HOW DO YOU KNOW WHAT YOU DON'T KNOW?

By Stephanie Maddocks

It sounds like a funny question, but when you start to think about it, it can lead to a little bit of panic. Jeez, how do I know what I don't know? Where do you go to find the answer when you don't even know the question to ask? When I do training on technology risk assessments, I start by asking this question. People don't know how to answer and sit there with a puzzled look on their face. It could be that it's usually morning and they have not had enough caffeine yet, but I'd like to think it truly challenges them to think about what they don't know. And to be fair, I do put the question in the context of gaming systems and technology, because I'm not prepared to discuss quantum physics or the genesis of the universe that early in the morning, either.

Here are some samples of questions that highlight systems technology risks within a casino operation. Do you know the answer to the following questions about your casino operation?

1. How often are your system passwords changed?
2. How often do player's club points expire?
3. How much can a casino employee can comp a guest?
4. How many people does it takes to authorize a $2,500 jackpot?
5. What is the maximum amount of points that can be adjusted onto a player's account in a day?

So while you're scrambling now to find the answers to these questions, calling your IT department, your internal audit and compliance departments, your marketing department, and your slot director, stop and think about why these questions are important. While the answers are important, the questions are designed to show casino management and regulators where risk lies within their operations. As part of our risk assessments, we examine various aspects of the casino's operation to highlight opportunities for fraudulent or improper transactions and risks to your data and network infrastructure.

How often is your system access password changed? Passwords can be the weakest link in a computer security scheme. Shared or copied passwords are one of the easiest ways to create a false transaction. If one employee knows another employee or supervisor's login and password, they can create bogus transactions, authorize fraudulent transactions or place the blame on an innocent employee. Many systems require password changes every 90 days; however many systems allow the user to re-use their previous password, which really isn't a change, it's just changing the password updated date. Password security is one of the primary safeguards for your data. Ask your IT department to confirm that you have a password security policy in place that defines how often and how passwords are changed for all operational systems.

How often do player's club points expire? Player's club points can be converted to cash in many casinos where they can be redeemed at the gaming device for credits as well as utilized at locations throughout your resort for goods and services. Player tracking systems allow many levels of casino employee's access to points for redemption, adjustment, expiration and revival. Employees in collusion with each other and with guests can easily steal funds with these system tools. Timely expiration of points is one line of defense against the creation of improper redemption transactions. Ask your marketing department how often they expire player's club points and how they handle unused accounts.

How much can a casino employee comp a guest? A wide-open and generous comp authorization matrix creates the opportunity for excessive comp issuance and redemption transactions. Additionally, without proper comp audit procedures, casino employees and guests can take advantage of the free goods and services they receive. We've seen systems configured where employees with player tracking system access could comp guests up to $5,000,000,000 (yes, that is $5 billion). Yes, this is an extreme example, but since complimentary dollars can be equivalent to cash, this is essentially the same as leaving the door to the vault open. Ask your audit department how often they review complimentary transactions and who maintains and authorizes changes to the comp authorization matrix.

How many people does it take to authorize a $2,500 jackpot? Incorrect jackpot payout limits provide the opportunity for employees to generate jackpot transactions that are greater than the amounts in the casino's Minimum Internal Control Standards. Improper jackpot authorizations can create collusion opportunities between casino employees. Interfaces between jackpot payout software and jackpot payout kiosks can result in improper funds being dispensed from kiosks. These are just three examples of jackpot scams. And now we're talking about *real money*, because jackpot payouts are made in cash. Ensuring that passwords are secure and jackpot authorization levels are maintained within the guidelines of internal controls and operational integrity is paramount. Some of the largest system scams to date have involved fraudulent jackpot transactions. Ask your slot department not only what the jackpot authorization matrix looks like, but how they schedule their employees to avoid collusion relationships.

What is the maximum amount of points that can be adjusted onto a player's account in a day? As mentioned above, points are equivalent to cash in many casino marketing configurations. If player's balances can changed, the proper controls must be in place to ensure that only supervisory personnel have access and that the audit department is reviewing transactions on a daily basis. Additionally, automated programs that update points, such as double bonus point times, or group events, or external third party software systems can also impact player's point balances. Many points-based scams evolve from incorrect point adjustment configurations and user access to adjustment and account merges. Ask the IT and marketing departments to review their user access parameters to see who has conflicting access to adjustment and redemption transactions.

Gaming commissioners, state and tribal regulators, internal auditors and compliance personnel are responsible for reviewing gaming operations and ensuring the assets of the organization are protected. When a business completes a financial audit, they typically utilize external auditors to review the financials as an independent and impartial auditor. There is just as much financial exposure through gaming management systems. In many instances, it benefits the organization as a whole to utilize external technology auditors who can provide impartial system configuration and operation reviews.

Technology risk originates from many sources. Internal risks come not only from blatant theft, but also from unskilled and untrained employees. Many employees think just because they have permissions to perform a specific function, they need to try it, even though they may not understand the implications of their actions. External risks can come from your vendors having unmonitored access to your systems. And, of course, the casino's own customers can be a threat alone, or in collusion with internal employee resources.

Understanding the source of technology risks and threats lays the foundation for closing the gaps within the operation. While a system audit is the first step to identify issues within technology system configurations, training and re-training on system configuration, operations and audit is key to ensuring that system risks are resolved. New hires, turnover and promotions each create educational opportunities for systems training, job skills training and an overall re-education on the casino's operational practices.

Learning "what you don't know" is important and scary at the same time. External resources for systems auditing are available and these experts can provide a thorough review of your technology configurations. A successful technology audit must include a review of casino operations and a review of system technology configurations and then a comparison of these two to identify gaps and provide mitigating strategies to minimize or eliminate risks. Because systems are ever-changing with upgrades, new modules, and new interfaces, risk assessments are best performed at least quarterly, in conjunction with daily, weekly and monthly audit procedures to review transactions on a timely basis.

While I might not be an expert on quantum physics (thank goodness!), I do know that protection of a casino's assets and integrity are essential to successful casino operation. It is possible to know what you don't know. Just ask.

STEPHANIE **MADDOCKS**

Stephanie Maddocks is President of Power Strategies, a Las Vegas-based technology consulting company that provides technology selection, planning and implementation, and business operations services. She can be reached at (702) 460-6600 or stephmaddocks@gmail.com.