Viva Casinos

6 Hotels & Casinos
Revenue Streams

- Entertainment 15%
- Food & Beverages 4%
- Gaming 28%
- Slots 44%
- Retail 9%

Divisions

- Security
- Gaming
- IT
- Administration & Personnel
- Food and Beverages
- Hotel and Guest Services

Looking to expand business

- Internet gaming

Publicly owned company
Nevada Gaming board oversees operations

Mission Statement
The Viva Casino organization is in the business of operating a legal gambling property that prospers through creative uses of technology to increase the ease and access of gambling to the general public both inside of the casino property and over the Internet.

To realize increases in revenue the casino is expanding beyond the gambling internal to the property along with the hotel and food services to include Internet gambling. The legacy information responsible for revenue sources need to be protected to ensure that confidence in the casino is maintained and customers that frequent the property will be encouraged to continue the experience online. In order to continue the growth in revenue it is imperative that both the gambling and client information is maintained in a secure manner that ensures confidentiality, accessibility and integrity.

To realize growth in online gambling a secure presence is required at all times. To achieve this the Internet presence must be available through multiple access points and with multiple providers with independent permissions and segregation of duties between providers. The web server farms will also require separation of duties between the server administration and application support. All financial information is to be encrypted at all times on servers and in transport both within the server farm and on the Internet access points.

To ensure that all information is kept secure an IDS system will be deployed on the access points and monitor both the inbound and outbound traffic through firewalls. The IDS results will be reported on at a reasonable interval and incidents reviewed with the concerned parties such that actions can be tracked and reported back to the ISO.

Night 2

Process Improvement

Process – The legacy information responsible for revenue sources need to be protected to ensure that confidence in the casino is maintained.

The legacy information within the Viva Casino's systems includes both personal and financial information as well as the gambler's trends in gambling. This combination of information resides on a database internal to Viva Casino's data center, which is secured physically. The data center does have network access from various points external to the data center including the internet for the newly forming on-line gambling venture. This new access point has exposed the information to new risks for confidentiality, availability, and integrity.

Level 1 – Policy and system log reviews

To increase the protection of the legacy information, the executive approved a new policy to enhance the privacy of the information. The Policy further separates the access of information to only those fields of data required by individual to successfully complete their roles within the casino. The policy went further to isolate the identity of each individual and assign a unique ID and password for each employee requiring the data. To ensure that the policy was adhered to an awareness program was completed by all individuals responsible for accessing the information as well as lunch and learn sessions for employees that deal with the information to understand the new processes.

The access server used to access the information had logging enabled and the logs are reviewed daily by the system administrators for any abnormal entries.

Level 2 – Firewall and DMZ log reviews – Implemented within 3 months of the Internet venture.

To further protect the integrity and confidentiality of the legacy information a new firewall will be installed between the database and all other networks. This firewall will have logging functionality enabled that will log events both to an internal log server for network administrators and an audit log server for auditing purposes.

The logs are to be reviewed daily by the network group and weekly by audit. Any discrepancies between the logs are to be forwarded to the security group within 1 hour of being discovered.

Level 3 – IDS and automated log reviews – Implemented within 1 year of the Internet venture

In order to ensure that all event logs are being correlated and maximum benefit of the data is being extracted an automated log reviewing application will be installed to review both the Internet firewall logs and the internal firewall logs. These reviewed will be augmented with the system logs from both the database servers and the web servers within the application to gain a complete image of the information environment.

To ensure that immediate responses are taken on the information or events an IDS platform will be deployed and connected to an escalation process. This system will monitor all access to and from the Internet as well as all access to the database. Copies of the alerts will be logged with the audit logging server as well as the network-logging server. All escalation will be based on elapse time and based on the severity of the incident. All alerts generated from the IDS will e treated as incidents and a review will be required for each including remedial action items that will be tracked and reported on weekly.

Night 3

Awareness program

In level 1 policy was used to increase the protection of the data as an immediate step. To ensure that the policy is understood and complied with an awareness program for both the data handlers and data users was proposed. The data users are considered the employees in any division that currently use the results of data base reports to complete their jobs within the roles and responsibilities of their job.

For the employees who use the results from the data base a series of lunch and learn sessions will be held in groups of associated people to emphasize the importance of the data and value of the information both to Viva Casino and the associated costs to the casino if the data was released. This could best be illustrated to the groups through hypothetical situations using the types of data contained in the database. For example, given that the employees themselves would have information residing in the database how would they feel about their information being used external to the Casino? Also any legal aspects of the release of data need to be imparted on the group. This group should leave the lunch understanding that they have "dodged the bullet" on this one and that it is the data base administrators that have the new task of guarding the information. This will foster some patients and understanding from the users when dealing with the administrators when asking for new reports and information.

The data base administrators will now become information stewards as well as administrating the "keys to the kingdom". The policy should emphasize to them that the value of the information on the systems has increased dramatically by connecting to the

Internet, not by the change in the information but by the change in the earning potential of the information. These people need to understand their new role in the growth of the casino and controls in place to help them manage this new role. During each of the implementation phases of new controls a presentation needs to be made to the group to enforce the policy and illustrate how the enhancements build upon the policy.

This group will have several issues with the new policy each needs to be addressed in the awareness program:

To bring the technology advantage into perspective for the administrators a story could be used about the inherent risks of the Internet. To illustrate how the technology is being used to observe the Internet bad guys and not spying on the network or database administrators a sample attack could be outlined showing how hackers "clean up" their tracks by modifying logs on the servers and why comparing the logs to the audit logs is important.

To combat the immediate response from the administrators about the loss of access to all locations of all servers due to separation of duty another story or anecdote would be required. For example, comparing the value of the information to the value of the chips used inside the casino to show how each step of the gambling process on the floor is separated. This results in the administrators feeling more a part of the gambling floor and the casino's business. To re-enforce the value of segregation of duties tours could be arranged of the casino floor with the people involved with the handling of chips or cash on the floor and their stories of the value of segregation of duties. By following the money/chips through the gambling process and comparing it to the data on the servers the administrators will have an appreciation of the value of the data. To keep the value of the data present in the administrator's minds a chart comparing growth of revenue from the Internet gambling versus the growth on the casino floor could elevate self esteem and create a greater team value for the administrators.

Night 4

BCP program

Loss of Data to Internet servers:

Worst Case Outcome:

If data availability was lost from the database servers to the Internet web servers then downstream revenue would quickly be affected and possible lasting negative monetary results would be noticed. In the worst-case scenario a change in the web server's configuration, either intentional or maliciously, could result in loss of information to the web servers that makes gambling on the web site impossible.

BCP Plan

In order to continue to realize Internet revenue and ensure that Internet clients do not move to other Internet gambling sites the web presence must be restored within 5 minutes. To achieve this data must be moved between the database servers and the Internet web servers in sufficient quantity to ensure gambling is restored.

To meet this timeframe a hot standby database server will be implemented. This server will maintain the same database as the primary server at all times using appropriate replication software that is tested on a weekly basis. This server will have an identical configuration to the primary server but will not have any connectivity to the external Internet network. In order to bring this server online the primary will be removed from the network and the standby server will have it's Ethernet card connected to the production network with a different IP address then the production server. The back up server will then be tested prior to the web server accessing the database. Once the standby system has been proven production ready the standby server will have it's Ethernet card configured with the same MAC and IP address of the primary server.

To continue to gamble without the database connectivity requires credit card verification and logging of gambling results for payments to credit cards. If the connection and verification of the backup database server will take longer then 5 minutes, then manual checks of the credit cards will be processed by internal Casino until the back server is connected.

By commissioning a standby server that is continually operating in the same environment as the production Internet gambling can continue to operate independently of the database source.

Night 5

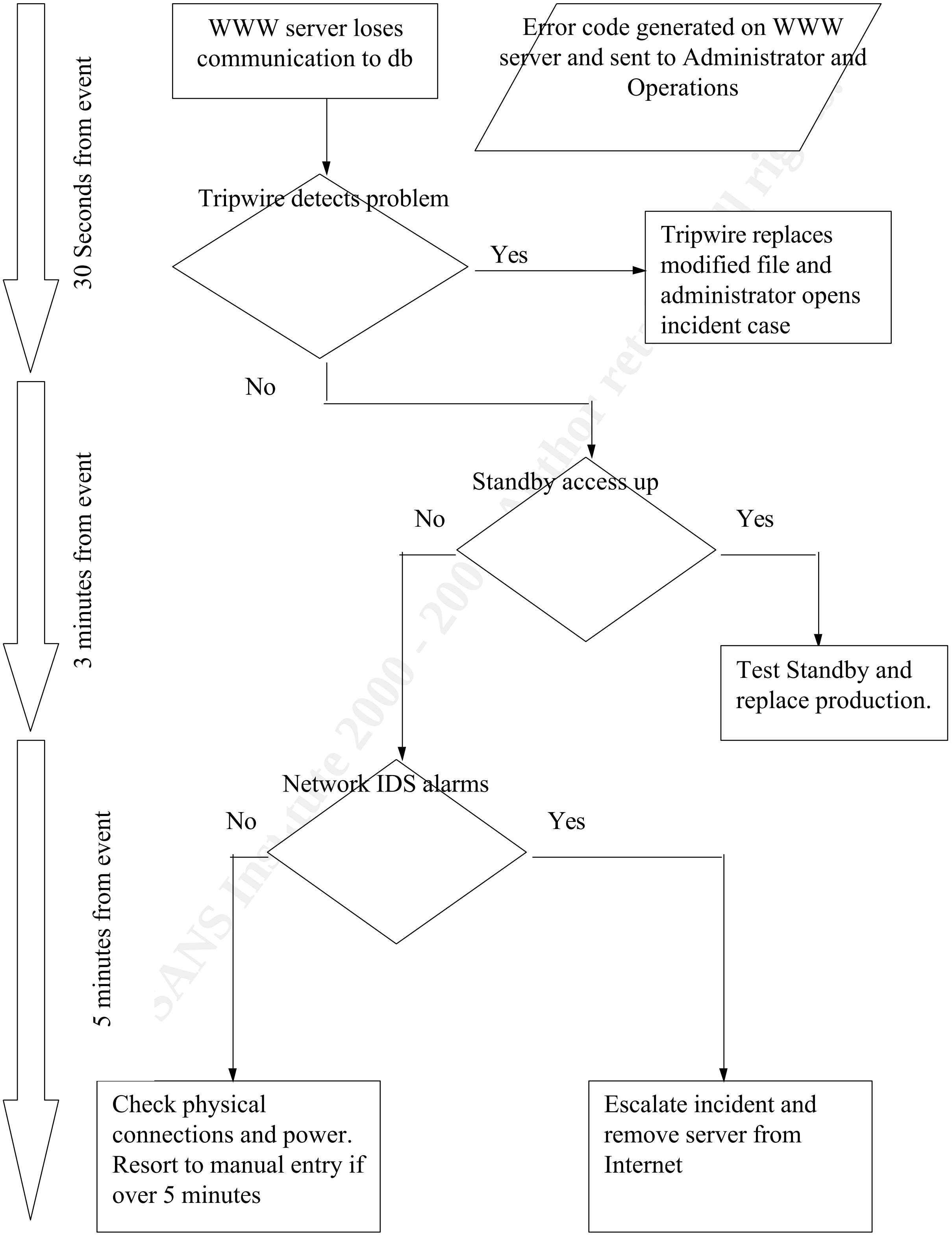
Risk assessment of BCP– Event tree analysis supported with Time based Risk Analysis

In the worst-case scenario a change in the web server's configuration, either intentional or maliciously, could result in loss of information to the web servers that makes gambling on the web site impossible.

Event – The web server generates an error from a database query
Detection – The web server detects the error generated and notifies operation and db
administration

The following event flow diagrams illustrate the BCP results with time frames.

From this analysis it is evident that detection controls would need to be implemented to ensure that the time frames for business were met. The two controls that would be added for BCP would be IDS systems for the network access and Tripwire for the host. The IDS system is required to meet the detection timeframe and would be triggered by any unauthorized access to the networks. The Tripware application would reside on the web server and the standby server and would automatically check the integrity of the configuration and key application files every 30 seconds. If the Hash changes on any of these key files the file would be replaced with the known good hash file.


30 Seconds from event
3 minutes from event
5 minutes from event
WWW server loses communication to db
Error code generated on WWW server and sent to Administrator and Operations
Tripwire detects problem
Yes
Tripwire replaces modified file and administrator opens incident case
No
Standby access up
No
Yes
Test Standby and replace production.
Network IDS alarms
No
Yes
Check physical connections and power. Resort to manual entry if over 5 minutes
Escalate incident and remove server from Internet