City of Austin

AUDIT REPORT

A Report to the Austin City Council

Mayor
Lee Leffingwell

Mayor Pro Tem
Sheryl Cole

Council Members
Chris Riley
Mike Martinez
Kathie Tovo
Laura Morrison
Bill Spelman

Protection of Personally Identifiable Information (PII) Audit

November 2013

Office of the City Auditor

City Auditor
Kenneth J. Mory
CPA, CIA, CISA, CRMA

Deputy City Auditor
Corrie E. Stokes
CIA, CGAP, CFE

REPORT SUMMARY

PII is any data, such as Social Security Numbers or health information, that can be used to distinguish a specific individual or can be linked to a specific individual. Although 88% of departments report collecting some form of PII from citizens, employees, or both, the City does not have an effective process to protect PII. This increases the risk for an unauthorized disclosure of PII, which could harm citizens, employees, or the City.

AUDIT NUMBER: AU13019

TABLE OF CONTENTS

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. 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 findings and conclusions based on our audit objectives.

AUDIT TEAM

Hector Gonzales, CPA, CIA, Assistant City Auditor
Andrew Keegan, CIA, CGAP, Auditor-in-Charge
JoJo Cruz, CRMA, CICA, Auditor

Office of the City Auditor
Austin City Hall
phone: (512)974-2805
email: oca_auditor@austintexas.gov
website: http://www.austintexas.gov/auditor

Copies of our audit reports are available at http://www.austintexas.gov/auditor/reports

November 2013

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AUDIT

Audit Report Highlights

Why We Did This Audit

This audit was conducted as part of the Office of the City Auditor's (OCA) FY 2013 Strategic Audit Plan.

What We Recommend

The City Clerk should create and lead a team of stakeholders from relevant City departments that will develop a compliance and monitoring program to ensure that PII collected or stored by the City is effectively protected.

For more information on this or any of our reports, email oca_auditor@austintexas.gov

Mayor and Council,

I am pleased to present this audit on the process for protecting Personally Identifiable Information (PII).

BACKGROUND

PII is any data that can be used to distinguish a specific individual or can be linked to a specific individual. Social Security Numbers (SSNs), personal email addresses, fingerprints, IP addresses, and driver's license numbers are just some of the types of data that could be considered PII.

Requirements for protecting PII depend on the type of data and are included in both federal and state regulations. Examples include the U.S. Privacy Act, the U.S. Health Insurance Portability and Accountability Act, and the Texas Utility Code.

OBJECTIVE AND SCOPE

The objective of this audit was to evaluate the process for protecting PII that is collected and/or stored by the City.

The audit scope included the City's policies and procedures related to the protection of PII for Fiscal Year 2013. The types of PII data were limited to SSNs, dates of birth, personal medical information, and personal financial information.

WHAT WE FOUND

The Austin City Code requires that the privacy and confidentiality of City records be protected, but the City does not have an effective process to protect PII. A survey of department directors indicated that although 88% of departments who responded collect or store PII:

- 52% of departments do not have written policies and procedures for the collection, access, storage, and disposal of PII;
- 45% of departments have employees who do not receive training on the collection, access, storage, and disposal of PII; and
- 38% of departments do not have an individual who is responsible for the oversight and security of PII.

Numerous public and private organizations have faced issues resulting from unauthorized disclosures of PII. Such disclosures could lead to serious harm, such as identity theft, for citizens or employees. The City could also face significant financial costs, negative publicity, and a loss of public confidence.

We appreciate the cooperation and assistance we received from Communication and Technology Management and City Clerk's Office staff during this audit.

Kenneth J. Mory, City Auditor

BACKGROUND

Personally Identifiable Information (PII) is any data that can be used to distinguish a specific individual or can be linked to a specific individual. Social Security Numbers (SSNs), personal email addresses, fingerprints, IP addresses, and driver's license numbers are just some of the types of data that could be considered PII.

Requirements for protecting PII depend on the type of data, and are included in both federal and state regulations. Examples include the U.S. Privacy Act, the U.S. Health Insurance Portability and Accountability Act, and the Texas Utility Code.

OBJECTIVE, SCOPE, AND METHODOLOGY

The Protection of PII Audit was conducted as part of the Office of City Auditor's FY 2013 Strategic Audit Plan, as presented to the City Council Audit and Finance Committee.

Objective

The objective of this audit was to evaluate the process for protecting PII that is collected and/or stored by the City.

Scope

The audit scope included the City's policies and procedures related to the protection of PII for Fiscal Year 2013. The types of PII data were limited to SSNs, dates of birth, personal medical information, and personal financial information.

Methodology

To accomplish our audit objectives, we performed the following steps:

- conducted a survey of 33 City departments for information related to the collection and storage of PII;
- conducted interviews with employees involved in the protection of PII;
- reviewed policies and training related to the protection of PII; and
- researched available policies for protecting PII in other organizations.

AUDIT RESULTS

An analysis by the Office of the City Auditor has determined that the City does not have an effective process to protect PII.

Survey results indicated that of 88% of departments who responded:

- 52% of departments do not have written policies and procedures for the collection, access, storage, and disposal of PII;
- 45% of departments have employees who do not receive training on the collection, access, storage, and disposal of PII;
- 38% of departments do not have an individual who is responsible for the oversight and security of PII.

Without an effective and efficient privacy program, there is an increased risk for unauthorized disclosure of PII, which could impact citizens, employees or the City.

Finding: The City does not have an effective process to ensure that PII is protected, which increases the risk that citizens, employees, or the City could face serious harm.

The National Institute of Standards and Technology's (NIST) Guide to Protecting the Confidentiality of PII[1] lists several recommendations that organizations should implement in order to effectively protect PII. NIST recommends that organizations:

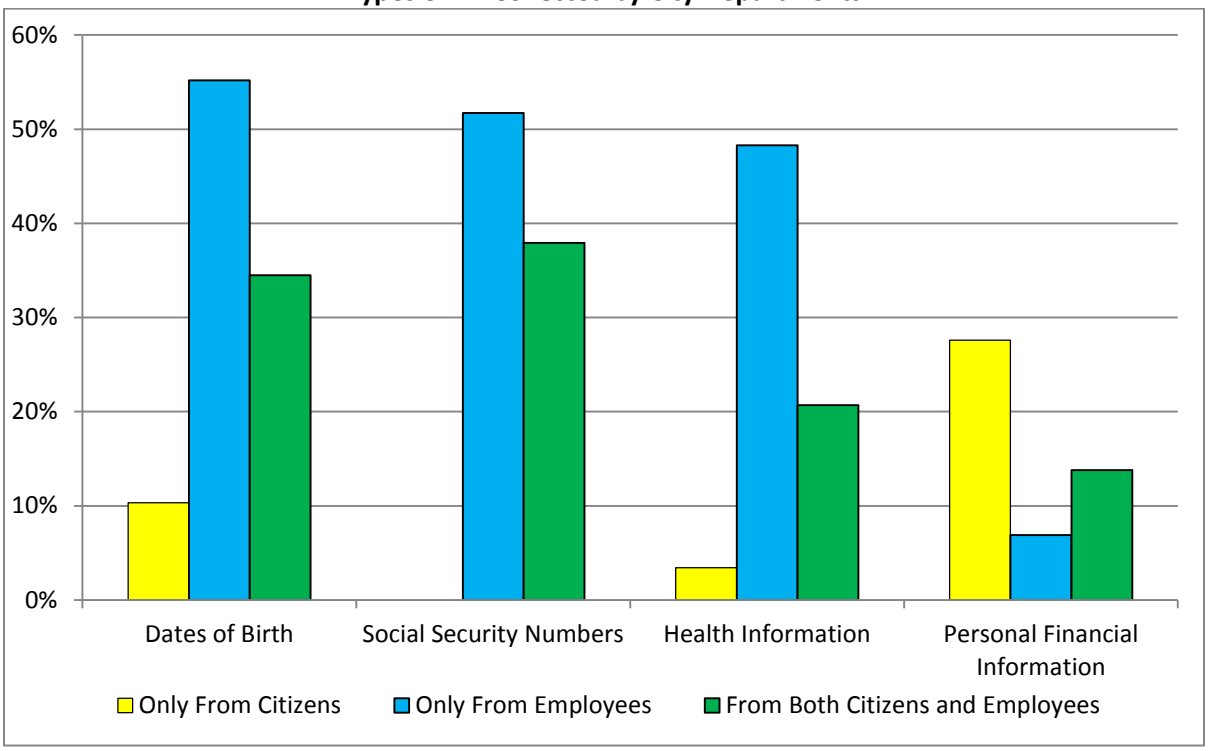
- identify all the PII residing in that organization;
- categorize PII;
- apply appropriate safeguards for protecting PII;
  - policies and procedures
  - training
- develop incident response plans; and
- encourage close coordination among senior officials in the organization.

Section 2-11-5 of the Austin City Code requires that the City Clerk develop a Records Management Plan (RMP). In order to accomplish that task, the City Clerk has identified 10-steps required to create an RMP. The steps identified in the plan include conducting a records inventory of all City records, developing records management procedures, creating a disaster plan, and providing records management training. While section 2-11-3(12) of the City Code references the City Clerk's responsibility for protecting the privacy and confidentiality of City records, according to the City Clerk the original scope of this responsibility is limited to protection of physical records stored in the City Records Center managed by the Office of the City Clerk; the RMP and the 10-step program were not intended to encompass the protection of PII collected and/or stored by the City.

As shown in Exhibit 1, a survey of City department heads indicated that 29 of 33[2] (88%) collect some form of PII from employees, citizens, or both. Although the survey only asked about four types of PII[3], departments likely collect and/or store additional information that could also be classified as personal, sensitive, or confidential.

[1] NIST 800-122
[2] The survey was sent to 40 department heads.
[3] The survey focused on SSNs, dates of birth, personal medical information, and personal financial information.

EXHIBIT 1
Types of PII Collected by City Departments



SOURCE: City department head survey, September 2013

The survey also asked department heads about policies and procedures for protecting PII, employee training related to PII, and the responsibility for the oversight and security of PII. Survey results indicated that for departments that report collecting PII of 88% of departments who responded:

- 52% do not have written policies and procedures for the collection, access, storage, and disposal of PII;
- 45% have employees who do not receive training on the collection, access, storage, and disposal of PII; and
- 38% do not have an individual who is responsible for the oversight and security of PII.

Based on a comparison of City practices to the NIST recommendations for protecting PII, as shown in Exhibit 2, the City does not have an effective process for protecting PII. Without an effective and efficient privacy program, there is an increased risk for unauthorized disclosure of PII. According to NIST, such a disclosure could cause serious harm to individuals and the City. Citizens or employees could have their identities stolen, be blackmailed with sensitive personal information, or face physical harm if medical information is altered. [4] Additionally the City could face significant financial costs in the millions of dollars, negative publicity, and a loss of public confidence.

Appendix B provides details from a 2013 study that examined the cost of data breaches. According to the study, the average breach involved almost 29,000 records and cost organizations an average of $5.4 million, for an average cost per record of $188.

[4] These examples of harm are specifically mentioned by NIST.

Appendix C includes information on recent high profile PII breaches, such as the 2011 breach at the Texas Comptroller's Office and the 2006 breach at the U.S. Department of Veterans Affairs.

EXHIBIT 2
City Practices for Protecting PII Compared to NIST Recommendations

NIST Recommendations	Audit Results
Identify all the PII residing in that organization	▪ 13 of 41 (31%) record types in record schedules for two department divisions that interact with a large population of citizens or employees reasonably contain PII. ▪ One of the 13 (8%) records identified PII in the record description. ▪ None of the 13 included instructions for record disposal.
Categorize PII by potential impact if lost/misused	The impact level, if the information contained in a record was lost or misused, is not used to categorize records.
Apply appropriate safeguards (Policies and Procedures)	15 of 29 (52%) departments do not have written policies and procedures for the collection, access, storage, and disposal of PII.
Apply appropriate safeguards (Training)	▪ 13 of 29 (45%) departments have employees who do not receive training in the collection, access, storage, and disposal of PII. ▪ Of the departments who reported employee training, 6 of 16 (37.5%) referenced the City Clerk's RMP training, which does not cover the protection of PII.
Develop an incident response plan	We could not identify a written plan to respond to the loss or misuse of PII. NIST recommends that a PII incident response plan should include elements such as: ▪ whether notification to affected individuals is required; ▪ timeliness of the notification; ▪ source of the notification; and ▪ contents of the notification.
Encourage coordination among senior officials	We could not identify a citywide effort to protect PII. ▪ 11 of 29 (38%) departments do not have an individual with responsibility for the oversight and security of PII.

SOURCE: OCA analysis of City policies and procedures and results from a survey of 33 City departments, October 2013

RECOMMENDATION

The recommendations listed below are a result of our audit effort and subject to the limitation of our scope of work. We believe that these recommendations provide reasonable approaches to help resolve the issues identified. We also believe that operational management is in a unique position to best understand its operations and may be able to identify more efficient and effective approaches and we encourage them to do so when providing their response to our recommendations. As such, we strongly recommend the following:

1. **The City Clerk should create and lead a team of stakeholders from relevant City departments that will develop a compliance and monitoring program to ensure that PII collected or stored by the City is effectively protected.**

MANAGEMENT RESPONSE: **Concur.** Refer to Appendix A for management response and action plan.

APPENDIX A

MANAGEMENT RESPONSE

City of Austin

To: Mayor and Council

From: Jannette Goodall, City Clerk

Date: November 12, 2013

RE: Response to Personally Identifiable Information (PII) Audit

Section 2-11-5 of the Austin City Code requires the City Clerk to develop a Records Management Plan. In order to accomplish this task, the City Clerk has implemented the "10-Step Program" which is designed to identify City records via departmental records inventories, develop records management policies and procedures, create disaster plans, and provide records management training. The 10-Step Program is based on core records management best practices and was not designed to include the protection of PII. While Section 2-11-3(12) of the City Code references the City Clerk's responsibility for protecting the privacy and confidentiality of City records, the scope of this responsibility was limited to the protection of City records stored at the Records Center.

The development of a Personally Identifiable Information Protection Program is a complex undertaking, requiring the involvement of many City departments and stakeholders. As the Audit findings show, no such program exists in any City department. In the Audit Findings on page 2, five key components of a PII Protection Program were identified. Each of those key components are multi-faceted and will require a detailed action plan having a direct impact on all City departments. A significant level of cross-function collaboration will be required and the City Clerk's Office cannot assume sole responsibility for the development and implementation of such a program if it is to succeed.

The OCC currently has lead responsibility for a number of complex projects including the acceleration of the 10-Step Program, development of a transition plan for Boards and Commissions, updates to existing electronic systems that are impacted by the transition to the 10-1 Council structure, and preparing for the historic election to be held in November 2014. These projects will consume significant resources within the OCC's staff during FY2014. That said, the OCC acknowledges that there is a logical interrelationship between the administration of a comprehensive, City-wide records management program and the protection of PII captured in City documents, databases, and business systems. As a result, the Clerk's Office offered to take the lead on a project to develop such a program as described below.

Recommendation: The City Clerk should create and lead a team of stakeholders from relevant City departments that will develop a compliance and monitoring program to ensure that PII collected or stored by the City is effectively protected.

APPENDIX A

Response: The City Clerk concurs with the Auditor's recommendation and proposes the following:

1. The City Clerk will incorporate initial estimated resources required for the development of a PII Protection Program into its FY15 budget. Those resources may include funding for (a) a consultant to guide the City through the development of a program, (b) a program coordinator to oversee and monitor the program, and (c) funding for a contract to out-source portions of the plan such as the notification process.
2. The OCC will form a task force consisting of stakeholders from relevant departments including but not limited to Communications and Technology Management, Human Resources, Health and Human Services, Financial Services, Communications and Public Information and OCC.
3. The City Clerk will coordinate and facilitate task force meetings.
4. With guidance from the task force, the City Clerk will incorporate the identification of PII into the inventory of physical records and digital management activities included in the response to Resolution 20130523-073.
5. The City Clerk will submit recommendations to the Records Management Committee for revisions to the Records Management Ordinance to define PII and roles and responsibilities.
6. The City Clerk will coordinate the submission of a PII Action Report including required resources and timelines to the Audit and Finance Committee.

APPENDIX A

ACTION PLAN

Protection of Personally Identifiable Information

Recommendation	Concurrence and Proposed Strategies for Implementation	Status of Strategies	Proposed Implementation Date
1. The City Clerk should create and lead a team of stakeholders from relevant City departments that will develop a compliance and monitoring program to ensure that PII collected or stored by the City is effectively protected.	**Management Concurs. See Management Response for additional comments.** **OCC has the following recommendations:** 1. Define Clerk's role in the protection of PII in the records management ordinance for clarification. 2. City Clerk will form a task force consisting of stakeholders from relevant City departments including but not limited to: CTM, HRD, HHSD, FSD. 3. Task Force shall submit a PII Action Report detailing recommendations for implementation, required resources and estimated implementation timeline to Audit and Finance for review.	1. Underway 2. Planned 3 .Planned	1. December 31, 2013 2. August 1, 2014 3. June 30, 2016

APPENDIX B

Ponemon Institute – 2013 Cost of Data Breach Study: United States

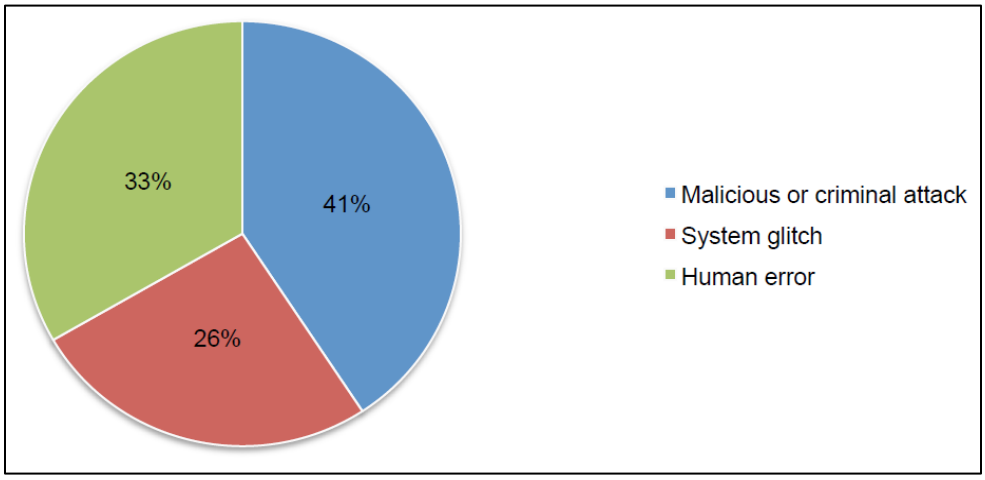
Symantec Corporation and the Ponemon Institute have conducted a benchmark study of the cost of data breach incidents for the last eight years. The 2013 study examined the costs incurred by 54 U.S. companies after those companies had a loss or theft of PII and had to notify breach victims. The number of breached records per incident ranged from approximately 5,000 to over 99,000, with an average of just under 29,000. The average cost of a breach in 2013 was $5.4 million. Breaches involving more than 100,000 records were not included in the study. Results from the study indicate that:

Cost of Breach – The average cost per record lost was $188, which declined from $194 in 2012. Per record costs ranged from $159 for breaches costs by human error to $277 for breaches caused by malicious or criminal attacks. This figure includes both direct and indirect costs. Direct costs include things such as engaging forensic experts and providing credit monitoring subscriptions to affected parties. Indirect costs include in-house investigations and customer loss.

The study only considered breaches of less than 100,000 records, but the size of the data breach and total costs were shown to be linearly related.

Cause of Breach – As evidenced by the Exhibit 2 below, malicious or criminal attacks were the most common cause of a breach.

EXHIBIT 3
Causes of Data Breaches



SOURCE: 2013 Cost of Data Breach Study: United States; Ponemon Institute

Factors Influencing the Cost – The study identified seven factors that influence the cost consequences of a data breach incident, including:

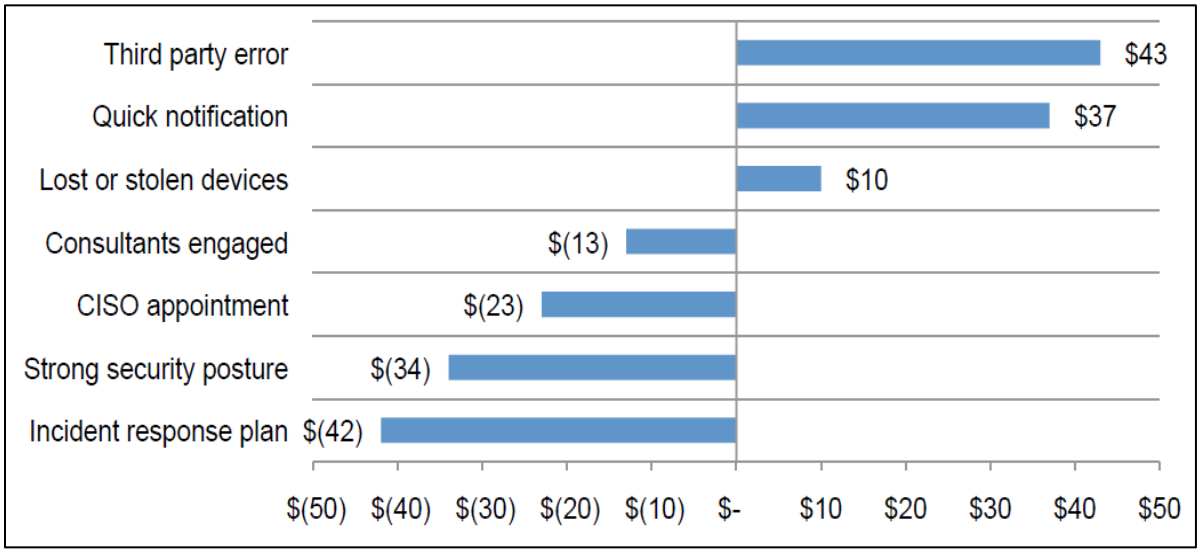
- **The company had an incident management plan**. Fifty-two percent of organizations in the benchmark sample had a data breach incident management plan in place at the time of the data breach event.
- **The company had a relatively strong security posture at the time of the incident**. Forty-seven percent of organizations had a security effectiveness score (SES) at or above the normative average.

APPENDIX B

- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Forty-three percent of organizations have centralized the management of data protection with the appointment of a C-level information security professional.
- **Data was lost due to third party error**. Forty percent of organizations had a data breach caused by a third party, such as vendors, outsourcers and business partners.
- **The company notified data breach victims quickly.** Thirty-eight percent of organizations notified data breach victims within 30 days after the discovery of data loss or theft.
- **The data breach involved lost or stolen devices.** Thirty-five percent of organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
- **Consultants were engaged to help remediate the data breach**. Forty-two percent of organizations hired consultants to assist in their data breach response and remediation.

Exhibit 3 shows the impact of those seven factors on the cost per record in a data breach.

EXHIBIT 4
Factors Affecting Cost of a Breach



SOURCE: 2013 Cost of Data Breach Study: United States; Ponemon Institute

APPENDIX C

Overview of recent PII breaches

Department of Veterans Affairs – A laptop and external hard drive with sensitive personal information of 26.5 million veterans and military personnel stolen from an employee's home in 2006.

Headlines
- "Vast Data Cache About Veterans is Stolen" – New York Times
- "Veterans Angered by File Scandal" – Washington Post
- "Veterans Affairs faulted in data theft" – CNET News
- "VA agrees to pay $20 million to veterans in 2006 data breach" – Boston.com

Financial Cost
- $160.5 million to pay for credit monitoring
- $25 million for a call center and notifications to affected individuals
- $2.65 billion class action lawsuit filed

Texas Comptroller - In 2011, PII for 3.5 million people held by the Texas Comptroller was inadvertently placed on a server that could be publically accessed.

Headlines
- "Breach in Texas comptroller's office exposes 3.5 million Social Security numbers, birth dates" – Dallas News
- "Texas Comptroller takes blame for major breach" –ComputerWorld.com
- "Don't Mess With Texans' Personal Data -- Texas Comptroller's Massive Data Breach Will Cost State Millions – Forbes.com

Financial Cost
- $21 million (potential) for credit monitoring
- $1.6 million for a call center and notifications to affected individuals
- $3.5 billion class action lawsuit filed

Sony PlayStation Network - Sony's PlayStation network was hacked twice within a few weeks, exposing PII for over 100 million users in 2011.

Headlines
- "Sony PlayStation suffers massive data breach" – Reuters
- "PlayStation Security Breach a Test of Consumers' Trust" – New York Times
- "Sony Faces Lawsuit, Regulators Scrutiny Over PlayStation Breach" – Bloomberg.com

Financial Cost
- $171 million for the investigation, customer support, identity theft insurance, and security improvements
- $1 billion class action lawsuit filed
- $20 million (analyst estimate) related to system downtime