IT: In Search Of Security Post Katrina/Rita Disaster Preparedness

Mona Ristovv-Reed, University of Louisiana at Lafayette
Ihssan Alkadi, University of Louisiana at Lafayette

ABSTRACT

What has been done to safe-guard the IT infrastructure and the mountains of data from future disaster, both natural and man made? Upgrading existing systems, building safe houses, and duplicating existing systems are some of the methods being utilized by Gulf Coast companies and business. Other options may be to relocate inland, away from natural disaster factors, though still not protected from terrorists, either from within or abroad. This study addresses many of the current problems which linger: unsuitable structures, costly relocation, escalating utility costs, security risks, weak disaster preparedness design, and conventional shortsightedness. Within the study, one can see that IT management is moving toward security, looking at future security as part of today's operational norm. Disasters hit many American companies squarely in the pocketbook, but not a single company surveyed relied on Federal funds to offset losses. Companies, who lost their physical structures, were able to rebuild despite the odds, and two years later are still solvent. This speaks to the management and the spirit of the company itself. This survey will be on-going, gathering information into the future as well as the perspective of the past. What will IT security look like in 2010? We will revisit this issue in real time as the survey results continue.

INTRODUCTION

The research we are currently conducting examines industry and business approaches to disaster preparedness in the Gulf Coast States. Investigation includes information from the past few years, current applications, and future planning. Major oil and gas exploration companies developed intricate emergency plans for personnel safety since Hurricane Ivan; however after the 2005 hurricane season, their plans centered on the computerized systems and their security as well as the oil exploration and production equipment (Santora, 2006). One large retailer, Wal-Mart, found itself at a standstill during Katrina, overwhelmed by the situation in spite of well rehearsed safety and data security plans (Mims, 2006); real estate-tied businesses were completely out of business for extended periods of time with no end in sight (Heavens, 2005). Will American companies and institutions be prepared for the next disaster? We hope this research will help lead to safer, more secure preparation for any types of disaster. We anticipate, both through research and ongoing interviews, a collection of information which can be used as a guide for all companies in the face of future disasters. We expect to both help and enrich commercial companies and public communities with seamless economic continuity and disaster management programs which have already been put in place at several companies and communities. There are several business types which we are in the process of studying, but each will be through the vision of the IT; its efficient protections and utilization of technology in that protection. We generally expected to find risk reduction in several areas, including: hardware backups, IT departments on electrical generators, additional removable external hard drives, added Smart Card security, as well as web access for HR needs (payroll, insurance, email, and interdepartmental operations). We would also hope to find off-site backups, mirrored sites (identical configuration of company's computer systems), and company-issued radio phones to all necessary employees.

METHOD

The research design is exploratory, done with a web-based survey interface, solely with IT departments. Questions in the survey address disaster preparedness for such unpredictable events such as natural disasters, human error, or acts of terrorism. This exploratory research will also utilize available literature in addition to the survey-generated data. We are not using any qualitative approaches (informal discussions with consumers, employees, management) at this time. That will be done at a later date to delve into specific examples.

The results from this research could provide significant insight into an existing dilemma, and enhance economic stability in the Gulf Coast States, if a proactive approach to disaster preparedness is set in place.

The on-line survey was developed as an anonymous link from within the webpage http://www.safesurvey.com. Once the company/institution was on this web-page, it could go directly to the survey by selecting the survey link. The link to this webpage was given to several Gulf Coast business and institutions including: petroleum, insurance, manufacturing, medical, higher education, gaming, retail, non-profit, media, food service, utility, religious, transportation, and government. Initially, each of the companies/institutions was given the link in person, not through an email. This gave them the opportunity to meet the researchers face-to-face. The limitation to this approach was the dependency on the person given the web-address to pass it on to the IT department. Additionally, a follow-up email was sent to each company/business. Finally, the researchers developed a business card with the webpage printed on the card. Each of the companies/institutions was sent a participation request with the Web-card included.

SURVEY DEVELOPMENT

The survey was developed through a literature search, looking for real-time issues concerned with disaster preparedness. Each survey question, other than the general demographics, addresses how these companies/institutions look at their continuity as a sustainable entity in the face of not only past disasters, but how they are prepared for the future. The survey addresses security both within the companies/institutions and externally. The survey itself is a real-time data collection tool. As new data arrives, new reports are issued and new graphs generated. In order to keep continue access to the survey, the researcher committed to monthly charges. This ensures on-going research with no cut-off date. It will be possible to track additional companies for several years, compiling longitudinal research. The longer the research continues the more comprehensive the data will become.

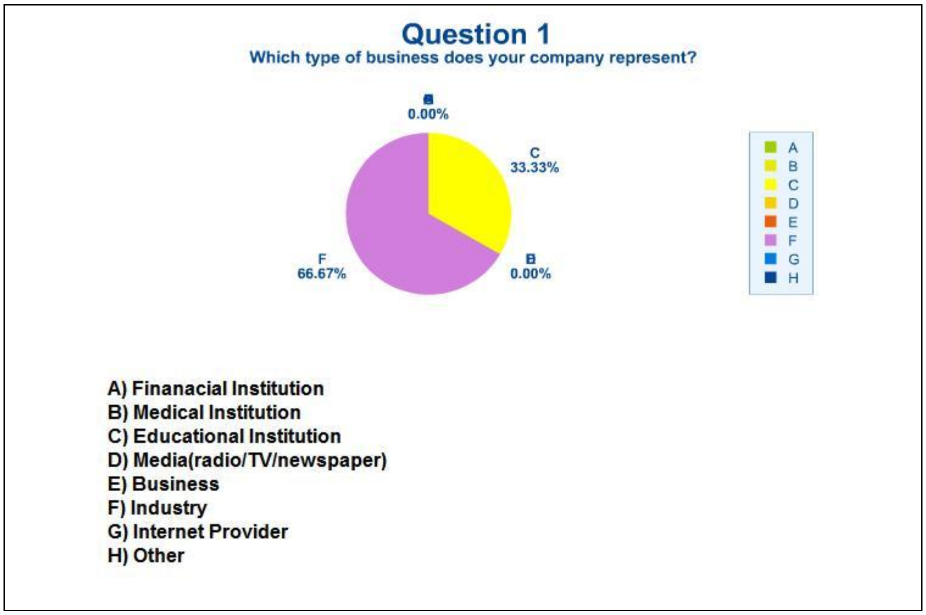
RESULTS

I. The On-Going Results Of The Survey Include 20 Direct Questions

These questions and the responses are shown below.

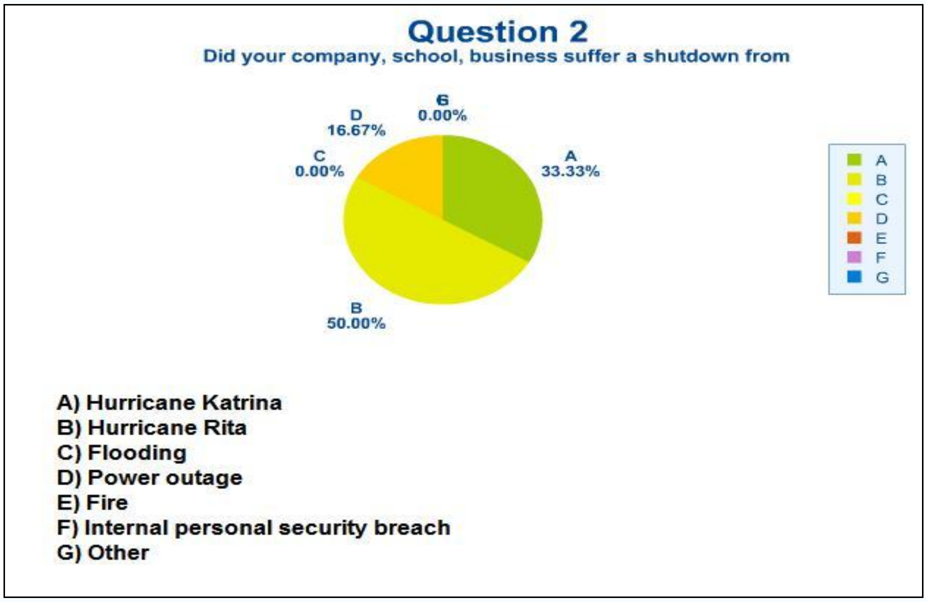
1. What Types of Businesses Participated

The early survey results indicate Industry and Educational Institutions are more readily agreeable to participating in an in-depth survey. Other results are pending.



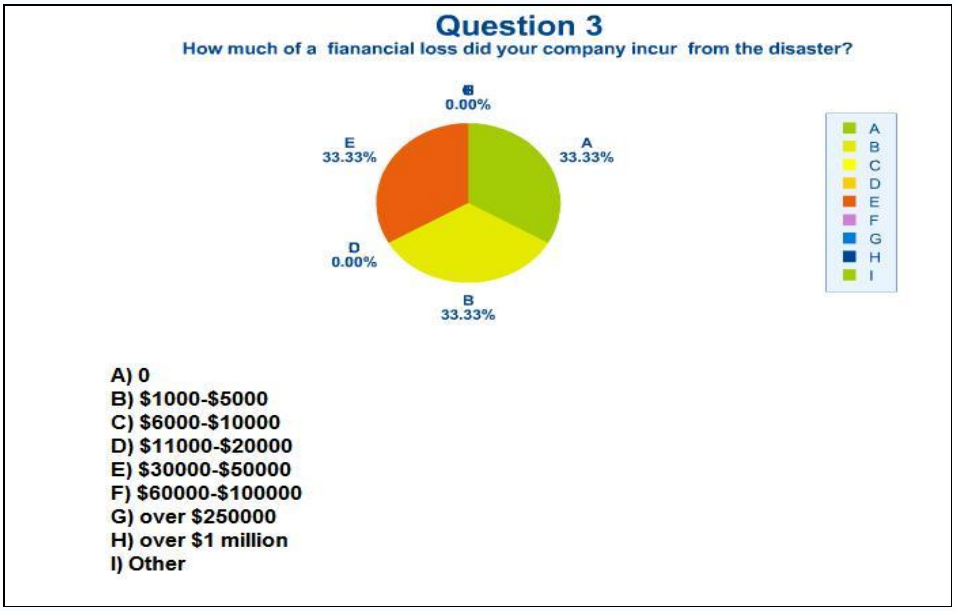
2. Shut Downs

Survey results indicate Hurricane Rita was more often chosen as the prevailing cause of shut downs in the area. Other causes were Hurricane Katrina and power outages, which may or may not have been directly caused by the hurricanes. Often the power outages were in addition to the hurricanes.



3. Financial Losses

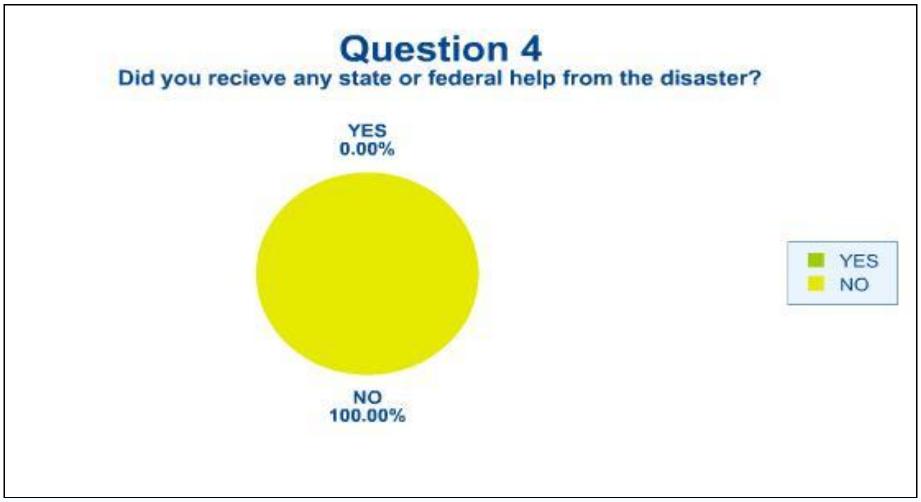
One third of the businesses were able to report no financial losses, however, the other two thirds suffered financial losses often in the thousands of dollars. This was a pattern seen around the Gulf. Hurricanes Katrina and Rita clouted the Gulf with over $66 billion in losses: three times the amount of loss associated with the World Trade Centers (Ashworth, 2007). It is estimated that 40% of the businesses hit by Katrina and Rita will be closed within five years (Jordan, 2006). Even insurance companies took huge hits. While some insurance companies were reimbursed through re-insurance, one of the major companies, Allstate, did not have this safety net and took an almost insurmountable financial hit (Richter, 2006).



4. *Loss Reimbursement*

Often we expect that losses will be covered by the state or federal government if insurance can not. Even with the costs ranging in the thousands of dollars, these particular businesses did not receive any help from either state or federal funds.

The *Economist* (March 17, 2007) reported that only 3% of those who applied for aid have received it in the State of Louisiana. In contrast to this dismal outcome, Mississippi applicants are beyond 78% in closing their applications after receiving funds. Calculating the exact amount that companies/institutions lost during the 2005 hurricanes is an on-going challenge. Even though we have numbers assigned to the losses, many of those come from companies that are seeking assistance to repair or replace lost material. The survey indicates that many companies either did not expect help or chose not to request help. Additionally, applying for insurance loans to rebuild was a two- edged sword; they may receive some of the funding they needed, but it was often at higher rates than they could afford as loan companies feared the delinquency rate would increase in the Gulf Area in general, and the hardest hit metropolitan areas (New Orleans), in particular (Cardwell, 2006) . One more interesting statistic is the loss of employees. Many companies' employees moved on to other areas in America. One example was a small security company out of eastern Texas. Over 40 of his employees were displaced and unable to communicate with their work. New employees had to be hired and trained under the most adverse circumstances and many of the former customers were themselves out of business (Culver, 2006). It was not the governments who stepped up to help employees; rather it was the individual businesses who were involved in keeping the economy going. A survey across six states revealed that 90 percent of the businesses continued to pay and maintain benefits for their employees. Only five percent of the companies reported hurricane related layoffs. Seventy-two percent of businesses kept the salaries of their employees at the Pre-hurricane levels even if they had no work for a period of time, and 95 percent of them did not reduce previously planned raises (City Business, 2006).



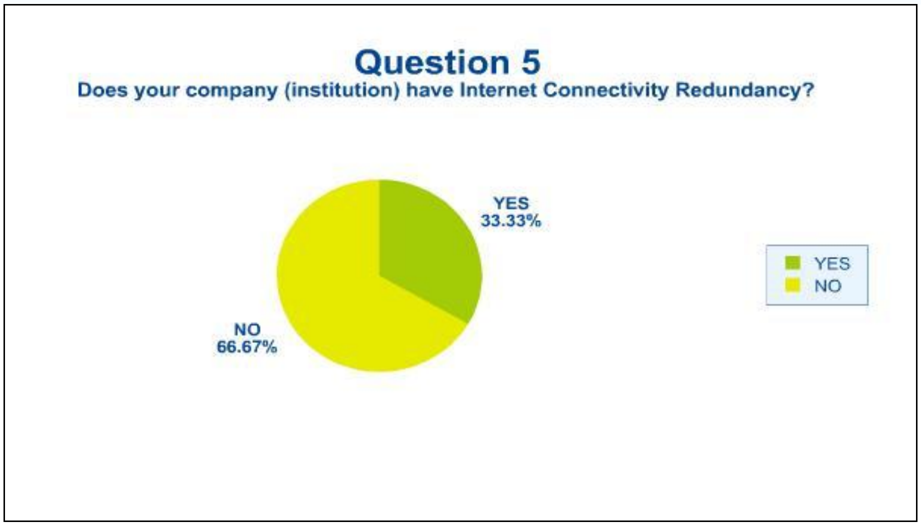
II Security After The Fact

Some Gulf business and institutions have looked at the disasters of 2005 as the proverbial “wake-up call”. It often motivated them to become proactive, to establish safety procedures which would prevent shutdowns and loss of data. The following survey questions address this area of disaster preparedness.

5. Connectivity Redundancy

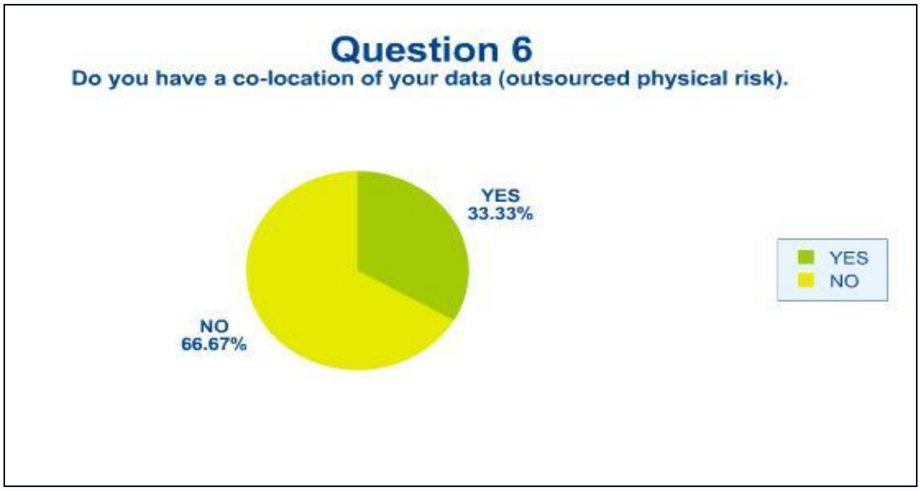
One of the more obvious ways to prevent downtime is having more than one way to connect to the Internet or company Intranets. Often satellite is used in addition to cable, T1, DSL, or ADSL for this purpose. For what ever reasons, this is still a weak area in most companies/institutions in the Gulf States. Perhaps the cost is prohibitive or the technology is unavailable. The more likely reason these businesses do not have connectivity redundancy is answered by Question 5.

Connectivity redundancy is a common technology for very large organizations such as AOL, NYSE, NASDAQ and others of such magnitude, and although smaller companies tend not to use it, it is available for them. One of the common products for this use is the *Fastiron* ® by Foundry (Weekly, 2000): it has been around for over ten years and has build-in redundancy capabilities (Asia Computer,2000).



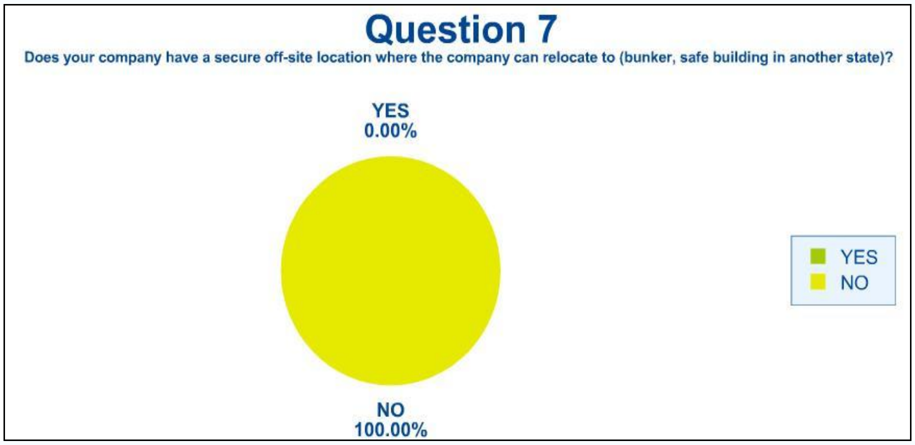
6. Co- Locations

Just as 1/3 of the businesses have connectivity redundancy, one third of them also have Co-Location or outsourcing of physical risk. This allows the business to "continue as normal" in the midst of a disaster. This survey did not require specifics regarding where the co-locations were, but it is assumed they would be out of an adjacent areas which could also succumb to shutdowns.



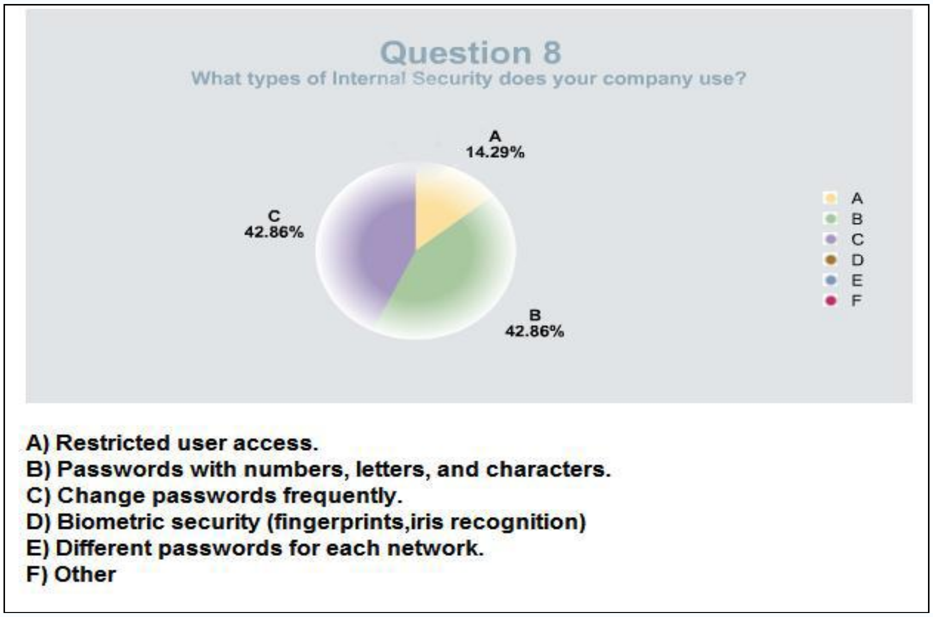
7. Safe Harbor

Physical safety in an actual "bunker-type" location is not part of disaster preparedness for the businesses surveyed. None of these companies had a secure location meant to weather a disaster. Their other choice may have been to evacuate. There were offers for companies to move their data to off-site locations. NovaStar in Southern California offered free off-site data storage to any company in the path of any major storm, free for 30 days (Diana, 2005). NovaStar was proactive, they contacted 225 customers in Rita's path. Data/ADD told their customers to install RAID servers which mirror the main hard drive allowing the IT department to take the hard drive with them upon evacuation. Tulane University lost 20 years of cancer research. They had never computerized older records and their newer medical records were on tape. Some of the tapes could be seen "floating down Canal Street" (Diana 2005). Hibernia Bank (now Capitol One), one of Louisiana's oldest banking companies did use another branch of their bank in Northern Louisiana as the primary back-up, allowing data integrity during the disasters (Bean, 2007).



8. *IT Security within the Company*

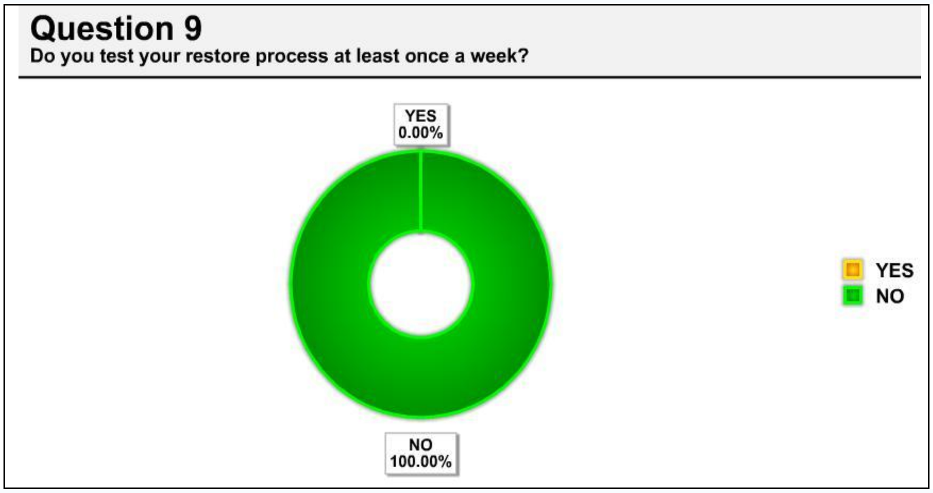
In the face of company espionage, hacking, and other vulnerabilities, many companies have improved their own security policies within from within. According to Patrick McBride (2002), 58.4% of security breaches come from within the company, not externally. Accordingly, many of these security vulnerabilities are due to lack of security expertise rather than maliciousness. To avoid exposure to attack, most common security measures for Internet access were restricting user access, difficult/safer passwords, and frequent changing of those passwords.



A) Restricted user access.
B) Passwords with numbers, letters, and characters.
C) Change passwords frequently.
D) Biometric security (fingerprints,iris recognition)
E) Different passwords for each network.
F) Other

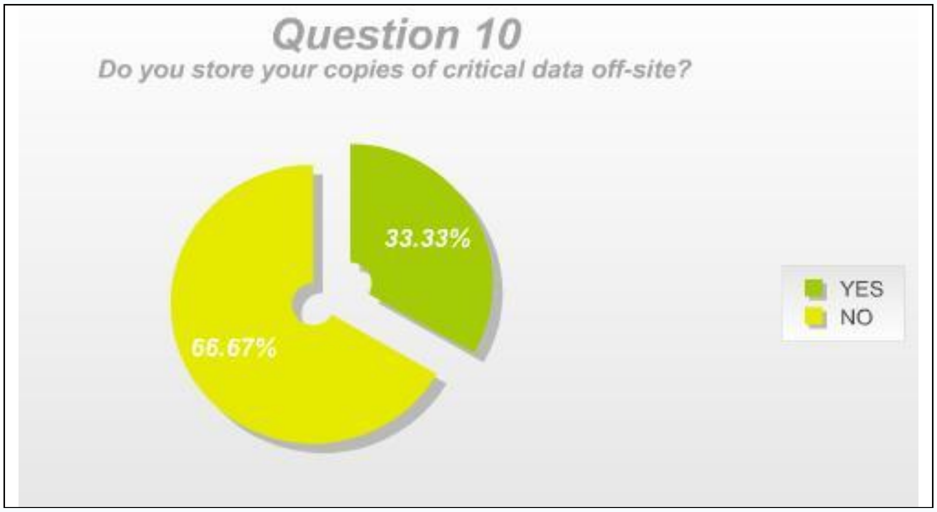
9. *Testing Restore Process*

A common means of preventing down time should be restore-process testing. In this survey, the question was very specific to what is considered an industry-standard procedure, once a week. This was not found as a preventative solution among those responding to the survey.



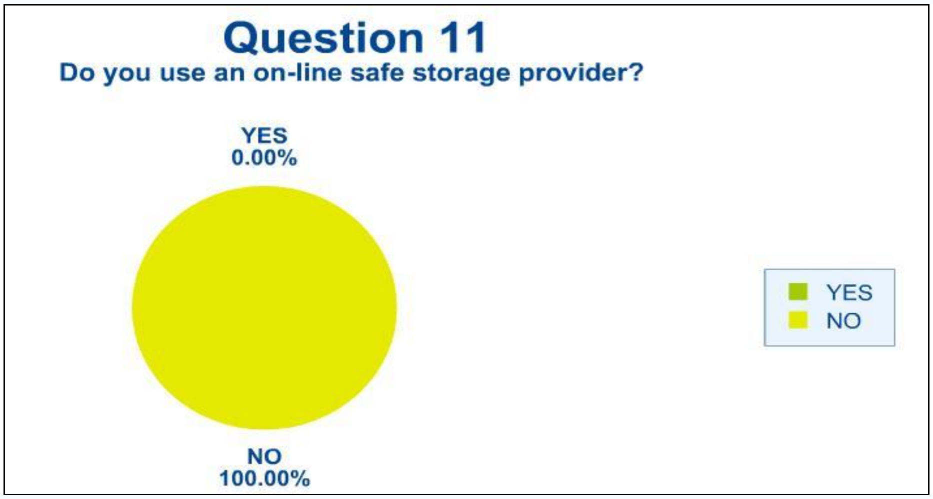
10. *Data Off-Site Storage*

An economical solution to data loss is found with one third of the businesses: off- site storage of critical data. This can be accomplished by storing data tapes or actual external hard drives in a secure off-site area. Some companies back-up to another location in a secure area. This would not work if the Internet were down, which is addressed in survey question No. 11. FEMA advocates companies using technology to preserve data for all types of businesses and homeowners even before the 2005 hurricane disasters (FEMA, 2004). Hibernia bank in Cameron had moved it primary backup site to Shreveport, Louisiana after hurricane Ivan in 2004. This move eventually kept the bank solvent and able to continue working in the disaster areas even when their own steel-walled bank floated away in the powerful surge (Bean, 2007).

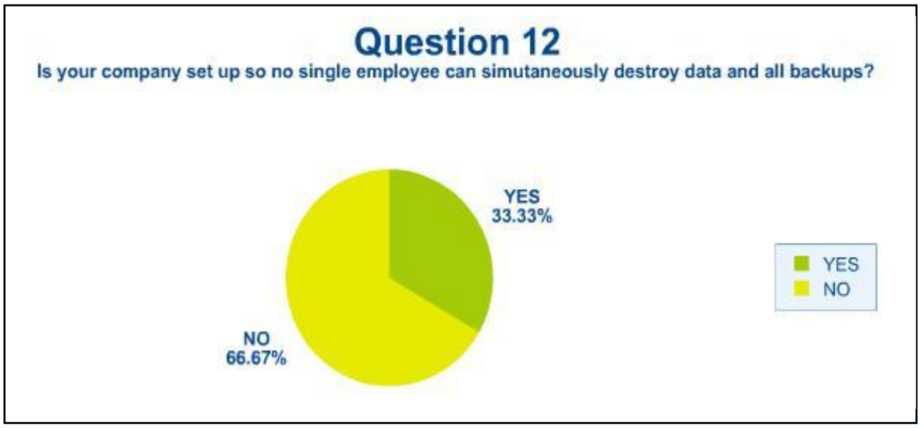


11. On-line Safe Storage Provider

None of the Businesses relied on an on-line Internet provider to store their critical data to. They did store off-site (See Graph 10). When the rate of down time for the Internet is restudied, this is understandable, especially if businesses do not back up their data more than once a week.

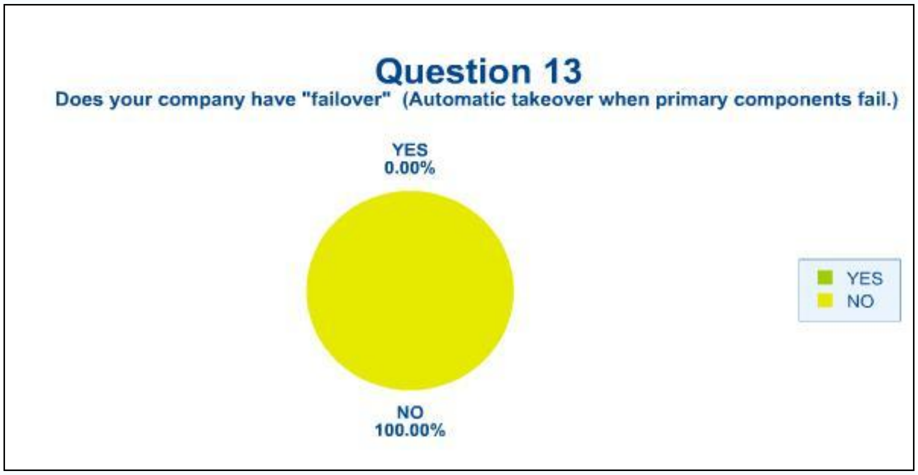


12. *As companies and businesses become more secure, they begin to look within* for internal weaknesses. One third of these businesses took extra care to insure that no single employee had single control over all data and back-ups. This may be one of the more obvious methods of deterring internal problems. Other steps are employee training, and attention paid to employee morale.



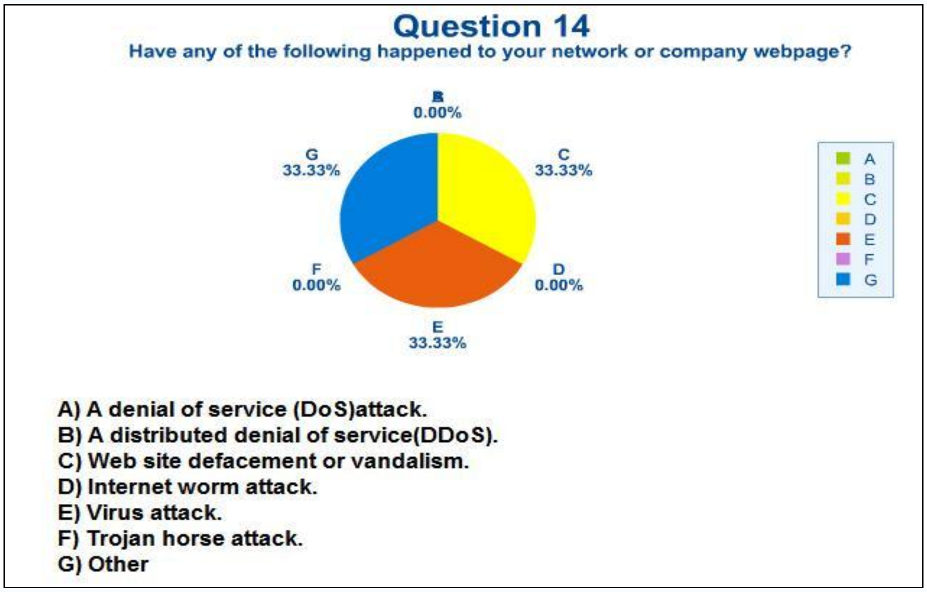
13. *Failover takeover is considered a technical advancement for businesses which are data-dependent.*

None of these companies had failover takeover. This was not surprising for even banks, built with disaster plans in place did not have "failover" ability. Some banks in Southern Louisiana were out of business for several months. Others, like Hibernia in Cameron, delivered checks by car into the hardest hit parishes and exchanged those checks for money from that same car (Beans, 2007).



14. *Attack of Website or Network*

Even with vigilance, many businesses are still susceptible to various attacks, most often these were Web site defacement or viruses. Although vendors are finding weaknesses within their own programs and creating patches accordingly, cyber criminals exploit zero-day flaws before the vendors patch them (Vijayan, 2006). Viruses and worm attacks are less frequent, but only because more Trojan horses and other covert malware are being directed at applications, many of them Web. According to Roger Gumming, "Attackers are increasingly moving toward developing exploit cod with a specific purpose" (Vijayan, 2006).Other vulnerabilities are Microsoft Office and Voice over IP (Keizer, 2006). Both of these applications are common in the businesses and Educational institutions. Criminals also engage in phishing by creating look-alike phony websites that are designed to snag the victim's information. Often times these websites appear to be a bank page or a Pay Pal page. After the information is recorded, they can access a bank card or an on-line Pay Pal accounts (Taylor, 2007). As businesses do more on-line supply acquisition, they become more vulnerable to these types of attacks. Even newer threats are aimed at radio frequency identification (RIFD) and multi-function cell phones (Hayati, 2007). Our survey saw Web site defacement, virus attacks and voice over IP (VOIP).

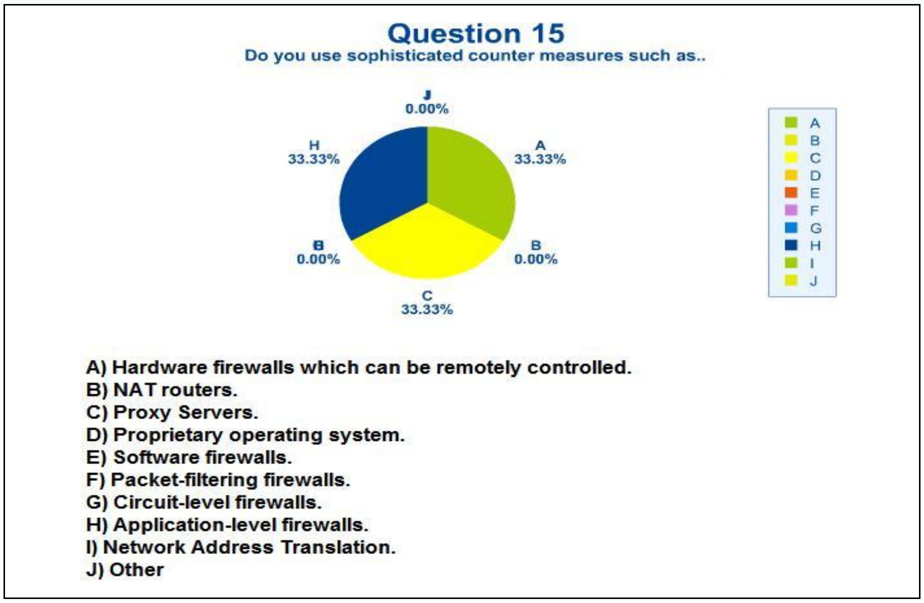

Question 14

Have any of the following happened to your network or company webpage?

A) A denial of service (DoS)attack.
B) A distributed denial of service(DDoS).
C) Web site defacement or vandalism.
D) Internet worm attack.
E) Virus attack.
F) Trojan horse attack.
G) Other

15. *Remote Firewall Management*

IT technology pushes businesses toward innovative responses. Some of these innovations include remote management of firewalls. One of the most versatile of these remote management firewalls includes Sonic Wall®. Proxy servers are used frequently. These give would-be cyber criminals a fictitious web-address rather than announcing their exact web presence.

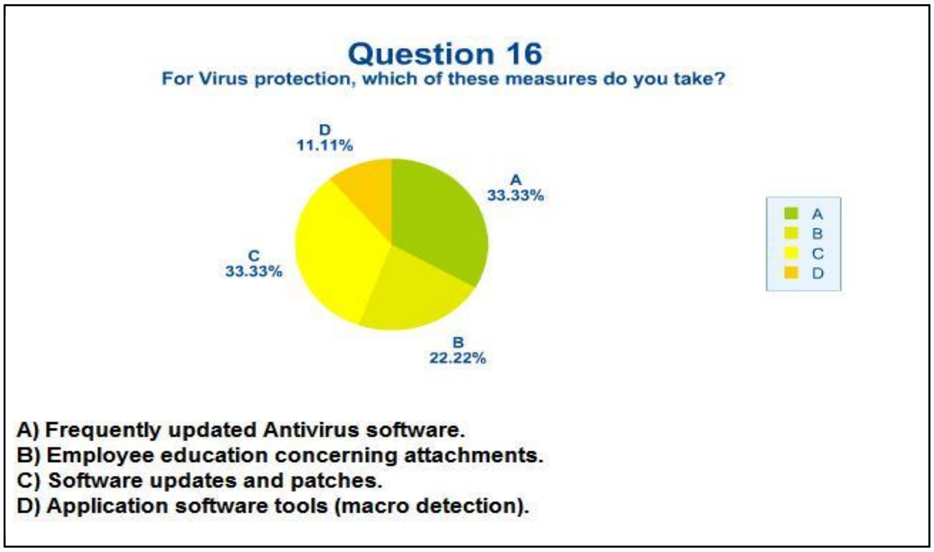

Question 15

Do you use sophisticated counter measures such as..

A) Hardware firewalls which can be remotely controlled.
B) NAT routers.
C) Proxy Servers.
D) Proprietary operating system.
E) Software firewalls.
F) Packet-filtering firewalls.
G) Circuit-level firewalls.
H) Application-level firewalls.
I) Network Address Translation.
J) Other

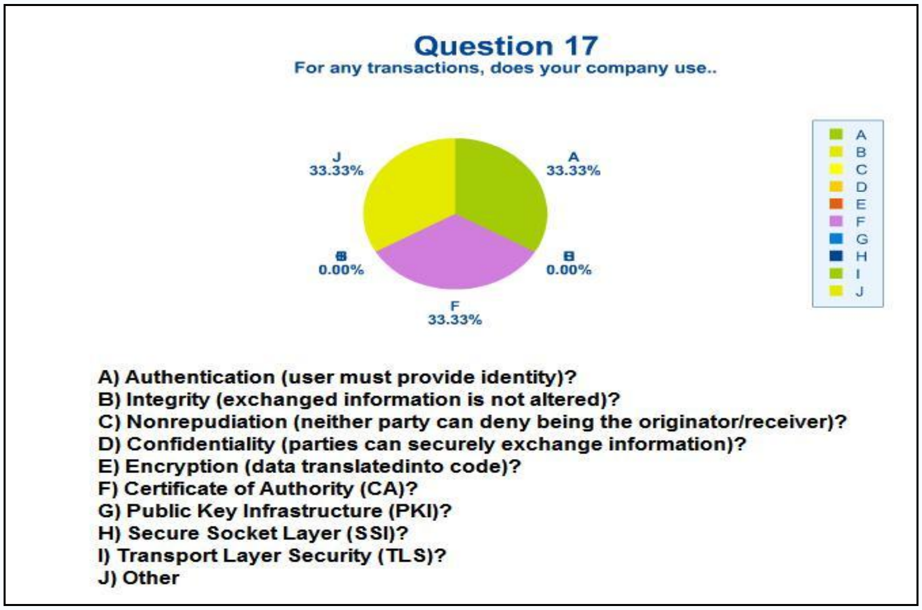
16. *Virus Protection*

One of the most frequently used software applications is virus protection. The competition is fierce as many of the virus protection software companies are only able to develop their products by selling their products first. Mcaffee is the world's largest company in this area, followed by Samantec and a score of others. Virus protection is one of the many types of malware they fight, often bundled with other programs which stake out spy ware, malware, or adware. Technically, these are all viruses, but the most effective software program is never completely effective against this new generation of spy ware (Davis, 2007). To combat today's cyber criminals take complete vigilance and employees training. The latest reports show that anti-virus and anti-malware are usually two months behind and are losing the battle. A shift to "white listing" instead of trying to prevent mal-ware is becoming more the norm with larger institutions. The white listing allows only approved applications and controls access. Additionally, behavior-based anti-malware (learns what types of programs to allow based on the client), is becoming more popular than traditional anti-malware (Fest, 2007) This survey directed the questions around virus protection, but it found that besides frequent virus protection and software updates, employee education was an important consideration among the companies surveyed. Macro detection was also frequently used.



17. Safe Transactions

It is no secret that much of our World's day-to day business in being done via the Internet. With all the threats and the multitude of layers within each company and the many educational institutions, the IT departments must be persevering, persistent, and patient. It is a tough order to fill, but there are systems available which make transactions as safe as possible. Combining firewalls, anti-malware with the authentication and certificate of authority over a transport layer of security (TLS), doing Web business is safer. It is safer, but not entirely safe. Companies and Institutions need to keep their systems secure and compliant to high standards of safety (Lailisan, 2007). They need to use authentication, non-repudiation, encryption and Transport Layer Security for any on-line transactions. One third of our companies/Institutions did just that, but only one third.



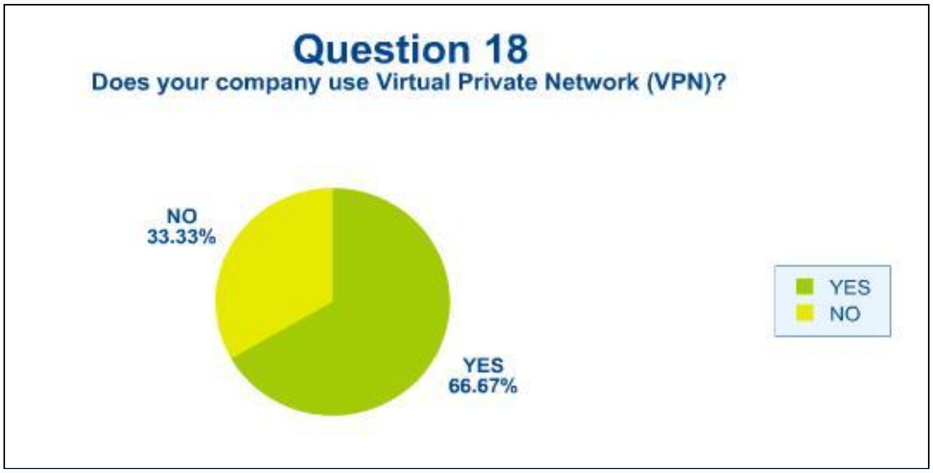
Question 17

For any transactions, does your company use..

A) Authentication (user must provide identity)?
B) Integrity (exchanged information is not altered)?
C) Nonrepudiation (neither party can deny being the originator/receiver)?
D) Confidentiality (parties can securely exchange information)?
E) Encryption (data translatedinto code)?
F) Certificate of Authority (CA)?
G) Public Key Infrastructure (PKI)?
H) Secure Socket Layer (SSI)?
I) Transport Layer Security (TLS)?
J) Other

18. Virtual Private Network (VPN)

VPN is becoming more the norm than the exception in America. As Americans we tend to believe we are more progressive than many nations. A program in Bahrain, "*Broadband Bahrain*" is leading the way, modeling what could be done here in America (Nazimuddin, 2007). Bahrain is offering true broadband to all its businesses and educational institutions. VPN should be considered a proactive arm of every businesses disaster plans. It allows quick, direct, secure, and uncompromised access to data. If VPN is bundled with hardware firewall units, it also has the ability to be remotely accessed and easily managed, an absolute must during a disaster (Kodogy, 2007). Another up and coming feature of VPN is the multi-path routing tree which allows VPN provisioning in the hose model (Poo and Wang, 2007). With multiple paths, a connection request selects available bandwidth more technically and increases its chances of being admitted.

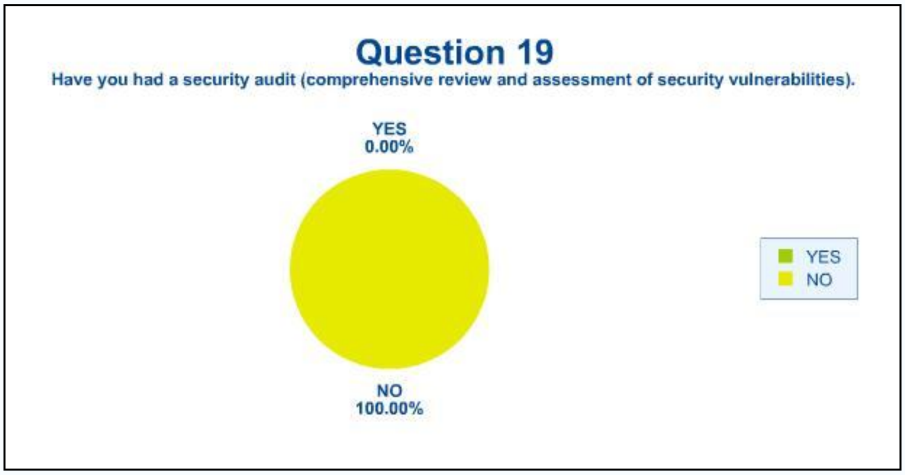


Question 18

Does your company use Virtual Private Network (VPN)?

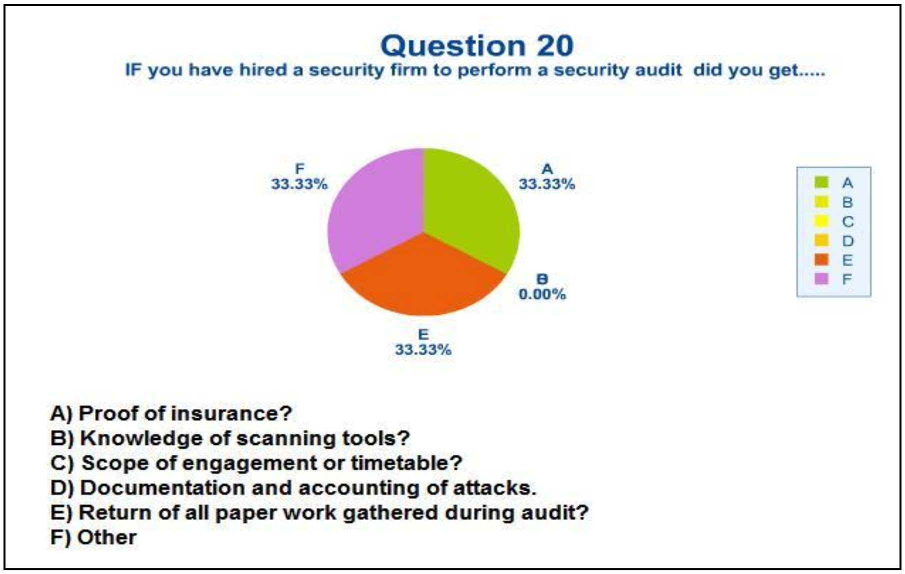
19. Comprehensive Review of Security Vulnerabilities from Within

Almost without question, a comprehensive review and assessment of security vulnerabilities must include employee training. Terry Curran (2005) a consultant in Information Assurance Awareness Programs (IAAP) incorporates legal imperatives from the Patriot Act II and Safe Harbor Acts to design training programs for employees across industries. Under her guidance companies implement programs in a similar fashion to industry itself: awareness of the need, development, training, dissemination of the program. Within the training programs, an internal security community defines the needs of the company. Key internal security- staff is brought into the circle of confidence, but other employees are not out of the "loop" (Hartman, 2005). All employees are made aware of the security risks and trained within their individual level of position. But none of this can work without management support ; and to obtain management support, the IT supervisors need to successfully sell security as the number one priority (Grill0, 2005). An example of a misguided and misdirected system is the tri-department attempted "conglomerate": the Justice, homeland Security, and the Treasury Departments (Fine, 2007). A security audit reveled there is no central control guiding the integrated-network project for American security. This is a debilitating communication gap between the three departments. The Gulf State businesses/Institutions have a weakness in this area which must also be addressed. None of the respondents to the survey have audited their own vulnerabilities within their businesses/institutions.



20. Hiring an External Company for a Comprehensive Security Review

It is often in a company's best interest to hire an impartial outside security auditor. Many businesses are strategically integrated into other companies (i.e. Procter & Gamble and Wal-Mart) and need continue security advances. As the markets become global over diverse political topography, it is imperative that the security amongst them is studied in real time and is continuously upgraded, and always proactive (Westcott, 2007). The testing is thorough, penetrating, and one of the fastest growing computer-related industries. The market in 2006 was a "mere" $2.56 (Moore, 2007). Reports often include an executive summary, risk assessment, cost justification, project scope, findings and recommendations, and a task list based on the client's vulnerabilities. Are the Gulf State companies getting outside security auditors? One third of the companies/institutions surveyed had an external security audit. Hiring outside security auditors allowed unbiased look into each businesses/institutions own security and gives them the opportunity to make adjustment to their systems on this valuable insight.



Question 20

IF you have hired a security firm to perform a security audit did you get.....

A) Proof of insurance?
B) Knowledge of scanning tools?
C) Scope of engagement or timetable?
D) Documentation and accounting of attacks.
E) Return of all paper work gathered during audit?
F) Other

CONCLUSION

Are the Gulf States prepared for another disaster? There have been some changes. Many of the companies are moving in a proactive manner. Some by hosting their data in off-site locations, some by using redundant servers with external, easily movable hard drives; others use VPN and on-line web storage. There are many areas which still need to be addressed, including internal security and insurance for monetary protection from “worst case scenarios”. The Federal Government, through FEMA, has given 47 states monies to develop and set in place pre-disasters plans in the Pre-Disaster Mitigation Program. The main thrust of the program is disaster preparedness. Some of the issues FEMA addresses are:

“Voluntary acquisition of real property (i.e. structures and land, where necessary) for conversion to open space in perpetuity; Relocation of public or private structures; Construction of safe rooms (e.g., tornado and severe wind shelters) for public and private structures”.

(“Design and Construction Guidance for Community Shelters”, FEMA, 2007)

As of May 10, 2007, $292 has been spent on this project.

Has any of the pre-planning been successful? Is the Gulf area more secure; yes, the area in general is moving toward security as individual businesses and institutions recognize the interlocked finances of IT and their businesses in general and the dependency on robust IT security specifically. Time will be the biggest factor and the most significant ally as companies rebuild their financial bases and recoup from disaster-induced losses. They will spend a greater portion on their IT security and enhance their companies’ and institutions’ solvency in doing so. Is this enough? Probably not. Just as the Sarbanes-Oxley Act of 2002 (SOX) was passed in reaction to the disastrous financial collapses, American businesses and institutions need to plan around the **u**nknown impending disaster which could affect, if not demolish their lives as they know them. Too little is too late. The lessons of the 2005 hurricane season need not frighten us, but they should change us into proactive, preventative-type managers of tomorrow’s data.

Keyword Glossary

- Adware: Typically a separate program that is installed at the same time as a shareware or similar program, adware will usually continue to generate advertising
- Authentication: the process of determining whether someone or something is, in fact, who or what it is declared to be.
- Behavior-based anti-malware: behavioral security software which shields the user from ordinary maintenance and administrative tasks while radically increasing the security of their system, using the user's own computer/Internet behavior as the model to match behavior and exclude deviations from the behavior.
- Botnet attack: usually a zombie computer that has been programmed to send viruses out, compromise security and wipe out hard drives internationally.
- Broadband Bahrain: Throughout Bahrain, a nationwide 3G/HSDPA network, to all homes and businesses, even includes wireless broadband services.
- Certificate of authority: (**CA**) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party.
- Co- Locations: the provision of space for a customer's telecommunications equipment on the service provider's premises.
- Company espionage: attempt to gain access to information about a company's plans, products, clients or trade secrets.
- Configuration: arrangement of functional units according to their nature, number, and chief characteristics, includes the choice of hardware, software, firmware, and documentation
- Connectivity Redundancy: Configuring a redundant link to the Internet for businesses.
- Cost justification: providing an economic argument for usability.
- Cyber criminals: criminal activity in which computers or networks are a tool, a target; criminal activity on the Internet.
- Data Collection Tool: different instruments which are used to conduct the assessment of users or customers on-line.
- Data Integrity: The quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data.
- Disaster-induced losses: the cost components that, when combined, would most accurately reflect the total cost of a disaster.
- Dissemination of the program: spreading information throughout the company or institution via electronic means.
- Encryption: the conversion of data into a form, called a cipher-text that cannot be easily understood by unauthorized people.
- Executive summary: a report, proposal, or portfolio, etc in miniature (usually one page or shorter). That is, the executive summary contains enough information for the readers to become acquainted with the full document without reading it.
- Exploratory Research: conducted because a problem has not been clearly defined or is unclear. It allows the researcher to become familiar with the problem/concept which is being studied, and create a hypotheses to be tested.
- Failover takeover: A system, method, and apparatus for active-active 1+1 redundancy for a plurality of bi-directional communication modules of a distributed point to multi-point communications network includes pairing active modules into redundancy groups for providing backup in the event of a failure.
- Firewalls: a program or hardware device that filters the information coming through the Internet connection into your private computer or network.
- Information Assurance Awareness Programs (IAAP): Air Force personnel, contractors, and users of the Air Force network are required to take and document annual Information Assurance training each fiscal year.
- Infrastructure: set of interconnected structural elements of the internal framework that provides support for the entire IT system.
- Longitudinal Research: refers to the analysis of data collected at different points of time, usually over a period of time.

- Macro detection: built-in macro detection tool which detects the macro and then minimizes the possibility that the macro is carrying a virus or worm.
- Maliciousness: deliberately harm or destroy with no clear impetus or reason.
- Malware: software designed to infiltrate or damage a computer system without the owner's informed consent.
- Mirrored-sites: Identical sites which synch simultaneously to provide redundancy in case of failure.
- Multi-function cell phones: Analog radio, digital phone, Internet, camera phones.
- Multi-path routing tree: use of bandwidth without any restriction on the maximum fraction of traffic on a path (MFTP), multi-path routing often turns out to be single path routing, and only reduces the total bandwidth requirement slightly at rare combination of network topologies and hose parameters.
- Non-repudiation: the concept of ensuring that a contract cannot later be denied by either of the parties involved. This protects both the buyer and the vendor.
- Off-Site Storage: any location away from the main location, considered safe and accessible.
- On-line Safe Storage: IT files or client's files will be updated and available, regardless of what happens on-site, 24/7 via the Internet.
- Online transactions: a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval processing used in commercial-business applications.
- Patriot Act II : "Domestic Security Enhancement Act of 2003" expand the powers of the United States while simultaneously curtailing judicial review of these powers.
- Phishing: sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information.
- Pre-Disaster Mitigation Program: FEMA supported program provides funding to states, territories and Tribal governments for planning and disaster preparation to reduce risk. Software part of Public Key.
- Proactive: to act before a situation becomes a crisis.
- Project scope: developing a common understanding as to what is included in, or excluded from, a project.
- Proxy servers: in computer networks it is a server (a computer system or an application program) which services the requests of its clients by forwarding requests to other servers.
- Radio frequency identification RFID: is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.
- Remote management of firewalls: resides either on the public IP network, or within the DMZ behind a firewall, and upon request, sets up a secure management channel between the configuration and management platform, and a Tenor Switch that is securely located behind a NAT firewall.
- Restore Process: dedicated disks and tape systems for each particular host server, with each host backing up its own data to its own locally attached tape drives or library.
- Risk assessment: process of quantifying the probability of a harmful effect to the IT and the businesses ‘or institutions’ infrastructure.
- Risk Reduction: to reduce the risk to life and property, which includes existing structures and future construction.
- Robust systems: near fail-proof IT systems with maximum protection and security.
- Safe Harbor: prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection.
- Safe Harbor Acts: legislation enacted both in the United States and the EU. There is a difference, though. The EU is very broad legislation placing the responsibility in the hands of the government. The US divides the responsibility amongst legislature, business, and individuals.
- Security audit: audit is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site.
- Security expertise: personnel who understand security technologies and how to deploy them.
- Security vulnerabilities: legitimate areas of weakness which an ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as penetration testing.

- Storage Area Networks (SANs): hardware/software designed to accelerate and simplify the data backup and restore process. SANs are ideal for backup-intensive environments, especially when there are clearly defined areas for isolating backup workloads spy ware
- Supply acquisition: is used in inventory management systems to determine the quantity of items needed to meet demand during the time required to order and receive replenishment stocks.
- Transport layer of security (TLS): cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.
- Trojan horses: a program that installs malicious software under the guise of doing something else. Known for installing backdoor programs which allow unauthorized remote access to the hard drive.
- Virtual Private Network (VPN): a private network that uses a public network (usually the Internet) to connect remote sites or users together. This is done through secure, encrypted connections between a company's private network and remote users through a third-party service provider.
- Virus Protection: Software that safeguards computers against various viruses. To do this efficiently, it must update continuously.
- Voice over IP (VOIP): technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.
- Vulnerabilities: a weakness in a system allowing an attacker to violate the confidentiality, integrity, of a system. They may be the result of a design flaw, or the result of a malicious attack.
- Web site defacement: Defacer breaks into a web server and alters the hosted website or creates one of his own.
- Web-based: on-line applications or commercial business housing
- White listing: a list of accepted items or persons in a set. This list is inclusionary, confirming that the item being analyzed is acceptable.

REFERENCES

1. Alison, Diana (2005). Channel steps up to Hurricane Rita preparation. Sept. 23. Retrieved March 22, 2007 from http://www.channelinsider.com/article/Channel+Steps+Up+to+Hurricane+Rita+Preparation/160827_1.
2. Ashworth, Jon (2007). Lloyd’s bumper profits tempered by threat of disaster. *Knight Ridder Tribune Business News.* Washington: April 7, 2007, p1.
3. Beans, Kathleen, (2007). Preparing for disaster. *The RMA Journal*, Philadelphis: Dec 2006/Jan 2007. 89 (4) p 22-28.
4. Buhain, Venice (2006). Olympia woman continues to see the devastation of Katrina, Rita (2006) *Knight Ridder Tribune Business News.* Washington: Aug 29, p.1
5. Cardwell, Gail (2005). Lending questions arise in wake of hurricanes. *National Real Estate Investor.* Nov. 2005. (47(11) p 74.
6. Culver, Denise (2006). Security. *BNP Media.* Feb 2006. Retrieved April12, 2007 from ProQuest Database.
7. Curran, Terry (2005). Information assurance awareness programs in multinational manufacturing organizations. Chapter 19 Leading Practices, Taylor and Francis Group.
8. Davis, James (2007). Spyware protection. . *Journal of Accountancy.* New York. April, 2007. 204 (4) pp.65-67.
9. FEMA (2007). Pre-Disaster Mitigation grant program fact sheet. Retrieved May 11, 2007 from: http://www.fema.gov/library/viewRecord.do?id=2070
10. Fest, Glen (2007). Antimal-ware: Calling of the watchdog; Bank opts out of ant-virus protection for whitelising approach. *Bank Technology News.* New York, March 1, 2007.20 (3), p.1.
11. Fine, Glenn (2007). Squabbling places network in jeopardy. *Knight Ridder Tribune Business News.* Washington April 3, 2007 p.1
12. Fonseca, Brian(2002). Ready with plan B. *InfoWorld.* San Mateo: Sep 9, 2002. 24 (36) pp.41-43.
13. Grillo, Christopher (2005). ISO 17799 Awareness for IT managers requires security mindset changes: Putting the cart before the horse. Chapter 19 Leading Practices, Taylor and Francis Group.
14. Hartman, Anita (2005). Education and awareness for security personnel. Chapter 19 Leading Practices, Taylor and Francis Group. *CRC Press Company.*

15. Hayati, Patrick (2007). Mcafee, Inc. researchers outline emerging threats in its latest edition of the global threat report. *Al Bawaba*. April 11, 2007. p.1

16. Heavens, Alan J. (2005). Hurricanes give Gulf Coast real estate market a stir. *Knight Ridder; Tribune Business News*. Washington: Oct 9, 2005. p 1

17. Jordan, Jim (2006). The Time Has Arrived For Disaster Recovery Plans. *Texas Construction.* Baton Rouge, LA :Feb. 2006. 25 (9). pp 14-16.

18. Katz, Jonathan (2006). Be flexible. *Industry Week.* Cleveland , OH, 225(9).p 14-16.

19. Keizer, Gregg (2006). The state of insecurity. *Information Week.* No 20, 2006. 1115, p15.

20. Kodogy, Charles (2007). SoniWall unit shipments pass the million mark. *Al Bawaba.* London, April 8, 2007, p.1.

21. Lalisan, Allan (2007). Cisco systems launches new security systems for networks. *Business World.* Manila; April 12, 2007. p.1.

22. McBride, P., Patilla, J., Robinson, C., Thermos, P.,& Moser, E. (2002). *Secure internet practices*. Auerbach Publications.

23. Mims, Bob (2006). Businesses told to ready for disaster. *Knight Ridder Tribune Business News.* Washington: Aug 31, 2006. 1

24. NA (2007). United States: The long road home; New Orleans' slow recovery. *The Economist.* London. March 17, 2007, 382(8520), p 59.

25. NA (2006). Kinder Morgan energy 4th uarter profit up, aided by insurance hurricane recoveries. Financial Wire. Forest Hills: Jan 18, 2007. p. 1 Retrieved April 11, 2007 from http://biere.louisiana.edu:2076/pqdweb?index=2&did=1196125691&SrchMode=1&sid=6&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1176391684&clientId=19873

26. NA(2006) Survey: Most employers stood up to Katrina *City Business Staff Report*. New Orleans City Business. Metairie: Apr 5, 2006. pg. 1

27. NA. (2006). Post-hurricane Postings Security. Troy: Feb 2006. 43(2) pp 62-64 Retrieved April 12, 2007 from http://proquest.umi.com/pqdweb?did=982918111&sid=3&Fmt=4&clientId=19873&RQT=309&VName=PQD

28. NA (2000). Foundry launches high-density LAN switch. *Asia Computer Weekly.* Singapore Nov.6, 2006 p.1

29. Olsztynski, Jim.(2005). Katrina Disrupts Gulf Coast. Industry Supply House Times. Troy: Oct 2005. 48(8,) pp. 20-22 http://biere.louisiana.edu:2076/pqdweb?index=5&did=918911561&SrchMode=1&sid=1&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1176390294&clientId=19873

30. Poo, Gee-Swee & Wang, Haibo (2007). Mulit-path routing versus tree routing for VPN bandwidth provisioning in the hose model. *Computer Networks.* April 25, 2007, *51(6)* p1725.

31. Richter Allan (2006). Insurance Catastrophe. *Journal of Property Management.* Chicago: Nov/Dec 2006 71(6) pp 28-31

32. Robb, Drew (2007). Instant It! *Computerworld*. Framingham: Mar 12, 2007. 41(11) p. A18. Retrieved April 10 from http://biere.louisiana.edu:2076/pqdweb?index=2&did=1238393181&SrchMode=1&sid=5&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1176391375&clientId=19873

33. Santora, Tommy (2006). New Orleans oil and gas executives discuss their preparation for the 2006 hurricane season **.***New Orleans City Business*. Metairie: Jun 5, 2006. *pg. 1*

34. Staff Report (2006). Survey: Most employers stood up to Katrina. *City Business.* New Orleans, Metairie April 5, 2006, p 1.

35. Taylor, Paul (2007).War on spies, bots, and Trojans. *Financial Times.* London, March 2, 2007, p11.

36. Vijayan, Jaikmar (2006). Security managers facing more targeted attacks. *Computerworld.* Nov. 20, 2006 40 (47) p.8.

37. Westcott, Ross (2007). Maximzing the ROI of a security audit. *Network Security.* Kidlington: March 2007. 2007(3) p.8.

38. Zwirn, Edward (2006). Shelter from the storm**.** *Chemical Market Reporter*. New York: Jul 17-Jul 23, 2006.270 (2) pp. 8-10.

BIOGRAPHY

Mona Ristovv-Reed is an adjunct instructor at the University of Louisiana, Lafayette, LA . She has been involved in IT as the owner of a small business and has worked at the University in the computer lab. She is pursuing an MBA and EdD co-currently. Her interest in IT safety arose out of the frustration of the Katrina- Rita hurricanes in the Gulf area where she resides.

Ihssan Alkadi is on the faculty at University of Louisiana at Lafayette (UL Lafayette). He received his B.S. Degree in Computer Science at SLU, May 1985. In May 1992 he earned his MS. In Systems Science from Louisiana State University (LSU). He earned his Doctoral degree in Computer Science at LSU. His areas of expertise include software engineering in general, testing in particular, Internet, HTML, and operating systems. His research interests include testing in object oriented systems, systems validation, and system verification.

NOTES