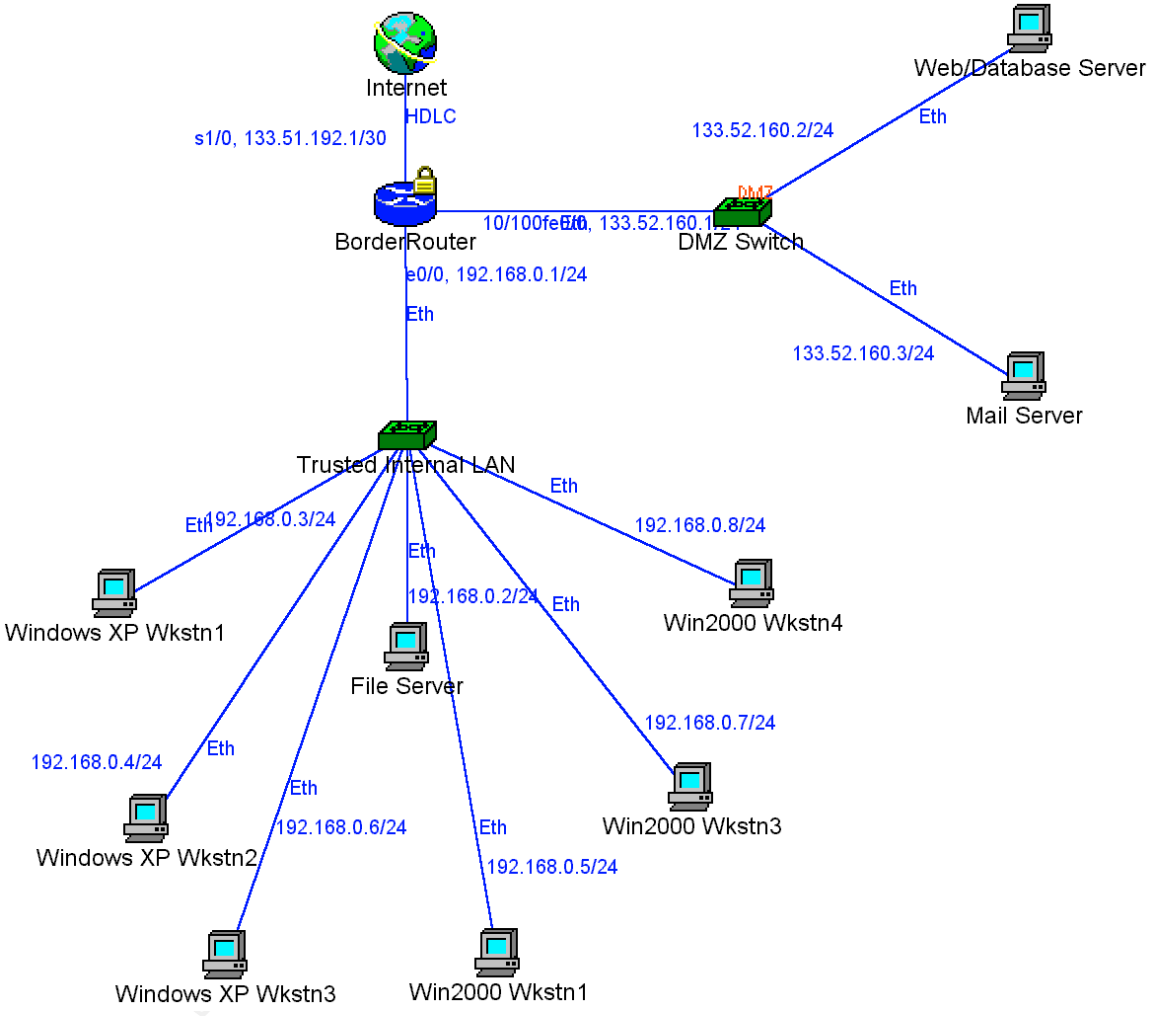
GIAC has two critical missions that have roughly equal priority: First, GIAC serves as an information repository and resource for its dues paying members. This aspect of GIAC's mission includes administering a glossy quarterly newsletter, operating an online bookstore, maintaining an online professional directory, serving as a press liaison, hosting an electronic bulletin board, and maintaining a library of printed and electronic documents that have continuing importance to the membership (e.g., code of ethics, guidelines for training, etc.). For each of these products or activities, GIAC also serves as a central locus for a large cadre of volunteer board and committee members who serve the organization.

The second mission of GIAC is to plan, develop, and administer an annual professional research and practice conference. The conference is always located at a hotel conference center in a metropolitan area of the continental U.S. and usually attracts over half the membership as well as a plethora of sponsors and vendors. Creation of the conference is facilitated by an online conference registration system that provides the means for members to pay their conference fees by credit card. The same system, with minor modifications, also provides an interface for annual dues payment by credit card. Development of the conference program is a complex logistical challenge because GIAC usually receives over 6000 presentation proposal submissions from its members, each of which must be reviewed and, if accepted, scheduled into one of approximately 20 simultaneous tracks over the three-day conference. The conference tracks are tailored to membership preferences in order to attract the maximum number of attendees.

Like many non-profit professional societies, GIAC comprises a relatively small administrative office (approximately 10 full time and part time employees) as well as a rather large volunteer board. Approximately 12 executive board members have essentially the same rights of access to GIAC's resources as salaried employees (although none is collocated with the office), and a further 50 committee members have more restricted access. An 80% FTE system administrator conducts most of the day-to-day IT-related activities for the office but also delegates a subset of IT tasks to knowledgeable volunteers from the executive board or committees.

GIAC's IT Infrastructure

In overview, GIAC's IT infrastructure comprises an internal network for the use of the main office staff plus an externally visible DMZ with servers for web hosting and email. Seven hosts exist on the internal network and two hosts exist in the DMZ. All of these resources are collocated in GIAC's main office space and no special facilities (i.e., other than outside door locks) exist for the physical security of the network infrastructure. The network diagram below provides a detailed view of the complete configuration.



(*Note: This network configuration was adapted from configurations portrayed in Cole et al., 2002, with modifications as needed to fulfill the requirements of the assignment and match the business operations of GIAC. The network diagram was prepared in Cisco ConfigMaker.*)

The figure depicts a Cisco 1751 router as the organization's border router. The router has network address translation enabled and this allows the hosts on the trusted network to share a single static IP address. One interface of the border router is connected to a Cisco 1548 switch that concentrates traffic from the DMZ. Behind this

switch, two hosts implement email, on the one hand, and all web pages and interactive web applications on the other (running IIS). The server with the interactive applications runs SQL server for database functions and ASP for interactive content. The organization does not have a DNS server: The organization's ISP provides DNS services.

The figure also depicts the border router connected to a second Cisco 1548 switch that manages traffic on the organization's internal network. The router uses network address translation with the hosts on this internal network. Behind the internal switch a file server runs Windows 2000 professional. This file stores most shared mission critical data, including an unencrypted list of credit card numbers recently used in e-commerce transactions at the online bookstore, for conference registration, and for dues payment.

This file server also stores the "reference" copy of GIAC's website: As modifications to the web site are completed and tested on this trusted server, they are uploaded to the publicly visible production server. The internal file server contains a tape drive that is configured to automatically backup the files on the server every Thursday night. Employees are encouraged to keep their own mission critical files on this system rather than on the hard drives of their individual workstations. Some employees use a Zip drive to save key files from their own workstations and it is routine for employees to take the Zip disks home so that they can work with the files outside of normal business hours. Six individual workstations are connected to the internal network and about half of these are running Windows XP while the other half are running Windows 2000 professional. All hosts on the internal network are running Norton anti-virus with the automatic update procedure enabled. None is running a personal firewall. The network does not have an intrusion detection system.

The ACL on the router is configured to restrict incoming traffic with a default DENY ALL policy, with selected services (SMTP, HTTP, HTTPS, ICMP) permitted for the two servers in the DMZ. The egress policy permits all types of outgoing traffic from the hosts on the internal network. The router ACLs were configured by GIAC's system administrator and were not crosschecked by anyone else. The router ACLs have remained essentially static since the router was installed and configured, although minor changes have been added from time to time to support extra services requested by employees.

GIAC has no computers or networks operating at geographically dispersed locations. Connections with vendors all occur by pushing data through vendors' websites (or through more traditional telephone and paper ordering and payment procedures). No VPNs, dial-ups, or other connections with vendors are initiated at GIAC. No wireless gateways or systems with wireless network components are connected to GIAC's network. The router is configured to disallow remote administration. Some employees own their own laptops and two individuals in the GIAC office have laptops owned by GIAC that they use when traveling. Files are exchanged on floppy disks and/or CD-RWs with the laptops. The GIAC-owned laptops do have Ethernet jacks, but are rarely, if ever, connected into the office network. When board members or committee members

(all of whom are offsite) need a file for GIAC business, the system administrator or GIAC's executive director typically send it to them by email attachment.

GIAC's system administrator tries to keep all hosts, both in the trusted network and the DMZ, updated with the latest patches from vendors, although no specific procedures exist to support this goal. All desktop systems used by employees have Windows auto-update enabled, and employees generally know to accept the patches offered by this procedure. Nonetheless, considering that GIAC's system administrator is only on 80% of full time, patches are not always applied expeditiously to the publicly visible servers. Thus for certain server applications, such as IIS, the installation of newly available patches may be delayed for a matter of a few weeks following their release. Additionally, GIAC has no formal record keeping system for maintaining a history of which patches have been applied. Likewise, GIAC does not employ any kind of image-based backup procedure that could be used to quickly restore a production system to its most recent known-good state.

GIAC's Business Operations

GIAC's three streams of revenue come from membership dues, the annual conference, and online bookstore sales. Among these three sources of revenue, membership dues and the annual conference contribute about equally and together provide more than 85% of operating revenues. In the past year, GIAC has made dues renewal and other aspects of membership management available online through ASP/SQL applications custom authored by the system administrator. Likewise, most aspects of preparing for and registering for the annual meeting are also available through web-based interfaces as of this year.

Both membership functions and annual conference functions center upon a master membership database. When individuals first join GIAC as members, they provide a professional profile that includes their educational background, skills areas, work experience, and employer information. The membership database also codes the type of membership (about a dozen categories exist), the dues level, and a variety of datestamps that record significant changes to the membership profile (e.g., when a member earns an advanced degree in their specialty area) and payment records (e.g., whether the registration fee for the annual conference has been paid for the current year).

Although in the past members updated their membership database information via mail or telephone, of late almost all updates occur through web-based interfaces. The typical workflow occurs as follows. A once-a-month batch query of the membership database identifies members whose dues payments are overdue or due in the present month. The query returns email addresses of those members and a mailer script sends email reminder messages to each member who needs to pay their dues. The automated email broadcast message contains a URL for the web-based dues paying interface. The same script also produces reminder postcards that are routinely sent to members who do not have email addresses. All members also routinely receive two such postcards

per year (once with a first reminder for dues payment, and the other with a first reminder for conference payment).

When members receive the email reminder message and follow the link to specified URL, they receive a prompt to enter their username and a five digit PIN. Usernames are unique. If a member enters an unknown username, he or she is prompted to telephone GIAC's administrative office. If the member enters the wrong pin, he or she receives a brief ASCII hint message. The hint was authored by the member during enrollment and stored in the membership database as clear text during an earlier transaction. If the member enters the wrong PIN a second time, he or she can click an option to have the PIN emailed to the current email address on file in the membership database. An ASP script queries the database and extracts the PIN, which is mailed in the clear along with the username.

Following a successful login, the member receives an SSL connection to access the dues payment interface. The member enters a credit card number and submits payment. These credit card transactions are logged for later batch processing: Real time verification of the transaction does not occur. Following completion of the payment process, the member has the opportunity to update their membership profile, including educational background, skills areas, work experience, and employer information. It is important to note that these changes are recorded in the form of updates on a shadow copy of the database that appears on the web server. The "real" database is hosted on the file server in the trusted area of the network. The database updates are applied to the real database in a batch once a week through a series of SQL queries. The updated database is then immediately uploaded from the trusted file server to the web server and the queue of pending updates is flushed. Similarly, the credit card transactions, which are maintained on the web server in a separate database file from the membership database, are downloaded to the trusted file server and processed (to the credit card processor) in a batch once a week, at which time the queue of recent credit card transactions is flushed from the web server. GIAC's system administrator runs a tape backup of the trusted server once a week and brings the most recent tape home with him. Of final note, credit card information is not stored at any time in a linked fashion with membership data.

The flow of data for conference registration and payment parallels that for dues payment. The web-based interface for choosing among the palette of available conference services (e.g., pre-conference workshops, extra conference activities, etc.) has a somewhat higher degree of complexity than the dues interface, but the underlying flow of data is highly similar. Likewise, purchases at the online bookstore follow the same essential flow, although one need not login as a member in order to make a purchase at the bookstore.

A further note is in order concerning telephone contacts to the office. A GIAC representative answers the main office number during normal business hours, and that representative can make changes to the membership database in response to caller's requests. The representative can also process dues, conference, and bookstore

transactions over the phone. No written policies or procedures exist with respect to handing these calls. More specifically, callers are not subjected to an identity challenge when they call.

As this account makes evident, the “crown jewel” of GIAC is the membership database. All GIAC revenue depends upon a continuing flow of communications and transactions with the membership and any substantial loss of the accuracy, integrity, or availability of this database would adversely affect the overall functioning of the organization. Although loyalty to the organization by its members is high, members need reminders, prompts, and invoices indicating when and how much they should pay in dues and in conference fees. Further, the authentication information in the database provides members with the means to submit proposals for the annual conference as well as conduct other activities related to the development of the conference program. Reconstructing all or part of the membership database following any significant data loss would be a time consuming, expensive, and imperfect process that would inevitably have a detrimental effect on revenue flow and member satisfaction.

GISO - Basic Practical Assignment Version 1.3
Assignment 2 - Identify Risks

Three Most Critical Areas of Risk

Risk Area 1: Catastrophic Loss of Membership Data and Related Operational Files

What the Risk Is. Through any of several loss mechanisms, it appears that the membership data and related operational files (such as general ledger information) are vulnerable to partial or complete loss. Several likely loss mechanisms exist. First, complete loss is possible because the backup tapes are never verified, they are not stored in a secure location, and they are not rotated and retired according to an established schedule. Thus, any reason for failure of the hard disk in the file server at GIAC's office puts the membership database and related files at considerable risk.

Partial losses of data could occur as a result of damage or destruction to files that occurred since the most recent backup. If one assumes that the most recent backup is valid, this would limit losses to only the most recent week, although it is important to note that if the system administrator is out of the office on the last working day of the week (e.g., for vacation, annual conference, etc.) the backup tape is not taken offsite. Thus the loss of updates could cover a longer period than one week. Additionally, it is important to note that because of the cyclical nature of GIAC operations, file losses during critical periods (e.g., the week before the annual conference) could have devastating effects on the organization and its members.

Damage or loss of files could also occur as a result of hacking from the outside, malicious insider activity, physical theft of the file server box from the office, fire or water damage to the server box, or hardware failure of the storage device. Among these risks, the last one is possibly the most likely. About two years ago, a hard drive in the server began to show signs of failure (bad sectors) and was replaced before any critical files were lost. Interestingly, this event did not trigger any changes to standard operating procedures.

Why this Risk is of Particular Concern. GIAC's crown jewel is the membership database; all of GIAC's operations and all of its revenue depend in one way or another on the accuracy, integrity, and availability of the database. Numerous other aspects of GIAC's day-to-day operations depend upon other files (e.g., general ledger, budget, and accounting statements, credit card transaction lists) that are stored on the same server with the membership database.

What Are the Possible Consequences. First, if a set of member profiles were erased or corrupted in the database, those members affected by the missing data might forget to pay their dues or to register for the conference. In the same vein, GIAC would lose track, at least for those missing records, of who had and had not paid their dues and conference registrations. Loyalty to GIAC by members is high, however, so it might eventually be possible to rectify these losses. Perhaps more devastating, however,

would be a scenario in which a malicious third party gained control of some or all of the membership database. Many GIAC members have high levels of personal income and would be desirable marketing targets. The stolen data could be used for a variety of forms of sales pitches, marketing campaigns, scams, or harassment against GIAC members and, if these were widespread, many members might lose trust in GIAC's ability to properly manage their data. Again, loyalty to GIAC is high, so this damage might eventually be rectified, but only at a very substantial cost. In addition to these problems directly related to the membership, the cost in time and effort at reconstructing missing or damaged records could be quite substantial. Perhaps of greatest concern, if losses occurred just prior to the annual conference, this could substantially disrupt administration of the conference, thus affecting revenue flow from conference fees/purchases and possibly adversely impacting contractual relations with the conference hotel and facilities.

Recommended Steps. The top priority is to regularize and formalize the file server backup process as part of an overall disaster recovery plan. GIAC's system administrator should run daily backups of the membership database and related critical files. These backup media should be regularly tested to ascertain that they can properly reload the complete set of restored files onto a production file server. A scheduled rotation process should be developed, such that recent backups are stored at multiple sites, including one secure, fireproof location, and such that older media are retired after a specified period or number of reuses. Each time the operating system on the server is patched, a new image of the full set of system files should be created, so that a new box could be brought online quickly. The executive director should have access to the rotation schedule and at least one of the backup sites, such that a recent backup could be retrieved even in the absence of the system administrator.

Risk Area 2: Compromise of Credit Card Transaction Data

What the Risk Is. Records of current and recent credit card transactions may be at risk of theft as a result of external or internal malicious activity. GIAC processes a relatively low volume of credit card transactions per week, and transaction records are flushed from the database running on the web server in the DMZ once a week. Nonetheless, when one considers that GIAC's web applications were all custom authored and that patches are not always immediately applied to the servers, it is likely that the host that processes credit card transaction is sometimes vulnerable to exploitation.

Of additional concern is the data management of the older records of transactions that reside on the trusted file server. GIAC does not have any policies for how long these are maintained, and the data handling with respect to updates, flushes, backups, and so forth is informal and unscripted. Relatedly, older transaction files are maintained in a location on the internal trusted server that is visible and accessible to all internal network users. As an illustrative example, GIAC had an incident several months ago where a temporary backup list of credit card transactions was uploaded to the public web server by mistake into an Internet-visible location on the server. It is unclear

whether this file was ever accessed from the outside, but several days passed before the mistake was discovered and rectified.

Why this Risk is of Particular Concern. Identity and credit card theft have emerged as major sources of loss for customers, small businesses, and credit card processing companies. Besides the financial loss that GIAC or its members might experience as a result of the theft of credit card numbers, associated identity information, possible charge-backs, and so forth, GIAC's continued ability to process credit card transactions depends upon maintenance of a favorable business relationship with the firm that provides its merchant account. Additionally, if credit card losses became widely known among the members, this could adversely affect GIAC's reputation with respect to its ability to protect member information.

What Are the Possible Consequences. If substantial financial losses occurred as the result of theft of transaction information from GIAC's servers, GIAC might be subject to one or more lawsuits. If the firm the provides GIAC's merchant account lost faith in GIAC's ability to competently manage credit card transactions, the merchant account might be revoked, forcing GIAC to work with another vendor on less favorable terms. If GIAC's reputation for competent handling of financial transactions became tarnished with the membership, this might result in delays or failures to pay dues and conference registration fees. In all of these scenarios, the flow of revenue to GIAC might be substantially interrupted over a considerable period.

Recommended Steps. GIAC should develop policies and procedures that lay out, in detail, a secure strategy for handling credit card transaction data throughout the data life cycle. In developing this policy, GIAC should attempt to emulate published best practices such as the 12 guidelines recently developed by VISA. The procedures developed through this process should be cast into appropriate scripts and other forms of automation to minimize the possibilities for human error throughout the data handling process. Finally, following all of these activities, GIAC should engage a commercial information security company to audit their systems and procedures. This audit should address technical vulnerabilities (e.g., web application level exploits) as well as possibilities for social engineering and human error in data handling of credit card transaction data.

Risk Area 3: Targeted Membership Data Corruption

What the Risk Is. GIAC's web site provides a variety of interactive features meant to serve the membership, the business community, and the press. Almost all of these upon the availability of accurate member profile information in the membership database. For example, members elect new officers, publish profiles of their expertise or the specialization areas of their firms, and organize the annual conference, all by means of web-scripted interactions with the membership database. A determined individual or group could interfere with any of these processes and could modify member profile information through unauthorized use of the website. Unfortunately, the way that authorization and access control are currently designed for these features, an

attacker could quite easily gain access to and modify a member profile (passwords are limited to 8 characters, numbers and letters only; the site automatically provides a password hint, originally authored by the member, and published as clear text in response to the third failure to authenticate; the site does not automatically lock out the account after a certain number of failed attempts; the site will email the member's password as clear text to a stored email address).

Why this Risk is of Particular Concern. Changes introduced in a subtle manner to one or more member profiles would likely go unnoticed for a substantial period of time and might even ripple through all available backups of the membership data. For example, an unauthorized user might modify the contact telephone numbers or email addresses associated with a member's profile such that the member no longer received any referrals from potential customers who used the GIAC website. Interference with processes involved in elections or the conference could cause a substantial amount of confusion or could delay the administration of the elections or conference. For example, an attempt to systematically "stuff the ballot box" might result in the wrong individual being elected to a board position (at least temporarily), or if detected quickly might result in having to rerun the whole election.

What Are the Possible Consequences. The primary consequences would lie in increased administrative costs to rectify any data problems that were detected. The secondary consequences would revolve around the loss of confidence by the members. With respect to administrative costs, GIAC has a very limited technical staff: They would certainly have to work overtime and it is possible that GIAC would have to hire an additional staff member, at least on a temporary basis, to help sort out the problems and clean up the data. Given GIAC's limited operating budget, either of these scenarios would be budget busters.

The erosion of member confidence in case of a very public data integrity failure, such as one of the scenarios described above, would result in losses that are harder to quantify than the staff time. It is likely that some members would react angrily. (True story: Following the recent security problem relating to credit card numbers inadvertently made available on the web by GIAC, one angry member affected by this problem responded to an anonymous feedback survey with a threat against a GIAC staff member). It is possible that other members would cancel their memberships. At a minimum, a substantial number of members would probably reconsider their decisions to make profile information available to GIAC for use in the web-based interfaces.

Recommended Steps. A critical first step lies in bolstering the authentication and access control procedures involved in using and modifying member profiles. Passwords for controlling member profiles through the web should be hashed rather than stored as clear text, the hint system should be disabled, a member account should be locked after a fixed number of failures (e.g., 3 or 4 failed tries), members should have to respond to a challenge question before a password reset request is honored, and members should have only a limited amount of time to change a reset password to a new value.

In addition, a greater degree of discipline should be imposed on the process of updating the (offline) stored membership database with updates obtained through web interfaces. All changes to a member profile should result in a diagnostic email message being sent to the member alerting them that their profile has changed and providing options for overriding the changes. Changes to critical elements of contact information should require an active confirmation by the member, either through email or by telephone.

Perhaps most importantly, the technical staff and GIAC management should agree on a basic policy or approach to authentication and access control with respect to member profiles so that all future modifications or additions to the web-based interface can be compared with an ideal or benchmark for the appropriate level of control.

GISO - Basic Practical Assignment Version 1.3
Assignment 3 – Evaluate and Develop Security Policy

The first and perhaps most serious risk identified for GIAC was the disastrous loss of the membership database and/or other critical files related to GIAC's daily operations. As noted in the previous section, GIAC's system administrator does create weekly backup tapes, but these are rarely if ever tested, and no formal plan exists for their management (e.g., there is no designated facility for offsite backup). As a first step in mitigating this vulnerability, a policy needs to be developed defining a range of disaster prevention, mitigation, and recovery activities. Dorey (1991) has commented that such policies provide an important first step in defining security objectives and requirements. To serve as an initial template for such policy, I have adopted excerpts from a university information systems policy (Syracuse University Computing and Media Services, 2003; see Appendix for the text) that describes roles and responsibilities with respect to management of data backups and disaster recovery. In evaluating and modifying the policy, I have considered the SANS guidelines presented for this assignment, as well as discussions of social-organizational controls by Spurling (1995) and Trompeter and Eloff (2001).

Evaluation of the Template Policy

The template policy (as excerpted) describes roles and a set of responsibilities. The roles include that of a cognizant information technology professional from a given organizational unit, a director level individual, and an oversight committee. The responsibilities pertain to the creation and management of backup tapes, as well as the activities pertaining to using those tapes to restore operations following a disastrous data loss. In basic outline, then, these policy elements have general applicability to GIAC's risks and concerns. In the specifics, however, these policy elements do not clearly delineate all of the critical areas that good policy development requires. In addition to the removal of redundant statements and material inapplicable to GIAC, the following areas need further editing and development:

- *A clearer understanding of what the policy addresses*: Although a subtitle in the policy indicates that the policy pertains to disaster recovery, the material could be better organized and subtitled to emphasize that the focus of the policy is on issues related to ensuring that the organization can recover from a disastrous data loss. Additionally, the policy excerpt makes no reference to differences between mission critical data/systems and non-mission critical data/systems. Given the importance of getting basic organizational functions back in order following a disaster, the policy should provide additional details about the nature, amount, and location of mission critical data relevant to disaster recovery.
- *More information on why the policy was established*: Although the general need for backup and disaster recovery is self evident, a good policy should nonetheless include a specific purpose statement. This policy excerpt does not contain a statement of purpose or any explicit justification.

- *Specific language indicating to what or whom the policy applies*: This policy excerpt describes several roles but fails to indicate who in the organization should fulfill each roles. At a minimum, the organizational unit and job title of the appropriate staff member or departmental representative should be mentioned. To the extent that these roles are interlocking (e.g., supervision of one person's activities by another person), this should also be evident from the policy. Additionally, wherever possible, the policy should mention specific systems or types of activities and systems to which the policy applies. Good policies should also contain a clear statement pertaining to the applicable scope of the policy.
- *Specific information concerning who should carry the policy out*: This policy does indicate that the disaster recovery staff member has primary responsibility for a number of tasks but does not specify whether certain of these tasks should or should not be delegated to other individuals in the organization.
- *Indication of what steps should be taken to address the policy*: This policy does specify a number of actions to be undertaken by the disaster recovery agent. On this point the policy is largely satisfactory, although adaptations of these actions should be undertaken when rewriting the policy for application at GIAC.

To elaborate further on this final point, as a small, non-profit organization, GIAC has a particular set of logistical restrictions that arise from its limited staff and infrastructure. The excerpted policy template, on the other hand, was created for generic use by a variety of organizational units in a large university setting. Thus, GIAC has much to gain by adding a higher degree of specificity to the policy statement. These specifics can account for GIAC's uniqueness by focusing on the specific role of GIAC's system administrator and by spelling out the concerns that are peculiar to GIAC's mission and information technology infrastructure.

Although policy statements do not all have to conform to a single template, a common structure for policy statements should beneficially include six distinct subsections: Purpose, Background, Scope, Policy Statement, Responsibility, Action. The excerpted policy does not contain an obvious structure, but rather moves freely from one consideration to another. In so doing, it fails to amply demonstrate sufficient coverage of each of these six areas. Thus, as a final consideration for improving this policy, it would be advisable to adopt a common and recognizable presentation structure for the policy text.

Revision of the Excerpted Security Policy

In the text below, I provide a revision of the disaster recovery policy that addresses the concerns and considerations discussed above. In keeping with the requirements of the assignment, the revised policy contains a number of verbatim excerpts from the original policy (Syracuse University Computing and Media Services, 2003; see Appendix for the text). These verbatim excerpts qualify for the fair use exception under U.S. copyright

law by virtue of their reproduction for non-profit educational purposes; Syracuse University retains copyright for all excerpted material (see appendix). Note that considerable rearranging of the excerpted text has occurred in order to adopt a more common and recognizable policy presentation structure.

1. GIAC Policy: Disaster Prevention and Recovery

1.1 Purpose

The purpose of the present policy is to help prevent, avoid, mitigate, and/or recover from disastrous loss of GIAC's critical information, data, and files. This critical information specifically includes the GIAC membership database and financial records and generally includes any other data necessary for day-to-day operations of the GIAC office.

1.2 Background

GIAC's daily operations depend upon the operation of a set of computer systems and the corresponding availability of a variety of critical files stored on those systems. At two times during the year -- just before the submission deadline for proposals to the annual conference and just before the annual conference itself -- the availability of these critical files takes on special significance because of the time sensitive nature of these activities. At these times, but also throughout the year, successful operations depend upon GIAC's membership database, accounting and ledger information, a reference copy of the currently operational website, credit card transaction records, and a variety of related files existing on host systems in the GIAC office. The purpose of this policy is to ensure that none of a variety of potential loss mechanisms disrupt GIAC operations, through corruption or loss of these data, for more than 24 hours during one of the critical times of year or more than 72 hours at any time of year.

1.3 Scope

The present policy applies to formally designated work activities of GIAC's primary information systems administrator with respect to disaster prevention and recovery. The present policy also applies to the oversight roles of GIAC's director and volunteer executive committee (president, secretary, and treasurer of the corporation) in ensuring compliance with this policy and its associated procedures.

1.4 Policy Statement

The formally designated work activities of GIAC's primary systems administrator shall include the daily and weekly management of backup procedures and media, as well as the development and maintenance of appropriate operational restoration procedures. The systems administrator shall make periodic reports to the executive director describing the status of the current disaster recovery plan.

The oversight roles of GIAC's director shall include regular compliance crosschecks as well as suitable periodic training to ensure that the executive director could perform restoration procedures in the system administrator's absence. The executive director shall take whatever corrective steps are necessary to internal staffing and procedures to ensure continued and appropriate disaster recovery capabilities.

The oversight role of GIAC's volunteer executive committee shall include obtaining periodic disaster preparedness reports from the director. The committee shall recommend to the director any necessary changes to current policy, procedures, or staffing to ensure an appropriate level of disaster preparedness.

1.5 Responsibility

GIAC's system administrator has day-to-day operational responsibility for disaster recovery on all computer hardware, software, or any other media used to process or store GIAC's data. The system administrator has responsibility for:

- Taking appropriate measures to guard against unauthorized modification, destruction, or disclosure of data, whether accidental or intentional.
- Establishing such standards, procedures, and guidelines as may be necessary to ensure data security and to provide controlled access to confidential, privileged, or otherwise sensitive data.
- Implementing frequent backup and secure off-site storage procedures to preserve vital data along with the software and programs which process that data in the event of destruction or a disaster.
- Ensuring the viability of backup media and restoration procedures through use of multiple media types and periodic verification of restoration procedures.
- Reprocessing all data between the time of the disaster and the time that the most recent disaster backup media were created.
- Developing and maintaining a contingency plan for continuing essential operations for a period of up to several days by means of restoration of backed-up data onto GIAC's own information systems or suitable alternatives (including a temporary emergency offsite operations center).

GIAC's executive director has responsibility for:

- Developing and maintaining GIAC's policies with respect to disaster recovery and related issues.
- Regularly crosschecking the efforts of the system administrator to ensure that GIAC policies are followed.
- Obtaining periodic training and information from the systems administrator to ensure that the executive director could access and utilize backup media and restoration procedures in the event that the systems administrator became unavailable.

GIAC's executive committee has responsibility for:

- Reviewing and approving changes to GIAC disaster recovery policies. These processes shall include the responsibility for triggering a biennial analysis and/or audit of all disaster recovery policies and procedures by the director and systems administrator.

- Receiving and reviewing an annual report from the director on GIAC's compliance with current disaster recovery policies and procedures, including a performance review of the system administrator in this area.
- Recommending, reviewing, approving, and funding policy, procedure, or staff changes to the director as necessary to ensure satisfactory compliance with GIAC disaster recovery policies.

1.5 Action

This draft policy becomes effective September 1, 2003. By October 1, 2003 the system administrator should provide the executive director with a written set of operational procedures reflecting the policies described above. By November 1, 2003, the system administrator should demonstrate a simulated recovery from a disastrous loss of the GIAC file server. By December 1, 2003, the director should report to the executive committee with respect to the operational disaster recovery procedures and their success and speed at recovering from a disastrous data loss. By December 31, 2003 the executive committee should recommend any changes to this draft policy. On January 1, 2004, the revised policy will become effective and the regular timetable for annual and biennial reporting and policy review will begin.

GISO - Basic Practical Assignment Version 1.3 – Assignment 4
Develop Security Procedures

The following procedure pertains to the third bullet under the system administrator's responsibilities in the revised policy described in the previous assignment (entitled "Implementing backup and secure off-site storage procedures to preserve vital data along with the software and programs which process that data in the event of destruction or a disaster."). In drafting this procedure, I have tried to remain cognizant of the issue of "buy-in" by the staff member who must fulfill these responsibilities (Ady, 2001): The system administrator, who works only 80% of full time, must incorporate these procedures into an already full schedule. Thus, this procedure attempts to follow the normal rhythm of business operations at GIAC in order to avoid overloading the system administrator with additional, time-consuming responsibilities.

1. GIAC Procedure: Backup Rotation and Secure Off-Site Storage of Backup Media

1.1 Justification

This procedure partially fulfills responsibilities designated under GIAC Policy 1, entitled, "Disaster Prevention and Recovery." The purpose of this procedure is to support this policy's aim to help prevent, avoid, mitigate, and/or recover from disastrous loss of GIAC's critical information, data, and files. This procedure supports these aims by describing the order of use and storage for backup media, as well as related steps for verification and media retirement.

1.2 Personnel

This procedure should normally be conducted by GIAC's primary systems administrator, but may also be carried out by other GIAC personnel in the event that the systems administrator is unavailable.

1.3 Schedule

This procedure includes elements that should be conducted daily, weekly, monthly, quarterly, and annually. This procedure includes elements that are conducted at the GIAC office and at the offsite storage vendor's location.

1.4 Verification

This procedure includes steps for periodic testing of backup media and the success of restoration procedures. See step 1.5.5.

1.5 Procedures

Introductory notes: These procedures assume that a storage vendor has been contracted to provide secure and environmentally controlled space for backup media.

The procedures also assume that the file server contains a functional tape backup unit as well as a DVD-R compatible drive. The system administrator's desktop must also contain an identical model of tape drive, a combo drive capable of reading DVDs, and a second hard drive with equal or greater capacity to the server. The systems administrator should possess one key to the storage space and the director should possess the other. The core rotation procedures described below were adapted from the Grandfather-Father-Son tape rotation schedule described in the best practices section of the Seagate website (http://www.seagate.com/products/tapesales/backup/A2g1.html).

1.5.1 Label 9 tapes (note that, at this writing, only one tape is required per set). Four of these tapes should be labeled Monday, Tuesday, Wednesday, and Friday. The remaining five of these tapes should be labeled with Week 1 through Week 5. Also label a set of 12 DVD-R disks with the names of the months.

1.5.2 On Monday through Wednesday and Friday of each week at the close of the business day, run an incremental backup of all files on the file server that have changed since the previous day. If possible, write a script to perform this function, use the operating system's scheduling capability to run this script at the appropriate time, and set a calendar reminder on your own PDA or personal computer to replace the media each morning. Store incremental tapes onsite in a cool, dry, and shaded location.

1.5.3 On Thursday of each week, starting with the first Thursday of each month, run a full backup of the file server system at the close of the business day. Begin by using the tape labeled Week 1 and use the subsequently numbered weekly tapes on succeeding weeks. As above, if possible, write a script to perform this function, use the operating system's scheduling capability to run this script at the appropriate time. On Friday morning, remove the weekly tape and drive it to the storage facility. Drop off the weekly tape that was written on the previous evening and pick up the weekly tape that will be needed for the following week (this will usually be the least recently used tape, but in months with only four Thursdays, the tape labeled "Weekly 5" will not get used.

1.5.4 On the last business day of each month, select the DVD-R disk labeled with that month. Run a full backup of the file server onto the DVD-R disk. Give the disk to the director for storage in GIAC's safe deposit box at the bank. There is room for up to six disks in the safe deposit box. The director will periodically give you older disks for permanent storage at the storage facility.

1.5.5 One the last day of each third month, the bookkeeper will close the books for the most recent quarter. On that day, following the creation of the monthly DVD-R disk (as specified in 1.5.4), verify the performance of the daily incremental tapes, at least one of the weekly tapes, and the most recently created DVD-R disk. Using the second hard disk in the system administrator's desktop as a target device, restore a weekly tape and a set

of incremental daily tapes. Enable full error logging on the user interface for the tape backup program to assess the level of dropouts and error correction on each tape. Take note of any reported media failures and retire the failed media. Use a file compare program to compare the contents of the hard drive (as restored from tape) with the contents of the DVD-R disk. Finally, use a file compare program to compare the contents of the hard drive to the contents of the file server. Ignoring any minor discrepancies (e.g., in temporary operating system files), follow-up on any restoration problems.

1.5.6 In the first full business week of each year, label a new set of DVD-R disks (as specified in 1.5.1) and use the following steps to retire the more heavily used tape media. First, retire the daily tapes (optimally these should be destroyed rather than discarded for security reasons). Next, re-label Weekly 1 through Weekly 4 as Monday, Tuesday, Wednesday, Friday. Re-label Weekly 5 as Weekly 1. Finally, label a new set of tapes as Weekly 2 through Weekly 5.

Cited References

Ady, W. E. (2001, August). *Secure this: Organizational buy-in (a communications approach)*. SANS Institute Information Security Reading Room. Available at: http://rr.sans.org/aware/buy-in.php.

Cole, E., Newfield, M., Millican, J. M., Northcutt, S. (2002). *SANS GIAC Certification: Security Essentials Toolkit (GSEC)*. Indianapolis, IN: Que Publishing.

Dorey, P. (1991). Security Management and Policy. In W. Caelli, D. Longley, & M. Shain (Eds.), *Information Security Handbook* (pp. 27-74). New York: Macmillan.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security, 3* (2), 20-26.

Syracuse University Computing and Media Services (2003). Untitled computer policy document. Author. Available at http://sumweb.syr.edu/ir/apm/acadaffr/CMPMDA.HTM.

Trompeter, C. M., & Eloff, J. H. P. (2001) A Framework for the Implementation of Socio-ethical Controls in Information Security. *Computers & Security, 20*, 384-391.

Appendix: Template Disaster Recovery Policy (Fair use excerpts from the policy statements of Syracuse University's Computing and Media Services department)

Complete, original text available at:
http://sumweb.syr.edu/ir/apm/acadaffr/CMPMDA.HTM

(Note that this policy has been copy-edited to remove specific references to individuals, departments, and facilities.)

Disaster Recovery Responsibilities.

<staff member> is responsible for the creation and off-site storage of copies of all application system programs and data files necessary to resume system operation in the event of a disaster which destroys the administrative computer facility at <facility>. <Organization> has in place a disaster recovery plan in which administrative systems operation would be resumed at an off-site location within several days of the time of the disaster. If there is a disaster, the <staff members> for the various administrative systems supported by <organization> are responsible for:

Reprocessing all data between the time of the disaster and the time that the most recent disaster backup tapes were created (up to five work days).

Having in place a contingency plan for continuing essential operations for a period of up to several days, during which time all administrative computer system processing would be suspended.

The <staff member> is responsible for:

Taking appropriate measures with respect to the processing of data to guard against unauthorized modification, destruction, or disclosure of data, whether accidental or intentional.

Adhering to all specified protection and control criteria for data processed by its computer facilities.

Establishing such standards, procedures, and guidelines as may be necessary to insure data security and to provide controlled access to confidential, privileged, or otherwise sensitive data.

Implementing backup and secure off-site storage procedures to preserve vital data along with the software and programs which process that data in the event of destruction or a disaster.

Following reasonable standards with respect to the selection, design, testing, and documentation of hardware, software, and computer programs to ensure proper use and accuracy of processing results.

<Director's Role>

The <director> is responsible for supporting the operation and information needs of the <organization>. This data may reside either in centralized facilities maintained by <organization> or on distributed facilities. In both cases the data is owned by the <organization> and in the custody of the unit responsible for maintaining the data.

<Director> is responsible for specific procedures governing access to and the use of <organization> data, whether it is stored locally or in centralized computing facilities. Additional guidelines governing access to widely-used data may be found elsewhere in this manual. In all cases, the <director> is responsible for:

Establishing collection, maintenance, access, distribution, and utilization criteria for the data.

Defining the criteria for archiving or destroying the data to satisfy retention requirements.

Determining the value of the computer data to the functioning of the organization and defining reasonable requirements for protecting the data asset.

Developing a workable plan for resuming operations in the event a disaster destroys all computer data except those which have been stored off-site.

Specifying data control and protection requirements to be adhered to. This includes determining the data classification for data within their area of responsibility.

<Committee's Role>

The <committee> is composed of representatives from the major data custodial areas. Additional representatives from other areas of the <organization> attend meetings as the need dictates. This group provides a forum for discussion of data-related issues and reports its recommendations and findings.

The <Committee> is responsible for:

Providing general standards and guidelines on creation, maintenance, use, retention, and disposition of data.

Making recommendations for policies and guidelines on the creation and maintenance of <organization> data.