Global Information Assurance Certification Paper

Night 5

Include:

- Business Objectives/ Mission
- HLSP
- Maturity model
- Addressing Objections in Awareness
- BCP (un-touched)
- Risk Assessment & Recommendation

* * * * * * * * * *

(DAY 1) - Business Objectives/ Mission

Business: VIVA CASINOS
6 hotels & casinos
Revenue Streams

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

Divisions

- Security
- Gaming
- IT
- Admin/Personnel
- Food & Bev
- Hotel & Guest Services

Business Information

- Looking to Expand
- Internet gaming
- Publicly Owned
- Nevada gaming Board Oversees Operations

Business Objectives:

- Provide entertainment and customer satisfaction for all types visitors
- Provide safe and comfortable entertainment environment (including Internet)
- Maximize profits for business and shareholders
- Minimize loss and liability
- Expand to new areas, specifically retail (9%) and internet markets (undeveloped)
- Compliance with any legal or regulatory bodies (Nev. Gaming Board)

ISMS Mission Statement

Our mission is to provide each of our patrons with the best entertainment experience and highest level of satisfaction possible. We are committed to providing a

safe and comfortable environment in all business areas. This commitment includes all of our hotels and casinos, as well as our Internet locations. We are dedicated to maximizing the profits of our shareholders and business, while minimizing all losses and liability where possible. We pledge to adopt and promote any and all the legal and regulatory requirements governing our business. We will remain committed to explore all promising new areas of business at all time, especially in the Internet and retail markets.

* * * * * * * * * *

(DAY 2)
High-level Principles to Implementation

Customer Satisfaction:
Throughout our various organizations, we will provide entertainment tailored to the enjoyment and satisfaction of all customers. We will strive to ensure that our customers always feel secure and comfortable while enjoying our business offerings.

Safety:
At all times, we will safeguard the customer and corporate confidential information in our systems. This will include protection of confidentiality, integrity, availability, and inappropriate disclosure or misuse.

Maximize Profits:
Our goal is to be as adaptive and efficient as possible through the monitoring and review of performance metrics. We will seek to minimize loss and risks wherever possible through a program of risk evaluation, monitoring, and reduction. To maximize our potential, we will encourage the exploration of innovative new areas of business, especially in the internet gaming markets.

Compliance:
We are dedicated to meeting or exceeding all regulatory and legal requirements in an effort to ensure the compliance and viability of our business. To this end, any potential violations must be reported directly to management for review and validation.

* * * * * * * * * *

(DAY 3) – Maturity Model

High-Level Security Principle –At all times, we will safeguard the customer and corporate confidential information in our systems. This will include protection of confidentiality, integrity, availability, and inappropriate disclosure or misuse.

Break into levels

Minimum – Cheap, easy, sufficient
Understanding the limited resources of the company, we will do what is necessary to do business in a safe and legal manner for our company and our business.

- An information security manager role will be assigned to deal with InfoSec issues and responsibilities.
- We will define policies which require staff to be trained in the legal requirements of the business, and in the minimum best practices for secure operations.
- Unless necessary for business reasons, we will ensure that all confidential customer data (personal information, credit info) is not displayed to anyone.
- All critical areas, including guest areas, are required to have staff participating in video surveillance with monitoring tapes kept for 3 days.
- We will make sure that all essential systems are backed up and stored in a secure offsite location.
- All essential systems will employ redundancy in data media (drives, backups).
- Our internet presence will have backup connectivity to prevent extended loss of availability.
- We will employ a firewall and IDS for all external connections. The logs generated by these systems should be reviewed regularly.
- We will employ antivirus and automatic updates on all applicable systems.
- We will require our internet gaming sites to be hosted by companies that meet our standards for security and operations (CIA).
- We will require an annual, external perimeter intrusion audits to provide information about our external connections.
- We will have a qualified in-house IT staff to provide on-site support for our computer systems.

Medium – Most efficient & comprehensive for the cost
We will meet or exceed best practices when possible.

- Contains all of the measures above, plus:
- An InfoSec Office with full-time staff will be created to monitor and handle information security issues.
- Staff will receive formal training on all applicable security standards and requirements for their positions.
- The logs generated by Firewall and IDS systems should be reviewed daily and issues reported to management.
- All uniformed associates must wear color-coded picture ID badges indicating their level of security and authorization.
- All physical access to critical facilities will require the use of individual key-fobs.
- All critical areas, including guest areas, are required to have video surveillance monitoring kept for 7 days.
- We will have a DR hot site for recovery of operations within 48 hours.
- All off-site backup tapes will be tested for errors and data recoverability before being sent.

- We will require an annual, external perimeter intrusion audits to provide information about our external connections.
- We will have a qualified in-house IT staff to provide on-site support for our computer systems.
- Redundant ISP, Redundant Websites with auto roll-over in instance of failure

Highest – The hotel is Mob-owned, lots of money/enemies, Gov't always watching
We must provide the highest feasible level of protection for our customers and company.

- Contains all of the measures above, plus:
- An accredited InfoSec security and audit organization will be created in the business to handle all InfoSec responsibilities.
- All staff must be fully trained by certified or accredited professionals in industry-standard security practices, and pass annual tests proving their competence. All data-handling staff must be themselves actively certified or accredited in their expertise as part of their continuing employment.
- All confidential data must be completely protected at all times by high-level, standardized encryption as defined by current industry best practices.
- The logs generated by Firewall and IDS systems should be reviewed hourly by an automated system and intelligent system-analyzed reports provided to security and management.
- A certified in-house security expert will perform daily perimeter and internal network scans for gaps and weaknesses.
- All data-handling associates must wear the standard color-coded badges, and use industry-standard biometric methods to validate authenticity.
- Dual-site, interconnected, high availability data centers for all critical operations.
- Separation of operational duties and responsibilities will be maintained at all times between data centers.
- Backup tapes will be generated daily and stored in a certified offsite vaulting location.

* * * * * * * * * *

(DAY 4) Addressing Objections to Security Awareness

High-Level Security Principle – At all times, we will safeguard the customer and corporate confidential information in our systems. This will include protection of confidentiality, integrity, availability, and inappropriate disclosure or misuse.

Minimum – Cheap, easy, sufficient

- We will define policies which require staff to be trained in the legal requirements of the business, and in the minimum best practices for secure operations. This training will be reviewed annually, or as necessary.

Staff Issue: This will cause a huge issue with staffing if everyone is required to attend. They feel that it is overkill to expect everyone to get trained in legal and security issues when most of the staff is involved with manual labor (dishwasher, cleaning, and food service). This is a total waste of time and effort.

Failure Result:
If the staff was not adequately trained in general security operations, there is a significant chance of mishandling of information. For example, the manager of the casino merchandising department leaves his password on a 3M note under his keyboard. One of the employees realizes this and commits it to memory. He then uses this password to go back to a less visible computer. There, he accesses customer credit card information and begins to make a significant number of retail and online purchases with delivery being made to a warehouse building owned by the casino. Customers begin to complain and it becomes evident that their information has been compromised by the casino. Several guests indicate that they will sue, they call the police, and a huge scene is made. The Casino owner demands to "know the details and extent of the situation". He's indicates that the casino information system may have to be shut down if the problem is too large or cannot be resolved quickly. He also stresses that the members of ISMS will be *very unhappy* for a *very long time* if this happens, as he cracks his knuckles.

* * * * * * * * * *

(DAY 4) Business Continuity Planning

Business Continuity Plan: (focus on availability)

Activate the BC Plan:

1. As soon as the problem is identified as a significant issue, the BCP is activated.

Notify Management:

1. Management is notified that a "possible" issue exists.
2. Another meeting is scheduled for later that day, after a rapid investigation has been performed to determine the veracity of the issue.

Quickly and quietly verify the problem:

1. The BC team members are activated & focus their full attention on this issue.
2. The customer information accounts are immediately audited for access information.
3. A report is created showing all access showing employee IDs and timestamps.
4. A correlation is made to between the customer information and suspicious staff activity.
5. If it becomes clear that there is unusual activity, ISMS disables the staff's userID and has a security representative escort them to a secure area for the police.

6. An additional audit of the account is then performed to search for additional customers that may have been defrauded.

Communicate with Management

1. Once the problem is verified, and the extent assessed, an emergency meeting is held with Casino management, security, legal counsel, and guest relations.
2. Management and Legal decide if the incident is sufficient to suspend casino operations and declare a disaster (activates the DRP).
3. If not, management ensures that incident be kept as quiet as possible.

Actions & Activities – Dealing with the Problem

1. The Security team notifies that casino's local police contact of the incident details, and casino staff aids in the investigation as requested.
2. The Management sends a representative to inform the (possibly) affected guests of the situation and accepts full responsibility for any and all credit card charges incurred during the period of the guest's stay.
3. The Guest Relations team upgrades the guests accommodations to a higher level, provides substantial amenities and additional service.
4. The legal representatives work with guests to contact credit card companies (to prevent further charges) and release information about when & where the fraudulent charges were made (credit card records).
5. The Security team / Police use the credit information to obtain information about any transactions and the delivery of purchased materials.
    a. For retail transactions, the Security team works with store management to provide surveillance tapes and eye witnesses contacts to the police.
    b. For online transactions, it ISMS team contacts the online retailers and gets contact information. ISMS provides the contact information to the police contact as a means of determining purchaser information (IP address/ISP, connection times, previous transactions, etc).

Closing Activities

1. As the investigation continues, the casino cooperates with the police at all times.
2. Staff members are prohibited from speaking to guests and the media about the incident in any way, and instructed to speak directly with the PR department.
3. Staff members are also are required to speak with management and legal counsel before making any unplanned statements to the police.
4. Management deactivates the BCP and emergency teams when the incident is sufficiently handled to return to normal operations.
5. As the incident is resolved, all staff involved are required to prepare an incident report which details there actions and any lessons learned.
6. The BCP is updated with any new information, and incorporated in the training program.

* * * * * * * * * *

(DAY 5) Risk Assessment & Improvement Recommendation

Work individually to perform a risk assessment of the business continuity problem that you addressed last night

- Select any risk assessment strategy that you wish and you may use more than one
- Recommend improvements to the process being considered to reduce the overall risk

Review the risk assessment results with your group and tone up your final results.

INCIDENT: Credit card fraud by stolen system password

Areas of Key Risk, Likely Failure, and Improvement Options

Scenario: If the staff was not adequately trained in general security operations, there is a significant chance of mishandling of information. For example, the manager of the casino merchandising department leaves his password on a 3M note under his keyboard.
Risks: Mishandling of information
Possible Faults: No training, poor training provided, or misunderstood training by individuals

Level 1: Ensuring training is performed for all staff.
All staff is required to attend security training classes at least annually to cover topics for their position. The casino HR department tracks the training attendance to ensure that everyone has been provided training. (audit)

Level 3: Ensuring training content is accurate and effective.
All staff required to take proficiency tests before and after each class to ensure the material is understood, and all topics are discussed during the class. Areas that are consistently failed are promoted more heavily during subsequent training classes. (audit)

Level 3: Ensuring training is understood by each staff member.
Staff evaluations include a section that requires a minimum score for security training tests. Staff members are allowed to repeat the test attempt up to 2 times during a year, as a demonstration of security awareness. (audit)

Scenario: One of the employees realizes this and commits the password to memory.
Risks: Information exposure, information theft
Possible Faults: lack of practical application of policy, lack of effective reporting mechanism, lack of real-time auditing.

Level 1: Prevent inappropriate access to a restricted information
As part of a Clean-Desk security policy, sensitive information is not kept exposed or unattended. When not occupied for more than a reasonable amount of time, desk are

required to be free from sensitive information and office doors are required be locked.

Level 2: Reporting known security violations.
Staff members are required to report security violations to a ISMS security staff member or as an anonymous message to the ISMS group (audit). Failure to report a known issue constitutes an additional security violation on the part of the witness. ISMS responds immediately to all violation notifications in a predictable and consistent manner.

Level 3: Inspections
As means of maintaining vigilance in sensitive areas, the ISMS team randomly conducts inspections of security adherence and provides violation reports to the Security training team. (audit)

Scenario: He then uses this password to go back to a less visible computer.
Risks: Unauthorized use of accounts, unauthorized access to critical information
Possible Faults: lack of physical security controls, lack of controls for access times, no certain means of identity validation.

Level 1: Limit computers with access to sensitive information
Computers with access to sensitive information are placed into special security groups within the domain and security is set to prevent access from all other machines. Access attempts from computers outside of these special groups are logged and reviewed (audit).

Level 2: Limit account access to business hours
Employees with access to sensitive information have accounts that are restricted to access only during scheduled employee hours. Access attempts from staff outside of these hours are logged and reviewed (audit).

Level 3: Verify employee identity
Employees with access to sensitive information must use biometric authentication in addition to the controls from Levels 2 and 3. Failed access attempts from staff outside of these hours are logged and reviewed (audit).

Scenario: There, he accesses customer credit card information and begins to make a significant number of retail and online purchases with delivery being made to a warehouse building owned by the casino.
Risks: Direct evidence of casino involvement, difficulty identifying perpetrator
Possible Faults: Lack of security controls governing access to shipping area, lack of package monitoring and handling procedures

Level 1: Security awareness at warehouse
All casino employees (including warehouse employees) must report suspicious activities and deliveries to ISMS staff.

Level 2: Shipping & delivery monitoring
All staff must use the shipping department to send and receive packages. The shipping department maintains records (to, from, date, etc) for all packages and that log that is regularly reviewed. (audit)

Level 2: Video Surveillance
Loading and delivery areas (including warehouse) have camera equipment installed to record activity. In the event of theft or suspicious activity, ISMS can review security video to identify possible violations and identify suspects.

Scenario: Customers begin to complain and it becomes evident that their information has been compromised by the casino. Several guests indicate that they will sue, they call the police, and a huge scene is made.
Risks: Further credit damage, damage to casino reputation, loss of system availability
Possible Faults: Poor identification of incidents events, slow response to incident, poor incident handling by casino management.

Level 1: Training
Guest Relations staff members have written procedures and training in response to possible customer fraud.

Level 2: Rapid Communication program
The Casino has a program immediately notify all necessary internal organizations to the possibility of an incident.

Level 3: Dedicated Response Team
An incident Quick Response Team is created to own communication, information gathering, and incident coordination between all casino organizations. This team has complete responsibility to ensure the problems are addressed and the customer considerations are addressed.