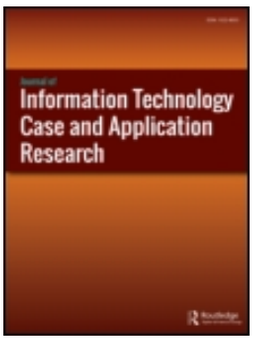

Routledge
Taylor & Francis Group

Journal of Information Technology Case and Application Research

ISSN: 1522-8053 (Print) 2333-6897 (Online) Journal homepage: http://www.tandfonline.com/loi/utca20

Pensource - Evaluating Information Security in a Software Services Company

Ms. Shaila Kuchibhotla, Dr. Frank Braun & Dr. Vijay V. Raghavan

To cite this article: Ms. Shaila Kuchibhotla, Dr. Frank Braun & Dr. Vijay V. Raghavan (2012) Pensource - Evaluating Information Security in a Software Services Company, Journal of Information Technology Case and Application Research, 14:2, 47-73, DOI: 10.1080/15228053.2012.10845701

To link to this article: http://dx.doi.org/10.1080/15228053.2012.10845701

PENSOURCE - EVALUATING INFORMATION SECURITY IN A SOFTWARE SERVICES COMPANY*

Ms. Shaila Kuchibhotla
Great American Insurance Company, Cincinnati, OH 45202

Dr. Frank Braun
Dr. Vijay V. Raghavan
Northern Kentucky University, Highland Heights, KY 41099

Journal of Information Technology Case and Application Research 2012.14:47-73.

ABSTRACT

This teaching case focuses on the importance of a formal evaluation of information security practices using established frameworks. Such an evaluation is especially essential for organizations dealing with sensitive customer information. This case first presents the prevailing security practices of PenSource, a pension services company. A description of security practices of PenSource is provided using three approaches: a narrative description, a diagram of PenSource's network infrastructure, and answers to a questionnaire eliciting information on existing practices on many dimensions such as security organization, policies and standards, and logical access controls. A set of questions to facilitate a reader to analytically reflect on how to improve the current practices of information systems security of the focal organization is included.

Keywords: Information Systems Security, Security Risk Assessment, Logical Access Controls, Contingency Planning.

1 INTRODUCTION

Ramesh Saxena, the CIO of PenSource, has just met with the executives of SecAdmin, a consulting company engaged to conduct a comprehensive review of PenSource's security policies and procedures. Ramesh's proactive stance on security-related Information Technology (IT) issues has earned him an industry-wide reputation and has shaped his career path. After becoming the CIO of PenSource in 2008, Ramesh successfully managed its initial growth strategies. Now he believes that, in light of the highly sensitive private and government information handled by PenSource, it is an opportune time to undertake a comprehensive security review including its security policies and administration procedures. Besides, he is highly confident of SecAdmin's expertise in conducting such reviews. SecAdmin is a consulting organization founded by Dr. David Schultz, a well-known professor from Stanford, who is highly regarded in the IT industry. During his initial consultation, Ramesh had assured Dr. Shultz that his employees would fully cooperate with the security review. Ramesh and his staff have responded to a comprehensive questionnaire eliciting information on security procedures (Appendix C). After completion of the

* Situations, names and descriptions of individual profiles, and geographic locations have been changed to protect the identity of the focal organization and its clients.

questionnaire, Ramesh met with Dr. Schultz and SecAdmin's consultants to discuss the security assessment questionnaire. The closeout meeting was planned in about fifteen days to discuss SecAdmin's findings and its recommendations to Ramesh and his team.

PenSource is a mid-sized company based in Cleveland, Ohio with its offices and data centers located in Kentucky, Ohio, and Canada. The company develops, implements, and supports pension administration solutions. The majority of its clients are state and local government organizations within the United States. PenSource was founded in 2004 and has roughly 150 employees worldwide, many of whom work remotely from home or at client sites. The company offers an on-premise and hosted pension solutions as well as data center services to its client base. PenSource is also a Microsoft Gold Certified Partner and its custom solution is built on the Microsoft .NET platform.

PenSource's customers primarily consist of state and local government agencies that have very specific security requirements. As a result, the company places a great deal of importance on maintaining an effective information security program that meets client requirements and ensures compliance with government regulations. PenSource is aware that to maintain an effective security management program, it is necessary to go beyond technical considerations and establish organizationally grounded principles and values (Dhillon & Torkzadeh, 2006). Being able to fulfill client needs is a critical success factor for PenSource and is vital to its current operating activities and future success. Since security plays a significant role in ensuring customer satisfaction, it is considered a top priority for PenSource.

2 SECURITY PROGRAMS AT PENSOURCE

The information security program at PenSource emphasizes the implementation of technology-based solutions in conjunction with logical and physical access controls to address security concerns. The company's infrastructure team is the main entity responsible for developing and implementing the information security program. Though the team initially started out small in 2004, it has since grown and handles almost all aspects of information security.

PenSource does not have a formally documented security strategy. However, security principles are currently in place that could be used to develop one in the future. PenSource also has a comprehensive enterprise level information security policy. While the majority of security activities are handled by the in-house infrastructure team, several functions such as annual auditing, penetration testing, and data center security are handled by third-party firms.

PenSource employs multiple layers of security involving both hardware and software based technology solutions to protect its information assets across the corporate network. The diagram included in Appendix A, Information Security Architecture, illustrates the various layers of protection and technologies implemented by the company. PenSource maintains data centers that host client data (which consists of retirement information and personal records) and offers a hosted version of its pension solution. The software, hardware, and networks used to host client data (and applications) are on a segregated network separate PenSource's corporate systems. This segregation ensures that the appropriate layers of security and controls are in place to protect against unauthorized access to clients' confidential information, ensuring data confidentiality, integrity, and availability.

Journal of Information Technology Case and Application Research 2012.14:47-73.

Some of the important corporate applications used at PenSource are listed below:

- Microsoft SharePoint (Collaboration Software for the Enterprise? SharePoint 2010 , 2011) a collaboration software for enterprise content management
- Numara FootPrints (Service Desk Software Solutions with Numara FootPrints, 2011) a web-based IT service management solution used to automate business processes, support service desk and help desk operations
- Microsoft SQL Server4(Microsoft SQL Server 2008 R2 — Database Management System, 2011) a relational database management system

Journal of Information Technology Case and Application Research 2012.14:47-73.

2.1 Security Organization

PenSource does not have a formal security organization established. Security functions are primarily handled by the infrastructure team which includes Ramesh Saxena (CIO), Mark Goff (Infrastructure Manager), and Chris Manning(Security & Network Administrator). The team consists of ten members whose security responsibilities include managing active directory services, VPN, network security, network access control (NAC), and the Cisco Security Monitoring, Analysis and Response System (MARS) (Cisco Security Monitoring, Analysis and Response System (MARS), 2011). While each team member works with different aspects of information security, only two are assigned actual security-based roles. When compared to their business counterparts, IT employees are more involved in developing, implementing, and ensuring the success of the information security program.

Certain members of the infrastructure group are also certified security professionals with a CISCO CCSP (CCSP? Career Certifications & Paths, 2011) qualification. The requirements for employee security certifications are determined by business needs and client requirements. In addition to the infrastructure team, a third party service provider called FishNet Security (FishNet Security — Vulnerability Assessment and Penetration Testing, 2011) conducts yearly security audits, regular nondisruptive penetration tests, and vulnerability assessment. PenSource also contracts with GeoTech to provide disaster recovery colocation services for its client information data center. GeoTech's facilities are audited regularly and maintain SAS 709 Type II compliance, a widely recognized auditing standard which indicates that a service organization has been through an in depth audit of its controls over information technology and related processes (See Appendix B Colocation Facility Overview).

3 POLICIES AND STANDARDS

As part of the contract agreement, SecAdmin examined PenSource's formal enterprise information security policy. The policy is developed, maintained, reviewed, and updated by the infrastructure team. There are no documented system-specific or issue-specific security policies. Information relating to specific systems or issues is included in the main enterprise information security policy. Security policies are published and made available to all employees at PenSource through the corporate Intranet. Although they must sign an acknowledgement form after reviewing company policies, employees are not required to demonstrate their understanding of the policy. Policies are updated as needed based on client requirements or after certain security events and incidents have occurred. So far the policies have not required many updates although

the latest policy revision was done last year. There are no measures in place to ensure that the policies are being enforced.

PenSource's information security policies cover the following areas:

- Logical Access Controls
- Auditing
- Change Control
- Privacy & Confidentiality
- Remote Access
- Email and Internet Usage
- Virus Protection
- Password Management
- Personnel Security & Hiring Standards
- Physical Access Controls
- Computer & Network Management
- Data Classification and Communication
- Vendor/Third Party Management
- Encryption

As part of the Information Security Program, PenSource has a detailed description of expected behavior and penalties for security violations in a document and provides all employees a copy of this document. It requires that they review the document and sign an affidavit that they have read and understood the company policies and standards. Although PenSource has many government clients, the organization itself is not required to explicitly follow any specific government regulation. The majority of PenSource's clients do have to comply with federal regulation, which is expressed in client requirements. As a result, PenSource is expected to abide by certain guidelines and standards in order to satisfy these requirements.

4 RISK ASSESMENT & MANAGEMENT

Evaluation of security policies, specifically access control policies are important to securing the network by ensuring that policies are correct and consistent. Quality of protection (QoP) of a policy depends on a number of factors (Abedin, Nessa, Al-Shaer, & Khan, 2006). Most of PenSource's efforts relating to risk assessment and management focus more on mitigation than identification of risk. The company emphasizes the implementation of important risk controls such as redundant hardware systems, vendor service contracts, and cross training employees to avoid single points of failure. However, PenSource has not developed adequate risk assessment tools internally. It does not have an Information Asset Inventory listing critical corporate assets along with asset attributes, sensitivity levels to threats, and related security policies. Instead, the importance of an information asset to PenSource is determined by client needs. Systems that directly impact the company's ability to provide effective customer service rank higher than all other assets. It is assumed that the third party service provider, FishNet Security develops asset and threat inventories when conducting a risk assessment. FishNet is also expected to complete a Business Impact Analysis (BIA). The absence of an internal governance committee or audit team that reviews the results of third-party findings indicates that the organization is not very involved in the risk assessment process. This can result in inaccurate risk identification and omission of important risks due to third-party oversight. It is important for the company to be involved in all aspects of risk assessment and management.

PenSource considers internal threats such as hardware crashes, software vulnerabilities, or malicious actions by disgruntled employees to be more damaging and important than external threats. This may be due to the very low occurrence of high impact external attacks. In addition,

the company has implemented more security measures (firewalls, IDPS, etc.) to protect against the external threats rather than the internal ones. As a result of its robust security technology solutions, PenSource has 0% tolerance for system-based risk. It recognizes that the greatest risk exposure comes from human error, failure to follow policy, and negligence. One of its biggest internal threats is an employee losing a laptop with unencrypted client data. Another threat is the loss of data from a laptop compromised by a Trojan or virus due its interaction with a public network. The client data stored on these systems is extremely sensitive and if it were to be compromised, the financial losses involved could bankrupt the company.

The most common risk strategy employed by PenSource is risk avoidance followed by mitigation and acceptance. Risk avoidance would mean not performing an activity that could bring risk. Risk Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits. The risk strategy used by PenSource depends on whether or not the information asset is Internet facing, on a segregated network, or using a VPN client. It also depends on customer requirements and the impact of the risk on important business processes that support service delivery. Risk avoidance and mitigation are accomplished using technical controls, which protect information assets from attack. If an employee's system becomes compromised, these controls reduce the risk exposure. There are some risks that the company has to accept, such as employees noting down passwords on sticky notes, visiting online poker sites which may expose them to malware, and losing laptops with unencrypted data.

With the security technologies currently in place, PenSource estimates with 10% uncertainty) that 97% -98% of risks are avoided or mitigated. As a result it believes that, the occurrence of an attack or data breach is extremely rare. In fact, in the past five years, there has only been one such incident. Due to its high risk avoidance and mitigation rate, the company expects its residual risk to be minimal. (Note: It is assumed that the residual risk is caused by human errors.)

4.1 Logical Access Controls

PenSource uses a data classification scheme to classify different sets of information. The scheme is not extensive and classifies data as either "Public", "Internal Use Only", or "Confidential." This classification is partly based on the organizational unit to which the data belongs. Access to data is determined by the data classification scheme. Each organizational unit has employee roles with specific access privileges based on security requirements. Microsoft SharePoint, though primarily a collaboration and content management tool, is also used to assign security clearances to each user based on their role. These clearances determine what types of data users are allowed to access. In order to obtain access to a given document, a user must submit a request through the ticketing system and wait for approval. Unauthorized access attempts prompt users with a notice informing them why they cannot access the requested content and what level of authorization is required. Although a formally documented access control policy does not exist, the company is currently working on developing one.

The company also has a password management policy requiring a unique username and password for user authentication. The password must be changed every 90 days and cannot be reused. All connections into the company's network from mobile devices, laptops, and remote users are

secured using advanced authentication have limited application access use a VPN connection, and require a personal firewall. In addition, 128-bit encryption is currently used to protect certain types of data such as passwords and sensitive client information stored in a database (i.e. SSN) (see Appendix C). However, file encryption of data stored locally has not been implemented. Initiatives were introduced to encrypt all data on employee laptops, but they fell through due to lack of support from senior management and other political issues.

For PenSource, access controls are in place in six different categories: preventative, deterrent, detective, corrective, recovery, and compensating. Preventive controls try to prevent security violations and enforce access control. Detective controls detect any security violations and alert the defenders if they occur. Corrective controls correct the situation after a security violation has occurred. Deterrent controls are in place to discourage potential attackers. Recovery controls recover and restore information and processing resources when security violations occur associated with loss of information or other resources. Finally, compensating controls provide alternative arrangements when other controls have failed or cannot be employed. (Whitman & Mattord, 2010). No emphasis is placed on any given category in terms of importance. Detective controls are in place to detect security violations and alert the defenders. However, the most common controls used by PenSource are preventive (e.g. well defined and documented backup procedures) and corrective. The company employs separation of duties and need-to-know based access controls. Important technical controls established by PenSource for the external network include firewalls, credential authorization, and intrusion detection and prevention systems. Controls for the internal network are much more relaxed. Managerial controls implemented by PenSource include employee termination processes, security policies, and the development of an improved disaster recovery plan.

4.2 Physical and Environmental Security

PenSource has very extensive physical and environmental security controls in place (see Appendix C), especially for its colocated data center at GeoTech (see Appendix B). The data center maintained by PenSource in Franklin, KY supports production databases with client information. In order to meet client requirements, PenSource has contracted with GeoTech to provide disaster recovery colocation services. This facility offers redundant power supply, cooling and humidification units, fire detection and suppression systems, alarm-based environmental monitoring systems, emergency lighting, and camera surveillance twenty four hours a day, all 365 days in a year.

All individuals require a key card, photo id, and biometric hand scans to gain access to the network operations center (NOC). NOC and facilities personnel conduct walkthroughs at 12 hour intervals and verify system operations. Access logs are maintained which contain information about the visitor, purpose of visit, date and time information, and form of ID used (see Appendix C). Data centers in Canada mainly house R&D data and as such do not require such robust security controls. Finally for the corporate offices PenSource requires ID badges to gain physical access.

Journal of Information Technology Case and Application Research 2012.14:47-73.

4.3 Personnel Security

All individuals are screened prior to being hired by PenSource. The screening involves identity checks, education/credential checks, and verification of references. New hires currently do not undergo orientation or training to help them understand policies and procedures. It is not clear what type of security screening or checks are conducted for third party personnel such as consultants, temporary workers, and contractors. Upon termination of an employee, PenSource terminates system access, conducts exit interviews, ensures return of organizational property (key card, ID), changes file cabinet locks, revokes ID card access, and removes employee's personal effects (see Appendix C).

4.4 Security Technologies

PenSource has a wide range of multilayer, hardware and software based security technology solutions implemented to protect against threats.

4.4.1 Network Access Controls

The company has enabled the AAA (Authentication, Authorization, Accounting) network security framework for its Cisco Solutions to manage access control (Davis, 2008). This process is handled by the hardware as the Cisco Access Control Server (ACS) (Cisco Secure ACS Appliance Overview, 2011) appliance that authenticates against Active Directory credentials and client credentials to enable access. The organization is currently in the process of implementing a NAC (Network Access Control) solution. This security technology is expected to verify the "posture" of the client system by checking for things like antivirus software, malware protection, and Windows updates before granting network access. This is to ensure that client systems are not infected with harmful programs. All activity on the network is tied to the user and the machine being used. Access is granted based on the profile of the user and the privileges provided by the Active Directory Services.

4.4.2 Firewalls

Cisco ASA (Cisco ASA 5500 Series Adaptive Security Appliances, 2011) (Adaptive Security Appliances) devices are context-aware hardware firewalls and are being used by PenSource to protect its company network. These devices provide sufficient protection at a hardware level. As a result, PenSource did not implement extensive firewalls at the software level. There were only a few instances where client requirements indicated the need for software firewalls and PenSource implemented them.

4.4.3 Intrusion Detection & Prevention Systems (IDPS)

Cisco Inline IPS (Cisco Intrusion Prevention System, 2011) (Intrusion Prevention System) is the technology being used by PenSource for intrusion detection and prevention. These systems are inherent in the firewall appliances and connect to the Cisco Security MARS (Monitoring, Analysis and Response System) box to correlate attacks and alerts. Network traffic is monitored by the MARS box , which is setup using a combination of preset and custom parameters. There is no companywide configuration documentation for this device. Usually, an employee with sufficient security expertise defines the parameters. The box logs and classifies incidents based on presets. Since the network is normally quiet, it is very easy for the appliance to spot anomalies in network activity that does not correspond to the baseline activity. In the event of an intrusion, the

MARS box can initiate shunning of IP address through the IPS for up to 30 minutes. Most attacks against the network are automated and detected and stopped by PenSource's IDPS.

4.4.4 Remote Access Protection

When a client system attempts to remotely access the network, the Network Access Control (NAC) guarantees client posture authorization and generation of an audit log of network activities. PenSource has many employees who work remotely from client sites, remote offices, or from home. The remote offices all have wireless connectivity with WPA2 encryption. Currently there is no physical security at the remote offices but once the NAC is completely implemented, PenSource is looking to adopt EAS (Electronic Article Surveillance) solution to protect and track assets such as laptops.

4.4.5 Scanning & Analysis Tools

PenSource uses Nessus (Nessus Product Overview, 2011), a vulnerability scanner developed by Tenable Network Security, to scan and analyze security vulnerabilities. This application contains a database of exploits which it uses to execute specific exploits and test for vulnerabilities on the network. It has different modes of operation including passive, nondestructive, and disruptive.

4.4.6 Other Technologies

Encryption is currently used at PenSource for specific areas (such as passwords, database content, wireless). However, initiatives to introduce file encryption for locally stored data fell flat due to a lack of political support and stakeholder buy-in. As a result, data on employee laptops is not encrypted. Although the company does not use dialup technology in any of its US offices, it may use it in Canada. Proper security controls must be established for dialup connections in company offices in Canada.

4.4.7 Cost Benefit Analysis and Feasibility Assessments

PenSource conducts an informal cost benefit analyses for each security technology prior to purchase and implementation. In addition to a cost benefit analysis, PenSource often conducts other feasibility assessments such as those for operational, political, and technical conditions. The cost benefit and feasibility analyses are discussed during the decision making process to provide a comprehensive overview of the security technology and associated costs/benefits. If a client requires the adoption of a security solution, the company will purchase and implement it regardless of its economic, political, operational, and technical feasibility. Sometimes PenSource does not implement certain security systems. This is primarily due to resource constraints on available manpower and time. It can also be due to political obstruction by senior executives. However, an implementation has never been put off due to technical limitations.

4.4.8 Metrics

PenSource does not use very specific or detailed metrics to evaluate the performance of its security program. The metrics that are used are not very extensive and provide a general overview of effectiveness. PenSource conducts a quarterly assessment of network activity and annual non-disruptive penetration testing. As the network is usually pretty quiet, the metrics used to evaluate security performance are audit log activity and lack of incidents (which for PenSource implies that the security system is effective). Audit logging verifies whether people are within the security boundaries (access controls) assigned to them. Most of the incidents that arise are false positives.

Journal of Information Technology Case and Application Research 2012.14:47-73.

4.4.9 Implementation Methodology

PenSource employs the Cisco security implementation methodology whenever adopting a new security solution. This methodology consists of four phases: Design, Prototype, Trial Deployment, and Full Deployment. Ideally the solution is prototyped in the lab and tested before implementation. Currently, PenSource is using non-critical production systems to prototype and test the solution prior to trial and full deployment.

5 SECURITY, EDUCATION, TRAINING, AND AWARENESS

PenSource does not have a security education, training, and awareness program in place. The company just ensures that everyone has the right software and tools on their systems.

6 CONTINGENCY PLANNING

During the past month, Kevin Galbraith, an executive from SecAdmin, had many discussions with Mark Goff on PenSource's preparedness to handle unforeseen emergencies in its operations.

In one of these meetings, Kevin asked, "Mark, can you tell us how the infrastructure team is prepared to handle emergencies? These seem important considering your continued success in the business is very much dependent on how we are handling such emergencies when they arise. We do not want one unanticipated event to negatively affect the high reputation we currently enjoy with our clients."

Mark responded, "We consider a business continuity plan to be synonymous with a disaster recovery plan. We are also developing a new disaster recovery plan which takes into account both natural and man-made disasters. The new plan will also include elements of a business continuity plan such as succession plans. Although we host a disaster recovery data center site for our clients, we do not have a hot or cold site of our own. However, work is underway to establish a secondary site of operations. We periodically have a tape backup of our data and have a third party service provider, Iron Mountain, handle pickup and storage." Many other aspects of PenSource's contingency planning came to light throughout Kevin's many meetings.

The findings concluded that PenSource does not have a crisis management plan or a documented alert roster to initiate in emergencies. The company does have an escalation plan, but it is not specific to disaster recovery procedures. Although it is available on the corporate intranet, the existing disaster recovery plan is very limited. One reason for this limitation may be that PenSource does not conduct its own business impact analysis and risk assessment but has a third party do it.

Contingency plans (business continuity, disaster recovery), like all other security documentation are developed by the infrastructure team and updated as needed. In the future, the plan development process may also involve business unit leaders and development teams to better align with corporate goals. Currently there is no formal training on the information outlined in the contingency plans. While the plan may be tested as part of an external audit, there is no formal testing procedure or timeline outlined internally.

The infrastructure team is probably the most familiar with the plan and as a result knows what to do during a disaster. Certain decisions regarding which primary/secondary systems to bring up

Journal of Information Technology Case and Application Research 2012.14:47-73.

during a restore operation, and how engage the escalation plan are difficult to make with the limited amount of information currently available. So far there have not been any major disasters or business interruptions. The last time the contingency plan was activated was due to a maintenance issue with the SAN (Storage Area Network). PenSource has SmartNet contracts in place for the SAN and once it went down, the vendors were contacted with details of the incident. Usually PenSource is required to report issues within four hours of their occurrence and the time taken after that point to resolve the issue depends on the situation.

PenSource understands the need for a business continuity and disaster recovery plan. As a result, it is working on developing a better and more robust and more effective contingency plan.

Journal of Information Technology Case and Application Research 2012.14:47-73.

7 RESEARCH NOTES

SecAdmin, the consulting company conducting the comprehensive security review at Pen-Source was founded in 2000 by Dr. David Schultz, a Professor of Computer Science at Stanford. The company has successfully conducted security reviews in many organizations representing diverse industries. In its final report, SecAdmin typically addresses the following broad areas:

- Evaluation of the Information Security Planning
- Handling of Customer Data
- Security Personnel – organization, responsibilities, reporting oversight
- Security Policies and Standards Governance
- Risk Management Practices
- Security Education Training and Awareness
- Contingency Strategies

In addition, SecAdmin's report typically attempts to answer to the following questions:

1. What are PenSource's strengths in its implementation of security policies and standards?
2. Previous research has pointed out the benefits of using alternative frameworks for information security evaluation such as NIST SP 800-37 (Farn, Lin, & Fung, 2004; Ross, 2007; Herath, Herath, & Bremser, 2010) . What are some of the frameworks that could have been used by PenSource? And what are their relative advantages?
3. Using the responses presented in Appendix C and in the data collected during its consulting engagement at PenSource (materials presented throughout this case), what are some of the areas of improvement for PenSource's Information Security program?
4. What are some specific recommendations to improve PenSource's Security Implementation?
5. Are the security-compliance procedures and mitigating controls in place sufficient for its current business practices? How would they hold in a changing environment of the firm's business?

Employees are often considered the weakest link in information security; but they can be turned into great assets in the effort to reduce risk related to information security. Previous research suggests that security behaviors of employees can be influenced by both intrinsic and extrinsic motivators (Puhakainen & Siponen, 2010). Pressures exerted by subjective norms and peer

behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions (Herath & Rao, 2009). Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, understanding compliance behavior is crucial for organizations that want to leverage their human capital (Bulgurcu, Cavusoglu, & Benbasat, 2010)

Organizations can choose how to integrate information security through planning and structuring of the information security function. The planning and structuring choices of the organization impacts the effective utilization of information security strategies. Studies have found that more mature information security planning integration is positively correlated with more effective utilization of information security deterrence, detection, and recovery strategies (Young & Windsor, 2010).

The idea of user acceptance and its impact on behavior has been studied in some well-known models such as the Technology Acceptance Model, the Theory of Reasoned Action, and the Theory of Planned Behavior. One of the most effective ways to get users to accept plans is by getting the users involved in the planning process (Peffers, Gengler, & Tuunanen, 2003). Users are more accepting of information security measures when they are involved in the process and contributed to the solution (Pattinson, 2007). It is important to study the security compliance at PenSource in light of these research findings.

Journal of Information Technology Case and Application Research 2012.14:47-73.

REFERENCES

1. Abedin, M., Nessa, S., Al-Shaer, E., & Khan, L. (2006). Vulnerability analysis for evaluating quality of protection of security policies. *In Proceedings of the 2nd ACM workshop on quality of protection* (p. 49-52). New York, NY, USA: ACM.
2. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010, 09). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34 (3), 523-A7.
3. CCSP? career certifications & paths (Vol. 2011) (No. April 10). (2011). http://www.cisco.com/web/learning/le3/le2/le37/le54/ learning certification type home.html.
4. Cisco ASA 5500 series adaptive security appliances. (2011). http://www.cisco.com/en/US/products/ps6120/index.html.
5. Cisco intrusion prevention system. (2011). http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html.
6. *Cisco secure ACS appliance overview.* (2011). http://www.cisco.com/en/US/docs/net mgmt/cisco secure access control se\ bibliography{SecurityCase Sub}rver for solution engine/3.3/installation/ guide/appliance/ovrvuap.pdf.
7. *Cisco security monitoring, analysis and response system* (MARS) (Vol. 2011) (No. April 3). (2011). http://www.cisco.com/en/US/products/ps6241/index.html.
8. *Collaboration software for the enterprise? sharepoint 2010 (Vol. 2011)* (No. May 1). (2011). http://sharepoint.microsoft.com/en-us/Pages/default.aspx.
9. Davis, D. (2008). *What is AAA and how do you configure it in the Cisco IOS? (Vol. 2011).* http://www.techrepublic.com/blog/networking/ what-is-aaa-and-how-do-you-configure-it-in-the-cisco-ios/664.
10. Dhillon, G., & Torkzadeh, G. (2006, 07). Value-focused assessment of information system security in organizations. *Information Systems Journal,* 16 (3), 293-314.

11. Farn, K.-J., Lin, S.-K., & Fung, A. R.-W. (2004). A study on information security management system evaluationassets, threat and vulnerability. *Computer Standards & Interfaces*, 26 (6), 501.
12. *Fishnet security — vulnerability assessment and penetration testing* (Vol. 2011) (No. March 24). (2011). http://www.fishnetsecurity.com/Service/Consulting/ Security-Assessment/Vulnerability-Assessment-and-Penetration-Testing.
13. Herath, T., Herath, H., & Bremser, W. G. (2010, Winter2010). *Balanced scorecard implementation of security strategies: A framework for it security performance management. Information Systems Management*, 27 (1), 72-81.
14. Herath, T., & Rao, H. R. (2009, 05). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47 (2), 154-165.
15. *Microsoft SQL server 2008 R2 — database management system (Vol. 2011)* (No. April 18). (2011). http://www.microsoft.com/sqlserver/en/us/default.aspx.
16. *Nessus product overview.* (2011). http://www.tenable.com/products/nessus/nessus-product-overview.
17. Pattinson, M. R. (2007). How well are information risks being communicated to your computer end-users? *Information Management & Computer Security*, 15 (5), 362-371.
18. Peffers, K., Gengler, C. E., & Tuunanen, T. (2003, Summer2003). Extending critical success factors methodology to facilitate broadly participative information systems planning. *Journal of Management Information Systems*, 20 (1), 51-85.
19. Puhakainen, P., & Siponen, M. (2010, 12). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34 (4), 767-A4.
20. Ross, R. (2007, 08). Managing enterprise security risk with NIST standards. *Computer*, 40 (8), 88-91.
21. *Service desk software solutions with numara footprints (*Vol. 2011) (No. April 22). (2011). http://www.numarasoftware.com/footprints/service desk software.aspx.
22. Whitman, M. E., & Mattord, H. J. (2010). *Management of information security (3rd Edition ed.).* Boston: Course Technology.
23. Young, R., & Windsor, J. (2010, 01*). Empirical evaluation of information security planning and integration. Communications of AIS, 2010* (26), 245-266.

Journal of Information Technology Case and Application Research 2012.14:47-73.

ABOUT THE AUTHORS

Shaila Kuchibhotla currently works as a Business Analyst at the Great American Insurance Company in Cincinnati, Ohio. Shaila received her masters degree in Business Informatics from Northern Kentucky University. As part of her graduate program, she worked with several companies in the Northern Kentucky/Cincinnati area, evaluating their existing systems and processes and identifying different ways to leverage information systems in order to better support key business objectives. Her areas of research interest include IT Project Management, Information Security, Database Design, and Business Process Analysis.

Dr. Frank Braun is an Assistant Professor of Business Informatics at the Northern Kentucky University. He specializes in IT governance, Information security, IT strategy and Project leadership. Dr. Braun has over 20 years of industry executive level IT management and consulting experience. His research domains include organizational reliability, project leadership, knowledge collaboration, and innovative techniques with instructional technology. He earned an applied research Doctorate in Management from the Weatherhead School of Management at Case Western Reserve University.

Dr. Vijay Raghavan is an Associate Professor in the Department of Business Informatics at the Northern Kentucky University. He also serves as the Director of the Master of Science in Business Informatics (MBI) program. He received his Ph.D. from the Kent State University. His research interests are in the areas of software-development processes, use of information technology in healthcare, and issues of project management. He has consulted with leading firms such as Johnson and Johnson, Cinergy, and Square D in the areas of database design and applications deployment. He has published in the *Information Resources Management Journal, Journal of Information Technology Theory and Applications, International Journal of Healthcare Delivery and Reform Initiatives, Journal of Systems Management, Journal of Information Technology Management, Journal of Information Technology Case and Application Research and Managing Software Development.*

Journal of Information Technology Case and Application Research 2012.14:47-73.

APPENDIX A: INFORMATION SECURITY ARCHITECTURE

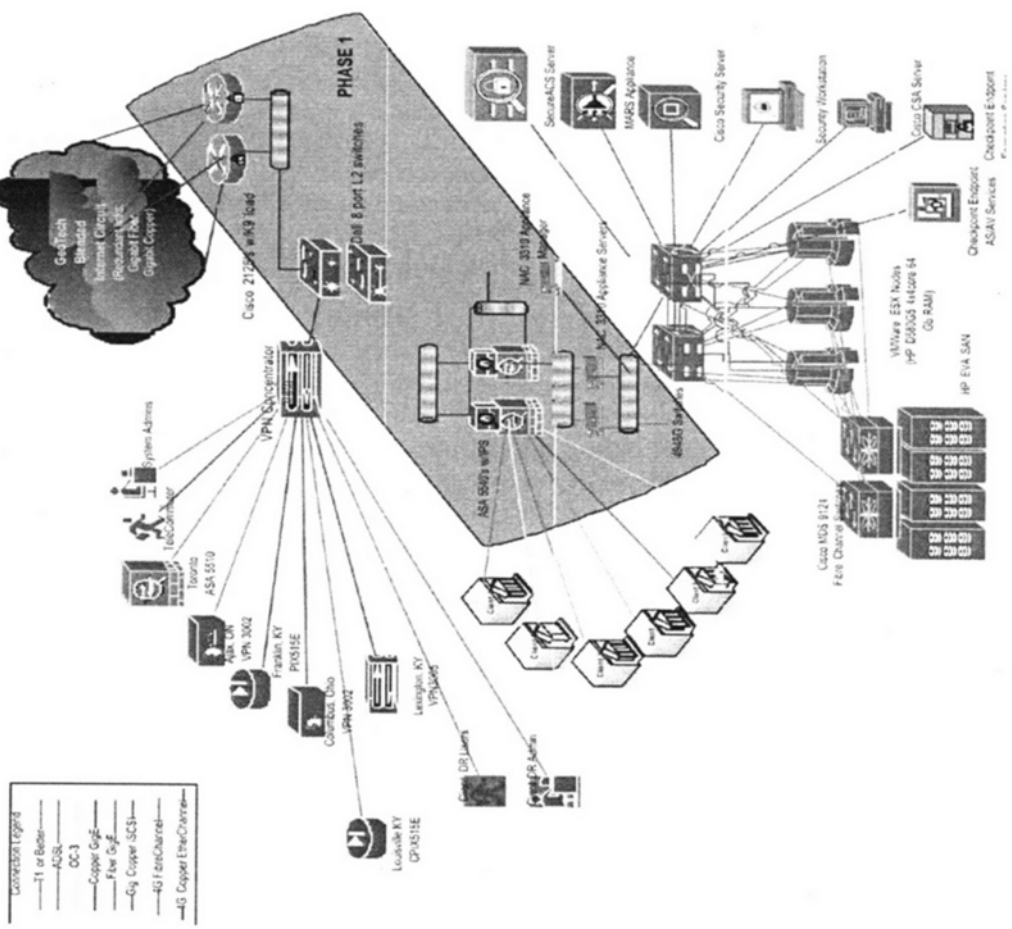

Figure 1: Information Security Architecture

Journal of Information Technology Case and Application Research 2012.14:47-73.

APPENDIX B: COLOCATION FACILITY OVERVIEW

B.1 Facility Overview

The PenSource data center that hosts the client disaster recovery site is collocated at GeoTech, which is located in Franklin, KY at the Business Park. The GeoTech 76,000 square foot facility features:

- Over 20,000 square foot of secured, monitored raised flooring.
- 24x7x365 assistance.
- Trained and professional Network Operations Center (NOC) staff who oversee the security and performance of the facility with state of the art monitoring and surveillance tools.

GeoTech's facility is a carrier neutral facility, which allows private and public telecommunications offerings with over 23 Gigabits of Internet bandwidth currently active over three Tier 1 providers. GeoTech ensures that their facility is audited and maintains yearly SAS 70 Type II compliance. The PenSource data center is housed in a secure cordoned cage, hosts the critical PenSource internal servers which contain sensitive intellectual property, other PenSource hosted client applications and disaster recovery sites.

B.1.1 Infrastructure

GeoTech's SAS 70 Type II facility has been designed to provide stability and reliability for their business. With over $30 million dollars invested, the data center infrastructure can support the necessary cooling, power and protection needs.

Power PenSource will be able to take advantage of GeoTech's redundant power with their unique power infrastructure. Two separate feeds from the energy company Xcel Energy feed into GeoTech's facility from the Surrey Ridge substation. Each power feed is routed through a separate bank of Uninterruptible Power Supply (UPS) units and backed by diesel generators.

GeoTech's power infrastructure uses:

- GeoTech's power infrastructure uses:
- Dual Megawatt+ capable diesel generators.
- Nine (9) Powerware UPS modules which provide power in the event of commercial power loss.
- Automatic transfer switches for all power sources to ensure smooth transitions to and from commercial power.
- A 24x7 on site NOC to monitor the power.
- Monthly full load tests on critical power infrastructure.

Power is fully conditioned by the UPS units to ensure that the power delivered to the disaster recovery site equipment is clean and free of defects. This protects the disaster recovery site from brownouts and surges that sometimes occur with standard commercial power and can cause damage to sensitive electronic equipment.

Journal of Information Technology Case and Application Research 2012.14:47-73.

Power is also monitored by multiple power monitoring points down to the individual power circuit level. This allows GeoTech's Data Center Operations and Network Operations Staff to monitor power flow, bus capacity and health of UPS units before an issue occurs. Individual power circuits are connected to intelligent power distribution systems that report usage back to a robust reporting system. This allows PenSource to get reporting on power usage and address any power consumption issues before it becomes costly.

All colocation customers have the option of having power provided from both of GeoTech power feeds delivering truly redundant power. All power is fed from above head power busses which allow the disaster recovery site to have power provisioned in as little as a few hours compared to several days with traditional power systems.

HVAC GeoTech's colocation and managed hosting facilities are built with redundant cooling and humidification units. Their cooling systems are separated into two systems. The first system, which provides cooling, includes ten (10) 26-ton Stulz air-handling units (AHUs) which provide N+1 redundancy. Six (6) DataAire Aire Flow and one (1) Leibert AHU power the second cooling system that provides cooling to the second cooling system, which supplies managed hosting environment.

Humidification is handled by a series of ultrasonic humidification units. Ultrasonic humidification provides an efficient method for evenly distributing humidity throughout the data center.

In addition to the equipment in place, GeoTech has a highly engineered airflow structure in place that forces cool air through the front of their equipment and reclaim the heated air as it exits. This is done with strict adherence to hot-and-cold isles within the data center.

Fire Detection and Suppression GeoTech's data center uses a multi-zoned above and below detection system. Their Network Operations Center (NOC) monitors any alarms internally and externally by a third party.

In the event of a fire, the fire suppression system is a dry pipe, pre-action system that will not pressurize until at least two (2) monitors are triggered. Should the fire system be engaged, it will only disperse in a tightly localized area directly affected by the triggered monitors.

Environmental Monitoring GeoTech has invested heavily in state of the art monitoring systems that monitor power, HVAC and other environmental controls. These monitoring systems are constantly displayed within our NOC and are backed up by thorough, regular physical walkthroughs that are performed by NOC and facilities personnel.

If trouble is detected, audible and visual alarms occur. NOC and facilities staff responds immediately to resolve any environmental situations. We also notify any vendors that have responsibility for systems to ensure that all issues are resolved completely and thoroughly.

Security GeoTech's Network Operations Center (NOC) is on site and manned 24x7x365. NOC personnel are trained to handle all aspects of security for the facility.

Physical access to all data center floor space and network meet me rooms is secured with a combination of digital camera, proximity card and biometric scanners. Upon arrival to GeoTech's facilities, customers and visitors must contact the NOC in order to gain access to the secured "man-trap" area. GeoTech require three factor authentication requiring a photo id to proceed past the "man trap", authenticated card key and biometric hand scan to gain access to the data center. Customers and visitors must then provide photo ID to receive a proximity badge and be checked into the facility. Only personnel that have been pre-authorized by the customers designated contact are given proximity badges and allowed access.

All activities are monitored via GeoTech's strategically located video cameras which are monitored and recorded to a Digital Video Recorder and then permanently archived to DVD. More than sixty-four motion activated digital cameras monitor data center entrances, data center space, and all areas of critical infrastructure. This includes cameras that line each and every row of cabinets in the main data center and strategic cameras for cage colocation customers. The cameras are motion activated and all images are displayed on a series of monitors within the NOC. Every twenty-four hours, all video is archived to DVD and stored indefinitely.

NOC and facilities personnel perform regular, thorough walkthroughs of the entire facility. These walkthroughs include areas such as the roof, outside perimeter of the building, data center space and vital operations areas. During this time, the NOC staff confirms that all security measures are intact, and that there are no operational abnormalities.

B.1.2 Network

GeoTech customers have access to 23 Gigabit of Internet access and the ability to connect directly with other telecommunication carriers.

Network Multi-homed bandwidth, where a business has access to more than one Internet carrier, can be the difference between near 100% uptime and an embarrassing (and expensive) outage. GeoTech has developed their premium network a blend of top IP carriers that are multi-homed to provide clients with a stable, redundant solution. A multi-homed network gives a client the flexibility to withstand carrier outages or performance problems as they receive bandwidth over multiple carriers automatically. GeoTech's premium network is provided by default to all colocation and managed hosting customers.

Unlike providers that limit to a single carrier in order to control their costs, GeoTech's premium network allows performance to drive how data reaches the users. Their network uses a device that monitors network health from the data center to the Internet. It probes their carriers and measures latency and packet loss. With several hundred route changes per minute, data is able to take the best route to their users.

Carrier Neutral GeoTech is a carrier neutral facility. A variety of telecommunications carriers have a presence that can be leveraged for their Internet or private line access.

Journal of Information Technology Case and Application Research 2012.14:47-73.

Resilient Data Center Network built on Cisco technology; GeoTech delivers data from their premium network to PenSource data center through redundant border, core, access and distribution layers.

All GeoTech network equipment is professionally managed by a team of certified Cisco network engineers. Regular monthly and quarterly maintenance is performed on all devices ensuring that they are up to date with the latest hot fixes and patches. The ability to communicate is backed by GeoTech service agreement with Cisco and on-site spares for equipment.

GeoTech offers a 99.999% Network SLA, commonly referred to as five-nines. They believe strongly in taking proactive maintenance to ensure your uptime and availability and aggressively work to ensure that clients never have to think about their SLA.

Journal of Information Technology Case and Application Research 2012.14:47-73.

APPENDIX C: INFORMATION SECURITY ASSESSMENT QUESTIONNAIRE

About the Company

Company Name	PenSource, LLC
Industry	Software Development Government/Private Pension Systems
No. of Employees	150
Vision Statement- Describes what the organization would like to become in the future (long-term goals)	N/A
Mission Statement- Describes purpose of organization, why it exists and what it does	PenSource is a global technology solutions company that delivers dynamic, purpose-built IT solutions to the public pension market. We partner with our clients to create pension systems that solve unique business problems and respond to complex, frequently changing environments. We help our customers realize their visions. We drive those visions into action.
Company Values- Principles and priorities that define organization's culture	N/A

Security Planning

Does your company have an information security strategic plan?	☐Yes ☑No
Which of the following are included in the plan	☐Major Security Stakeholders ☐Mission/Vision for Information Security ☐Core Values ☐(Desired) Strategic Outcomes ☐Key initiatives ☐Budget ☐Security Analyses
Are there additional sections in your plan that is not listed above? If so, please describe:	N/A
How does your organization operationalize the strategic plan?	☐Short-term security project plans (1yr to 3yr) ☐Day-to-day operational plans ☐Security policy implementation ☐Security training and awareness

What is the primary goal of information security in your organization?	☐Reduce Risk ☐Add Value to Business ☑Protect Assets (Confidentiality, Integrity, Availability) ☑Threat Detection & Prevention ☑Meet Client Requirements ☑Compliance with Government Regulation

What percent of your IT budget is allocated to security?	☐>75% ☐ 50-75% ☐25-50% ☑ 0-25%
Does your company have an information security organization? ☐Yes ☑ No	☐ The board of directors or audit committee provides oversight for the security function ☐ Information security roles and responsibilities are clearly defined, documented, and address separation of duties ☐ A security contact has been designated at each company site or facility ☐ The name and contact information for the security contact has been communicated for users ☑☐A third party service provider handles some or all of the security function
How many members of the IT department are responsible for security functions?	2
How many members from business divisions are responsible for security functions?	0
Does your organization implement a specific governance framework	Yes No
Name the governance model or framework employed:	NA
Who is responsible for the security function? *(involved in developing and implementing information security program, and ensuring its success)*	☑**Business:** ☐Executives (CFO, COO, etc.) ☑Managers ☐Data Users ☐Data Owners ☑**IT:** ☐Executives (CIO, CSO, etc.) ☑Security Managers ☑IT Managers ☑Infrastructure Team ☑Security Technicians ☑Developers

Journal of Information Technology Case and Application Research 2012.14:47-73.

Journal of Information Technology Case and Application Research 2012.14:47-73.

Security Configuration Management

Is there technical configuration documentation for technologies or major business applications in your organization?	☐Yes ☑NO
Technical security configuration documentation exists for:	☑Firewalls ☑Routers ☑Operating Systems ☑Infrastructure Applications (e.g. IIS, Exchange) ☐Other Business Applications (please list below)
If applicable, please list two business applications for which configuration documents exist:	N/A
Technical security configuration documents are reviewed:	☑Once a year ☐Twice a year ☐When new vulnerabilities are identified ☐Not reviewed at all
Are your systems configured to provide only essential capabilities and prohibit the use of specific functions, ports, protocols, or services?	☐Yes ☑ No

Physical & Environmental Security

Does your organization have physical security controls in place? ☑Yes ☐No	☑A security perimeter has identified and documented, which includes computer rooms, media storage rooms, data centers, etc. ☑A current list of personnel with authorized access to these facilities is maintained ☑The list is periodically reviewed and approved The following authorization credentials are used: ☑ID Badges ☑Smart Cards ☑Biometric Access ☑Other ID Cards (e.g. Driver's License) Some or all authorization credentials are required for: ☑Employees ☑Clients ☑Business Partners ☑Vendors ☑Visitors

Journal of Information Technology Case and Application Research 2012.14:47-73.

	☑Surveillance cameras are used to monitor premises ☑Security guards verify credentials before allowing access to facilities ☑Electronic systems verify credentials before allowing access to facilities ☑Physical access to information transmission lines (cables, ports, etc.) is restricted and controlled to prevent eavesdropping or tampering ☑Computer, media storage, and telecom rooms are secured and restricted to authorized personnel ☑Computers are physically secured with lock devices ☑Disposal of computer systems and media storage devices is handled in a secure fashion ☑Remote locations have the same physical security
Does your organization maintain access logs?	☑Yes ☐No
What data do the logs record ?	☑Name of visitor and company ☑Signature of visitor ☑Form of identification ☑Date of access ☑Time of entry/departure ☑Purpose of visit ☑Person or organization being visited
Other physical controls include:	☑Power equipment and cabling is protected from damage and destruction (accidental or intentional) ☑Power can be remotely shut off for specific facility (server room) that may be malfunctioning (due to electrical fire) or threatened (by water leakage) ☑Short-term uninterruptible power supply is in place ☑Automatic emergency lighting is activated in the event of a power outage or disruption to cover exits and evacuation routes ☑Fire detection and suppression systems is in place ☑Monitors and maintains acceptable levels of temperature and humidity ☑Water leakage/damage prevented against by ensuring access to master shutoff valves and regular maintenance

Personnel Security

Are individuals screened prior to being hired by your organization?	☑Yes ☐No
What type of screening is conducted?	☑Identity Checks ☑Education/Credential Checks ☐Previous Employment Verification ☑Reference Check ☐DMV Records ☐Drug Testing ☐Credit Checks ☐Civil/Criminal Court History
Do new hires undergo orientation to make them understand policies, procedures, access levels, etc.?	☐Yes ☑No
Which types of screening are conducted for third-party security personnel (consultants, temporary, workers, etc.)	N/A

Which types of screening are conducted for third-party security personnel (consultants, temporary, workers, etc.)	N/A
When an employee is terminated the organization:	☑Terminates system access ☑Conducts exit interviews ☑Ensures return of organizational property (keys, ID) ☑Changes office/file cabinet locks ☑Revokes keycard access ☑☑Removes employee's personal effects ☑Escorts employee from the premises
Which termination activities are conducted for third-party security personnel (consultants, temporary workers, etc.)	N/A
Which of the following personnel controls does your company use?	☑Separation of duties ☐Two-person control and review ☐Job rotation ☐Mandatory Vacation ☑Need-to-Know based access to data

Logical Access Controls

Does your company enforce a password management process? ☑ Yes ☐No	☑Unique username and password required for user authentication ☑Users are required to change passwords every: ☐30 days ☐60 days ☑90 days ☐Other-Pease specify: ☑Password cannot be refused
Are connections from laptops, mobile devices, and remote users into the company's network secured? ☑Yes ☐No	☑Advanced authentication is in place for remote access ☑Remote access is limited to only those applications needed ☑Remote users must have personal firewall to connect using VPN ☐VPN software is configured to prevent users from accessing corporate network while accessing the internet
Does your company have a process for managing user accounts? ☑Yes ☐No	☐There is a documented process to approve new accounts and modify privileges ☑User privileges are based on job function ☑User privileges are based on business unit ☑User privileges are revoked on termination ☐Users are required to verify their identity prior to a password reset User privileges are reviewed: ☐Annually ☐As needed ☐Not reviewed
Is encryption used to protect sensitive data? Yes No	☑Public/Private keys are used for encryption of sensitive data ☑128-bit encryption products/algorithms are used ☑Database encryption is used for sensitive information (SSN, credit card data) ☑Passwords are encrypted ☐File encryption is used for locally stored data
Is access to data based on a data classification scheme?	☑Yes ☐No
What is the classification scheme? *(e.g. public, private, internal)*	**Public, Internal Use Only, Confidential**

Journal of Information Technology Case and Application Research 2012.14:47-73.

Security Technologies

Which of the following security technologies do you have in place?	☑Firewalls ☑Intrusion Detections and Prevention Systems ☑Remote Access Protection ☑Wireless Networking Protection ☑Scanning and Analysis Tools ☑Encryption ☐Dial-up Protection ☑Virus Protection ☑Internet/DMZ
List the specific products your organization uses for each of the above technologies (e.g. Cisco NAC)	Cisco ASA Devices, MARS appliances, NAC Clean Access appliances, Cisco Inline IPS
Check all that apply:	☑Virus definition files are update on servers, workstations, and laptops: ☑Hourly ☑Daily ☑Weekly ☐After an outbreak ☑If an outbreak occurs, employees are alerted with actions to be taken ☑Email attachments, downloads, etc. are pre-screened for viruses by network filtering devices ☑Internet accessible systems are tested for vulnerabilities before being placed into production ☑All essential protocols are securely configured (DNS, SMTP, FTP, etc.) ☑Host based firewalls are implemented between segregated networks ☑Server performance metrics are monitored (CPU, memory, etc.) ☑Critical applications on internal networks are monitored 24 x 7 for security violations ☑Systems are scanned for unauthorized software installations ☑Security vulnerability scanning and testing is performed ☑Attack and penetration testing is performed by independent third party ☑Critical systems receive full security testing before deployment ☑Staging, test, and development systems kept separate from production systems ☑Password protected screensavers activate after a pre-determined period of inactivity

Journal of Information Technology Case and Application Research 2012.14:47-73.

Compliance & Vendor Management

Does your company have a program in place to periodically test security controls? ☑Yes ☐No *Can be internal/external audits or security consultations*	Security assessments include: ☑External specialists perform penetration testing ☑Automated vulnerability scanners ☐Policy compliance checking tools ☑Performance tools ☐Modern sweeps ☐Source code comparison tools ☑Secure configuration checkers
Does your company maintain system logs? ☑Yes ☐No	☑Logs are stored securely in a central location ☑A copy of the logs is stored ☐The copy is located offsite Logs are maintained for: ☑Internal connections ☑Access attempts ☑Critical applications ☑Internal network devices (firewall, IDS, etc.) Logs are reviewed for security events: ☑Daily ☐Weekly ☐After an outbreak ☑Using automated tools ☑By trained personnel
What government regulations is your organization required to be in compliance with? Please list:	N/A
Does your company enforce security standards for third parties that connect to your network? ☑Yes ☐No	☑Requests for third party connections are reviewed before approval ☑Risk assessments performed on third parties that request access ☑Third party connection monitored for security events
Do third party contracts include security provisions? ☑Yes ☐No	Third party contracts include: ☑SLA that specifies security requirements and responsibilities ☐Provisions for compliance with regulations (GLBA, HIPPA, etc.) ☑Right to audit clause ☑Procedures for escalating security events
Do third party contracts include security provisions?	Third party contracts include: ☑SLA that specifies security requirements and

Journal of Information Technology Case and Application Research 2012.14:47-73.

☑Yes ☐No	responsibilities ☐Provisions for compliance with regulations (GLBA, HIPPA, etc.) ☑Right to audit clause ☑Procedures for escalating security events
Does your company require all vendors to maintain liability insurance? ☑Yes ☐No	Liability Insurance covers: ☑Loss from vendor negligence ☑Loss from breach of security ☑Limits of ☐$0-$100,000 ☐$100,001-$500,000 ☐$500,001-$1,000,000 ☑$1,000,001 and above

Future Improvements

Which of the following areas are you looking to improve in the **near future** (1 year- 5 years)?	☑Access controls ☑Business Continuity ☑Compliance ☑Disaster Recovery ☐Physical Security ☐Personnel Security ☑Security Technologies ☑Security Policy ☐Security Planning ☑Security Training & Awareness
Which of the following areas are you looking to improve in the **long term** (5 years- 10 years)?	☑Access Controls ☐Business Continuity ☐Compliance ☐Disaster Recovery ☐Physical Security ☐Personnel Security ☑Security Technologies ☐Security Policy ☑Security Planning ☑Security Training & Awareness