



Texas Lottery Commission

Internal Audit

An Internal Audit of

Personal Identifiable Information Handling Processes

October 2, 2018

Report #18-001

Prepared by:



This report provides management with information about the condition of risks and internal controls at a specific point in time. Future changes in environmental factors and actions by personnel will impact these risks and internal controls in ways that this report cannot anticipate.



INTRODUCTION

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for the Texas Lottery Commission (TLC) performed an internal audit of the agency’s Personal Identifiable Information (PII) handling processes and internal controls. This audit was included in the approved FY 2018 Annual Internal Audit Plan.

We conducted this audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Pertinent information has not been omitted. This report summarizes the audit scope, objectives and our assessment of TLC’s PII handling processes and controls.

Objectives and Scope

PII is defined as information, in electronic or any other form that can be used:

- ✓ Directly to uniquely identify, contact or locate a single person.
- ✓ With other sources to uniquely identify, contact or locate a single individual.

For the purpose of this audit, PII includes any individual information or combination of full name, date of birth, social security number, medical health records, marital status, financial

data, photographic image, ethnicity/race, school records, biometric prints, tax identification number, and credit or debit card numbers.

TLC is responsible for handling personal identifiable information of commissioners, lottery retailers, bingo licensees, bingo workers, prize winners, employees, vendors and contractors.

We completed the audit of the agency’s PII handling processes to assess management controls in place to ensure reasonable assurance that:

- ✓ PII is protected from unauthorized use.
- ✓ Internal controls ensure regulatory compliance and data protection.
- ✓ Employees, vendors and contractors are trained on how to handle the agency’s PII.
- ✓ Employees and contractors handle PII according to agency policies.
- ✓ Processes are in place to protect against potential data breaches.
- ✓ Processes are in place to quickly identify and respond to potential data breaches.

We evaluated internal controls and business processes related to PII handling for the period of September 1, 2017 through March 31, 2018. Some test procedures were performed as of fieldwork date. This work product was a point-in-time evaluation that cannot address the inherent dynamic nature of subsequent changes to the process/procedures reviewed.



Audit Procedures Applied

Audit procedures applied during this audit included the following.

- ✓ Conducted interviews with division directors and the agency's Information Security Officer.
- ✓ Reviewed the agency's Information Resources Security Manual.
- ✓ Reviewed the agency's employee handbook for confidentiality policy.
- ✓ Observed PII and sensitive data handling procedures in the claims center.
- ✓ Reviewed employee security training roster.
- ✓ Reviewed each division's policies that incorporate PII and sensitive data handling procedures.
- ✓ Reviewed forms that capture PII.
- ✓ Reviewed TLC's incident reporting procedures.
- ✓ Reviewed Information Security Agreement forms.
- ✓ Reviewed TLC building physical access roster.
- ✓ Reviewed information system and applications list for PII contents.

Results and Conclusions

We determined that TLC's processes and controls over PII handling are effective. TLC has comprehensive PII program components in place to cover all aspects of protecting PII in electronic and paper formats. These include policies, processes and training. We noted that the agency's Information Resources Division has processes and controls in place to protect unauthorized access to electronic PII and each of the agency's divisions and departments have controls in place for handling PII. During the time of fieldwork the agency did not have a function or individual responsible for coordinating the agency's data security and privacy program efforts. TLC took immediate actions when we informed the leadership team of this. TLC has now designated an Enterprise Risk Officer to coordinate their comprehensive data security and privacy program efforts. **Figure 1** provides a description of the internal control rating.

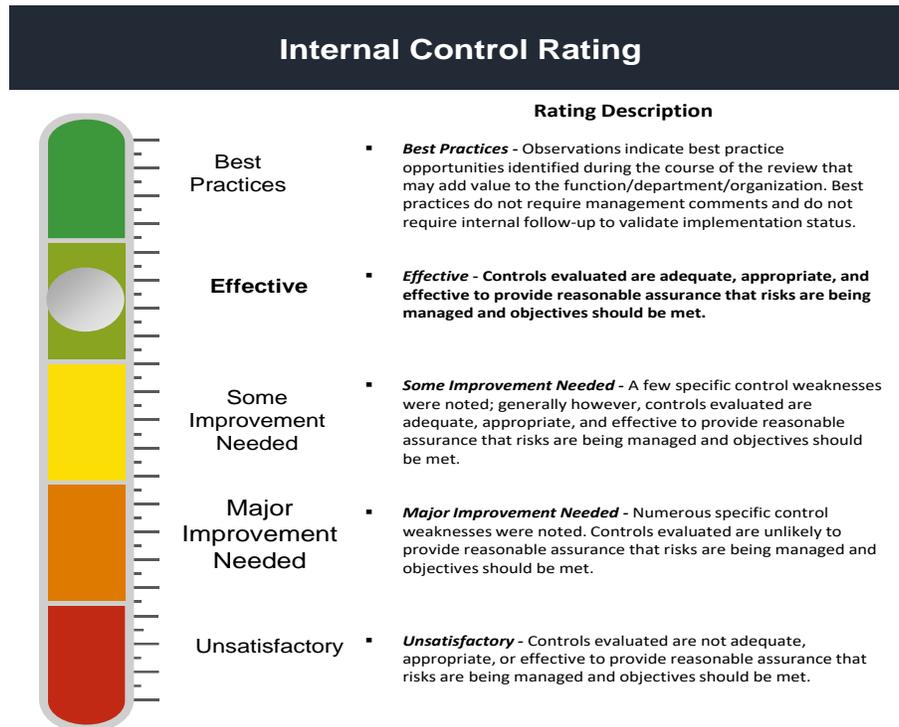


Figure 1 Internal control rating description.

Acknowledgement

We wish to thank all staff involved in this audit for their professionalism and positive outlook towards the assessment of their data handling and security processes. We also are

appreciative of management’s actions to enhance their data security and privacy program components.

BACKGROUND

The Texas Lottery Commission handles personal identifiable information of commissioners, lottery retailers, bingo licensees, bingo workers, prize winners, employees, vendors and contractors. In addition to names, this information includes:

- ✓ Social Security Numbers
- ✓ Driver’s License
- ✓ Birthdates

- ✓ Birth Certificates
- ✓ Addresses
- ✓ Bank Accounts
- ✓ Health Information
- ✓ Family Member Names
- ✓ Criminal Background Check Results

Retailer and prize winner information is maintained in the lottery system which is managed by the lottery contractor as well as



in internal TLC systems. Bingo licensee and bingo worker information is maintained in an internally developed information system. Commissioner and employee information is maintained in TLC’s personnel system and the state’s employee systems. PII information related to complaints and investigations against retailers, bingo licensees and employees is maintained in an internal complaint system. Access to each of these systems is restricted to authorized users.

Some PII is obtained on paper forms. This includes prize winners, retailer license applications, bingo license applications, bingo worker registry applications, vendor banking information, employment applications and new hire forms. Each of these records is maintained according to the respective department’s policies which includes securing the forms in locked cabinets. Access to the TLC building and each department requires authorized electronic badges. Completed prize winner forms are secured at the claims centers in sealed bags in locked safes overnight and then transported to the Austin claims center by a contracted courier.

TLC's Legal Services Division staff includes a Certified Information Privacy Professional/Government from the International Association of Privacy Professionals.

Why Data Security and Privacy Programs Are Important to TLC

TLC staff handle significant amounts of Personal Identifiable Information that is obtained from multiple sources through various submission and collection methods. TLC could suffer significant reputational damage if any of the PII was to be

compromised through data breaches or employee mishandling. This in addition to the financial consequences of remediation efforts makes it imperative for the agency to protect their electronic and paper data.

Currently, there are three primary influences on policies, security and processes that TLC must have in place to protect PII. These are:

- ✓ Regulatory Environment
- ✓ External Environment
- ✓ Customer Expectations

Regulatory Requirements

Personal Identifiable Information is protected by federal and state regulations. These regulations include, but are not limited to:

- ✓ U.S. Privacy Act
- ✓ U.S. Health Insurance Portability and Accountability Act (HIPPA)
- ✓ Texas Business and Commerce Code (Identity Theft Enforcement and Protection Act)
- ✓ Texas H.B.8 – Cybersecurity Act

The applicable regulation depends on the type of data that is handled. Although TLC, as a state agency, is not subject to the Texas Business and Commerce Code, it is important to understand that the state takes protection of PII seriously.

External Environment

Data is often referred to as the “oil” of the digital economy. There is a booming market for personal data. So much so, that companies who own large subscriber information databases often have high valuations, even though the data is a non-tangible asset that has not been sold for a profit.



This proliferation of electronic data and the internet created an underground economy that continues to thrive. This economy has created the following cyber-crime industries:

- ✓ Research
- ✓ Cyber-crime tools
- ✓ Infrastructure
- ✓ Developers
- ✓ Hackers
- ✓ Sellers
- ✓ Buyers

It is important for all organizations to realize that it is no longer a matter of “if” they become infected and breached, it is a matter of “when”. Cyber-attacks are categorized into the following groups:

- ✓ Cyber crime
- ✓ Cyber espionage
- ✓ Cyber warfare
- ✓ Hacktivism

Cyber-crime comprises the largest motivation for cyber-attacks and continues to grow as the primary motivator. **Figure 2** provides the motivation behind the 94 top cyber-attacks reported in 2017.

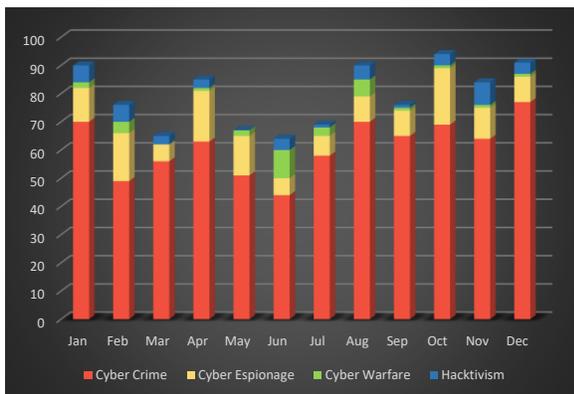


Figure 2 2017 cyber-attack motivation. Source: Hackmageddon.com

The Texas Lottery Commission has large databases of licensee and prize winner data. This information could be very valuable if it were to be compromised.

The sale of personal data has created a marketplace where each piece of information sells for specific prices which are based on various factors such as credit lines, credit card balances and geographic location. The more data that is grouped together, the more valuable it becomes. Bundled information is more desirable because the information can be used to do a lot more immediate damage. Fullz is a term used to indicate that the information being sold is a full package of information; name, social security number, birthdate, account numbers and other data.

Figure 3 provides the average price of personal information sold on the dark web as of December 2017.

Information	Price
Social security number	\$1
Driver’s license	\$20
Diplomas	\$100-\$400
Online payment services login info	\$20-\$200
Loyalty accounts	\$20
U.S. Passports	\$1,000-\$2,000
Credit or debit card	\$5-\$110
With CVV number	\$5
With bank information	\$15
Fullz information	\$30
General non-financial institutions login	\$1
Subscription services	\$1-\$10
Medical records	\$1 - \$1,000
Tax information	\$40-\$50

Figure 3 Average price of PII on dark web. Source: Experian December 6, 2017

While cyber-crime draws the most media and public attention because the single event



tends to impact more individuals, organizations need to protect data on all fronts. This includes their cyber security, employees and devices. According to Shred-It, the loss of portable devices accounted for 41 percent of reported data breaches in 2016. The Identity Theft Resource Center (ITRC) tracks and reports on data breaches each month. ITRC reports that 9,395 data breaches exposing 1,115,562,716 records were reported between January 1, 2005 and August 31, 2018. According to ITRC's 2017 Data

Breach Year-End Review report, almost 60 percent of the 1,579 on breaches reported in 2017 were due to hacking while 10 percent was due to employee error/ negligence/ improper disposal/loss and about five (5) percent was due to theft. This demonstrates a need for organizations to implement a holistic data security and privacy program that incorporates electronic and paper; external and internal threats. **Figure 4** provides ITRC's 2017 data breach by type of attack.

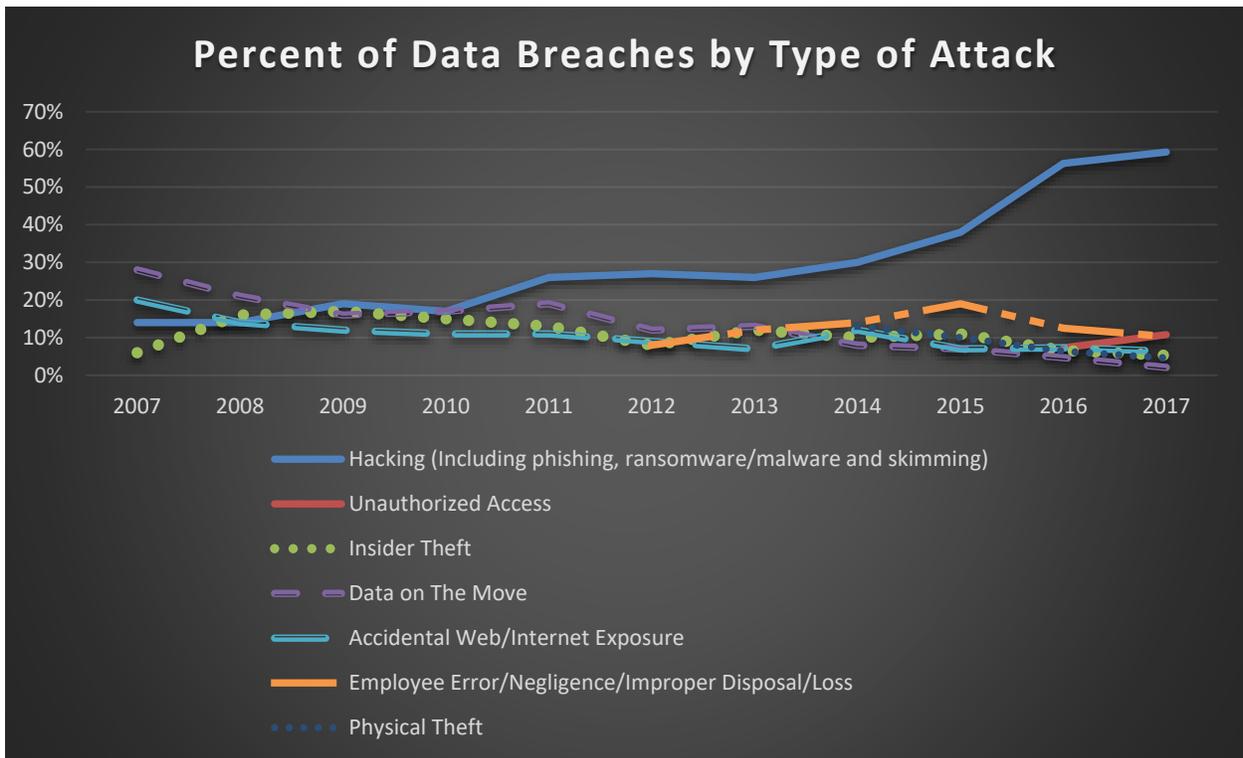


Figure 4 Data breach by attack type.

Source: Identity Theft Resource Center 2017 Data Breach Year-End Review

Customer Expectations

Winners, retailers, licensees and staff have expectations that their information will be

secured and not exposed to malicious attacks or unauthorized usage when they submit requested information to TLC.



OPPORTUNITIES AND RECOMMENDATIONS

This section of the report provides a discussion of the Texas Lottery Commission’s opportunities to enhance their data security and privacy program.

Opportunity 1: Comprehensive Data Security and Privacy Program Coordination

The Texas Lottery Commission does have processes and controls in place to protect PII and confidential data against unauthorized use and recently designated an Enterprise Risk Manager to coordinate the agency’s data security and privacy program.

Comprehensive data security and privacy programs build the organization’s PII oversight framework. A strong data security and privacy program includes defined policies; PII risk

assessments; reporting and monitoring processes; and incident review and reporting. The data security and privacy program also ensures that all divisions, functions and departments follow the same standards when handling PII. **Figure 5** provides an overview of TLC’s comprehensive data security and privacy program components in place at the time of this audit.

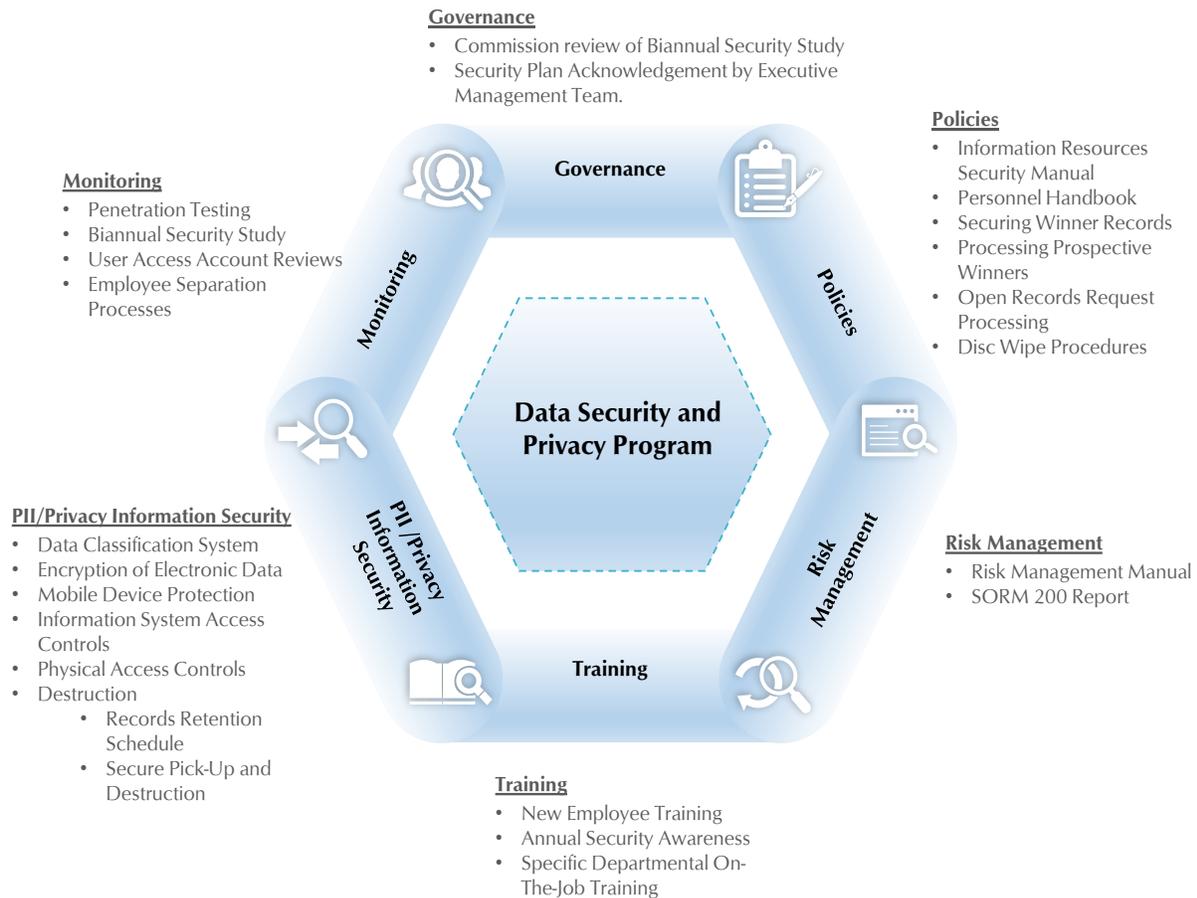


Figure 5 Comprehensive data security and privacy program components.

Organizations must also develop a comprehensive matrix of all the types of information it handles, who handles it, where that information is maintained and how it is disposed of when it is no longer needed. There should be clear written protocols about how to properly handle that information and how to dispose of it, which should include:

- ✓ Disposing applicable paper documents.
- ✓ Permanently deleting electronic files.
- ✓ Properly destroying / wiping old computers and data storage devices.

TLC has an approved agency records retention schedule that is based upon Texas

State Library guidelines. The records retention schedule lists the documents handled by TLC and the retention period.

Additionally, each division’s processes include training staff on PII and sensitive data handling and protection responsibilities. TLC also requires all staff and contractors to review their security training video upon initial employment and as an annual refresher.

Recommendation 1: Comprehensive Data Security and Privacy Program Coordination

TLC should continue to enhance their data security and privacy program through the Enterprise Risk Manager’s coordination activities. This includes preparing a written



document that defines the data security and privacy program components, responsibilities and references supplemental agency policies and manuals that include data security and privacy. Additionally, the Enterprise Risk Manager should report the agency’s data security and privacy activities on a regular basis to the Commissioners.

Management Response: Comprehensive Data Security and Privacy Program

Management concurs with this recommendation. The Enterprise Risk Manager will coordinate with divisions to develop a written document that defines the agency’s data security and privacy program components. The Enterprise Risk Manager will be responsible for updating the document as needed.

Opportunity 2: Information Inventory and Mapping

While each division knows the data they handle in both electronic and paper format, TLC does not have a master listing and mapping of confidential and PII data stored in the information systems and on paper. TLC’s Information Resources Department is responsible for all internal systems used in the agency’s business processes. At our request, TLC’s information security officer completed an information system list that named the system and whether it contained PII. However, this listing did not contain which PII or sensitive data was maintained in the respective system and modules.

enable TLC to quickly identify the type of data that may be compromised in the event of a data breach.

The agency should also prepare a data matrix for paper based information. This matrix would include the document, form or report name; the division or departments that have access to, or use, the respective document, form or report, and the sensitive or PII information that is included; how the document is stored; and when and how the information is destroyed.

Recommendation 2: Information Inventory and Mapping

Management Response: Information Inventory and Mapping

TLC’s information security officer should expand the information system listing to also list each item of PII or sensitive data that is maintained within the respective system. Ideally this would be mapped to the specific module or table within the system. This will

Management concurs with this recommendation. The Information Security Officer will update the information system listing to identify each item of PII maintained within the respective systems. The Information Security Officer will be responsible for updating the document as needed.

Opportunity 3: Staff and Contractor Training

TLC requires all staff and contractors to review their security training video upon initial employment and as an annual refresher. This video covers the basics of information security

but is focused on information systems and is not engaging to the point that it makes individuals think about what they would do in various scenarios that they face in their jobs.





For example, what should an employee do if they are asked to deliver documents for strangers, how employees should interact with new people at conferences and how employees should respond to email and telephone inquiries.

Recommendation 3: Staff and Contractor Training

TLC should explore different security training videos that are more informative and

engaging so that participants gain a better understanding of situations that may arise and how they should respond to various situations that they are likely to encounter.

Management Response: Staff and Contractor Training

Management concurs with this recommendation. Information Resources will update the annual security awareness training to include specific components related to PII.

