Global Information Assurance Certification Paper

Mission Statement/Objectives:

Missino Statement:

Viva Casinos exists to provide a safe, family friendly entertainment experience providing value to both our customers and shareholders. We provide this value in a moral and ethical manner. We are always looking for new ways to improve and expand so that we can offer even more value to our customers and shareholders.

Objectives:

Viva Casinos provides a safe environment for the enjoyment of our guests. We respect the privacy of all our guests and will treat all information about our guests as confidential. Our Casinos welcome everyone regardless of race, sex, nationality, age or any other differentiating factor. We will offer the widest and best array of entertainment of any casino to our guests.

Viva Casinos will comply with all laws, regulations, and rules issued by the federal, state and local governments and the Nevada Gaming Board. We will make decisions based on the principles of security, ethics, and revenue, in that order.

In order to provide the maximum value to our customers and shareholders, Viva Casinos will search for ways to improve and expand. Areas where we can better serve our customers or create more revenue for our shareholders will be sought out and developed aggressively.

Maturity Model for an Issue:

Confidentiality customer data

- Level 1
  - Confidentiality policy signed by all employees
  - Confidentiality training program
- Level 2
  - Customer data only available through secure "customer service" portals available to agents throughout casino
  - Portals available in private, but monitored and controlled room to track usage and proper data retrieval
  -
- Level 3
  - Wireless handheld pocket computers for all customer service agents with realtime access to all data about their customers
  - Encryption used for communications and storage of this data
  - Custom Application that allows access to only appropriate customers and appropriate levels of data based upon employees job duties

Addressing Objections in Awareness:

1.

- Confidentiality policy signed by all employees
    - Why do we need a confidentiality policy, we never had one before.

The users will be concerned about why we have to have a confidentiality policy. What if they "have" to break the policy to get their jobs done – what will happen to them? This seems rather "big company-ish" and legalistic

Awareness Plan:

Send weekly emails to the employees with sample situations taken from the policies. We'd send an email each week with a situation related to one of our policies every week. Some weeks it would be drawn from the confidentiality policy. For example, we might use an example of grandpa calling from out of state to see what day his family checking out of the hotel and which flight they will be on. Would the customer service person give out the info? The situation would be setup in the email and the question asked, but for the answer they'd have to click on a web link to get the correct answer or end of the story. We could use the link and website to keep track of which employees are going to the site and which aren't. This could then be fed back to managers whose employees aren't reading through the end of the story and the reasons for the different policies.

Why will this plan work:

This keeps the policies in front of the employees every week. The goal is to keep the stories interesting and fun. Hopefully some of them will be clever enough to result in "water cooler" conversations about the situation and why a policy exists. The constant interaction with the employees through email and the website will encourage them to keep the policies on their minds and when they find themselves in a situation, they'll likely remember a related story and/or the policy.

2.

- Portals available in private, but monitored and controlled room to track usage and proper data retrieval
    - Why only in certain rooms and why are these rooms monitored?

The users will be concerned about being forced to use a room that is "monitored" and controlled – control is really just a form of monitoring after all. Is the company checking up on me? What about my privacy when I'm in that room looking up customer data?

Awareness Plan:

We will discuss this concern during security awareness training with a story. We'll tell a story about a customer service rep at another casino. There was "high roller" in town at our casino and lots of people knew. The customer service rep was pulling up client information in an insecure location. Two thugs saw her log in and then took the

opportunity to "jump" her to get access to the database. They were after personally identifiable information about the high roller, and possibly after his room number. The thugs were interested in either robbing the guest, or stealing his identity. The employee was just doing her job when she was physically hurt so that somebody could get at the customers info.

Why will this plan work?

This plan shows that the use of these rooms is actually a safety mechanism for the employees. The company is going to some expense to try and keep our employees safe. The data our employees deal with is very valuable to lots of people, many of whom will commit violence to get the data. We are interested in not only our customers security, but also our employees safety.

3.

- Custom Application that allows access to only appropriate customers and appropriate levels of data based upon employees job duties
    - Why can I only see certain customers data?

The users will be concerned about the company not trusting them. They used to be able to see data on all of our customers – now they are restricted to just data they need to know. Doesn't the company trust them? What if they need access to more data?

Awareness Plan:

With the announcement of the new application, we'll include a short list of "pre-emptive" concerns and answers. This concern will be addressed in 2 parts. First, its not about trust, if the company didn't trust you – you woldn't be working here. A casino is based on trust between employees and the company. We trust you to handle money, food, alchohol, machinery and equipment, etc. If you weren't trusted, you would have already been terminated. Secondly, if you went to the hospital, and your personal information (weight, height, reason for treatment, annual income, complete medical history, social security number, etc.) were given to every employee in the hospital, how would you feel? Not just your doctors and nurses, but also the janitors (day and night shifts), cafeteria staff (no wonder they are all laughing at you when you get your lunch), and even the hospital IT staff (imaging the emails about you) all get your complete personal information. Not such a good idea? We have the same respect for our customers privacy that you would want when entering a business.

Why will this plan work:

This points out first that its not about trust. Secondly, it gives the employees an example they are familiar with. It puts them in the customers shoes and shows them how giving out too much information is inappropriate and should be avoided. Also, since we will include this concern in our original communications about the new program – we are pointing out that we know it's a concern and addressing it up front before they have time to "Stew" on it and get worked up about it.

Business Continuity Plan:

Issue: Customer data only available through secure "customer service" portals available to agents throughout casino

Worst case outcome: Our secure customer service portal is unavailable.

The unavailability of our portal could occur in many ways, it could be from data corruption, it could happen from a physical failure, or it could be the result of a targeted attack (physical or electronic). Since these types of incidents would result in similar outcomes – our current customer service application is no longer available, we have a single continuity plan for dealing with them all.

In the event that a data corruption has occurred in our customer service application, all our layers of physical redundancy don't matter. Because of this, we utilize mass storage systems, specifically NetApp filers. This "disk drive" gives us the ability to take "snap shots" of the data periodically. Our current policies perform this function every 10 minutes and retain the snapshots for 8 days. If we discovered the data corruption within the first 8 days of its occurrence, we could simply roll back the data to a copy from before the occurrence. (Identification of the time of occurrence is a key piece of the incident handling procedure found at http://inweb.vivacasinos.com/dept/security/procedures/incidenthandling.pdf).

Once a data corruption has been identified:

1. Contact the Incident response team
2. The incident response team will assess the extent of the corruption.
3. If the data loss is small, manual repairs to the data will be performed.
4. If the data loss is extensive, or manual repairs cannot be made, a backup of the data is used to return to a "known good state"
5. The incident response team will contact the System Administrator for the affected application
6. The SA and the Incident response team will identify a good copy of the data from the snapshots
7. The last snapshot will be verified.
8. The "last known good copy" snapshot of the data will be imported into the current database.
9. The now current copy of the old data will be verified for accuracy and completeness.
10. An immediate snapshot of the data will be taken.
11. The system is now back online with accurate data.

Risk Assessment & Recommendations

> The "last known good copy" snapshot of the data will be imported into the current database.

Based upon an event tree analysis of this step, Viva Casinos may be able to improve this process. Event Tree analysis of this process indicates that attempted recovery of the archived data may be impossible and/or result in an unacceptable failure. If the archived data wasn't found or was found to be inaccurate, or the identification of the "Last known good copy" of the data took longer than the SLA for recovery, this would be an unacceptable failure. Potential root causes of this failure could be that the data was never verified after the archive was made or the archive recovery process is too time consuming.

To mitigate these two risks, I would recommend the following changes to the current processes of Viva Casinos: First, the data archiving or "snapshot" process needs to be audited. On a periodic basis, the snapshots need to be verified. A level 1 response to this control would be a manual check of the snapshot, or an advanced version of this control would be a fully automated system that verifies the integrity of each backup as soon as it is made. Verifying the data ensures that we will have backup data to recover too in the event of an outage. Secondly, I would recommend extensive training for the system administrators responsible for the recover of data to the customer service portal. A well trained employee in this situation will be able to recover much quicker and much more reliably than a novice employee. Due to the critical nature of this data and the potential for large financial losses when this system is unavailable, extensive training of the appropriate system admins would provide a much more reliable and timely recovery.