Smith system consulting essay sample

Law, Security

Smith Systems Consulting was founded in 1984 by Blair Smith. In the late 70s, Blair Smith was a partner with a large public accounting firm in Houston, Texas. Having an advanced degree in computer science and an undergraduate degree in accounting, Mr. Smith would often use technology applications to solve the finance and accounting problems of Mr. Smith clients. Seeing the explosive growth of the personal computer industry, Blair Smith decided there were sufficient market opportunities to launch an independent technology services consultant business (Smith, 2006).

From an initial group of five, Smith Systems Consulting has grown to become a major regional consulting company with locations in Houston, Texas (headquarters), Atlanta, Georgia, and the newest venture to Beijing, China. Smith Systems Consulting clients for technology services are from a wide variety of industries including: Transportation, retail, financial services, manufacturing, and education.

Smith Systems Consulting services include: Designing and implementing network or website or custom programming project; offering the latest server technology to provide safe and secure web site hosting; developing new technology and upgrading current system; providing web site maintenance; programming and offering premier support services. Smith Systems Consulting offer these services to their clients with high value Web and Business application services.

AREAS OF THE BUSINESS TO BE IMPROVED

Smith Systems Consulting is exploring the possibilities of enhancing Smith Systems Consulting security procedures and methods to maintain an honest,

corporate workplace that will in turn benefit the customers in which Smith Systems Consulting serve.

The number one priority is the safety of the data that Smith Systems Consulting maintains on Smith Systems Consulting servers and who has access to that data. Everyday, hundreds of transactions are taking place on Smith Systems Consulting servers for Smith Systems Consulting customers that include sensitive data, such as social security numbers, credit card numbers and bank account numbers.

For the safety and security of Smith Systems Consulting employees, proximity readers have been installed all throughout the building and are maintained at certain workstations. The proximity readers grant or deny access to a particular area of the building or database within a computer. Each employee is issued a picture identification card with encoded information implanted in the cards microchip, denoting what access the employee is given.

Smith Systems Consulting has about 50 servers at each location, Texas, Georgia and China. These servers maintain the company’s products that help them service their clients. All websites, personal databases and local area networks are maintained on Smith Systems Consulting servers for easy access to Smith Systems Consulting customers and Smith Systems Consulting employees working on projects for Smith Systems Consulting customers. All databases, websites and software created at Smith Systems Consulting are copyrighted and fully non-pirated. This gives the client the full rights to Smith Systems Consulting software and to no one else.

THE PURPOSE OF THE PROJECT

Client’s information must be held and kept secure from outside sources as well as employees that might see to compromise integrity. There are controls and checks in place to monitor employees and the information that they are passing to ensure security.

At Smith Systems Consulting the employees that work there have different levels of access as to the information that Smith Systems Consulting can see and access for Smith Systems Consulting clients. Depending on what the employee works on or is the employees’ job duty will depend on the access. If the employee works directly with a client than naturally the employees have access to that information. If the employees work indirectly with a client than the access the employee have to that clients information is limited. Thus, having monitoring tools, badge access stations and monitors for information that is being passed on that client is highly monitored. This is another way to keep client information secure and confidential.

STAKEHOLDERS ASSOCIATED WITH THE PROJECT

Some of the industries that use Smith Systems Consulting services are transportation, retail, financial services, manufacturing and education. Smith Systems Consulting strives and has achieved this excellence because of Smith Systems Consulting employees, they take care of the employees, the employees take care of the customers and the rest will take care of itself (Smith, 2006).

Smith Systems Consulting is looking at expanding Smith Systems Consulting services to the entire United States. Currently, only the Western United States from Houston Texas is being served. Expansion of services will mean quite a bit for SSC. More customers will create a demand for more work and more work requires employees. Smith Systems Consulting goal is to continue to maintain Smith Systems Consulting target audience of companies. The companies have given Smith Systems Consulting experience to create new idea and implement new strategies not only for Smith Systems Consulting customers, but for Smith System Consulting as well.

SERVICE REQUEST

SERVICE REQUEST

ORGANIZATION NAME:

Smith Systems Consulting

LOCATIONS:

Houston Texas, Atlanta Georgia, Beijing China

REQUESTER:

Tanika McClain, Chris Posey, Josephine Smith and Hilary Wilton

DESCRIPTION OF REQUEST:

Smith Systems Consulting (SSC) evaluating ways in which the process of security and data management can be improved to protect the employees of

SSC as well as our clients and their business. Outside evaluators will work closely with internal staff at SSC to determine weak areas that can be improved with up -to-date procedures to establish 100% satisfaction within production.

BACKGROUND OF REQUEST:

In early 2006, SSC expanded its United States operations to Beijing China for the 2007 Olympics as well as future business after the Olympics are completed. The Olympic board chose SSC as their top choice to maintain the website and all databases for the Olympic games being held. Our websites and databases would travel information all over the world in real-time so no one is left out. SSC feel that a security analysis will be beneficial to us at this time, as the Olympics taken very seriously and are considered a prestige around the world.

EXPECTED RESULTS/IMPACT WHEN COMPLETED:

When the evaluation is completed, SSC plan to sit down with internal department team leaders and discuss the recommendations that the outside auditor has recommended and take them into consideration for implementation. The results of the audit are not to tell SSC what to change, but to establish new ideas to make data management and security that much more secure.

Smith Systems Consulting is exploring the possibilities of enhancing security procedures and methods to maintain an honest, corporate workplace that will in turn benefit the customers in which Smith Systems Consulting serve.

The number one priority is the safety of the data that Smith Systems Consulting maintains on Smith Systems Consulting servers and who has access to that data. Everyday, hundreds of transactions are taking place on Smith Systems Consulting servers for Smith Systems Consulting customers that include sensitive data, such as social security numbers, credit card numbers and bank account numbers.

For the safety and security of Smith Systems Consulting employees, proximity readers have been installed all throughout the building and are maintained at certain workstations. The proximity readers grant or deny access to a particular area of the building or database within a computer. Each employee is issued a picture identification card with encoded information implanted in the cards microchip, denoting what access the employee is given.

Smith Systems Consulting has about 50 servers at each location, Texas, Georgia and China. These servers maintain the company’s products that help them service their clients. All websites, personal databases and local area networks are maintained on Smith Systems Consulting servers for easy access to Smith Systems Consulting customers and Smith Systems Consulting employees working on projects for Smith Systems Consulting customers. All databases, websites and software created at Smith Systems Consulting are copyrighted and fully non-pirated. This gives the client the full rights to Smith Systems Consulting software and to no one else.

Client’s information must be held and kept secure from outside sources as well as employees that might see to compromise integrity. There are

controls and checks in place to monitor employees and the information that they are passing to ensure security.

At Smith Systems Consulting the employees that work there have different levels of access as to the information that Smith Systems Consulting can see and access for Smith Systems Consulting clients. Depending on what the employee works on or is the employees' job duty will depend on the access. If the employee works directly with a client than naturally the employees have access to that information. If the employees work indirectly with a client than the access the employee have to that clients information is limited. Thus, having monitoring tools, badge access stations and monitors for information that is being passed on that client is highly monitored. This is another way to keep client information secure and confidential.

SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

In order for Smith Systems Consulting to remain confident in the organization's ability to demonstrate due diligence for information security and privacy, SSC hired KPG auditing company to conduct a high-level security review called the Compliance Infrastructure, Policy and Physical (CIPP). The CIPP provides IT management with insight into the major issues surrounding the management and maintenance of information and network systems, as mandated by current federal regulations and industry certifications. The CIPP will assist management in identifying existing security and non-compliance weaknesses specific to the organization and

provide clients and vendors with acceptable documentation that the information is protected.

ANALYSIS

The investigation conducted by KPG auditing company detected weaknesses within the database server and software for data protection. To help secure database connections and define access controls, a data flow diagram was created to track how data flowed through the applications. Next, places where data enter or exit were identified and the trust level assigned to these entry and exit points. Privileges of any external user or process requiring access to the system were defined. The purpose of the flow diagram is to configure and build database applications with security as a key driver to ensure that data stay secure.

DESIGN

The CIPP is the most cost-effective, non-intrusive (1-2 day) way for a security review to be performed. At the completion of the CIPP review, a detailed written report with the findings and the recommendations were given to the senior executives and IT management. The findings and recommendations will prove to be very effective in helping to identify the weaknesses. The costs that are associated with the audit are estimated at $3500 for each security review.

Recommendations included, installing software for data protection, such as a detection engine and a data blocker. IT security of this type will protect customer or employee information with names, addresses, social security

numbers, and other identity-related information. IT security will protect customer lists that could be used by a competitor for poaching clients, trade secrets and intellectual property, confidential engineering and manufacturing plans for products, and financial information or marketing plans.

KPG recommended three leading companies that created data-leakage prevention tools. They are Vontu, Inc., Reconnex Inc. and Vericept Corp. TheVontu 6. 0 suite from Vontu, Inc. contains a set of tools that can monitor all types of web traffic. Vontu 6. 0 can be finely tuned to target specific groups of employees, locations, or types of content.

Reconnex’s iGuard is a network appliance that monitors the content of outbound traffics and spots malicious activity. The Reconnex platform can be tuned to suit a company’s needs.

Vericent’s 360-degree Visibility and Control is a customizable tool predominantly used for content monitoring. Vericent from Vericent Corp not only monitors the whole range of web traffic but also monitors blog postings, chat rooms and Web sites, all places where sensitive company data and secrets could end up.

IMPLEMENTATION

From the findings of the KPG auditing firm, Smith Systems Consulting has decided to implement two of the three data leakage prevention tools. The first to be implemented is the software Vontu 6. 0 suite. Keeping information secure is the highest priority with the company so a tool that monitors all

web traffic and can be customizable to monitor employees, other locations and types of content is the tool that is needed. After Vontu 6. 0 suite is implemented, the staff is fully trained, and monitoring processes are in place, the Vericent software will be implemented. This software will give the company the capability the go beyond monitoring web traffic.

This will allow for the monitoring of all blog postings, chat rooms and websites. This software will be on chat rooms and web sites that are known for hackers and crackers to visit so that the company can ensure that our content is not placed there. Smith Systems consulting believes that these tools will enable the company to go above and beyond in client's expectations of security. To implement both software packages will take approximately eight months with four months set aside to implement both software packages. In order to prepare staff there will be training over a 6-week period per software package for a total of 12 weeks.

SUPPORT

In order to ensure that the process that is implemented stays fine-tuned and refined a support structure will be developed and created to ensure accuracy. Smith Systems Consulting will have KPG Auditors come in every six months to monitor these new software packages and the processes that are put in place for these systems. Outside of that Smith Systems Consulting will create two teams one to monitor and continuously support both Vontu 6. 0 Suite and Vericent. These teams will be dedicated personnel that will strictly work with these software companies in the event of an outage problem, provide on-going training to personnel and keep the software's in

compliance. With these two strategies in place the company should receive maximum performance from this new-implemented software.

CONCLUSION

The overall project proposal is to enhance the atmosphere in which SSC operates while providing their clients the most reliable and secure services possible. With locations in Texas, Georgia and China, SSC is committed to the accuracy of its work as well as the security and protection of sensitive client data held within our data infrastructure.

The audit from KPG will allow senior IT staffers to identify and modify any area that may show a flaw or weakness and that could possible be a threat to our clients or their business. The objective of SSC is to take the considerations into account and to maintain open communication between the employees of SSC and KPG.

Security systems that currently monitor all SSC data are our first priority. This data contains sensitive information such as social security numbers, credit card numbers, phone numbers and addresses. Smith System Consulting’s firewall system will undergo a strenuous test to determine if there are any loop holes within the system. KPG will attempt to hack into the system to test the strength of our firewall.

The assessment of secured access data at terminals is recommended to be not only password protected, but security clearance authorized. All employees will be issued a proximity card which will then in turn give the employees access to the building, but at their desk also, they will be the only

one to access the data at his or her terminal by presenting the proximity card to the reader at his or her desk.

KPG has also informed us that they will be reviewing our systems development life cycle plan. SSC like to stay ahead of the technology realm and maintain the highest quality of servers, firewalls, and personal computers and laptops. This newer, rapidly equipment will save SSC time and money and will prevent SSC from having to use the same computer for 10 years. The same will go for our servers. The server room is currently house at the main headquarters of SSC in Houston Texas. The server room is a massive space housing more than 100 servers holding millions of bits of data for our clients.

The Chief Information Officer of SSC hope that with the current audit of KPG, SSC will be able to provide the customers with a standard of excellence and a readiness to server. Smith System Consulting’s data will be ready available to SSC employees at the point of a mouse click. Smith System Consulting’s clients will be able to access their data 25 hours a day from secured server locations, and are guaranteed not to lose data. At SSC, they guarantee, they will “ make the net-work for you”!

References

Smith Systems Consulting Virtual Organization. (2006). Retrieved November 16,

2006, from https://ecampus. phoenix. edu/secure/aapd/CIST/VOP/Business/Smith/SmithHome003b. htm