Global Information Assurance Certification Paper

GIAC Insurance
And
Internal Service Providers.

GIAC ISO Certification Basic Practical Assignment - Version 1.3

Graham Moore June 2003

Business Security Officer GIAC Insurance.

Table of Contents

Table of Contents-

Assignment 1

Abstract

This paper is for the GIAC ISO Certification program.

The organisation environment in which GIAC Insurance operates is real.

The GIAC group is a result of extensive merger and acquisitions during the late 1990's. The biggest challenge to the security officer in GIAC Insurance is the provision of network and infrastructure services by the sister company GIAC Networks. This sister company has its own security staff and follows the same group principals.

Investigating the sister companies security has proved invaluable for GIAC Insurance and has confirmed many suspicions.

If you're a security officer you are responsible for the information in your company and internal organisations providing services to your company need to be scrutinized just as much as external providers.

Description of GIAC Enterprises

GIAC Insurance is a general insurance company in the United Kingdom. The company is a subsidiary company of GIAC UK. GIAC UK is the UK holding company for GIAC Insurance, GIAC health and GIAC life. The other two companies being the responsible for the healthcare and life insurance products in the UK.

GIAC is a global financial services company with business operations spanning the globe. The GIAC Group head office is in Madrid, Spain.

The GIAC Group own a technology company called GIAC Networks. GIAC Networks are the preferred supplier of all network and infrastructure services to the GIAC group.

In the UK GIAC Insurance and the other UK companies use the network and infrastructure provided and managed by GIAC Networks UK.

GIAC Insurance's main products are, motor, household, travel and pet insurance.

GIAC Insurance is also heavily involved in developing niche market products with insurance intermediaries.

The company employs 4750 employees in 3 locations in the UK and 1 location in India.

Manchester (1000 staff) IT, Finance and HR
Bristol = (1000) Claims, Marketing, Management Functions

Birmingham = (2500) Broker Support, Renewals, Underwriting - Call Centres
Bombay (India) = (250) Contract Maintenance (Technically Independent Subsidiary Company)

Birmingham is also the location of GIAC Networks UK.

IT Infrastructure

Network Description
GIAC Insurance uses the GIAC UK network provided by GIAC Networks UK. GIAC Networks UK reports to GIAC Networks Group and is the network and infrastructure provider for all companies in the GIAC Group Worldwide.
The global organisational structure has effectively outsourced the network, infrastructure and management from GIAC Insurance. Other users of the GIAC UK network are GIAC Life and GIAC health being the other two operating companies in the UK.

The network for GIAC Insurance is split into 4 zones,
1)Untrusted zone
This comprises of External ISP router (CISCO 3620) and the External GIAC router. (CISCO 3620).
2) The DMZ and Firewall zones.
The firewall is a Nokia IP 440 Checkpoint FW1.
The Firewall will perform Network Address Translation (NAT) to external IP address range. It is GIAC Network UK policy to only use 10.* IP address convention for internal machines.
There are four DMZ's off the firewall. The Hubs are all HP 10mb.
DMZ1 The Domain Name Server and the Mail sweeper server. All email entering and leaving the company is sent via the mail sweeper server. These are Win NT machines running sp6a and are patched regularly as required.
DMZ2 The companies Iplanet web server hosted on a Sun E250 server running Solaris 8. This DMZ is the entry point for all ecommerce sales traffic. The external ports are 80 and 443. The administration server is on port 14555 and is only available to internal IP traffics (ie 10.* address)
DMZ3 The ecommerce application server (in house design) and the database server (Oracle 8i). These are running on Sun E250 servers running Solaris 8. The firewall rules for DMZ3 will only allow traffic with internal IP address (10.*) The application on the Web server (Java Servlet) passes data to the application server. No external IP address need direct access to DMZ3.
DMZ4 is the India VPN using Nokia IP330 Checkpoint FW1and 3DES encryption.

3)Trusted Zone
The internal trusted zone is connected to the firewall by a fast Ethernet switch (CISCO 2524). The Master proxy, Mail Server(Netscape mail on Sun e250) and Firewall management (Sun Netra)are connected to the switch. The switch connects to the GIAC UK Private Managed WAN.

4) Private Managed WAN / LANS

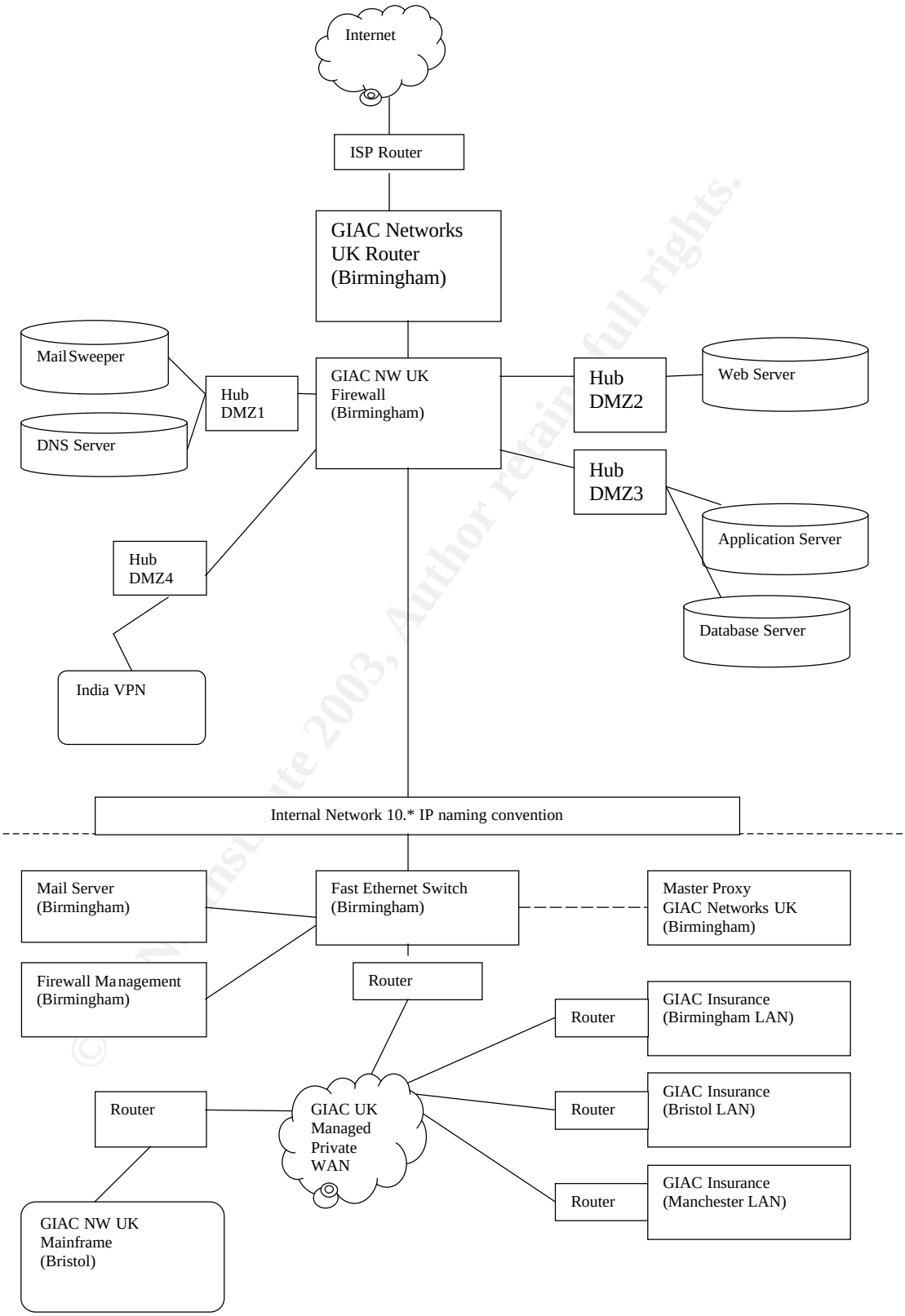
The private managed wan is where each of the local area networks connect to the GIAC UK WAN

For GIAC Insurance this is where the Birmingham, Bristol and Manchester LANs connect and for the GIAC Insurance network and provides access to the GIAC Networks UK mainframe.

The other operating companies in the UK (Life and Healthcare) share the resources in the ecommerce area and also use the Managed WAN.

Data Backup

Business data is backed up on a daily basis on all platforms. GIAC Insurance normally operates with one weeks worth of backups and these are copied to a separate storage facility in Spain.



Desktop
Desktops are Dell GX260 PC's with Windows NT 4 Service Pack 6a.
All software is distributed via SMS. (Unrecognised software is logged and deleted).
All desktops have McAfree Antivirus as standard. Virus signatures are updated on login.

Business users do have access to admin functions and no network programs are available.
The business users profile does not allow access to the floppy or CD Rom drive and the network drives are preconfigured cannot be changed by the user. A standard "plus" version is available where CDRom access is permitted. Business users also have a restricted view of the C drive.

The majority of business users fit the desktop profiles that are available. Non-standard builds are available but requests must be presented with genuine business requirements.

Laptops
Laptops are Dell Latitude machines.
Laptops have a similar set of profiles as desktops with the addition of Safeboot
Safeboot is used to provide an extra layer of protection to the data stored on the laptop.

Hardening procedures.

All machines in the DMZ's undergo a process of hardening during first installation only.
Scripts fro NT and Unix are applied by GISC Networks UK staff.

Primary Business Operations

Every Business unit requires its staff to have
a) LAN ID and Password.
b) Email address, id and password.
c) Mainframe id and password.

Logical Access restrictions are described in each section.

Physical Security
Entry to all GIAC Buildings is by way of a swipe card with a photo ID. All visitors are signed in and allocated temporary passes. All sites must be inspected by local law enforcement crime prevention team and recommendations should be implemented.

IT Applications
Mainframe (OS390)

All mainframe applications in GIAC Insurance are developed in house and are standardised on
COBOL, CICS, DB2.

LAN/Desktop (NT4 sp6a)
All bespoke applications are developed in house and are standardised on
MS Office /VBA or Visual Basic with MS Access or Microsoft Sqlserver 7.

Ecommerce (Sun Solaris 8)
All bespoke ecommerce applications are developed in house and are standardised on
HTML, XML, XSL, Javascript, Java Servlets and Oracle 8i

Underwriting
The underwriters determine the rates at which GIAC Insurance will do business for each contract type. They rely on bespoke mainframe applications to provide them with the management information they need.

Data is extracted from the sales channels and the claims system daily and fed into the underwriting mainframe application in order to produce the information required for the underwriting function.

Access Control :NT Access Groups for underwriting have been created.
ACF2 Access controls are used to restrict access to the mainframe underwriting.
Underwriting applications also run under their own CICS Region.

Sales
The sales channels will capture a customers personal, financial and contract information. The information must be collected in accordance with the UK Data Protection Act.

a) Direct (Telephone sales).

Telephone calls are routed to the GIAC Birmingham call centre.
In order to process a quote or take on new business staff must follow a prepared script in order to capture the customer information. The script is to ensure that the legal information relating to data protection is given to the caller and to ensure that all the appropriate data is captured.

Customer information is keyed on to the sales mainframe application.
Underwriting information is extracted by an overnight batch program (Cobol/db2) and added to the underwriting database.

b) Internet Sales

Internet sales are hosted on GIAC Networks Infrastructure in Birmingham.
Customers key in the appropriate information in via the website to obtain a quote. The screen flow includes data protection information and the customer

must undertake a positive action to confirm that understand the data protection information that is presented to them.
Once a quote is accepted the data is passed to the mainframe via a Java program running data through a mainframe CICS socket connection into a bespoke Cobol application that validates the format and integrity of all the fields before storing the data in a DB2 table.

The Cobol program acknowledges the data transfer and the status of the transfer. The Cobol program cannot be used to retrieve information from the mainframe tables. The Cobol program is schedules to run at set periods of the day and cics will only except connects from a specified internal 10.* IP Address and is on a specific port. All other data extracts are taken from the mainframe tables.

c) Broker (Intermediary)

Brokers capture customer information and using rates provide by GIAC insurance and other insurers calculate a price for an insurance contract. When a Broker sells a GIAC Insurance contract the details are emailed to the GIAC Insurance broker support team in Birmingham.

Brokers have a legal requirement to capture information in accordance with the UK data protection act.

Brokers email the contact sales to the Broker support team. The information is typically in Excel and the spreadsheet is password protected for its transmission across the Internet. The password is 20 characters long and is applied and unapplied by visual basic applications in the Broker and GIAC Insurance offices. One in the GIAC office screen scrapping is used to play the data into the mainframe sales application. This has the benefit of ensuring the data is validated by the application rather than inserting the data straight into the DB2 Tables without validity checks.

d) Bespoke Broker Contract Sales.
Brokers capture customer information and use rates provide by GIAC insurance.
The broker takes responsibility for the policy maintenance and documentation using the brokers own business partners. The broker responsible for the contract provides monthly management information and quarterly financial settlements.

These bespoke broker contracts are effectively outsource agreements and are working with a wide range of business data. MS Office applications are used to manage the information and email is used to exchange the information.

Access Control : NT Access Groups for sales have been created. These are not split between sales channels. ACF2 Access controls are used to restrict access to the mainframe sales applications. Mainframe Sales applications also run under their own CICS Region.

The business relationship with the brokers is critical to the success of GIAC Insurance. There are over 600 brokers who are regarded as the companies primary agents and 1000 additional brokers whose business is important to GIAC Insurance.

Contract Maintenance.
The day-to-day contract maintenance is performed by the India Office in Bombay.
The India office is connected to the GIAC Insurance network via a VPN and work is scheduled via the LAN and the contracts management system on the mainframe. Additional bulk administration projects are often allocated to the India Office and paper based information is sent overnight via trusted carriers.

Some contract maintenance is performed by the Birmingham Renewals Team . This is usually processing that cannot afford the 24 hour delay in delivery to India.

Access Control :NT Access Groups for contract maintenance have been created. The access groups have been on a geographical basis and allows India to have its own set of NT groups.
ACF2 Access controls are used to restrict access to the mainframe contract maintenance and again the ACF2 rules have been split to allow India to have a separate set of rules.

Mainframe Contract Maintenance applications run under their own CICS Region. India operates on a separate CICS region to that of the UK users.

Broker support
The broker support team are located in the Birmingham Office. The team is to ensure brokers receive current information from the underwriters and the marketing team. The broker support team also work closely with brokers when developing new bespoke broker contracts. This team is also responsible for ensuring that the brokers partners are assessed from a security point of view before GIAS insurance approves the new bespoke contract.

Access Control: NT Access Groups for broker support have been created. Broker Support do not have mainframe access. The Broker support team use MS Office based Applications in their areas of the LAN. Email is a business critical application and is the most cost effective way of communication with the brokers.

Renewals
Renewals are largely an automated process but clerical support for the process is covered by the renewals team in the Birmingham office.

Access Control:NT Access Groups for renewals have been created.
ACF2 Access controls are used to restrict access to the mainframe renewals applications.
Mainframe Renewals applications also run under their own CICS Region.

Claims
The claims function is located in the Bristol Office. Customers either telephone, email or write in to request claim forms. The claims teams responsibility is to gather the claim information and to coordinate the support activities that are required when processing a claim. The claims team is responsible for passing information through to finance to pay the claim via the mainframe application.

Notification of claims are entered on to the mainframe claims system. MS office is used to produce customer correspondence.

Access Control :NT Access Groups for claims have been created.
ACF2 Access controls are used to restrict access to the mainframe renewals applications.
Mainframe Renewals applications also run under their own CICS Region.

Email is a business critical application and is the most cost effective way of communication with the external business partners supporting the claims process.

Finance
The Finance team are located in the Manchester Office. Finance is responsible for ensuring all receipts and payments are processed by the mainframe accounting system. The finance team also handle all credit control and commission payments. The finance team need to share information with the claims, sales and broker support teams. Financial management information is also produced for the management team and for the industry regulatory authorities to ensure correct accounting practices are being observed.

Information is passed to the finance applications from the sales and claims mainframe applications. Customers information relating bank accounts and credit control is processed by the credit control team in finance. Customer correspondence is retained in the customers file. The customers file and all electronic records are retained for 7 years. After 7 years all information is destroyed. The exception to this are customers who have been involved with a claim. These are retained indefinitely as further legal action would require the information.

Access Control: NT Access Groups for finance have been created.
ACF2 Access controls are used to restrict access to the mainframe accounts applications.
Mainframe Finance applications run under their own CICS Region.

Remote Access
Remote access is via the GIAC Networks RSA Secure ID RAS server and is limited to IT support and senior management. (Not included in the GIAC Insurance Infrastructure Diagram).

Crown Jewels
The commerce production environment is a crown jewel of GIAC Insurance.

This is the public face of GIAC Insurance and is a measure of the integrity of GIAC Insurance. If this public face is not available or proven to be insecure then it will reduce the confidence of anyone interacting with GIAC insurance.

Lack of confidence in GIAC insurance would have a very serious impact. Also the impact of any problem is not limited to the UK. There is a very real threat to the Global Brand of the GIAC group.
It is the policy of the GIAC Group that a single GIAC brand will be used worldwide.

Damage to the global brand will have serious consequences.

There are numerous threats that come from the Internet and it should be regarded as a hostile environment.

Assignment 2 - Risk Assessments

The 3 main risks in GIAC Insurance are;

1) E Commerce Production environment.
2) The GIAC email system
3) Security assessment of partner organisations.

Why not the backoffice ?

The GIAC backoffice is mainframe technology. GASC Insurance have not exposed this mainframe to the internet and the backoffice processes are well established.
Some process are those that were introduced in the late 1970's. As a result processes have had time to mature and have been repeatedly been subject to audits and security assessments.

1) eCommerce Production Environment.

   The ecommerce production environment has been selected for a risk assessment because it is regarded as being part of the "Crown Jewels" of GIAC Insurance. The ecommerce environment is open to the public and the availability and integrity of the environment sends a public message to customers, partners and industry regulators on the well being of the company.

Threats
The Internet is a hostile environment and the firewall log provides daily evidence of the threats from outside the company. Most of the threats are from the general attacks that many companies face.

Occasionally more determined hacks have been attempted and these pose a real threat to the production infrastructure. In these circumstances the hacker is usually running scripts designed to exploit know vulnerabilities.

Network aware viruses are increasing in complexity and these operate on a 24 * 7 basis looking for vulnerabilities.

Although in a DMZ a misconfigured or breached firewall could allow access to the company LAN.

Modern news reporting is a serious threat to global companies. Small local incidents can be escalated and misreported and can leave the reputation of a global brand in tatters.

Regulator bodies can impose considerable fines on companies who do not protect customers information.

Vulnerabilities:
The existing ecommerce production infrastructure is quiet basic and has little to offer in terms of fail over capability and is dependent on a single firewall.

The ecommerce production environment is a shared environment for all GIAC companies operating in the UK Group. There is scope for error in communications as four companies are sharing resources. Cross company change management procedures are not in place.

Vulnerability scanners are in place but no procedures or resource has been formally allocated to deal with the information from these reports.

No formal approach to the security of router4s or switches.

Some Host Based IDS is in place but no procedures or resources have been allocated.

No formal application monitoring is in place.

No penetration test has been performed on the environment.

Applications are not tested for security weaknesses.

Senior security management at GIAC Networks have changed without a complete handover.

GIAC Networks previous security programme stalled.

Although in a DMZ a misconfigured or breached firewall could allow access to the company LAN.

Incident response procedures are not formalised or tested.

Audit trails / Server logs / Application logs are not formally reviewed.

Business Vulnerabilities:
The GIAC Group has a policy that all regional operating companies will be recognised by the global brand. When companies are global brands an incident in other parts of the world can have an impact on all other areas.

In short , Global Brand = Global Impact

Business Communications managers may not familiar with the Incident response process.

Value of the Asset
Losing the ecommerce environment is a serious loss of a sales channel. A single days outage would be a loss of thousands of pounds but there are other sales channels and it would not cause the company to fail.

Losing the environment for more than a couple of days is a more serious problem and the cost of the adverse publicity is just as important as the loss of sales.

The cost of negative publicity on the business is severe if customers (or partners) private information is lost , stolen or made public.

GIAC Insurance is part of a global brand and negative publicity could have a global impact. Severe negative publicity would require a major investment to relaunch the brand once the original problem is fixed.

Risk:
There is a risk that the loss or breach of the ecommerce environment or information contained in that environment could have a significant impact on the company reputation if the breach becomes public knowledge. In these circumstances a breach would likely to be investigated by the industry regulatory bodies and could result in a significant fine.

Although the ecommerce environment does have some basic protection it does not have a comprehensive level of protection. The likelihood of a breach is probably quiet high (within 12months). The impact of the breach does depend on the press coverage it gets. If public then the financial regulatory bodies will start an investigation and could result in a significant fine for not protecting customer information. Cost of an incident is between £10,000 – £200,000.

Recommendations:
There are a number of recommendations that will improve the overall level of security and improve the ability to monitor and handle incidents.

With the existing good practices these cover the main security activities that are required in an ecommerce environment.

Budget and Resource are always big issues. There are freeware and shareware tools available. GIAC Insurance has a legal and regulatory obligation to take care of its customer information.

These measures should form part of a business case that is aimed at ensuring the company meets its regulatory obligations.

Recommendations - Support Processes

- Log monitoring practices are poor – Formal procedures are needed.
- Incident handling procedures need to be tested and need to include the business communications team.
- Business continuity requirements from the business management need to be formally agreed. Business management must formally accept the risk if no continuity capability is required.

Recommendations - Current Good Practice

- Anti Virus practices are good, procedures should be reviewed in order to keep them effective.
- Hardware hardening is good, procedures should be reviewed in order to keep them effective.
- Patch policies in the ecommerce environment are good - procedures should be reviewed in order to keep them effective.
- Good working practices do need reviewing to keep them as good working practices.
- Network and Infrastructure access controls are monitored daily and reviewed quarterly.

Recommendations - Network and Infrastructure.

- The current architecture and ecommerce DMZ is fairly basic. Fail over capability would be beneficial and an additional firewall should be implemented.
- An additional Firewall should also be installed to segregate the LAN from the Ecommerce environment and the DMZ. The Firewall should be of a different brand to the existing firewall.
- Vulnerability Scans need to be arranged.
- Intrusion Detection (Host and Network) needs to be arranged.
- Network and Application Penetration tests performed by a reputable 3rd party company should be conducted annually.

Recommendations - Application Security

- Training and Awareness of Application security testing needs to be arranged.
- Application logs need to be reviewed on a regular basis.
- Application Access control needs to be monitored.

- Application Audit trails need to be monitored.

GIAC Networks UK is a sister company with the same overall objectives GIAC Insurance should not assume that an internal partner will fulfil their security obligations. Reviewing a companies internal suppliers is just as Important as a companies external suppliers. Going forward there must be control measures introduced.

2)Email Communications

Email has been selected as a primary risk for GIAC Insurance because the company has a complex relationship with many business partners of all sizes. For many of the smaller partners email is the most cost effective means of exchanging business critical information.

Threat
Email is one of the most hostile environments a company has to deal with. Most companies are subjected to a barrage of attacks on a daily basis.

Email is a primary channel for distribution Viruses and Trojans.
A good source of Anti Virus information can be found from most Anti Virus Vendors websites. Sophos have a comprehensive website covering this subject.
See www.sophos.com

Spam is a growing issue with most companies and if not filtered can overload an email system reducing the ability to deliver genuine business related emails in a timely manor. It is often related to xxx rated subject matter, which does offend staff.

Spam Blacklist. If a company is suspected of sending or relaying or sending spam some blacklists add the company to the list automatically. ISP's and other companies receive the updated spam blacklist with your companies name on it and your emails start to bounce.

Large business emails can have a severe impact on the performance of a companies email system.

Snooping email is relatively easy to do. The software is easy to get hold of and could be used to monitor the contents of email traffic.

Vulnerabilities
Server misconfiguration could enable the email servers to be used for email reply, which could be used by spammers and result in the email system being entered on a spam blacklist.

Inappropriate use of the email system by users can expose the company to vulnerabilities ranging from, Spam distribution, Pornography and other offensive emails.

Downtime caused by new viruses – Time delay between discovery and fix being released.

Inadequate business continuity – disaster recovery plans.
Email is one of the most hostile of IT environments at some point something will cause a problem with the system.

Value of the Asset
The email system is a business critical application. Being unable to send business data for processing by partners means the core business functions of the company have stopped.

There are contractual obligations as to levels of work that must be distributed and received from suppliers. A breach of contract would occur if the email system were not available for more than a day.

An outage of more than 3 days is likely to incur penalties of around £20,000 per day. There is also the cost of dealing with backlogs created by email outages and the lost productivity for GIAC Insurance.
Adding these together and the lost of email for 4000 users is likely to cost the company a minimum of £100,000 per day.

Risk
Losing the email system for short periods during the working day does interrupt the business operations but does not cause a significant loss. These events happen several time a year and can be related to virus updates, emergency maintenance.

Losing the email system for more than one day is a risk to the company and does have serious consequences. Experience in GIAC Insurance has found that it is rare for a single incident to contribute to the failure of the email system. GIAC can expect to have a 2 to 3 day outage once per year with a loss of £100,000 per day in staff productivity

Total loss of the email system is a possibility but unlikely.

Recommendations
There are a number of recommendations that will improve the security and risks facing the email system.

There is no single improvement that will achieve a great benefit to the security of the email system. A more holistic approach and further clarification of acceptable use is required.

Recommendations: Total Loss

- Total loss of the email system should be included in Business continuity and Disaster Recovery plans. Total loss of the email system will probably be related to an event that has caused the total loss of other applications.
- The ability to communicate should not be overlooked or underestimated when planning business continuity plans.

Recommendations: Current Good Practices
All good practices need to be reviewed to ensure that stay good practices.

- Email monitoring practices are good and have dedicated resource.

- All emails entering and leaving the GIAC Insurance email boundary are checked by mimesweeper servers. The mimesweeper servers have been configured to apply a set of business rules to every email.
- Email Policy enforcement is good although it is not clear to the users what the disciplinary procedures are for email policy abuse.
- Operating System and email application Patch policy is good and patches are implemented. Review to ensure it continues.
- AntiVirus processes are good. Ensure these continue.
- Users are forced to change passwords and email passwords meet company password standards.
- User accounts are removed when users leave the company.

Recommendations : Improve support information.

- Positive instructions for what email users should do with spam need to be introduced to the email policy.
- Acceptable Email forwarding needs to be added to the policy
- Limitations on Email size need adding to the policy
- Create an abuse@GIACInsurance.co.uk email account and add it to the legal

Disclaimer on all outgoing emails inviting people to report abuse to the company.

3) Security assessment process of partner organisations.

Before business can commence with a 3rd party GIAC Insurance must ensure that the 3rd party is capable of meeting its security obligations. There are many partner organisations that process GIAC Information and it is critical that the security ability of the partners are audited on a regular basis.
This risk is focused on the process of auditing 3rd parties.

Current Process: A self-assessment questionnaire is issued to the third party organisation. This questionnaire is the initial security risk assessment. The returned questionnaire is reviewed and further information is requested on an ad hoc basis.

Threats

Industry Regulatory bodies may insist on evidence to prove 3rd parties have been reviewed.
Internal / External Auditors may require evidence to prove 3rd parties have been reviewed.
Legal proceedings may require evidence to prove 3rd parties shave been reviewed.

GIAC Insurance could be prosecuted for actions taken by a 3rd party partner who is acting on behalf of GIAC Insurance.

Loss of confidential information provided to GIAC Insurance could result in a breach of security at the third parties.

Vulnerabilities.
Poor security practices at a third party could leave GIAC Insurance liable for the loss, corruption or unauthorised disclosure of the information.

The current risk assessment process is not formally documented.
The current risk assessment is subjective.
Limited ability to compare assessments.

The process and questionnaire does not establish roles and responsibilities regarding security functions in the partner organisation.

The process and questionnaire does not establish roles and responsibilities regarding the partner organisation in GIAC Insurance.

The application security questionnaire is poor and fails to cover distributed computing and multiple platforms. Application Service providers are not catered for in the questionnaire)

No formal declaration as to the accuracy of the information is gathered from the 3rd party performing the assessment.

Value of the Asset.
Without a formal approach to the security evaluation of 3rd parties GIAC insurance will not be able to demonstrate that it had taken reasonable measure to protect the information of its customers. This protection of customers information is a requirement of the industry regulatory body and the UK Data Protection act.

The Industry regulatory has the power to impose significant fines on companies and fines of over £250,000 have been issued in the past.

The value of this process could be regarded as the saving of a fine from the industry body. The existing process does review the risk but fails to produce evidence that would be acceptable by the industry regulator.

Risk
Having no evaluation process is not acceptable, partner organisations often have little or no security experience. The industry regulator would not accept this. It is highly likely that the Industry regulator would impose a fine. The publicity from such an event would be quiet negative for the company.

It is highly likely that the industry regulator would recommend an improvement in the process. Failure to improve the process could be subject to a fine but negative publicity would also be a factor to consider.

Recommendations
Create a central repository to store all documentation for 3rd party security risk assessments.

Request feedback from people who have completed previous questionnaires

Review current questionnaire considering.

a) Current Regulatory body standards
b) Previous Assessments
c) Feedback
d) Known vulnerabilities

Deliverables
a) Repository
b) New Questionnaire's
c) Formal Process Documentation
d) Formal Report Structure
e) Cross reference mechanism for comparing companies.

Internal Service Providers of sister companies are subject to assessments and this formal approach should be considered when dealing with internal partners.

Assignment 3

Policy Evaluation – Email Policy

The current policy subject to review is in Appendix A of Assignment 3.
The revised policy subject to review is in Appendix B of Assignment 3.

The policy is aimed at users of the email system. The email policy is included in the staff handbook and is formally reviewed by the GIDC Insurance security team on an annual basis.

Changes to the staff handbook are reissued every year and followed up with an email to all email users to make them aware of the changes.

Staff are aware that there is a policy that applies to them and the policy itself starts with the words "Electronic mail users".

The policy than proceeds with a paragraph that will leave most "electronic mail users" wondering if they dare continue.

The policy does not address the purpose for its existence and does not inform the user that the email system is a business critical application.

The policy does have strong statements relating to monitoring and information ownership but fails to highlight the issues that the policy is aimed at.

It is a "Do this because we say so" approach. This approach does work but misses a great opportunity to make the user more aware of the real issues of using email.

The consequences of inappropriate use either for the individual or the company are not evident in the policy. If a person is aware of the issues and the consequences they are more likely to adopt a more appropriate orientation.

There are also, genuine business activities that can cause problems for all email users and these issues are not reflected in the policy.

For example;

- Sending large files can have a major impact on the performance of the GIAC email system.
- Setting up auto email forwarding can end with secret information leaving the company without the original senders knowledge.

- Marketing departments running mass email campaigns can result in the company being added to spam blacklists.
- Replying to Spam emails even to request removal from the distribution list often results in more Spam.

On the whole the issues surrounding the legitimate use of email have been overlooked.

The first part of the email policy (7.1) does have good statements that do influence the orientation of email users in GIAC Insurance.

There are 3 main messages in section 7.1

1 – The user must only use their own user id .

It does state that authorisation is needed but it fails to inform the user who that should be.

2 – Email will be monitored, and why.

This bullet point is good but some indication of the consequences would be good to include.

3 – The company does not guarantee the availability or the integrity of the information being sent through the email system.

A worthy point, but on a day to day basis many users fair to appreciate the impact of this statement.

All the other bullet points are supporting points for these three.

Restrictions
The Restrictions section (7.3) is aimed at providing more specific examples of what is not acceptable.

The initial wording is good as the statement is flexible enough to cover the majority of circumstances and is re enforced by the 1st bullet point.

It then goes on to list some examples of what is not accepted.

Throughout the policy there is little reference to the consequences or who is responsible for what actions. Some points state that authorisation is required but do not clarify who is responsible.

There is no reference to who is responsible for the policy or who is responsible for supporting users who need further information about the content of the policy. This is the policies biggest weakness.

The policy has a basic level of information on what actions should “not” be taken but does not give any positive actions that would be beneficial to the organisation.

IE The policy does not provide support for users wanting to report email abuse.

Policy Enforcement
GIAC Insurance monitors email usage on a daily basis. Mail sweeper is installed and checks every incoming and outgoing email.
GIAC allocate 1 hour per day to enable the GIAC Insurance security officer to review the emails referred by mailsweeper.

Users who are in breach of the email policy are sent the appropriate warning messages and in more serious cases are referred to the human resources department who will arrange formal disciplinary procedures.

By actively monitoring the referrals from mailsweeper the GIAS security officer has a feel for what is normal activity and can spot a change in the usage of the email system.

When odd things happen, security can tell.

How successful is the current policy.
Overall the enforcement of the current email policy on a regular basis has resulted in a position where serious abuse of the email system is quite rare.

Statistics are kept on the type of emails that mailsweeper refers and this enables trends to be monitored. These statistics are invaluable when

presenting a business case for any additional security work on the email system.

The mailsweeper rules are confidential to GIAC Insurance but are geared towards monitoring the general risks and threats to the email system.

The security team do not allow managers to directly monitor staff email accounts. Individual email monitoring can only be performed if the manager has other evidence to suggest that the individual is abusing their email account. This is to prevent managers from "fishing" into their staff's email accounts and protects the individuals privacy.

The number of staff under email investigation is frequently zero and rarely exceeds 5 at any one time.

There are 5000 users of the email system. On average 0.5% send inappropriate emails. After one informal warning most (75% of the 0.5%) no longer send inappropriate emails.

Primary Issues
Based on the statistics and a general awareness of the email system the current issues for the GIAC Insurance email system are;

- Incoming Spam
- Email Forwarding from Internal email accounts to users home email accounts.
- Large emails
- Support processes

The current policy does not give much support to these primary issues. The email policy has been rewritten and is aimed at providing the user with more support information that gives them the chance to improve their orientation and to behave how we would want them to.

The revised policy is longer than the original but is considerably more focus on what is expected of the user. The additional clarity is worth the extra length.

Appendix A GIAC Insurance Current Email Policy

The following policy is based upon a policy in the author's organisation and was active as at June 2003.

7 Electronic Mail

Electronic Mail users should be aware that with modern technology the boundaries between internal and external mail are now very blurred, and one should never assume that Electronic Mail will remain within the GIAC Insurance network.

7.1 Electronic Mail

- Use of any electronic mail system is conditional on compliance with all GIAC Insurance Policies and Procedures.

- All messages, information and data sent over the Company's computer and telecommunications networks are the property of GIAC Insurance

- GIAC Insurance reserves the right to access, view and disclose any outgoing and incoming electronic mail messages for the purpose of ensuring that no material that is either illegal or adverse to GIAC Insurance or its clients or staff is being produced or transmitted. All traffic in and out of GIAC Insurance will be subject to monitoring and periodic audit. Users are therefore advised that they have no expectation of privacy for Internet based communications, including electronic mail.

- Electronic mail is subject to "legal discovery". This means that GIAC Insurance could be forced by a court to disclose the contents of electronic mails to a third party – even those e-mails that have been deleted from your system may be electronically recovered.

- The sender must keep copies of business critical or legally sensitive electronic messages for as long as determined by the Retention Period of the document type of that message.

- Unauthorised persons must not access Electronic Mail Accounts. Messages must not be sent from another user's account without valid authorisation and business need.

- GIAC Insurance cannot in general guarantee (with the currently available technology) the integrity, timeliness or availability of information transmitted via electronic mail or other electronic methods. Therefore matters of authentication, non-repudiation and proof of delivery must be agreed between the transmitting and receiving parties for each individual transmission or type of transmission.

- Confidential or Top Secret information must be encrypted in accordance with the current GIAC Insurance encryption standards. Successful delivery of any such document should always be confirmed with the desired recipient.

- To legally protect GIAC Insurance information assets from unwanted disclosure, the following message must be included on all outgoing e-mails of Classified information which have not been authenticated and encrypted:

    - "This e-mail is confidential and intended only for the addressee(s) shown. If you are not an intended recipient, please be advised that any use, dissemination, forwarding or copying of this e-mail is strictly prohibited. The sender does not

accept liability for errors or omissions in the contents arising from transmission. Should you receive this transmission in error, notify the sender immediately. Thank you."

7.3 Restrictions on the use of Electronic Mail facilities

- GIAC Insurance electronic mail must not be used for any use deemed unethical, illegal or unauthorised by GIAC Insurance either now or in the future, including:
    - Excessive or inappropriate private or personal use.
    - Any profit related activity not sanctioned by GIAC Insurance.
    - Knowingly altering or destroying the integrity of any information.
    - The transmission of any GIAC Insurance computer id or password in plain text.
    - Transferring Company credit card numbers via e-mail in readable form.
    - Downloading, transmitting or viewing of pornography or any vulgar, profane, insulting or offensive message.
    - Downloading or using games or entertainment software, on GIAC Insurance owned equipment.
    - Propagating chain mail messages.
    - Electronic harassment of any kind.
    - The defamation of, or allegations about any individual or organisation.
    - Copyright infringement.
    - Unauthorised use of the GIAC Insurance network or gateway.

Appendix B Revised Email Policy GIAC Insurance

Electronic Mail Policy

Issued by GIAC Insurance Security Date July 2003 Version 1.1

Approved by: <name> GIAC Insurance Chief Executive
Approved by: <name> GIAC Insurance Security Manager

The Current version of the Email Policy is available from the GIAC Intranet Intranet. http://giac-insurance/infosec/

Contact Tel: 123 1234 Email: infosec@GIAC-insurance.co.uk

Background
Email is a business critical application and all email users are subject to the objectives of this policy. Users should also be aware of the GIAC Information Security Policy
Copies of the Email Policy and the GIAC Information Security Policy
Are available on the GIAC Insurance Intranet

Access
Attempting to access the email system without an authorised id and password will be subject to the Computer misuse act 1990.

Users must use their allocated id and password to access the email system and will be accountable for all actions taken using their email id.

A user must only access their own email account. Accessing other users email accounts must be authorised by the information security team.

Monitoring
GIAC Insurance reserves the right to access, view and disclose any outgoing and incoming electronic mail messages for the purpose of ensuring that no material that is either illegal or adverse to GIAC Insurance or its clients or staff is being produced or transmitted.

All traffic in and out of GIAC Insurance will be subject to monitoring and periodic audit.

Users are therefore advised that they have no expectation of privacy for Internet based communications, including electronic mail.

All messages, information and data sent over the Company's computer and telecommunications networks are the property of GIAC Insurance

Integrity
GIAC Insurance cannot in general guarantee the integrity, timeliness or availability of information transmitted via electronic mail or other electronic methods.

Authentication, non-repudiation and proof of delivery must be agreed between the transmitting and receiving parties for each individual transmission or type of transmission. Please contact the information security team for advice.

Mass Mailings
Sending emails externally to a large number of recipients (more than 20) is not permitted without the authority of the email administrators and the information security team.

Large mailings even those with good intensions may be reported as spam and could have a significant impact on the company.

Internal Email Forwarding
Where an email account is being forwarded a returned message to the original sender must be enabled. The return message must provide the contact details of the person who the mail is being forwarded to.

External Email Forwarding
Not permitted unless it has been agreed with the information security team.

SPAM – Unsolicited Emails
Any unsolicited email received from an external source that is abusive, obscene, or regarded as junkmail, must be forwarded to

abuse@GIAC-insurance.co.uk

Never reply to these emails.

Virus Warnings – Security Alerts
Any unsolicited email received from an external source that is relating to a Virus Warning or Security Alert must be forwarded to

abuse@GIAC-insurance.co.uk

All Security Alerts or Virus warnings will come from the usual internal communications channel.

Protection
Email offers no protection to the information contained in the email. Your email is equivalent to you sending confidential information in a clear plastic envelope. Anyone or any machine involved in the delivery of your email could - Read the contents - Change the contents - Lose the email completely.

Please see the Company security policy for further information on information protection and the classification of information.

Abuse and Legal Disclaimer
Users should be aware that the following statement would be added automatically to every outbound email.

"This e-mail is confidential and intended only for the addressee(s) shown. If you are not an intended recipient, please be advised that any use, dissemination, forwarding or copying of this e-mail is strictly prohibited. The sender does not accept liability for errors or omissions in the contents arising from transmission. Should you receive this transmission in error, notify the sender immediately.

If this email is abusive or inappropriate please forward the email to abuse@giac-Insurance.co.uk

Note: The message contains an email address to enable other companies to report any email abuse originating from GIAC Insurance.

Size
Large emails take longer to process and do slow the email system.

Business email should be no larger than 20MB. Delivery of larger emails can be arranged. Please contact the security team for advice.

Non business related emails must not be greater than 500kb in size.

Non Business Emails
The email system belongs to GIAC Insurance. All messages are the property of GIAC Insurance.

Occasional personal use is permissible at the discretion of your line manager. All emails are the property of GIAC Insurance and all personal emails are subject to and must abide by this policy.

At no time must the personal use of the email system interfere with the business use of the email system.

Policy Breaches - Disciplinary
Any users sending or receiving emails relating to actual or suspected criminal activity will be reported to the local law enforcement agencies.

Any users sending pornography or other vulgar, insulting or offensive message will be reported to HR for formal disciplinary proceedings.

Any users sending information externally through the email system without appropriate levels of protection will be reported to their line manager. The information security standards detail the protection required. I.E User id's and passwords must never be sent externally without protection.

Any users sending excessive or inappropriate emails will receive a warning from the information security team. Where a user continues to abuse the email policy a second warning will be issued from the security team. All abuse following a second warning will be referred to HR for formal disciplinary procedures.

Examples of inappropriate emails are;

Games, Jokes, Chain Mails, Harassment, Video Clips, Breach of Copyright, Distributing Software.

Any User receiving abusive or inappropriate emails from any source should forward the email to abuse@giac-insurance.co.uk

---

Assignment 4 -

GIAC Insurance

Email Policy Compliance Procedures

Email Forwarding

Objectives:

This procedure is to provide members of the security office with the information required to assess the compliance of the GIAC Insurance email policy relating to the automatic forwarding of email messages.

This procedure will generate a list of email accounts that have an email forwarding addresses.
The current procedure has been tested with Netscape Communicator 4.7 and is intended to be performed by GIAC Insurance Security Offices.
Access to the appropriate directories and software is assumed.

Process Owner: GIAC Insurance Security Office.

Location: A3 Manchester
Contact: A.N. Other – Business Security Manager
Telephone: (Internal) 123 4123
Frequency: Monthly (2nd week of each month)
Version: (1.2) 11th February 2003
Next Review Date: February 2004
Classification: Internal

S:\security\policycompliance\email\mailforward\compliancefwd.doc

---

1) Prepare the results directory.
1.1 Create a new directory for the query results in
S:\security\policycompliance\email\mailforward\

Follow the existing naming convention of YYMM
Ie The Directory for March 2003 would be named 0303
S:\security\policycompliance\email\mailforward\0303

2) Perform the query.
2.1 Open Netscape Communicator 4.7

2.2 Enter the following URL into the Location bar of Netscape Communicator.
ldap://localldap:389/OU=people,O=GIAC Insurance??sub?(mailforwardingaddress=*)

2.3 Press Enter. The query will generate the results in the web browser.

Note: Appendix A contains additional sample LDAP URLS

3) Save the query

3.1 From the Netscape Communicator menu options .(top left) select the "File" option. This will present a further menu to appear.

3.2 Select the "Save As" option, and a pop up box will appear.

3.3 In the pop up box Set the "Save In" value to
S:\security\policycompliance\email\mailforward\YYMM
Change the file name to YYMMGeneral.html (YYMM are the current Year and Month)
Select the Save Button.

4) Compliance

4.1The Saved Query now contains the information required to review each email address against the email policy for email forwarding and enables appropriate action to be taken in or to enforce the policy.

4.2For each email address assess if the configuration is compliant with the policy objectives in relation to email forwarding.

4.2.1 Internal email forwarding
Must have an auto response message that informs the sender of who the email has been forwarded to and the contact number for that person.

If the email account is not complaint see 5.2.3 below.

4.2.2 External email forwarding
Must be on the approved forwarding list.
S:\security\policycompliance\email\mailforward\externalfwd.xls
Must have an auto response message that informs the sender of who the email has been forwarded to.

If the email account is not complaint see 5.2.3 below.

4.2.3 Where email forwarding is in breach of the email forwarding policy issue the standards standard email forwarding policy abuse warning message to the individual via the security teams email account.
S:\security\policycompliance\email\warnings\EmailAbuseFwd.txt
Add the persons name to the warnings log
S:\security\policycompliance\email\warnings\2003warnings.xls

4.4 Reviewing users who want to register for external email forwarding is a separate procedure.

5) Retention

5.1Within the directory structure

S:\security\policycompliance\email\mailforward\
Delete any Directories or files older than one year.

Appendix A LDAP URLS

General Query
ldap://localldap:389/OU=people,O=GIAC Insurance??sub?(mailforwardingaddress=*)

General Query Internal Only
ldap://localldap:389/OU=people,O=GIAC Insurance??sub?
(mailforwardingaddress=*GIAC-insurance.co.uk)

General Query External Only
ldap://localldap:389/OU=people,O=GIAC Insurance??sub?(&(!(mailforwardingaddress=*GIAC-insurance.co.uk))(mailforwardingaddress=*))

References:

These references have been used for general information.
No extracts have been taken directly from these sources.

A Complete Hackers Handbook
DR-K
ISBN 1-85868-943-0

Mastering Local Area Networks
Christa Anderson and Mark Minasi
ISBN 0-7821-2256-2

TCP/IP
Craig Hunt
ISBN 1-56592-322-7

Java Security
ISBN 1-861004-25-7