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
"Introduction to Cyber Security (Security 301)"
at http://www.giac.org/registration/gisf

Justin L. McLaughlin

Submitted on 7 December 2003

Information Security Fundamentals (GISF)
Practical Assignment Version 1.0

In Partial Fulfillment of the Requirements for
Information Security Fundamentals (GISF) Certification

© SANS Institute 2004, Author retains full rights.

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

Abstract/Summary

The following practical is submitted in partial fulfillment of the requirements for GIAC's Information Security Fundamentals (GISF) Certification. It approaches these security fundamentals from the standpoint of a small, fictitious subsidiary of GIAC Enterprises, InvenTraq Incorporated.

© SANS Institute 2004, Author retains full rights.

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

Table of Contents

Table of Contents 3
1.) Description of GIAC Enterprises 4
2.) Diagram and Description of GIAC Enterprises 5
3.) Describe your office, or department at GIAC Enterprises 7
4.) Describe your Job Description at GIAC Enterprises 8
5.) How does GIAC conduct its business? 9
6.) What applications and/or what type of access are required to carry out these business operations? 10
7.) Identify three "crown jewels" your office has access to and is responsible for 12
8.) Insider threat vector for each of your office's crown jewels 14
9.) Outsider threat vector for one of your office's crown jewels 16
10.) Malicious code threat vector for one of your office's crown jewels 17
11.) Identify the most severe threat 18
12.) Recommend a remediation strategy for one of the threat vectors you have described 19
13.) Review the backup strategy 21
14.) Review offsite backups 23
15.) Devise a guerilla business continuity plan 25
List of References 27

© SANS Institute 2004, Author retains full rights.

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

1.) Description of GIAC Enterprises

InvenTraq, a subsidiary of GIAC Enterprises, specializes in inventory management for grocery chains. InvenTraq consults with grocery chains to set inventory and ordering thresholds, coordinates volume purchases for grocery chains from manufacturers, receives daily inventory data feeds from customers, and conducts regular analyses of sales and inventory data. InvenTraq added a new subscription service for grocery chains in which participating chains provide customers with "Super Shopper" cards. These cards entitle users to price breaks in return for valuable demographic and longitudinal data on their shopping patterns. These data, too, are transferred to InvenTraq for daily tabulation, allowing the company to offer additional data mining and analysis services.

InvenTraq's primary source of revenue, to date, has been its inventory management services. More recently, InvenTraq has "grown" existing contracts with its 10 major customers, all of whom have found the additional discount card subscription and data analysis services to be a boon to their own bottom lines. This growth is reflected in InvenTraq's increased revenues from fiscal year 2002 to fiscal year 2003, $20 million and $35 million, respectively.

InvenTraq's primary source of revenues comes from data gathering and data analysis, both IT-dependent functions. Historically, the President and CFO of InvenTraq have remained focused on a very simple business model, ensuring that IT costs were tightly controlled. Recently, IT spending has increased substantially as InvenTraq has begun to provide new services to its customers.

InvenTraq is based in a high-rise office complex in Silver Spring, Maryland. However, given the nature of InvenTraq's business, the company has recently piggybacked on an existing contract between its parent, GIAC Enterprises, and a Philadelphia-based third-party for disaster recovery/hot-site services.

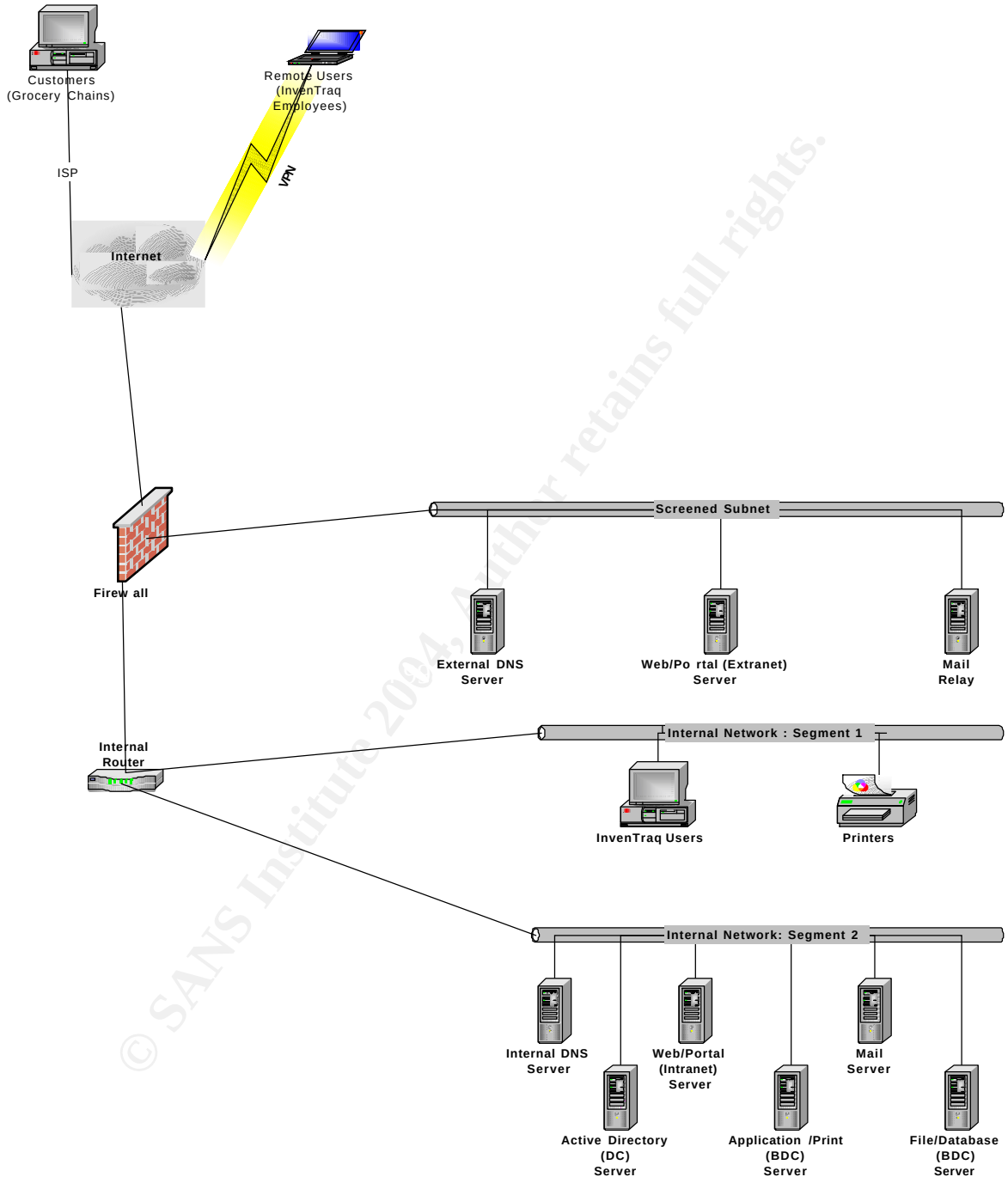
The company employs a total of 18 full time staff.

InvenTraq's base payroll costs are approximately $1.4M, broken out as follows:

- President/CEO (1 @ $200 thousand);
- CFO (1@ $100 thousand);
- Clerical Staff (4 @ $30 thousand);
- Vice President of Sales (1 @ $150 thousand);
- Sales Staff (2 @ $100 thousand);
- Vice President of Analysis (1@ $100 thousand);
- Statistical Sales and Inventory Analysts (2 @ $65 thousand);
- Vice President of IT/CIO (1@ $100 thousand);
- IT Support Specialists (2 @ $45 thousand);
- Programmers (2 @ $70 thousand); and
- IT Security Officer (1 @ $70 thousand).

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

2.) Diagram and Description of GIAC Enterprises[1]



© SANS Institute 2004, Author retains full rights.

[1] Lemick, Andrew. GCFW Practical, Version 1. 9. 1 May 2003. URL: http://www.giac.org/practical/GCFW/Andrew_Lemick_GCFW.pdf. Although not identical, the InvenTraq network design borrows heavily from Mr. Lemick's referenced network diagram.

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

2.) Diagram and Description of GIAC Enterprises (continued)

InvenTraq's network has a single internal router. The router lies just inside the firewall. It is configured to direct the path of authorized internal network traffic, as well as traffic resulting from authorized external connections (HTTP, FTP, VPN, etc.).

InvenTraq's network has one firewall. The firewall lies at the border of the network, providing the first layer of security for authorized traffic coming in and the last layer of security for authorized traffic going out of the screened subnet and internal network (segments 1 & 2).

The network contains two internal segments, which lie beyond the internal router. Segment 1 consists of InvenTraq's user workstations and printers. Segment 2 consists of InvenTraq's internal servers.

The screened subnet, which lies between the firewall and internal router, contains mail, DNS, and web servers.

InvenTraq's key servers reside on Internal Segment 2. These include DNS, web, mail, Active Directory, application/print, and file/database servers.

InvenTraq's utilizes a VPN to grant authorized remote users (InvenTraq employees) access to the network.

© SANS Institute 2004, Author retains full rights.

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

3.) Describe your office, or department at GIAC Enterprises

The mission of the InvenTraq's IT Department is to provide quality, comprehensive IT services and support to the Customers and Staff of Inventraq.

The IT Department is responsible for developing, supporting and maintaining the company's network, including hardware, software, and IT security. It does not maintain or support telecommunication or electrical services. InvenTraq's parent, GIAC Enterprises, contracts for these services, as well as physical security.

The Vice President of IT/CIO reports to the President/CEO of the company.

InvenTraq's business model of the company is increasingly dependent upon the IT Department. While recent increases in sales are strongly correlated with the quality of InvenTraq's work, this quality is due in large measure to the IT Department's support of existing and new technologies, development of client- and web-based applications for customers, and network and data security.

The Vice President of IT/CIO is responsible for all IT assets of InvenTraq, including firewall, router, servers, workstations, printers, and software. Other IT staff members are charged with the day-to-day tasks associated with these responsibilities. Each user is issued and responsible for a monitor, keyboard, mouse, laptop (used at work and from home, for telework), and docking station.

The roles of the individual members of the IT Department are as follows:

- The Vice President of IT/CIO is responsible for personnel, project, and budget management. As mentioned, he is also indirectly responsible for purchase, configuration, maintenance, disposal, inventory, and security of all IT assets.
- InvenTraq's IT Support Specialists are directly responsible for configuration, maintenance, disposal, inventory, and security of all hardware and software. They are responsible for supporting the work of management, clerical staff, the Sales and Analysis Departments, and the IT Department Programmers.
- The Programmers are responsible for developing, deploying, and supporting client- and web-based applications and providing support to customers.
- The IT Security Officer is responsible for providing guidance on technical and policy questions, publicizing and enforcing IT security directives, and maintaining documentation on existing InvenTraq systems.

InvenTraq is based in Silver Spring, Maryland. InvenTraq's IT Department numbers six, including, a Vice President, two IT Support Specialists, two Programmers, and an IT Security Officer. The total budget of the department is $1.3 million, of which payroll, adjusted to include benefits and training, accounts for $800 thousand. The remaining $500 thousand is budgeted for hardware, software, maintenance contracts, and overhead for office space and services contracted by InvenTraq's parent company, GIAC Enterprises.

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

4.) Describe your Job Description at GIAC Enterprises

The job title for the work assignment is InvenTraq IT Security Officer. The salary is set at $70,000, plus benefits, training, and bonuses, as appropriate.

The IT Security Officer is assigned to InvenTraq's IT Department. As mentioned, InvenTraq's IT Department numbers six, including, a Vice President, two IT Support Specialists, two Programmers, and an IT Security Officer.

The InvenTraq IT Security Officer answers directly to the Vice-President of IT/CIO. The Vice President of IT/CIO reports to the President/CEO of the company.

The responsibilities of the IT Security Officer can be broken into two areas. The first area of responsibility is Policy. Policy activities include, developing policies and procedures to ensure systems reliability and accessibility and to prevent and defend against unauthorized access to systems, networks, and data; conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs; promoting awareness of security issues among management and ensuring sound security principles are reflected in InvenTraq's visions and goals; developing systems security contingency plans and disaster recovery procedures; developing and implementing programs to ensure that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures; and ensuring the rigorous application of information security/information assurance policies, principles, and practices in the delivery of IT services.

The second area of responsibility is Technical. Technical activities include participating in network and systems design to ensure implementation of appropriate systems security policies; facilitating the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes; assessing security events to determine impact; and implementing corrective actions conducting systems security evaluations, audits, and reviews.[2]

[2] Office of Personnel Management (OPM). Job Family Position Classification Standard Administrative Work in the Information Technology Group, GS-2200. May 2001. URL: http://www.opm.gov/fedclass/gs2200a.pdf. Many of the individual duties for the primary and secondary responsibilities sections are taken directly from this standard.

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

5.) How does GIAC conduct its business?

In a typical grocery store transaction, a customer chooses products, takes them to the checkout to have their bar codes scanned, and makes payment for the products. The information from the transaction then flows directly into the grocery inventory system. In this way, the grocery inventory system knows exactly how many of each product the store has at any given time.

The InvenTraq software runs in conjunction with existing inventory systems. In the simplest terms, the software outputs data from the inventory system and forwards it to InvenTraq. At InvenTraq, the inventory data are used to generate bulk orders on behalf of all of its customers. Once generated, these orders are then automatically sent to and fulfilled by the grocery suppliers. In this way, InvenTraq eliminates the need for its customers to manage its own inventory.

For customers subscribing to the "Super Shopper" service, the software also pools and sends customer demographic data and purchase patterns to InvenTraq. Data are automatically fed into the into the Analysis Department's systems. The analytical staff reviews and analyzes the data for each client on a weekly and monthly basis. These micro- and macro-level data analyses are then made available to the customers. There, customers are provided with an array of web-based tools to help them understand and make use of their data.

While external customers require periodic technical support from the IT Department, this usually entails walking through client-side installations of inventory data collection tools, data transfer connection setups, VPN access questions, etc. IT Support Specialists also dedicate a great deal of time to providing support for internal users and servicing the servers and other equipment upon which InvenTraq's work depends. Programmers dedicate some time to bug fixes and higher-level support for the existing products. However, their major focus is on the development of new client- and web-based tools to allow grocery chains to leverage more from their own data. Due to its web exposure and the sensitivity of customer data, security has recently become a greater concern at InvenTraq. To this end, the company has begun to invest in personnel and integrate IT security into its processes.

Finally, account maintenance is a major concern at InvenTraq. In addition to drumming up new customers, the Sales Department is responsible for handling any customer service concerns and negotiating contracts with the grocery suppliers used by InvenTraq.

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

6.) What applications and/or what type of access are required to carry out these business operations?

InvenTraq's customers have very limited access to company's network. They connect for two primary purposes. The first purpose is to push inventory data up to InvenTraq's systems. The client-side InvenTraq software, which operates in conjunction with grocery chains' existing inventory systems, is configured for scheduled daily data pushes. These typically occur automatically (without user intervention), in the late evening or early morning hours when network usage is low. These connections take place using customers' own ISP's. There is no direct dial-in access to the InvenTraq network. The client-side InvenTraq software identifies and authenticates itself to the web server, located in InvenTraq's screened subnet, using a combination of customer ID, software ID, IP address, and MAC address. Once authenticated, the software transfers data from the customer to a specific upload directory on the web server. When the transfer is successfully completed, the client-side InvenTraq software automatically terminates the connection to the network. The second purpose for customer access to InvenTraq's network is for customers to view their own data, including current inventory information, inventory trends, the status of orders/shipping, micro- and macro-level data analyses, and management reports. Given the proprietary nature of the grocery chain data and the privacy concerns that come with maintaining longitudinal data about grocery chains' individual customers, access to this information requires a secure connection to the web server located in InvenTraq's screened subnet. Individual users from the grocery companies connect to the secure site via a URL, individually identifying and authenticating themselves. There are no group accounts.

Employees need access to a range of applications to do their job. Laptops are configured with Windows XP. In terms of office applications, InvenTraq is a Microsoft shop, and makes use of the full suite of Microsoft Office Products including Access, Excel, FrontPage, Outlook, PowerPoint, Project, Publisher, Visio, and Word. For web access, users have Internet Explorer. Analysis Department users require access to a range of statistical software. The IT Department uses a range of application and web development tools, network operating system and database tools, and security applications. Management makes use of several management reporting tools and requires additional analytical software. The Sales Department does not require access to any non-standard software. In terms of access, internal network access is strictly controlled. Users are provided only the level of network access required to do their job. The desktop is locked down to prevent user intervention and changes. Access control lists prevent users from gaining access to areas on the network outside of their direct purview. Internet traffic is monitored closely and access to many sites is prevented.

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

Many of the staff frequently telecommute or travel. As a result, the list of InvenTraq's remote users includes the entire staff. Users access the network remotely via VPN using a number of personal dial-up and broadband ISP connections. There is no direct dial-in access to the InvenTraq network. Once users authenticate, an additional layer of authentication and remote access security is provided through the use of SecurID token cards. While no guarantees can be made regarding the throughput of users' various ISP connections, the IT Department does its best to ensure the same level of application, database, and file access for users at home and at work. In this vein, users' laptops contain all of the software that they need, but are configured with separate profiles for the office and home.

© SANS Institute 2004, Author retains full rights.

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

7.) Identify three "crown jewels" your office has access to and is responsible for

InvenTraq's customer and contact lists are stored on its internal file/database server. These data are located in a shared database accessible by all staff via the company's intranet. All employees have rights to view and change this information. However, activities in the database, including changes to these data, are audited. Finally, for the protection of all concerned parties, all customer contacts originating from within or from the customer to InvenTraq are documented.

Contracts with InvenTraq's customers, grocery suppliers, IT and non-IT service providers are developed by the Sales Department, President/CEO, and CFO. These contracts are also stored on its internal file/database server. Electronic files containing these data are closely guarded and contained in secure shared directories. Access to these files is typically limited to those who maintain them, namely the President/CEO and CFO of the company, as well as their clerical staff. Departmental vice-presidents and Sales staff can access the contracts with which they are directly involved. These files are off-limits to the general Analysis, Sales, and IT staff. Accesses to these files are audited.

Management information including salary, performance, background investigations, and awards are developed by the Vice-Presidents of each department in conjunction with the President/CEO and CFO. These data are located on InvenTraq's internal file/database server. These data, too, are closely guarded, accessible by the President/CEO and CFO of the company, as well as their clerical staff. Departmental Vice-Presidents can access the information on employees for whom they have direct responsibility. These files are off-limits to the general Analysis, Sales, and IT staff. Accesses to these files are audited.

Included in InvenTraq's "crown jewels" are its data. The company's very existence depends upon the confidentiality, integrity, and availability of these data. The grocery data maintained by InvenTraq include sales and inventory information for each of its customers. These data directly reflect the current relative financial health of its customers' businesses. The greatest risk for this "crown jewel" is exposure of a customer's information to its competitors. Beyond potentially damaging the customer's financial welfare, a leak of this sort could be catastrophic to InvenTraq. One such leak would likely result in other customers abandoning InvenTraq due to fears about the security of their own data. Further, the demographic and longitudinal data on individual consumers is also highly prized information. The greatest risk here is exposure of consumers' personal information that could be used by unauthorized outside parties for purposes of marketing, or worse, identity theft. Such exposure would have an obvious negative impact on the consumers, themselves. It would also impact the grocery chains' ability to keep the shopping public's trust. Such a disregard for the

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

security of consumers' information could be seriously detrimental to InvenTraq's own credibility and reputation and would likely result in serious legal problems. Both types of data are stored on InvenTraq's external web server and internal file/database server. As mentioned, authorized users inside and outside of the company have access to these data via the internal network (InvenTraq users) and the internet (InvenTraq customers). Data are actively used by both InvenTraq's customers and the Analysis Department. However, the responsibility for maintaining the databases falls under the IT Department. The IT department is also in charge of maintaining accounts of authorized users internal and external to InvenTraq.

© SANS Institute 2004, Author retains full rights.

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

8.) Insider threat vector for each of your office's crown jewels

InvenTraq's customer base is public information. InvenTraq regularly updates the list of current customers on the company's web site. Customers are aware of this and generally view the inclusion on InvenTraq's web site as free advertising. However, specific information about customers and internal contact lists are confidential. Customer and contact lists contain private contact information not only about InvenTraq's current customers, but also about potential customers. These lists also contain information about companies that provide services for InvenTraq. Any of this information would be quite valuable in the hands of a competitor of the company. Since all employees of InvenTraq have a need for and access to this information, one major threat vector for this information is the possibility of a disgruntled current or past employee obtaining and using this information outside of the scope of InvenTraq's business for material gain or simply to "get back" at the company. While staff turnover at InvenTraq is quite low and job satisfaction levels are typically quite high, there is always the possibility that an employee could use this information against the company. The customer and contact lists could be used in any number of ways. Most likely, however, they could be provided to competitors of InvenTraq interested in drawing current customers away from the company or attracting the very business InvenTraq is currently pursuing.

InvenTraq's contracts with its customers, as well as service providers and grocery suppliers, govern nearly every aspect of the company's business processes. Without them, the company would cease to exist. The contracts also contain a great deal of confidential financial information about the company. For this reason, access to InvenTraq's contract information is limited to a small group of users, including managers at the level of Vice-President or above. Due to logical access controls placed on this information, InvenTraq's vulnerability is greatly lessened. Yet while the electronic versions of the files are protected and audited, printed versions receive less attention and constitute another threat vector. When users print contract information to networked printers used by other staff, they introduce the possibility that other users may view or intercept the information. Individuals initiating print jobs do not always closely monitor them. Sometimes people forget, leaving jobs in the tray for days before they are picked up or removed. Furthermore, some users take printed information with them to locations on- or even off-site. In these cases, contract information is exposed to additional eyes and the possibility for loss and/or interception. Intentional or inadvertent exposure of this information to competitors, the public, and InvenTraq's rank-and-file would likely do substantial damage to the company's relationships with customers, service providers, and employees.

Like contracts, the confidentiality of management information is very important to InvenTraq's inner workings, is highly sensitive and closely guarded. Management information contains a great deal of private longitudinal data collected about the

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

people who make up InvenTraq's staff. Accessible by the President/CEO and CFO of the company, Vice-Presidents, and respective their clerical staffs, these data are frequently used in hiring, firing, evaluating, reprimanding, and rewarding employees. The primary concern with these payroll, performance, background, and award data is privacy. InvenTraq must collect and maintain these data to function as a corporation, but has a responsibility to protect these data for the sake of its employees. Here, too, logical access controls are in place to protect the data, diminishing the vulnerability of the data to internal threat vectors. However, one major threat vector lies in these data being included in email by authorized users to unauthorized users. Frequently, those who have access send these data back and forth to one another via email. They are motivated to do so because of the email system's ease of use. The process of hiring, firing, evaluating, reprimanding, and rewarding employees often entails the participation of multiple parties in management. Frequently, the best way to coordinate efforts and request input from these multiple parties is through email. While the email system is secure, the real threat vector lies in the users' understanding of a.) the sensitivity of the data, and b.) the need to protect these data when sending, replying, and forwarding it to other individuals. The simple truth is that email is typically easy to use. It is also quite easy to unintentionally send something the wrong individuals. One slip could expose this personnel data to someone who, regardless of his/her own intentions, should not have access to the information. Such a breach of confidentiality could result, at best, in a very uncomfortable situation for the employees of InvenTraq, and at worst, litigation that could seriously impact InvenTraq's bottom line.

As discussed, the heart of InvenTraq's business lies in the data collected and analyses performed for its customers. The confidentiality, availability, and integrity of this "crown jewel" are of great concern to the company and its customers. These data are available to an array of internal and external users. To mitigate risks associated with these data, there are a number of logical controls in place, including identification/authentication routines, ACL's, and auditing. The vast majority of authorized users are customers. Customers have limited access to the data, including the ability to read the data, manipulate the data, and create reports. Vulnerabilities to the integrity of the data from the outside are lessened because of this. However, the Analysis Department has very broad access to and is charged with the overall integrity of the data. Many of the processes involved in retrieving data from customers, uploading analysis data, and sending orders to suppliers are automated. However, human intervention is frequently required along the way and constitutes a major internal threat vector for these data. Motivated by the need to make the data available to InvenTraq's customers as quickly as possible, staff of the Analysis department may overlook steps or protocols along the way. This human intervention introduces the possibility for mistakes that could affect veracity of the data, the decisions made by customers and suppliers, and ultimately, InvenTraq's credibility.

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

9.) Outsider threat vector for one of your office's crown jewels

As discussed, InvenTraq's customer base is public knowledge. Also public knowledge is the general process by which InvenTraq does its work: How customers flow data to InvenTraq, how InvenTraq makes the data and analytical tools available to customers, how InvenTraq places orders to suppliers, etc. The fact that this is public knowledge is unavoidable but constitutes a vulnerability. While outsiders with malicious intent may not be aware of the specific proprietary means by which InvenTraq conducts its business, knowing the general framework provides would-be attackers with clues necessary to do damage. Thus, one major external threat vector to each and every "crown jewel" from those with a basic knowledge of the company is social engineering. With this little bit of public knowledge and the unwitting assistance of someone from InvenTraq's IT Department or Analysis Department, a motivated individual could pose convincingly as a customer or supplier in need of assistance with system access. Given the customer-service centered nature of InvenTraq's staff, it is conceivable that someone "experiencing difficulty" using the system might receive all of the help that they need to activate a new account or reset a password. If a social engineer can gain access to a single system through this sort of activity, it is likely that he/she could then exploit other more technically based vulnerabilities to do still further damage. The social engineer can potentially gain the "keys to the kingdom", and access to not one or two, but any or all of the company's "crown jewels". The motivation for this type of threat vector is varied. The threat could arise from someone such as an old employee, angry with InvenTraq or with InvenTraq's customers or suppliers. It could come from someone with an agenda, trying to "prove" something to the IT or hacker community. It could come from an individual with too much time on his/her hands.

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

10.) Malicious code threat vector for one of your office's crown jewels

The confidentiality, availability, and integrity of InvenTraq's data and customer analyses must be protected. One of the major threat vectors to this "crown jewel" lies in malicious code. To InvenTraq's credit, the company has enterprise anti-virus, patch management, and firewall strategies in place. The IT Department does its best to stay current on both of these fronts, but often falls one to two months behind the curve. Unfortunately, in this time, new vulnerabilities in software and operating systems are discovered and exploited with regularity.

One malicious code threat vector is the W32.Blaster.Worm, or MS Blaster.[3] [4]

The "crown jewel" resides on the file/database server, which runs Windows 2000 Server. As mentioned earlier, InvenTraq is a Microsoft shop. Since all of InvenTraq's data reside on Microsoft Windows-based servers and workstations AND nearly all of these machines are connected to the internet, the exposure to this malicious code threat is great. Given servers, workstations, and firewall rule sets that are not updated, it would be quite possible for the worm to find its way in from the outside and spread to the entire network without any trouble at all.

The Blaster worm takes advantage of a vulnerability in Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). While it can only move from node to node in a Windows 2000 and XP environment, the worm can reside on and affect systems running Microsoft Windows NT, 2000, XP and Server 2000. Once it infects a machine, the worm ensures that it auto starts each time the machine is brought online, generates "random" IP addresses and uses the RPC DCOM Buffer Overflow vulnerability to propagate itself to machines with these addresses, and launches DDoS attacks on the Windows Update web site.

Infection from MS Blaster could affect InvenTraq, and its parent GIAC Enterprises on a number of fronts. First, it could infect all internal Microsoft-based network resources. Second, it could drag down network resources and performance of all affected systems. Third, it could further infect external resources, including those of InvenTraq's customers and suppliers. The greatest impact of all of these is cost. In addition to the cost of lost time for personnel and data processing, InvenTraq may incur a loss of existing or potential customers. A company tied to the field of information technology must be current on preventative measures and is expected to protect itself, its customers, and the greater IT community. A failure to do so may be interpreted by customers and suppliers as a gross oversight and a reason to take business elsewhere.

---

[3] Information on this worm was drawn from: Microsoft. What You Should Know About the Blaster Worm and Its Variants. August 2003. URL: http://www.microsoft.com/security/incident/blast.asp.

[4] Information on this worm was drawn from: Trend Micro. WORM_MSBLAST.A: Technical Details. August 2003. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A&VSect=T

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

11.) Identify the most severe threat

Threats to the confidentiality, integrity, and availability of InvenTraq's "crown jewels"--customer data, contracts, management information, and customer data--include purposeful misconduct, printing security issues, email exposure, social engineering, and malicious code. From a technical perspective, InvenTraq reacts somewhat slowly at times. However, it generally has a well-configured firewall and router. The company requires that remote users must use personal (software-based) firewalls and access the network via a VPN. The company makes use of an enterprise wide anti-virus package. Strong identification and authentication routines, ACL's, and auditing and review mechanisms are in place. Although the company is not always timely in applying patches, InvenTraq has procedures for patch management and incident reporting/response in place. Physical concerns, from server room security to sprinkler systems, are addressed. The company's network, processes, and procedures are well documented. Yet despite all of these controls, there is a common thread that runs through each of the threats discussed earlier. That common thread, the lack of user education on security, makes InvenTraq's users the most severe threat of all.

The likelihood of this threat leading to InvenTraq's exploitation is great, due to the history and current state of the company. When the company was initially formed, the focus was on developing new, innovative, and valuable services for customers. The camaraderie between young, creative collaborators was strong. The workday typically began late and stretched into the evening. Items like procedures, documentation, and security were distractions from ideas and experimentation. Soon, however, success forced the company to become more corporate in its outlook, employing controls not seen to that point by employees of the company. While the company is still relatively young in age and employs a young, creative workforce, things have changed. In the world of IT security, the necessity to change was reinforced over the past year due to several incidences of virus outbreaks at the company. The company began to realize its exposure to risks, investing heavily and putting into place IT security-related infrastructure, including hardware, software, personnel, and training for the IT Department. Unfortunately, however, the company did not invest in user education. As a result, users frequently conduct themselves in ways that threaten InvenTraq's security.

The potential damage to InvenTraq due to uneducated users is great. Any number of scenarios, all detrimental to InvenTraq, may result from this threat. Users may inadvertently expose customer data to the public or other competitors. They may share internal data that should be held in confidence. Security-related incidents may go unreported due to a lack of reporting procedures or poor publicity. All of these, and other scenarios, could bring InvenTraq's work to a grinding halt, hurt its credibility, or worse, erode its customer base.

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

12.) Recommend a remediation strategy for one of the threat vectors you have described

The lack of user education on security constitutes one of the greatest threats to InvenTraq. It can result in users intentionally or inadvertently conducting themselves in ways that threaten the confidentiality, integrity, and availability of data. InvenTraq is developing a phased approach to deal with this shortcoming. The primary assumption here is that to educate InvenTraq's staff on the company's IT security policy and practices, those policies and practices must be clearly defined from the start. While many technical security controls are in place, the company has historically had a mish-mash of standard operating procedures and unwritten policy, usually written in an attempt to mitigate temporary crises. One unintended result has been that it is difficult to enforce the standard operating procedures and security policy.

> **Phase I:** Conduct a survey of industry best practices, existing company policy, and standard operating procedures documentation.
> **Phase II:** Revamp InvenTraq's current IT security policy.
> **Phase III:** Implement a mandatory education program including a yearly computer based training module and quarterly brown-bag luncheons to discuss IT security-related issues for all users.

With the understanding that InvenTraq requires an aggressive approach to IT security education, the company hopes to have these elements in place no later than one year from this date. Phase I of the project will take approximately two months. Incorporating the results of Phase I into the revamping of policy during Phase II may take some additional time, up to four months. Phase III of the project will take approximately six months to complete. It is anticipated that most of the work done in the later phases necessarily requires the end products of the earlier phases to be in place. However, some practices and policy are in place and ready for implementation, allowing for one of the quarterly brown-bag lunches to be held within the next two months.

While willing to provide oversight and clerical staff for support, InvenTraq management looks to the IT Security Officer to do the vast majority of work associated with this ambitious project. Given that Phase I will primarily involve research, the IT Security Officer will examine industry practices, existing company policy, and standard operating procedures. Phase II will require the IT Security Officer to serve in a project management capacity; drawing from his research, rewriting existing policy, and obtaining input and buy-in from with the Vice-President of the IT Department and other InvenTraq managers. Phase III will require the IT Security Officer to work with GIAC Enterprises, InvenTraq's parent, to piggyback off of their existing computer-based training program. As part of GIAC's own attention to enterprise-wide IT security, this program was developed in-house by GIAC and is licensed at minimal cost to all subsidiaries of

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

the company. The IT Security Officer will work with IT Department programmers to customize this web-based application according to InvenTraq's newly honed IT security policy and procedures and make it available for employee use on the company's intranet server. He will also work with the clerical staff to develop and distribute instructions on using the training. Finally, the IT Security Officer will also be responsible for coordinating the quarterly brown-bag lunches. This will involve researching potential speakers, obtaining management approval, bringing in the speakers, writing agendas, and working with clerical staff to provide information on the luncheons to the rest of InvenTraq's staff.

In terms of new purchases, the three-phase program outlined above requires very little. Since the training program will run off of existing hardware, new purchases will be limited to the price of the computer-based training module from GIAC, plus the per seat license fee. Together, the total charge for the purchase will be $11,800 ($10,000 server license + 18 seat licenses @$100).

As mentioned above, the total dollar cost of implementing the program will be $11,800. However, the number does not reflect the other resource costs associated with its implementation. The greatest cost among these is for the time of the IT Security Officer, who will dedicate approximately 50% of his time for the year to developing and implementing this program. In the process, he will draw on other human resources including programmers, clerical staff, and management, who will each dedicate a percentage of their time to this process. The demands placed upon these individuals will be continually variable, depending heavily on the progress of the IT Security Officer.

© SANS Institute 2004, Author retains full rights.

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

13.) Review the backup strategy

InvenTraq's current enterprise backup system does not include backing up users' desktops, which are laptops used both at work and at home (for telework). The recent discovery that data are stored on users' laptops raises concerns that these data will become inaccessible and unrecoverable in the event of a disaster. Further discussion with the IT Department Support Staff has indicated that the company must minimize user downtime, not only in cases of disaster but also times when PC's crash and cannot be repaired. Management and the Support Staff agree that the best approach will involve performing off hours, monthly, full backups of users' laptops, and storing these backups on a network server. When put into practice, this approach will allow for the rapid restoration of operating system, software, and data, and will eliminate the extra time required for Support Staff to perform installations and search directory-by-directory for users' missing data. The major shortcoming of this approach lies in the potential loss of data modified in the intervening period between backups. Further, it is anticipated that off hours scheduling will be complicated by the fact that users often take their laptops home during these hours. Management is aware of and accepts these risks, viewing this as a step in the right direction.

InvenTraq's enterprise backup software is Retrospect 6.5 Multi-Server. To this point, the software has been used to perform weekly taped backups of InvenTraq's servers. However, the software offers additional scheduling and scripting tools that allow for the backup of laptops. These tools will enable InvenTraq to perform laptop backups once per month during off hours, or at the next time the laptop is connected to the network. InvenTraq is already licensed to use the full functionality of Retrospect 6.5 and anticipates no initial cost for software. However, InvenTraq will need to update its licenses and support contract with Retrospect in the coming year. This cost will depend upon InvenTraq's choice in vendor, but is estimated at $2,000.

InvenTraq runs the Retrospect software on its Windows 2000 application server. Due to recent upgrades, the server has approximately 1 terabyte of free disk space available. Given that InvenTraq does not plan to maintain multiple historical backups for each user, the amount of space required for backup storage for the laptops should not exceed 720 gigabytes (18 laptops @ 40 gigabytes apiece). InvenTraq anticipates no additional cost for hardware.

As discussed, laptop backups will be stored on InvenTraq's application server. In terms of physical security for the server,[5] a contractor manages InvenTraq's site in Silver Spring, Maryland. Entries and exits to the building are monitored and logged by security personnel at the front desk, twenty-four hours a day, seven

[5] Heare, Sean. Data Center Physical Security Checklist. December 2001. URL: http://www.sans.org/rr/papers/index.php?id=416. Information for this section, dealing with physical security of InvenTraq's server room, was drawn directly from Sean Heare's work.

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

days a week. Within InvenTraq's offices, the application server is located in a locked room with all of the company's other servers. The door to the room is clearly labeled, indicating that authorized access is required. Access to the room is typically restricted to IT Department staff, and is controlled and logged. The computer room is equipped with cameras, monitored by the security desk. The server room has high ceilings and 18" access floors. The temperature of the room is controlled to be in the 55-75 degrees Fahrenheit range. The facility has access to redundant power and cooling. The server room is equipped with emergency power-down switches. There is a Halon fire extinguishing system in place. Additional technical/logical controls will be put in place prior to implementing the new backup system. The backup software will run on the application server under a dedicated administrative account. Backups will be stored in new directory on the server. This new directory will be secured by an ACL limiting access to the backup software and IT Department Support Staff charged with its management. Auditing for the software will be enabled and monitored on a regular basis. Finally, taped backups of the application server, itself, will be stored with other server backup tapes away from the server room in a locked safe.

As discussed, InvenTraq will need to update its licenses and support contract with Retrospect in the coming year. This cost will depend upon InvenTraq's choice in vendor, but is estimated at $2,000. InvenTraq will incur no additional hardware costs associated with the implementation of this laptop backup strategy. Since the IT Department Support Staff is already familiar with the general workings of the Retrospect software, ramping up will be easier and take less time. Implementing the software will require time to develop scripts to automate the backup process, install the Retrospect Client on each of the laptops, test the process from backup to restore, and create documentation on the new process. The time it will take the IT Department Support Staff to perform these tasks and perform monthly maintenance over the course of a year is estimated at 220 hours. Given the hourly rate of IT Department Support Staff, $21.63 (annual salary of $45,000/work hours in a year of 2080), the estimated cost of implementing and supporting the laptop backup strategy is $4,760. The total estimated cost of the system for the year is $6,760.

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

14.) Review offsite backups

InvenTraq's enterprise backup software solution, mentioned above, is Retrospect 6.5 Multi-Server. The software is currently used to perform taped backups of InvenTraq's servers. It will also be used to backup user's desktops. Taped server backups are stored away from the server room in a locked safe. However, in the event of a disaster rendering the taped backups inaccessible, InvenTraq has no current means of recovering the data. InvenTraq plans to begin storing copies of its backups offsite for access in the event of a disaster.

Putting this plan into action will require certain initial and repeating steps. Fortunately, InvenTraq has recently piggybacked on an existing contract between its parent, GIAC Enterprises, and a Philadelphia-based third-party for disaster recovery/hot-site services. InvenTraq has already taken the steps necessary to gain hot-site access in the event of a disaster. However, InvenTraq will need to expand the scope of its agreement with GIAC Enterprises and the service provider to include offsite backup storage. As a part of the agreement, InvenTraq will ship copies of the weekly backup tapes of its operating systems and data to the Philadelphia site. The service provider will ensure secure storage for current tapes and will cycle old tapes back to InvenTraq for reuse. In the event of a disaster, the service provider will use the current tapes to restore operating systems and data to machines dedicated to its agreement with GIAC Enterprises and InvenTraq.

Confidentiality refers to the requirement that data are kept private and are not disclosed to unauthorized parties. Loss of this confidentiality could prove fatal to InvenTraq's credibility and ultimately, its bottom line. Confidentiality is protected by ensuring that taped backups are stored in fireproof safes both at InvenTraq and at the Philadelphia site. However, one of the problems with shipping the data lies in the possibility that the data may fall into the wrong hands somewhere along the way. Confidentiality is provided through the backup software, Retrospect, which encrypts the data using Data Encryption Standard or DES. Given DES' age, InvenTraq remains concerned that this may not be the best means of encrypting the data. However, the company has not yet considered implementing a PKI solution and has no plans to do so within the next year.

Integrity refers to the requirement that data are complete and have not been tampered with by unauthorized parties. The integrity of InvenTraq's data is also very important. Orders are placed and management decisions are made upon the basis of "good data". As mentioned earlier, taped backups are protected at InvenTraq and the Philadelphia site by ensuring that they are kept under lock and key. Retrospect's encryption, too, aids in preventing data tampering preventing access to it. The Retrospect software also ensures the integrity of the backups by applying checksums to backups to ensure the integrity of files. Finally, older

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

tapes are rotated out of and new tapes are rotated into circulation to ensure the integrity of the media and data contained on it is protected.

Availability refers to the requirement that data are accessible to users and customers when they need it. InvenTraq receives data from and provides data to customers and suppliers with great regularity. In the event of an emergency, InvenTraq's data must be available for use within a matter of hours. To ensure availability of the data, InvenTraq has a regular schedule for sending tapes and logging activities. When weekly backup tapes are shipped from InvenTraq, the shipper is given a receipt and tracking number, which are both added to the log. Upon receipt, the Philadelphia site is required to sign for the tapes. Information about the shipment and the recipient's acknowledgement are subsequently made available to InvenTraq via the shipping company's web site. This information, too, is logged.

The Vice President of the IT Department plans to conduct a yearly audit of this process in conjunction with InvenTraq's contingency planning test. This audit component will involve taking a look at both internal and external activities. InvenTraq's internal activities include scheduling and capturing backups, packaging the weekly copies of taped backups, sending the tapes, and logging the shipment and receipt. Verification of this process will be relatively easy to perform. However, auditing the external activities conducted at the Philadelphia site will require a visit to the service provider to verify that receipt of the backup tapes is logged, that storage of the tapes is secure, and that the integrity of the data is intact. In this vein, the audit will entail testing the restore process to ensure that InvenTraq has properly backed up the data, that the Philadelphia site has adequate staff, equipment, and space to perform restore operations, and that together, InvenTraq and the service provider can get up and running in the event of an emergency.

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

15.) Devise a guerilla business continuity plan[6]

InvenTraq is just starting to look at disaster and business continuity planning. In these early stages of planning, management has opted for the "one percent approach" outlined by SANS. As such, management has identified its inventory management capabilities as most critical to its operations. More specifically, the company must be able to receive data from its customers and send orders to suppliers. In the event of a disaster, the company will focus first on restoring these operations, and second on restoring its analytical and sales operations.

Infrastructure: InvenTraq's electronic resources, including data, hardware, software, and connectivity, lie at the heart of its business. In the case of an emergency and loss of access to its primary site, InvenTraq must restore its critical inventory management operations in a matter of hours. The company is already building upon its existing backup strategy to protect its data. The company also has a strategy for shifting its operations to its hot-site in Philadelphia. Within hours of a disaster declaration, data, hardware, software, and connectivity will be available at the hot-site.

Premises: In the event of a disaster, the primary Silver Spring, Maryland site, the site will be abandoned. All business activities will be shifted to the hot-site in Philadelphia, Pennsylvania.

Personnel: Given that InvenTraq is a small company, the company wishes to keep the Disaster Recovery Team lean and mean. The primary roles to be filled in the event of a disaster include Disaster Recovery Coordinator, Procurement Coordinator, Damage Assessment Coordinator, and Public Relations Coordinator. These roles will be occupied by InvenTraq's President /CEO, CFO, Vice President of the IT Department/CIO, and Vice President of the Sales Department, respectively.

Resources: Data, hardware, software, and connectivity will be available at the hot-site, as will all necessary office equipment including desks, chairs, and mailing equipment. In the event that additional resources are necessary, the Procurement Coordinator will be on hand. Given InvenTraq's scaled-back operations, a skeleton crew including eight of InvenTraq's eighteen staff members will shift limited operations to the hot-site. These personnel include the four members of the Disaster Recovery Team outlined above, one member of the Clerical staff, one IT Department Support Specialist, one IT Department Programmer, and the IT Department Security Officer. Backup personnel have not yet been identified. This listing of personnel, their disaster recovery roles, and contact information have been provided in electronic and wallet-sized hard-copy format to each member of the team. The Disaster Recovery Coordinator, InvenTraq's President/CEO, will manage the recovery efforts from the hot-site in Philadelphia, Pennsylvania. The Public Relations Coordinator, InvenTraq's Vice President of the Sales Department, will speak with the press and any customer/supplier contacts, as necessary. The Damage Assessment/Recovery Coordinator will conduct the damage assessment. The primary criteria for declaring a disaster will be building and office accessibility.

---

[6] SANS. Track 9 – SANS Security +S, 9.6 Security Start to Finish. 2003. URL: http://giactc.giac.org/cgi-bin/momdnld/s=9.6.5/a=BZ1T3m6dQbc/SECPLUS_65_0403_pdf/SECPLUS_65_0403.pdf. This guerilla business recovery strategy was developed using the guidelines and questions from the SANS material found in Chapter 36, Assignment 7.

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

Notification Procedures: In the event that the criteria for a disaster declaration are met, the Disaster Recovery and Damage Assessment Coordinators will work together to notify the remaining six members of the hot-site team. Once the hot-site team has been notified, they will coordinate the notification of the rest of the staff. The eight members of the hot-site team have been provided with cellular phones. The Disaster Recovery and Damage Assessment/Recovery Coordinators will attempt to contact members of the hot-site team via their cellular telephone numbers. As a backup, the coordinators also have the home telephone numbers of the staff. The coordinators will then notify the remaining staff through their home telephone numbers. Notification of the hot-site team and remaining staff will take place within two hours of disaster declaration.

Plan Activation: Once the Damage Assessment coordinator reports back on the condition of InvenTraq's primary site in Maryland, the Disaster Recovery Coordinator will make the decision to trigger the Disaster Recovery Plan. The Disaster Recovery Coordinator will first notify the other hot-site team members and the hot-site service provider in Philadelphia. The Damage Assessment and Disaster Recovery Coordinators will then work with the Procurement Coordinator to begin gathering necessary resources (rental cars/vans, hotel rentals, etc.) to shift the hot-site team and operations to the secondary site.

Executing Recovery Procedures: The entire hot-site team will bear responsibility for executing the recovery procedures. Each member has been provided updated electronic and hard copies of the recovery procedures for safe storage at home. In the event that the Disaster Recovery Plan is triggered, members of the hot-site team will be aware of their roles and responsibilities. The disruption will be considered resolved when the primary site in Silver Spring, Maryland becomes available and is restored sufficiently to support InvenTraq's operations OR management decides on a new primary site. The primary criterion for recovery is the ability of the old or new site to support the full scope of InvenTraq's business operations.

Recovery Procedures (High-Level):

1. Event
2. Disaster Recovery/Damage Assessment Coordinators in contact
3. Damage Assessment conducted (Damage Assessment Coordinator)
4. Disaster declared (Disaster Recovery Coordinator)
5. Hot-site contacted (Disaster Recovery Coordinator)
6. Hot-site team contacted (Disaster Recovery and Damage Assessment Coordinators)
7. Remaining staff contacted
8. Resources procured (Procurement Coordinator)
9. Hot site team travels to Philadelphia
10. Hot site team installed at secondary site, tests capabilities.
11. Customers/suppliers contacted (Public Relations Coordinator)
12. Limited operations resume at hot site (Hot-site team)
13. Damage to primary site repaired or alternative site found (Damage Assessment Coordinator)
14. Hot site team returns to primary/alternative site, tests capabilities.
15. Recovery declared (Disaster Recovery Coordinator)

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

List of References

[1] Lemick, Andrew. GCFW Practical, Version 1. 9. 1 May 2003. URL: http://www.giac.org/practical/GCFW/Andrew_Lemick_GCFW.pdf.

[2] Office of Personnel Management (OPM). Job Family Position Classification Standard Administrative Work in the Information Technology Group, GS-2200. May 2001. URL: http://www.opm.gov/fedclass/gs2200a.pdf.

[3] Microsoft. What You Should Know About the Blaster Worm and Its Variants. August 2003. URL: http://www.microsoft.com/security/incident/blast.asp.

[4] Trend Micro. WORM MSBLAST.A: Technical Details. August 2003. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A&VSect=T

[5] Heare, Sean. Data Center Physical Security Checklist. December 2001. URL: http://www.sans.org/rr/papers/index.php?id=416

[6] SANS. Track 9 – SANS Security +S, 9.6 Security Start to Finish. 2003. URL: http://giactc.giac.org/cgi-bin/momdnld/s=96.5/a=BZ1T3m6dQbc/SECPLUS_65_0403_pdf/SECPLUS_65_0403.pdf

© SANS Institute 2004, Author retains full rights.

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