Global Information Assurance Certification Paper

Project

Submitted

for

Audit 411 – SANS 17799 Security & Audit Framework

SANS Florida
February 8, 2005

Submitted by

Nassar Nizami
nassarn@greenhosp.org

Table of Contents

Business Objectives, Mission Statement & HLSP:

Mission Statement:

The mission of Viva Casinos is to provide a secure, friendly and entertaining environment to our customers while complying with the rules and regulations set by Nevada Gaming Board.

Objectives:

The main objective of our business is to

- Protect the privacy of our customers by giving access to the database on a need to know basis.
- Protect the confidentiality of all customer personal and financial information by implementing principles of least privilege and complete mediation.
- Provide a safe and friendly environment for our customers and employees
- Protect the interests of our shareholders
- Be the most profitable Casino company in Nevada
- Enter the Internet Gaming Market and be the number one market share holder within two years
- Comply with all governmental laws and regulations

Maturity Model for an Issue:

Objective:

Protect the confidentiality of all customer personal and financial information.

Problem:

Secure backups of the system database containing customer personal and financial information.

Current Process:

- The database is backed up on tapes
- Tapes are stored in the data center on open shelves
- Operators rotate the tapes daily
- Data is retained for 30 days

Process Improvement:

Level 1:

- Backups are stored in secondary data center
- Tapes are stored in a fire rated safe with access limited to data center operators only
- Request to retrieve a tape is approved by department manager

Level 2:

- Backups are encrypted using encryption algorithm approved by Information Security department
- Tapes are bar coded with access to the bar code reader limited to data center

manager
- All restore operations are logged by data center manager

Level 3:

- Copies of backups are stored on mirrored Storage Area Network (SAN)
- Backup/restore activities are only possible from one server which is password protected
- The access to backup server is limited to approved administrators
- All backup/restore activities are logged. The logs are reviewed on a weekly basis.

Addressing Objectives in Awareness:

New Control:

Request to retrieve a tape is approved by department manager

Issue:

The user community believes that it is unnecessary to get manager's approval to retrieve data. Some users don't want the managers to know that they deleted a folder or overwrote a file.

Awareness Steps:

- This policy will be announced in the monthly corporate managers meeting. This will make sure that all managers know about the policy and understand that is meant to prevent users from requesting data that they don't own. It is common for users to delete files by mistake.
- This policy will be published in the company publication. The publication will explain that the policy actually protects the data that they own. It makes sure that the users are requesting retrieval of data that they own. It makes their data secure!
- A copy of the policy will be posted on the company notice board.
- It will be one of the points on the mandatory web based Information Systems training with at least one question in the quiz at the end.

New Control:

Backups are stored in secondary data center

Issue:

The operators have to make trips to the secondary data center which is 5 miles away in a different building to retrieve and store tapes. They believe it is sufficient to store tapes in the same building and that 'we will have bigger problems' if something catastrophic were to happen to the current building.

Awareness Steps:

- There will be a special session to educate the IS staff on the business disaster recovery plan. This will help them understand that even if something were to happen to building, the company will still be in business.
- News articles about fire in data center in one of the area casinos will be distributed to the employees. The only reason the casino stayed in business was because they were able to recover all customer data from backups at remote site. This will help operators understand the importance of storing tapes in a different location.
- Data center manager will discuss the best time to pick/drop the tapes. The morning shift operator can bring the new tape from secondary data center on his way in and the night shift operator can drop the tapes on his way out. Operators will learn that management realizes that they have an additional responsibility and is flexible.

New Control:

Backup/restore activities are only possible from one server which is password protected

Issue:

System administrators have always been able to create backup/restore jobs from their computer or any server with the backup software installed. Now they have to remotely connect to or physically be in front of backup server. They see the new process as time consuming and unnecessary.

Awareness Steps:

- The policy will be signed by the CIO. This will make sure that everyone understands that it coming from the top.
- Awareness program will include a 30 minute session with the administrators to go over the complete process of backup and restore. This will demonstrate that if done correctly the new process is not that time consuming.
- Story: Last month just before the deadline for budget submissions, the marketing

department heads called and complained that the budget file in his department folder 'went back' to two weeks old version. All the changes he made were gone! He was furious and wanted to know what happened. The logs showed that a restore job was executed from one of the computers logged on with a generic ID. This job restored the older version. Information systems department was not able to give a satisfactory answer to the marketing department head. The new process will eliminate any issues like this in the future because

- There will only be one place to configure backup/restore jobs.
- The backup server will be password protected and no generic IDs will be allowed.
- All activities will be logged and centrally stored.

New Control:

All restore operations are logged by data center manager

Issue:

The operators and system administrators see this process as lack of trust. They also see it time consuming.

Awareness Steps:

- CIO will discuss this issue in the monthly IS meeting. He will make sure that everyone understands that operators and administrators are trusted. The new control will make the restore process more efficient.
- The benefits of the new process will be highlighted in a meeting with operators and system administrators. The logging will provide IS a tool to measure who is requesting most restores. Most likely these users need to be trained. This process may actually reduce the time spent in restoring data.
- The results of the logging-measuring-training-logging-measuring process will be shared with operators so that they can see the improvements.
- One of the benefits of this process is to ensure that the backup/restore requests are completed in a timely fashion.

BCP:

New Control:

Backups are stored in secondary data center.

Issue:

The operators have to make trips to the secondary data center which is 5 miles away in a different building to retrieve and store tapes. They believe it is sufficient to store tapes in the same building and that 'we will have bigger problems' if something catastrophic were to happen to the current building.

Business Continuity Plan:

If the operators don't store the current backup tapes in the secondary data center, the data on the tapes will be old during a disaster.

The development team in charge of developing the front end of the application has a separate system with a replica of the customer database. The development server is located in a separate building two miles away. The database is replicated to this system every night. This system is also backed up every night. If the tapes were found to be old, we will convert the development system into a production server. The following will happen:

1) All access to developers will be revoked.
2) Web servers will be configured to point to the development server database.
3) All new records will be stored on this server.

The data on this system can be one day old. The billing department keeps a hard copy of all customer information for two weeks. Typically a thousand to fifteen hundred new

customers register everyday. The hard copy of the customer information will be

1) Scanned
2) Parsed by OCR and
3) Fed into database using scripts.

This process is expected to take less than two hours.

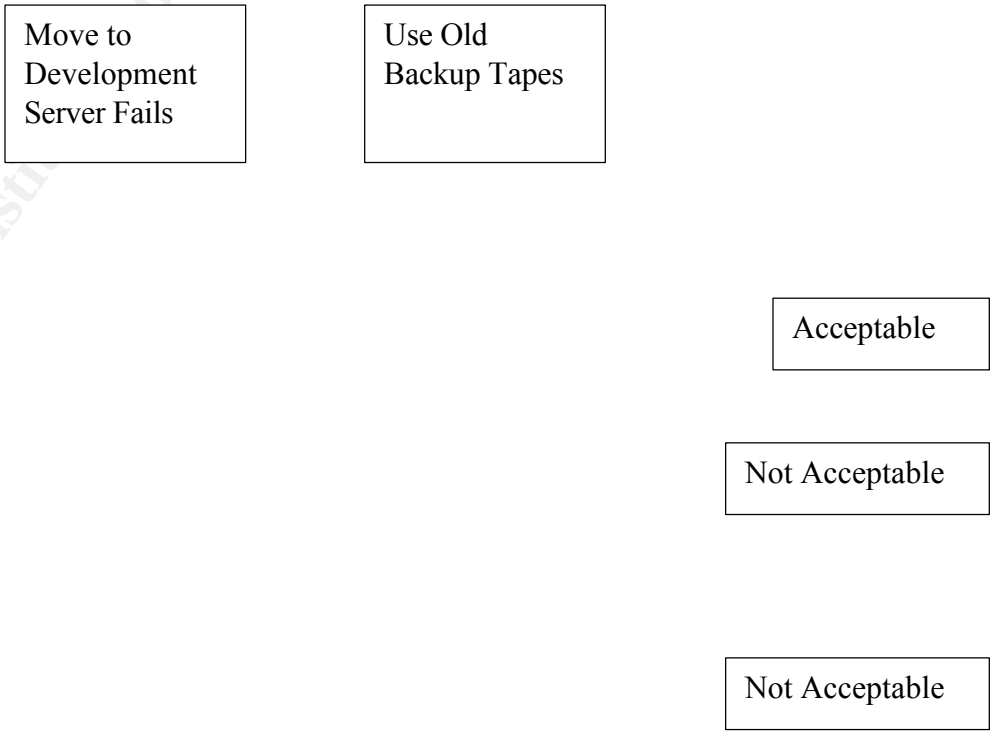
The development server will then be backed up to tapes and the tapes will be restored to the server in secondary data center. Once all the tests are successful, web servers will be configured to point to the new servers. At this point the servers in secondary data center will act as the production servers. The development server will be configured to replicate the data from the new server.

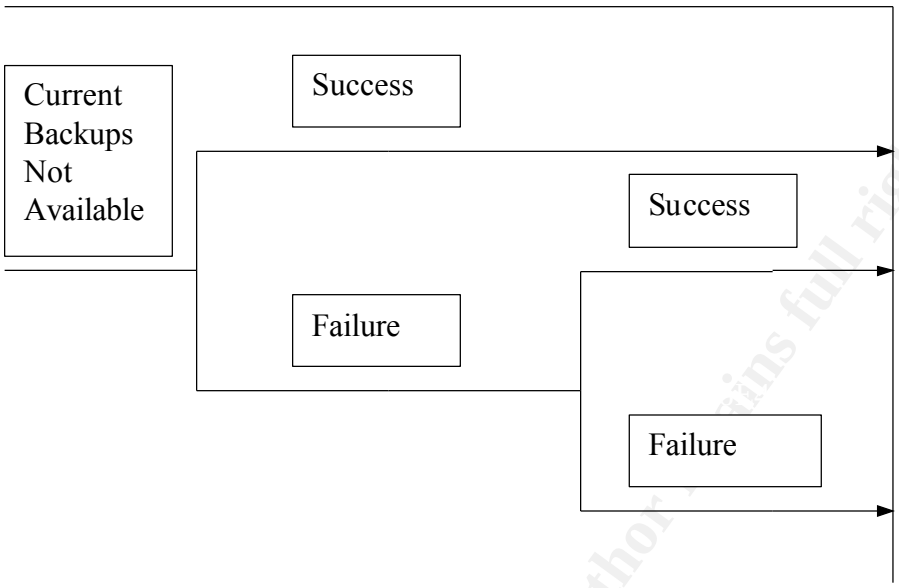
The above process will be tested quarterly. During the test the test web server will be configured to point to the development server. The new customer data will be scanned and fed in the database as planned.

Risk Assessment & Recommendations:

Risk Analysis Based on Event Trees:

Following is the event tree diagram of the event in which the primary system fails and current backups are not available.





Based on the event tree analysis we can see that if the move to development system is successful, the losses will be bearable and the business will continue. On the other hand if the move to development server fails, the outcome will be catastrophic. Therefore we need to introduce additional controls to ensure that the development servers are available and can be moved to production in case of emergency. The suggested controls are:

- The WAN connection to development building is not reliable. We will add a PRI as a backup connection. Furthermore the connections are currently not monitored. We will also start monitoring the connection. If the connection goes down, the network engineer will be paged. Network engineer responds within two hours.

- At times replication process hangs and operators have to manually restart the replication process. We will automate the process using scripts. In addition, an email will be sent to the operators.

- Development department have multiple servers. We will start replicating data to another server.

- The backups of development server are kept in development department. We will start moving the backups to secondary data center. These backups will be audited quarterly.

- According to current BCP, the move to development server is tested quarterly. We will change the frequency to monthly tests.