Information Security in the Lottery Sector

By Dr. Christos K. Dimitriadis, CISM, CISA
Head of Information Security, INTRALOT Group

Introduction

The current economic crisis has elevated the need for effective business risk management, while corporations struggle to remain profitable in an ever changing risk environment. The academic definition of information security is *"the preservation of confidentiality, integrity and availability of information."* Confidentiality is the preservation of secrecy of crucial information by ensuring their sole viewing from authorized persons. Integrity is ensuring that information is not manipulated by anyone deliberately or not. Finally, availability ensures that information is at hand when needed.

This article presents the business aspect of information security in the Lottery sector and describes the case study of GIDANI, the National Lottery of South Africa, as an example of efficiently addressing information security needs.

The Business Aspect of Information Security in Lotteries

Lotteries sell games to the public. These games have to be trusted in order to achieve customer (player) acquisition and retention, directly affecting the Lottery's revenue. ***Player trust*** is a key success factor that is directly related to:

- **Game integrity:** each game is conducted as described in its official rules. It is fair to the players, the draw results are integral and winners are selected/drawn and paid according to the game rules. Information integrity (avoiding data manipulation), is a key information security component related to player trust.
- **Player asset protection:** Players need to be confident that their money, credit card numbers, bank account numbers are safe. Especially in online gaming where player participation is conducted with electronic money, players have to trust the lottery for securing their financial assets. Confidentiality, integrity and availability are crucial security parameters.
- **Player privacy:** Players and especially winners are providing their personally identifiable information to Lotteries. As in player asset protection, trust in the lottery is important for making the player feel comfortable with sharing such information. Especially is the case of high winning amounts, the player has to feel safe and his personal data have to be protected.

Providing lottery games to the public also has a societal and political nature/aspect. Lotteries are usually controlled directly by the local government and are always subject to a regulatory and legal framework. The provision of secure and fair lottery games to citizens is a matter of social responsibility. Moreover, in most of the cases the government is a shareholder of the Lottery (directly or indirectly though taxing), thus its business success affects the corresponding governmental revenue and increases the amounts that are allocated to good causes.

The above are clarified in relation to information security if the drivers of ***shareholders' trust*** are studied in more detail:

- Each licensed Lottery has to comply with rules and terms of the license. Shareholders need to be confident that the Lottery complies with the license obligations and the legal and regulatory framework, since this is a main corporate viability factor.
- In competitive environments, where more than one Lottery operates in the same region, or in the case where illegal gambling is present, information security acts as a competitive advantage, which in turn ensures customer acquisition. Shareholders trust the Lottery if it operates as a competitive corporation.
- Shareholders are risk averse entities in relation to the Lottery's brand name. They need to be ensured that the Lottery brand name is resilient to information security threats that may cause reputation loss.

Having identified information security needs in the Lottery Business, a holistic approach is required for addressing them.

Case Study of Effective Information Security Business Modeling

Being an innovator in the Lottery information security field, GIDANI has implemented a business model, in order to be able to understand and address its information security needs deeper and make them an integral part of its business processes. This modeling is based on ISACA Business Model for Information Security[1], illustrated in *Figure 1*.

Information Security at GIDANI is an integral part of the business strategy of the Lottery. **Governing** of all information security activities is the responsibility of an executive committee chaired by the CEO. Strategic plan execution including strategy definition as a result of business analysis (e.g. information security analysis in the life cycle of a new game development), resource management and lottery operations are controlled by the executive committee that monitors security performance, value delivery and risk levels of all integrated information security controls.

From a technical perspective, GIDANI has implemented a Lottery System with built-in security controls from INTRALOT SA, the first international vendor that has been certified according to the most recognized Lottery Security Standard: the World Lottery Association's Security Control Standards[2]. **Architecture** is based on a Lottery-specific threat model serving the security requirements of all critical business

processes as identified through **Governing**. For example, there are technical controls in place for protecting game integrity, controlling access to Lottery business reports, securely managing game configuration, establishing secure communication lines for game transactions (communication between the central system and terminals at the point of sale), isolating the computer room physically and ensuring game continuity by the implementation of a disaster recovery site.

Enabling and support represents how security processes are automated by the use of technology, as well as which processes are used to complement automated security controls, evaluate them and improve them. GIDANI has automated all Lottery related processes by the deployment of the Lottery system. Transaction engine (ticket processing) security configuration, support and operation is implemented by a number of written and continuously improved processes. At the same time, there is a security technology evaluation process in place that is used for calibrating and extending Lottery system security for addressing business needs. For example, the business need for providing Internet gaming goes through a security assessment of the current technology, automation controls are identified (such as the player identity management mechanism) and complemented by manual procedures (e.g. review of player access rights) following official GIDANI rules. Since selling Lottery games through the Internet has been identified as a key business enabler in **Governing**, information security controls become a priority.

Human factors affects both **Architecture** and **Enabling and Support**, since they are used for identifying security issues of the interface of people and technology. For example, if a security mechanism, such as the creation of a new Lottery Operator (who monitors ticket sales), is too cumbersome for the security operator to implement, this issue is reported to the security officer, the technology is assessed and opportunities for improvement or extension are being identified. One improvement may regard the extension of the security training program of GIDANI. Another may relate to the reconfiguration of the security control or its extension.

Culture is an element of the GIDANI security model that has a tremendous positive effect in making information security work in practice. GIDANI is characterized by a clear set of hierarchy levels with the roles of each level having been defined accurately and supported by specific operational procedures. The management model as defined by the **Governing** dynamic interconnection encourages free communication at all levels of personnel, especially as feedback on the security operations is concerned. That means that GIDANI has "low power distance" in terms of free communication of information security matters from the bottom to the top of the hierarchy. For example, if an employee identifies difficulties in implementing in practice a security process or use a security technology, she freely reports it to the security officer for investigating the improvement of the process. At the same time if an employee identifies a security incident (e.g. confidential gaming information left in a meeting room) he reports it immediately as a security incident. This reporting is not translated as an offensive action between employees, but instead as collectivism, giving the opportunity to management for taking preventive or corrective actions.

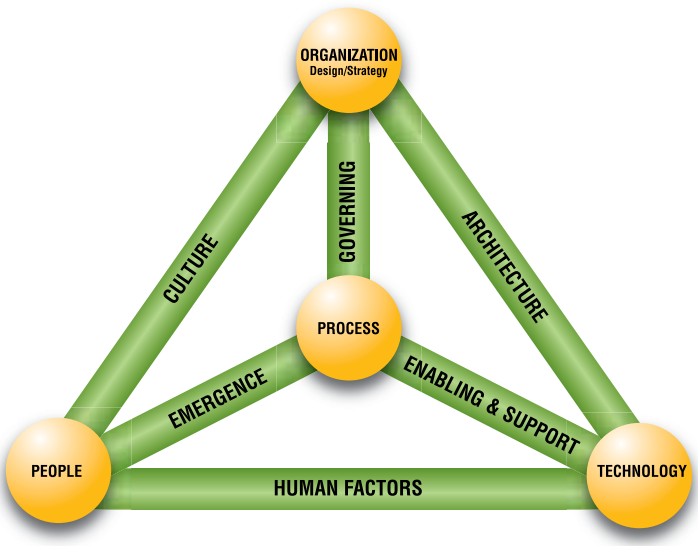

Figure 1: The Business Model for Information Security of ISACA

Emergence is one of the most important dynamic interconnections of the business model since it is dealing with the uncertainty factor in information security at GIDANI. Due to the human nature, the execution of processes within a corporation by people cannot be characterized as deterministic. Despite the detailed procedures, humans sometimes act in an ad hoc manner and make mistakes. Emergence is about the patterns that arise when people execute processes. While nobody can ensure the absence of security incidents, there are solutions through the study of emergence that limit the possibilities to a minimum level. Strong security culture for example, as described above, permits GIDANI to have on time reporting of security incidents. After reporting, the root cause analysis process takes over, where the actual reasons for the realization of the incident are identified and corrective actions are implemented.

For example, a security operator due to increased stress may assign incorrect access rights to a retailer manager (the role that monitors the status of retailers). This will be reported to the security officer through the processing of alerts and logs (potential access to critical information) and by the role that monitors security records (for every change in user access rights a signed form is required). One could assume that this was an unpredictable event (stressed employee). The truth however may relate to an increased workload in defining access rights, caused by a major change in the Lottery System, which in turn makes the user access management procedure too difficult to implement and no longer effective. Through the study of **emergence**, within the framework of the model, GIDANI is in place to link **architectural** changes with **human factors** (usability of security controls), **enabling and support** (combination of technical and procedural controls) and **governing** (limited number of employees in relation to the workload) and correct the user access management procedure on time.

Even then, humans will continue to insert uncertainty in the security processes and some security incidents will still be unavoidable. Through the operation of the model, however, the whole picture of information security will be clearer, providing the opportunity to security experts to learn more accurately from mistakes and improve information security.

Conclusions

Player and Stakeholder trust are the key ingredients of information security in the Lottery Sector, unveiling its societal, business and legal nature. While technical security controls are important, what distinguishes a typical information security management system from an effective one is the ability to correlate all parameters in the operation of a Lottery and especially the human nature. While absolute information security is theoretically unachievable, lotteries have the ability to reduce uncertainty and continuously improve their approaches toward making information security a business enabler. ◆

1. An introduction to the Business Model for information Security, http://www.isaca.org. 2. World Lottery Association, http://www.world-lotteries.org