GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

GIAC Security Leadership Certificate (GSLC)
Practical Assignment
Version 2.0

© SANS Institute 2004, Author retains full rights.

Rita Hamby
October 11, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper describes the current and proposed network security design for fictional GIAC Fortune Cookie Company. The current design is evaluated for appropriateness for existing operations and potential improvements. Business and regulatory forces impacting GIAC are also identified and suggested improvements are analyzed, including total cost of ownership and return on investment. Finally, recommendations for changes to GIAC network security are proposed.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I. Executive Summary:

GIAC Fortune Cookie Company has enjoyed success with its migration to an online environment. Customer contact is easy, supplier updates take place more quickly, and the infrastructure supporting the overall operations, including the security components have contributed to higher net sales.

GIAC has determined that in order to continue to maintain our status as a growth company there are two key factors impacting GIAC business that need to improve. First, while net sales figures have increased, internal costs have risen disproportionately higher. GIAC is already using outsourced providers for various business functions: payroll, payment processing, etc. To aid in keeping costs better controlled, GIAC management has decided to outsource the IT application support to COOK-E, a third party consulting firm with resources located in India.

Second, GIAC net sales increase has partly been attributed to the strength of our suppliers. Initially, GIAC used primarily its own internal resources for creating the fortunes. As business expands, the need to expand the fortune database, and ultimately the source of fortunes, is also required. As such, our supplier network is getting larger which has both a positive and negative impact. We now have a broader base of contributing resources for our fortune database, but we need additional flexibility to manage the transfer of information to these suppliers from GIAC

In addition to these business driven requirements, GIAC is also impacted by Sarbanes-Oxley regulations. While GIAC initially started as a family owned business, GIAC became a publicly traded company last year. While we have a number of well documented processes and controls in place, - including written policies and procedures, documentation for network and applications, standards for server hardening etc – as part of the S-ox pre-audit there are several areas of controls identified needing improvement. Specifically, our logging and monitoring processes need to be documented and managed accordingly; we need to provide effective awareness training on our policies and standards both internally and to our outsourced partners; and we need to strengthen some of our existing operational processes. In addition, as part of the proposed changes to the infrastructure to accommodate third party application support, we will need to ensure that documentation and tight procedures are in place for managing a third party partner.

With these considerations in mind, the following upgrades are required to support both the business and regulatory requirements:

- Changes to our infrastructure to manage third party support in a cost effective manner with appropriate security consideration for managing the risk to our proprietary information

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Use of additional transfer mechanisms to support the need for access to our growing list of suppliers and customers, and
- Improvements to our business/IT processes to position GIAC to better meet regulatory requirements
- Improvement to our infrastructure to support and secure additional communications, and provide better vulnerability management for GIAC proprietary information.

Our challenge is to continue to provide cost effective operations to support the growing business needs, provide the appropriate process and documentation, and maintain an appropriate level of security for GIAC infrastructure and proprietary information.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

II. Current Infrastructure

Network topology

GIAC current network design is a straightforward implementation detailed in Brian Ridzonis' paper from February 2004. A copy of the network design can be referenced at http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf.

Internal Infrastructure
Database:

GIAC fortune database, which is the heart of our business, resides on an internal SQL server database. This application architecture is a two-tier architecture consisting of the web/application component and the database component. The database resides on a Microsoft hardened server running Microsoft SQL 2000. Internal SQL security configuration standards were followed for the database implementation and only the required services are running. Access to the database is via the Fortune application, which resides on the web server in the DMZ. The application architecture features a separation of the application server from the database server to provide an additional layer of protection for the internal database.

Database views are defined based on user functional requirements, so access is limited to necessary data and or functions. There is no direct user access to the internal database. System administrator activity is logged for all support activities performed.

PC's and laptops

Internal PC's and /or desktops used by employees have been locked down and secured. Symantec anti-virus has also been installed on all desktop and laptop computers. This applies for both internal and remote employees, including the traveling sales staff. In addition, the remote users have a personal firewall installed on their laptops to disallow everything except Ipsec when not connected to the network.

VLAN segmentation

The internal network is segmented into two VLANs, which separate the internal users workstations and the datacenter servers. This provides an additional layer of protection by segmenting core business data from the rest of the internal network as well as providing an infrastructure that can be scaled or upgraded depending on GIAC future direction for use of outsourced ser vices.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other internal infrastructure components:

As part of the internal infrastructure there are additional servers providing business services and security management:

- A domain controller which knows all servers that are part of the internal GIAC infrastructure and is also running Active Directory to manage internal user authentication and access. This server has been hardened per internal standards and is managed by GIAC staff
- A syslog server, which is a centralized server that stores, logs from the multiple servers that comprise the infrastructure. This provides a single source for log information for ease of management,
- A mail server which handles all internal and external mail for GIAC enterprise, which has also been hardened and is reviewed regularly for patches and upgrades, and
- A backup server that provides redundancy for recovery of the database server, which is the core of GIAC business.

The datacenter housing the hardware and software for GIAC is physically secure. There is card key controlled access to the datacenter; environmental controls and UPS back up systems in place.

DMZ Segment

There is a DMZ segment that houses the web facing application server and a DNS server. The DMZ is a protected area that separates GIAC from the internet and routes data bound for internal GIAC services and from GIAC to the internet. The DNS server is responsible for resolving addresses bound to/from internal GIAC. The DNS server has been hardened and all other services except for DNS have been disabled. The web server houses the fortune application as well as GIAC's web site and is accessible by customers from the internet.

Web application

The Fortune application itself resides on a web server sitting in the DMZ. This server is a Microsoft Windows 2003 server running Internet Information Services (IIS) 6.0. The application server resides in the DMZ to allow for web access for customers and suppliers from the internet. Customers and suppliers have the ability to access the web server using HTTP/HTTPS, which is secured using secure socket layer (SSL). The server has been hardened based on internally documented security configuration standards. Communication between the application residing in the DMZ and the internal database server are via SQL calls and HTML code.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Access to the application is defined by roles. Customers wishing to place orders for fortunes are either set up by the GIAC sales force or can set up a user account via the web application. These accounts default to the customer role. The user accounts are managed via userid and password. This role provides the ability for the customer to place an order with GIAC via the web application.

Border router and firewall

The DMZ is separated from the internet by a border router and a firewall that are the first line of defense in protecting the perimeter for GIAC. The router filters traffic that is targeted for GIAC from the internet as well as ensures that traffic from GIAC can route to the internet. The router uses a small set of ACL's for ingress and egress filtering.

The Cisco Pix firewall is configured to determine specifically what traffic is allowed to continue into GIAC, thereby providing a level of risk mitigation for connecting to the internet. In addition, the PIX firewall is configured to statefully track connections and policy for GIAC to provide filtering for permissible traffic initiated at GIAC and slated for the outbound internet. The Cisco firewall appliance provides a dual role of firewall and VPN, providing the end point for VPN access.

VPN

VPN is an important component of the secure infrastructure. This provides a virtual private circuit across the internet, providing for secure communication for sales force and telecommuting personnel who need to access email and internal servers. The VPN client is installed on the client device and configured per internal standards.

Intrusion detection

Last but not least is the monitoring and logging of potential security events using an intrusion detection system (IDS). There are three IDS sensors placed in key positions to monitor events:

- Between the router and firewall to monitor for suspicious network activity,
- On the DMZ network segment to monitor for potential attempts to hack into systems, and
- On the internal network segment to monitor for specific events.

In these positions the IDS provides at multiple layers, monitoring for security events that may get past the initial layers of security architecture. The Snort

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

product was chosen for IDS due to its wide install base and cost (no licensing fee) as well as its known effectiveness.

III. BENEFITS OF CURRENT INFRASTRUCTURE

The key components that mark the effectiveness of the current design are:

- Meets business requirements for on-line/internet access to GIAC with appropriate risk mitigation for GIAC,
- Provides a cost effective infrastructure that was implemented within planned budget
- Utilized a defense in depth approach to security which afforded a layered security model appropriate for GIAC, and
- Provides scalability for GIAC growth

Business requirements and risk mitigation

Core to GIAC was the need for access via the internet and enabling customers and suppliers to have easy access to the GIAC fortune application and to place orders. The current architecture enabled GIAC Fortune Cookie to compete in the e-business world with easy access to GIAC by its customers and suppliers via use of the internet and email. Customers and suppliers access GIAC's application via the web to place orders or upload new fortunes. In addition, they have access to GIAC resources via email for questions, order status, follow up, etc.

The current infrastructure provides a network perimeter secured by a standard, practical firewall implementation:

- Use of a border router for filtering traffic from the internet and
- Implementation of a name brand Cisco PIX firewall to separate GIAC's network and the internet.

The router functions as a layer of security between the internet and GIAC, utilizing access control lists to filter traffic for ingress and egress. The Cisco PIX firewall is configured to block certain addresses from the internet and access from multicast source addresses. The router-firewall combination provides the basic security for a company that is internet accessible.

Cost effective design

The current infrastructure provides a cost effective entry into the e-business world and was accomplished within designated budgetary constraints. There are three specific area that demonstrate the cost considerations taken into account as part of this implementation:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Intrusion detection software: Snort IDS solution is an effective intrusion detection product and was obtained at no cost to GIAC. There is no license fee for Snort.
- Hardware selection and sizing for routers, firewalls and servers: The hardware selected for each of these components was streamlined for the most functionality with the least cost. Specifically the Cisco router selected has the functionality of high-end appliances but is a low end cost model. Similarly, the appliance used for IDS uses this same model. The PIX firewall selected also has multi-functionality. It serves as the firewall appliance as well as the VPN end point and eliminated the need for separate appliances providing the most cost effective solution for GIAC.
- Leverage vendor synergy: Cisco products were chosen for both routers and firewall appliances. GIAC IT personnel are familiar with Cisco products. This implementation allowed GIAC to leverage compatibility of products, leverage their knowledge of these products, and eliminate additional overhead associated with multiple vendor technologies to support.

Scalability

The infrastructure supporting GIAC's internet access was built with key components that support both the operational functionality as well as the security requirements. The overall design using a DMZ zone, combination of routers and firewall for filtering, VLAN segmentation of internal resources and 2 tier architecture for the application are architected in a manner that enable growth for GIAC by potentially expanding or adding appliances to the existing network design. As mentioned previously, hardware components of this design were selected for cost effectiveness as well as functionality. In essence the router and firewall chosen are scalable for GIAC growth. The router can be expanded to add additional communication links to the internet or other offices. The firewall design can be expanded as well to add additional firewalls if needed (e.g. on the internal side of the DMZ) or to separate VPN functions to its own appliance. The DMZ may be expanded to include FTP, or other web application servers if GIAC business dictates. A number of these components will be addressed in section V in the discussion of recommendation based on business drivers.

Defense in Depth

The current infrastructure utilizes a defense in depth approach that provides various layers of security utilizing multiple techniques and services. Using a defense in depth posture provides a network that that is 'crunchy, not soft and chewy throughout' by relying on not only perimeter security, but providing security at various layers of the architecture design.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

"The foundation for a self-defending network is integrated security – security that is native to all aspects of an organization. Every device in the network – from desktops through LAN and across the WAN – plays a part in securing the networked environment" [2]

The defense in depth approach utilizes security measures designed at the following layers:

- Router filtering and Firewall implementation
- Secure communications
- System hardening
- Two tier application architecture
- Physical security
- Vulnerability management
- Intrusion detection
- Security policy

Router filtering and Firewall implementation:

The router is designed to filter traffic coming from the internet as well as route packets coming from internal GIAC to the internet. The firewall separates GIAC from the internet and applies GIAC security policy to traffic coming from and going to the internet. The border router and firewall combination make up the first line of defense in securing GIAC's perimeter from the internet. The protected DMZ zone hosts the external facing components of GIAC services.

Secure communications (HTTPS and VPN)

The web server uses SSL to ensure the security of communications from its customers and suppliers. For GIAC remote sales force and telecommuting employees, a VPN solution is in place for secure communications.

System hardening

GIAC has security configuration standards developed for operating systems and databases used internally. When a new system is implemented, the system is built using these configuration standards and security settings to ensure uniformity of controls and documentation of security settings. These standards have been followed for each of the components of GIAC's infrastructure.

[2] Meta group: The Evolution of Network Security: From DMZ Designs to Devices Oct 2004

Two-tier application architecture with hardened servers

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The application architecture uses a 2-tier model with the application/web component residing on a web server in the DMZ and the database residing on a separate server internal to GIAC. In addition, all servers have been hardened per policy and only necessary services running.

Physical security of the data center and equipment

The data center housing the equipment is on premises at a GIAC location. The data center uses card key access control requiring employees to swipe cards to gain access. The data center utilizes a dedicated UPS system to manage power fluctuations and short outages. There is also temperature control and AC as well as a fire protection system in place.

Vulnerability management for client

The overall security architecture would not be complete without management of the user/PC component. Desktops and laptops have been locked down based on GIAC policy, run anti-virus software that automatically scans the device on boot up and automatically download updates for the virus signature files. In addition, all laptops used for remote access are configured with the Black Ice personal firewall.

Intrusion detection

While the IDS is not a preventive solution, it provides monitoring and notification for key events on the network. GIAC personnel are alerted based on documented policy and can react to alerts promptly. The syslog server provides a central repository for messages and alerts. This allows GIAC personnel access to logs and alerts from multiple systems for problem resolution and follows up.

Policies, standards and procedures for security, awareness and compliance

GIAC has an information security policy, security standards and configuration standards for specific operating systems, database and devices. These policies and standards have been communicated to employees, are available internally, and are part of the overall security awareness program at GIAC.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

IV. Challenges with the current infrastructure configuration

The current infrastructure and security design has been successful in bringing GIAC Fortune Cookie to a new level of productivity and customer satisfaction. With the experience of this new business enabler under our belt and the identification of additional business requirements, several opportunities for improvement have been identified.

Secure communications between application and internal database

While our initial infrastructure design provided for a two-tier application architecture, and secure communication between the customer and web, it did not account for securing the transmission between the application server and the back end database. Since the Fortune database is GIAC's proprietary information and internet threats abound, we need to add an additional element of security. "Most companies install a corporate firewall to keep intruders out. They assume that the firewall is good enough, so they let their application server talk to their database in the clear. Assuming that the data in question is important, what happens if an attacker penetrates the firewall? If the data is encrypted, the attacker won't be able to get at it without breaking the encryption--or, more likely, breaking into one of the servers that stores the plaintext data."[1] This is a commonly overlooked security measure that is fairly simple to accomplish by obtaining SSL certificate for the server.

Third party access

The initial infrastructure was designed to accommodate GIAC internal business, web enabled access for suppliers and customers, and communications with third party business partners (e.g. outsourced payroll, accounts payable, etc.) using only web access and email. There is no accommodation in the current design for third parties that GIAC may contract to provide services that require internal network access. The current need to better manage or reduce the increasing operational costs has resulted in a decision to include application support in the list of outsourced services. This requires changes to our infrastructure to manage third party access to internal resources in a cost effective manner with appropriate security consideration for managing the risk to our proprietary information. This requirement does not change the basic infrastructure designed, but will add to elements both externally and internally to support the operational and security requirements. This functionality will be built to accommodate the existing need for third party access but will also be able to scale for other uses (e.g. employees who travel, acquisitions where limited access is required, and for specific application access (vs. entire network access).

1 Juniper networks: http://i.nl02.net/netscreen000b/h/lyrd2_pdf.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Focused file transfer capability

With the increased sales activity there are additional requirement for flexibility for data transfer between GIAC, its suppliers and customers. An FTP server sitting in the DMZ will be required to handle these file transfers. An FTP server, separate from other functional servers will eliminate the possibility of hacking into one server and gaining access to other key components of the infrastructure. This server will be implemented using GIAC security configuration standards, allowing only services required and will be patched on a regular basis. In addition, data from this server will be purged from this server on a regular basis. For files containing confidential information, PGP will be used to encrypt the data files for transfer.

Security administration

The current GIAC process allows sales personnel to create user ids and passwords. This allows access to the application by the entire sales force to manage user administration. This process needs to be tightened to provide better control for role based access to the application, and to document authorized approvers.

Log monitoring

The current GIAC network architecture includes implementation of system monitoring, intrusion detection, and an aggregate server for hosting the log information. While GIAC anticipated the need for both the monitoring and aggregation of logs for ease of use, the volume of data and time to review was not adequately considered. As such, logs are reviewed sporadically, and GIAC has encountered instances of missed alerts. The security policies for logging and monitoring must be reviewed to determine the appropriate level of logging (e.g. streamline the logs to log information that is critical or that will be acted upon rather than every circumstance). Once this is done, procedures for reviewing the logs can be implemented: for daily, weekly, monthly or quarterly review.

Email security

GIAC currently has a single mail server internal to the company. Email traffic for GIAC has increased, and along with this traffic there is an increase in the hazards associated with managing mail: proliferation of viruses from mail attachments, spam, denial of service attacks, etc. To more effectively manage mail resources and provide additional filtering, a public mail server serving as a gateway and residing in the DMZ is recommended. This mail gateway would perform content filtering, virus scanning, spam filtering and forward only acceptable mail to the internal mail server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Additional network segmentation

In order for GIAC to allow third party business partners to access components of the internal network to provide application support, GIAC will need to provide additional segmentation of the internal network. The current network architecture already uses VLANs to segment employee workstations from the servers. To provide an additional layer of security and management, an additional VLAN segmenting the fortune database and other supported applications should be implemented. ACL's can be used to further restrict traffic to the VLAN. This solution would limit Cook-e personnel from accessing other internal GIAC systems. Since VLANs don't inherently talk to each other, an additional interface card is required. The existing Cisco 3550 can be used with the purchase of an additional card to route traffic for the additional segment. Internal GIAC network staff will create ACL's.

V. Recommendations

The following changes are necessary to address both the business and regulatory requirements for GIAC. These proposals are grouped into 3 categories:

I. Point Solutions addressing business or security issues:

- Secure communications to the internal database
- Provide segregated, secure file transfer capabilities
- Implement email gateway to improve mail capabilities

II. Process and/or policy changes:

- Implement FTP policy
- Create policy for 3rd party access (based on item III)
- Tighten security administration procedures for Fortune database
- Improve system monitoring procedures

III. Upgrades to the network to build an infrastructure that can accommodate the proposed third party access for application support. This infrastructure will be designed to support future external access requirements.

Point Solutions

1.Secure communication to the internal database

Issue: Communications between the application server in the DMZ and the fortune database residing behind the firewall are currently not encrypted.

Solution: Implement SSL for the database server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Benefits: Provides security for proprietary information. If we do not implement, in the event a hacker was able to penetrate our existing defenses and gain access to GIAC's network, they may be able to access this proprietary information.

Cost: $400 annually

2.Segregate and secure file transfer communications with outside suppliers and customers

Issue: Need ability to transfer files securely between GIAC and its customer and suppliers.

Solution: Implement an FTP server in the DMZ to segregate the file transfer services and implement PGP encryption capabilities for transfers of confidential information.

Risk: FTP is an accepted and widely used protocol for file transfer. A separate FTP server in the DMZ, segregated from other functional servers will eliminate the possibility of hacking into one server (for FTP) and gaining access to other key components of GIAC network. Placing a hardened FTP server in the DMZ reduces the risk for sharing services and placing an internal server at risk. Without PGP, confidential information will be sent without encryption, placing our information at risk.

Cost: FTP server and PGP licensing $4,000 with annual maintenance based on number of license and configuration.

3.Improve mail capabilities

Solution: Implement a public mail gateway in the DMZ to provide additional filtering and offload resources from critical network devices (e.g. firewall). This will more effectively manage mail resources and provide content filtering, virus scanning, and spam filtering as well as reduce the load on the firewall appliance.

Risk: The current configuration uses the firewall appliance for multiple tasks, including mail routing to the internal mail server. This key network resource needs to offload some of its workload. In addition, using a separate gateway for filtering will lessen the load on the internal mail server as well as eliminate undesirable and/or inappropriate mail before it hits the internal network.

Cost: Gateway server and software re-licensing: $10,000

Process and/or policy changes

1.File transfer policy:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Create new FTP policy to identify when FTP is an acceptable file transfer process, requirements for FTP services, requirement for encryption based on information classifications, and if/when approval is required for use of FTP. The new FTP policy will be communicated to GIAC employee through the annual security awareness training.

2.Third party access policy:
Create new policy to identify circumstances for acceptable 3rd party access and requirements to secure communications and internal resources. The new Third party access policy will be communicated to GIAC employees through the annual security awareness training.

3.Tighten security administration controls:

Issue: Lack of controls for administration of user accounts for Fortune application.

Solution: Tighten the security settings at the application level to restrict the ability to set up user accounts, create and document the process for security administration and create an authorized approvers list.

Benefits: Demonstrates documentation and appropriate level of controls that can be tested as part of Sarbanes-Oxley audit.

Cost: 6 man-hours plus communication of new process to sales force.

4.Improve system monitoring procedures

Issue: Logs are not reviewed on a regular basis. Information provided via logging is large and needs to be streamlined.

Solution: Review event log settings to determine appropriate level of logging. Determine procedures for daily, weekly, monthly, quarterly logging. Ensure personnel are assigned to review logs based on procedures.

Benefits: Improved event management and response based on log reviews, eliminate unnecessary log data. Will also demonstrate operational controls that can be tested as part of Sarbanes-Oxley audit.

Cost: 50 man-hours plus ongoing review

Implement solution for 3rd party access

Issue: Third party vendor has been contracted to provide application development support for GIAC internal applications. Network infrastructure must change to allow 3rd party access to internal resources in a cost effective yet secure manner that protects GIAC resources

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Solution: Implement Cisco SSL VPN allowing browser based SSL remote access for 3rd party. Implement Citrix server in the DMZ to manage authentication and allocation. Create new VLAN segment for the Fortune database and create ACL's to restrict access.

Benefits: Solution provides secure encrypted transmission, two factor authentication and hardened servers as well as method to restrict access to appropriate internal resources. Solution will be the template for future applications/instances requiring similar internal access by third parties.

Costs: See total cost of ownership (below)

Total Cost of Ownership

The total cost of ownership is calculated only for the recommended solution for third party access since the other solutions are relatively low cost and will be managed with budgeted dollars and/or requires internal man hour/process changes that are considered part of ongoing operations. The total cost of ownership reflects the cost of implementing the technical solution to manage third party access. The commitment to the outsourced vendor would be a 3-year commitment for services.

Direct Costs	
Hardware and software	$ 35,000
Maintenance @ $2k/yr	6,000
Network connection	
At $24k/yr	72,000
Indirect Costs	
Additional power, space, etc	0
Switch card	1,000
Depreciation (5 yr SL)	(5,000)
Implementation	
Staff time (40 hrs/$100/hr)	4,000
Training (Citrix $3k)	3,000
Ongoing management	
(10 hrs/wk @ 100/hr)	156,000
Grave costs	0
Total Cost of Ownership	$272,000

Return on investment

The ROI is calculated to determine if it is cost effective for GIAC to outsource their application support.

Benefits

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(Headcount reduction 3/$105k) Loaded w/benefits	315,000
Costs	
Outsourced consulting/yr	125,000
Hardware and software	35,000
Maintenance	2,000
Network connection	24,000
Switch card	1,000
Total costs	187,000

First year ROI= ($315,000 - $187,000)/$187,000 = 68%

Payback period is $187,000 / $10416 = a little over 17 months

VI Conclusion

"Risk comes from not knowing what you're doing" - Warren Buffet

There are several 'quick hits' that will have little overall cost and will provide ample benefits for either improved security and/or in meeting regulatory requirements. GIAC should proceed immediately with the following:

- Secure communication to the database server using SSL
- Implement an FTP server to provide secure file transfer communications to customers and suppliers
- Create file transfer security policy and communicate to employees
- Create third party access security policy and communicate to employees

GIAC should continue to evaluate the impact of the traffic on the firewall server to determine if/when the mail gateway should be implemented. While this is a reasonably low cost solution, it makes sense for GIAC to statistically compile information on firewall traffic to determine the impact prior to approving the spend.

GIAC should move forward with the proposed outsourcing of application support. The infrastructure to support this access will serve as the standard for securely providing future external third party access and can be scaled for additional growth. The ROI at 68% is reasonable, and reviewed over the life of the contract, will be cost effective for GIAC.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1.Cisco Integrated Network Security. "Building a Self Defending network": http://www.cisco.com/application/pdf/en/us/guest/netsol/ns413/c643/cdccont_0900aecd800efd71.pdf

2. Juniper networks: http://i.nl02.net/netscreen000b/h/lyrd2_pdf.html

3. McGraw, Gary and Viega, John. "Securing Software -Practice Safe Software Coding' *Information Security Magazine* August 2001 http://infosecuritymag.techtarget.com/articles/september01/features_securing.shtml

4. Mackey, Richard. "Layered Insecurity" *Information security magazine* June 2002 **http://infosecuritymag.techtarget.com/2002/jun/insecurity.shtml**

5. Rudzonis, Brian. " How to protect a cookie empire- A secure perimeter design for GIAC enterprises" SANS Practical, Feb 2004

6. Meta Group: " The Evolution of Network Security: From DMZ Designs to Devices: October 2004

© SANS Institute 2004, Author retains full rights.