Salim Adatia

Chief Executive Officer, GLI Interactive

PGRI Introduction: Established in 1993, and having established itself as one of the world's most experienced gaming test labs, Technical Systems Testing (TST) became a part of Gaming Laboratories International (GLI) in 2010. GLI has laboratories all across the globe and work closely with industry operators, software suppliers, gaming manufacturers and jurisdictional regulators to verify compliance with stringent regulatory requirements, supplier technical specifications, and world best-practice industry standards. Their clients include gaming regulators in jurisdictions all over the world, more than 450 in all. GLI employs a world-class team of professionals that test and certify equipment, including mathematicians, hardware and software engineers, compliance engineers, system and communication engineers, high-tech engineers and quality assurance specialists. GLI's dedication to service and preserving the integrity of the gaming industry has earned it a very special place in the industry.

The consumer is driving the current expansion of platforms, channels, and increasing variety of games, making this an incredibly exciting time of change and progress. This expansion has introduced increased levels of complexity that need to be managed properly. The CIO may be responsible for implementation. But there are some basic concepts, like layered levels of security, like Funds Transfer Blocking (FTB), like specific project management principles, that should be understood by everyone, including the CEO. Reputation and brand equity is everyone's business, including or even especially the CEO. The multi-channel approach that all successful operators are rushing to implement makes system security more complicated, and more important, than ever.

I turned to Salim Adatia to help me sort out these issues as communication and transaction-processing technologies change the face of the gaming and lottery industry.

Paul Jason, Public Gaming: *Where are the fault lines with respect to the integrity of operating systems?*

Salim Adatia: The first fault line occurs at the beginning of the process, when the operator first starts to think about any new initiative - be it a new game, new channel of distribution, new medium of communication, or whatever. This is a complicated business, involving game development, market development strategies, acquisition of hardware and communication technology, new transaction-processing technology, and so much more. The key is that security and preservation of system integrity needs to be a part of the dialogue from the very beginning. Unfortunately, it often-times is not. And then, when it is introduced to the process, it is assigned to the CIO who is left to figure it out in a vacuum. And even then, it sometimes does not get the resources it needs because security is a viewed as a cost center that does not contribute to the revenue generating mission of the business.

The first problem with this scenario is obvious. The technology that ensures system integrity may not be a revenue generator, but even a minor compromise of security can be devastating to the business, to the brand, to the reputation - business assets that can be priceless because they are so hard to rebuild. The second problem is not so obvious. It costs more to overlay the technology onto an existing infrastructure than it does to integrate new IT and security into the system from the beginning. And the results are so much better if system integrity is a priority from the very beginning. So, the first fault-line to close would be to have the CIO (or equivalent) be a part of the executive team from the very beginning of the process, and for the CEO to have this basic understanding of the how and why system integrity needs to be baked into the process from the beginning. Budgeting from the beginning for robust security and system integrity technology and processes absolutely saves money in the long-term, produces superior results in the form of a fully integrated technological infrastructure, and protects the most valuable assets that a gaming operator owns: their reputation and brand equity.

The relevance of this idea would seem to be compounded as we enter an era of multiple channels and the management of consumers' personal information.

S. Adatia: Of course. The more access points there are, the more important it is

to have higher levels of security to avoid compromise of the system. Think about iGaming, especially the social games, and distributed networks of electronic games. Then think about how player information will soon be, and in some cases already is, migrating across these different platforms. The complexity and number of access points not only increases, it explodes exponentially. The importance of budgeting for effective security in the initial stages of building the system becomes critical. A failure to do this ends up costing more in the long-term and a lapse in security can negate everything the business has invested in building.

Project management is a challenge because input from the different corporate divisions is needed but there really needs to be one project manager who has the ear of the CEO and the authority to coordinate the input from marketing, operations, finance, sales, customers service, and all others with IT.

What exactly is meant by "system integrity"?

S. Adatia: Security can be broken into three different spaces. First, transaction processing must be error-free. Second, personal information must be protected. And third, fraud must be prevented. Failure in any one of those areas would be hugely damaging to any business. Proper investment in, and management of, a robust system to preserve security on those three fronts should be considered mission-critical.

The registration process required to open an internet account of any kind involves the storage of personal player information. That is true for internet gaming of any kind, even play-for-free. The minimum information is name, e-mail address, and date of birth. Electronic financial transactions include extremely sensitive banking information. All of this personal information must be safeguarded. Regardless of whether any money is being transferred, protecting the privacy of the consumer is mission-critical. And then there are external threats. The threats can take the form of malicious attacks without discernible objectives, or people that are trying to thwart or manipulate the games for their own personal gain, and people attempting to just get the personal player information to leverage for their own personal gain.

There are also internal threats. Fraud prevention needs to focus not just on external threats of cheating, malicious hacking, money-laundering, and theft of personal player data. Protection from compromises that come from within the organization are just as important, and requires even higher levels of security because of the increased number of access points that exist from within the organization.

Two benchmarks that provide assurance that an effective security system has been implemented the standards and certifications provided by ISO 27001 and also World Lottery Association (WLA) Security Control Standards.

France is having trouble keeping out illegal internet gambling operators. Why is that? We know that the technology and capability is there to control access, and identify the criminals and enforce the laws on illegal operators. Fund transfer blocking (FTB) has proven to work effectively as has UIGEA-type mechanisms that enlist merchant banks in the effort to stop illegal iGaming that involves criminal financial transactions.

S. Adatia: The technology to safeguard information is proven to be reliable. Online banking and internet gaming itself has been operating for years without incidence of technical failures. Cases of fraud that the industry has recently seen, were cases of internal criminality, not compromise by external threats and technical failure.

France is one of the jurisdictions where they really depend upon the internet service provider, or ISP, to block unauthorized URL. In order to be a permissible gaming site within France, the operator must have a ".fr" URL extension. That still leaves an enforcement challenge for the ISP's, which are not set up to be an enforcement or policing agent. The ISP's are really looking for some guidance on which sites to black-list or prohibit.

Why is that a challenge? This is the list of legal operators and websites. If they are not on this list of legal sites, you block them.

S. Adatia: It is not necessarily a challenge to make the list and block the sites not on the list. The challenge is to keep up with it. It is very easy for illegal operators to have a system of putting up new sites whenever the old one is blocked. You are correct in saying that it should not be that hard. It's just that someone needs to allocate the resources and manpower to do it.

Maybe there could be a form of mutual recognition that is working in reverse of the way the remote operators would want it to work. Instead of recognizing the right of operators to operate everywhere if they are licensed in just one EU jurisdiction, each country could recognize the rights of neighboring countries to have laws and enforce those laws. Wouldn't Italy or Spain, or even Malta or Gibraltar, extradite convicted criminal back to the country where the crime was committed? Why not turn over the criminals who operate illegal gambling establishments in the same way?

S. Adatia: There's nothing really to stop that kind of collaboration to fight illegal gambling. There is evidence that regulators are working towards some form of that. Regulators from all the different jurisdictions are meeting with each other to address these and many other issues. And we sponsor Regulator Roundtables to provide information and the tools to know what their options and technical capabilities are. The Roundtables also serve as a forum in which they explore issues like this work to solve cross-border problems. And our job at GLI is to take direction from the regulators and help them to understand the technology and means of enforcement. We do not get involved with the political and legal dimensions of these issues.

U.S. state lotteries could benefit by collaborating on internet gaming, much like they do on multi-state lottery games. What kinds of security and systems integrity issues will they need to think about?

S. Adatia: Implementing a multi-state internet gaming platform will require a more complex IT infrastructure than selling lottery tickets. But many of the same issues need to be addressed. Simple questions like, where will the central servers reside and who will manage them? Who's going to monitor them? If you're going to engage a third party to monitor it, who's going to be in charge of that and who will have final decision making authority? If some portions of IT requirements are outsourced, how will you decide exactly what will be outsourced? And how will you en-

…continued on page 34

sure that the third party service providers are held to the highest standards, because these service providers will have the keys to the kingdom as well? Which jurisdiction will have final say or how exactly will all the countless decisions be made? What exactly happens if a dispute arises between players from two different jurisdictions? Or when one jurisdiction has a problem with a service provider who reports to another jurisdiction? Or, where criminal charges that involve parties from two different jurisdictions, whose laws apply? There are many detailed questions that need to be addressed ahead of time to avoid confusion and potentially crippling conflicts when these issues arise. Most importantly, a clear definition of responsibility and accountability is the first step towards building an effective IT system with the right kinds of security and controls. In today's electronically oriented business world, it is more important than ever for enterprises to get security and integrity right. For that reason GLI has assembled the world's leading experts for one reason: to protect your business and its profitability. Our Professional Services group at GLI is one that you can rely on for accurate, up-to-date, professional audit, diagnostic, testing and advisory services.

As games are implemented across different channels, and consumers access the games from different devices and media, doesn't that create a whole new level of complexity to secure this kind of a system?

S. Adatia: Multiple channels of distribution do mean more access points. The more system access points you have, the more difficult it is to secure. Combine that with distributed venue models, electronic machines installed in a large number of venues over a big geographical area, and the challenge is compounded. Building in the highest levels of security becomes even more important for that reason. The technological sophistication of the systems that deliver central server-based gaming across multiple platforms requires an equally sophisticated layered approach to building security and integrity into the system. Fortunately, all the technological tools and the skills to implement them are readily available.

What is meant by "layered approach"?

S. Adatia: This is a simple but vital concept. The most important element to effective security is having a robust layered approach. The key concept to understand is that nothing is 100% guaranteed. Misplaced confidence that a particular feature, process, or security measure is fool-proof is what leaves systems vulnerable. Nothing is fool-proof. There is, though, a way to make a system totally secure. The application of different layers of security can render a system impregnable. Think of it as a number of different nets that have been layered one upon another. Adding multiple and different kinds of layers of security effectively plugs all the holes and becomes virtually impossible to penetrate. Some of those layers should be provided by a third party to ensure the patterns are different and can't be deciphered by criminals. The registration process, age and identity verification, credit rating mechanisms, geo-location verification should all involve a third party agent to ensure that your in-house team is not inadvertently leaving clues and footprints for criminals to decipher. This layered approach to building a robust system of controls is effectively fool-proof.

Think about how banking has evolved. We no longer think twice about transacting business through the ATM or over the Internet. We trust the system to be secure, mistake-free and impenetrable to criminals. All the same tools are applied to internet gaming and deliver the same level of glitch-free security.

Any particularly challenging weak link in the process of securing the system?

S. Adatia: We need to have sophisticated communication protocols and encryption to thwart what's called "man in the middle attacks". That's where somebody is trying to acquire confidential information by interrupting the flow of data while it is in the process of being transmitted, while it is in the channel. Once interrupted, the criminals attempt to gain possession of it by re-routing the data to their own unauthorized server. Multiple distribution channels create not only more access points, but also more communications and data flow. Then, when you add in the complication of multiple jurisdictions that include multiple system administrators and monitoring centers, the business of securing the system becomes even more interesting.

It would seem that the challenge increases exponentially as the number of access points increases. How does GLI help its clients deal with this complexity?

S. Adatia: It's our job to stay not just one step ahead of the technology and anticipate new areas of vulnerability, but to stay three steps ahead. Our clients expect us to counsel them on how to future-proof them so that their systems provide maximum reliability and security even as the sophistication of hackers and criminals increases over time. It is our business to identify best practices and technology to help regulators, operators, and systems and software suppliers to always be ahead of the game.

I have always thought of GLI's leadership role deriving in part from your genuine desire to help the industry. You have a business model and clients who pay for your knowledge, consultation, and testing capabilities. And yet you share your knowledge and skill-sets with the industry for the benefit of everybody and the industry as a whole.

S. Adatia: GLI is in a special position to help the industry. That is our business, and it is also our mission to help the industry, completely apart from our own business agendas and objectives. Our decades of experience with numerous jurisdictions that are both long-established and emerging new markets gives us a perspective that we are pleased to share with everyone. We work so closely with operators, regulators, and commercial suppliers, that a wealth of information passes through us that could help everyone to improve the way this industry operates. So we hold regular roundtables with regulators and operators to help them to understand the business, especially the way in which technology is evolving and the impact of that on issues of security. I think a lot of the industry brain-trust would stay locked in silos if we did not do what we do to facilitate its dissemination throughout the industry. We also have internal networks that push information out to all our different clients, sharing ideas and alerts that

help everyone. An example of this would be our GLI Client Advisories. We are also proud to develop and share our technology to increase overall industry integrity - for example GLI Access and GLI Verify tools. Technology has always evolved and improved at a pace that's faster than the shapers of public policy can move the regulatory frameworks forward. The only way to accelerate the rate of adoption of regulatory structure is to facilitate understanding by sharing information.

It seems like the challenge of keeping up with technological progress will only get more difficult. Cloud computing will now add a whole new layer of complexity. Will public policy and regulations ever catch up with the industry?

S. Adatia: No. Technology has always evolved faster than the laws and regulators can keep up with. That won't change because by definition the laws have to apply to existing technology and circumstances so those technologies and circumstances have to come before the laws and regulations. The only way for laws to catch up with technology would be to stop technological progress and nobody wants that to happen. That is, of course, one of GLI's primary missions: to analyze emerging technologies and how they will be integrated into existing infrastructure, assess the impact they will have on the industry, and share this research with regulators. You are correct to question whether the increased rate of technological change will be even more challenging for regulators and lawmakers to keep up with. The answer is yes, and we are also picking up the pace to help everyone keep up. In fact, the challenge to do so has inspired us to find better ways of keeping our clients better informed and so, perhaps paradoxically, we feel that the regulatory arm of the industry is actually adjusting quite well to the increased rate of technological change.

Another part to your question related to whether the new technologies like cloud computing will make it even more difficult for regulations and policy to keep up. It doesn't need to and we are committed to doing what we can to ensure that it doesn't. GLI will continue to develop the tools and the communications networks and forums to enable regulators to stay abreast of technological progress. Regulators will need to evolve their standards just as GLI continually upgrades its internal standards and processes. Our goal is to help everyone identify and understand the risks and to address the risks in development of the appropriate standards. We do not prescribe solutions as such. Our role is to help everyone understand the technology and intelligently assess the pros and cons of different approaches, especially regulators.

It is not GLI's mission to weigh in on matters of public policy. But this publication has taken the position that prohibition of iGaming only contributes to the growth of the illegal, untaxed, unregulated markets that serve only to enrich criminals and put the consumer at risk of being victimized like they were with the formerly reputable Full-Tilt Poker. Isn't regulation preferable to prohibition as a means of controlling illegal activity?

S. Adatia: You are correct that it is not GLI's place to weigh in on questions of public policy. But, my personal answer to that specific question would be yes, for the same reasons that drive the position your publication takes. Policy-makers are beginning to realize that effective regulation is the best way to protect its citizens from underground operators and also to channel the economic benefits back to support the schools, hospitals, road improvements, and so forth in their own jurisdictions.

It's important to emphasize that GLI is completely neutral as to who should operate iGaming. It could be state lotteries, but it could be casinos, it could be tribes, it could be domestic or foreign operators. It could be regulated by at the federal government level or at the state level. They are all are important constituents to GLI and we are pleased to help them all accomplish their goals. GLI's job is to support whatever system the policy-makers decide to implement, and to help regulators implement it. Our job is simply to ensure that if gaming is taking place through interactive means it is doing so in a manner that is fair, secure, auditable. Moreover that itmeets the proscribing regulator'stechnical standards, and operates as intended both by the operator and the manufacturer.

As regards to iGaming, GLI tests to ensure the effectiveness of all age, identity, location verification tools, and the security protecting confidential information and guarding against money-laundering. What else?

S. Adatia: We test for fairness to the players and non-predictability of the games. That is just as mission-critical as all other aspects of security is to the preservation of integrity and the reputation of the operator. So GLI tests to ensure that the games operate exactly as intended, to be fair and honest and not allow any players to manipulate the play to give them an unfair advantage. We test to make sure the random number generator, or alternative method of game outcome determination used, is unbiased and non-predictable. Part of that is to ensure a properly operating tracking system and database is in place so that if there is ever a dispute, there will be activity logs in place to review the game play history.

Most of these issues are not different from what you have been dealing with for years in the off-line world.

S. Adatia: That's exactly correct. Many of the same principles, and solutions, are simply being updated to apply to new channels and media. I'll circle back to the original example of online banking. e-Commerce sites are now processing much of what was handled at the cash register in a store. The solutions are technologically different, but the objectives and even the fundamental problems are not so different.

Who is your customer?

S. Adatia: Our primary customer is the regulator. GLI serves the needs of different constituents, including the commercial firms who manufacture the products, supply the technology, write the software, etc.; and the operators, casinos and lotteries and such. And we may be called upon to consult for the governments which are formulating policy. We also seek to help facilitate the entire process, identifying issues of risks and non compliance, and to ensure that the process moves fluidly. But our core mission is to serve as an independent testing lab, and in that capacity, our customer is the regulator. ◆