Key Ingredients to Information Privacy Planning

Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP
Is a senior associate at Coalfire Systems Inc./Veris Group LLC. He has more than 18 years of experience in IT security and privacy. Wlosinski has been a speaker on a variety of IT security and privacy topics at US government and professional conferences and meetings, and he has written numerous articles for professional magazines and newspapers.

The metrics associated with privacy data breaches are astounding. In 2016, 554,454,942 records were breached from 974 reported incidents.[1] To break down the type of data affected, 48 percent of data breach incidents were for personally identifiable information (PII), 27 percent were for credit and debit card data, and 11 percent were for physical health information (PHI).[2]

The root causes of privacy incidents include the outsourcing of data, malicious insiders, system glitches, cyberattacks, and the failure to shred or dispose of privacy data properly. The human element of data breaches is the result of social engineering, financial pretexting (the practice of obtaining personal information under false pretenses), digital extortion, insider threat and partner misuse.[3] Conduit devices used include Universal Serial Bus (USB) infection, rogue network connections, manipulation of account balances and backdoor access accounts. Configuration exploitation and malicious software are also causes of data compromises.

This article will review many aspects of privacy and is intended as a primer for information privacy. Topics to be reviewed are categories of privacy, privacy officer (PO) concerns, governance strategy, privacy controls and the privacy plan.

Categories of Privacy

ISACA® has identified seven categories of privacy that every enterprise must address, as shown in **figure 1**.[4]

Privacy Information Concerns

To address the personal and organizational concerns of data privacy, the position of PO was created. **Figure 2**[5] shows data concerns, areas of risk and questions the PO must ask.

All of these concerns help to identify the scope and complexity of the work. Data governance methods and techniques that need to be employed include data identification, protective measures, intrusion detection monitoring and reporting, responding to privacy events and incidents, and recovery of the organization to normalcy (when possible).

Governance Activities

Governance of privacy-related information requires that a custom strategy be developed for any organization. Governance activities should include:

- Identifying the stakeholders and internal partnerships.
- Developing vision, mission and value statements with goals and objectives. This information would be a reference and resource for a privacy charter that can be used throughout the course of the privacy policy development effort.
- Establishing connections within the organization to ensure cooperation and efficiency.
- Writing a privacy policy (described in a following section) to address warning banners; system compromise alerts; key persons to contact; and response, containment, and recovery processes and procedures.
- Developing a data governance strategy that includes data collection, authorized use, access controls, information security and destruction of the data/information. The key functional aspects are assessment, protection, sustaining privacy operations and responding to compromises.
- Establishing a privacy budget that includes outreach activities and a contingency reserve for recovery and emergency expenditures. The expenditures would include forensic investigations, victim notification, call center support, outside counsel (e.g., litigation costs), security enhancements, lost revenue and stock value, insurance, remediation actions, punitive costs (e.g., civil penalties and fines), customer retention, card replacement, victim damages, and opportunity costs.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2sU0fhc

Figure 1—The Seven Privacy Categories

Category	Area of Concern	Examples
Data and image (Information)	Rules that govern the collection and handling of personal information	• Financial information • Medical information • Government records • Records of personal activity
Person/bodily	Person's physical being and invasion thereof	• Genetic testing • Drug testing • Body cavity searches • Birth control • Abortion • Adoption
Communications	Protection of the means of communication	• Postal mail • Telephone conversations • Email • Hidden microphones • Other forms of communicative behavior and apparatus • Not informing citizens when surveillance occurs
Thoughts and feelings	Protection of individuals to ensure that their thoughts and feelings are not shared inappropriately with others, or they are not forced to share and have negative impacts against them in some way	• Being forced to provide social media passwords when applying for a job • Being forced to reveal religious beliefs or political views when applying for a job
Association	Addresses the right people have to associate with anybody they wish to, without unauthorized monitoring or marginalization, and addresses the types of groups that individuals belong to, for which they have no control, e.g., ethnicity or ancestry	• DNA testing that demonstrates ethnicity or ancestry • Denying membership of any kind after DNA testing revealed predisposition to an "undesirable" condition • Employers using DNA testing to make termination decisions • Any type of segregation based on religion, behavior, assembly or membership
Location and space (Territorial)	Concerned with placing limits on the ability to intrude into an individual's location, space and general environment. The environment is not limited to the home; it also includes the workplace and public spaces. Invasion into an individual's territorial privacy typically takes the form of monitoring, such as video surveillance, the use of drones, identification checks and use of similar technology and procedures.	• Home • Workplace • Public space • Video surveillance • ID checks • Other technology, e.g., flying a drone over an individual's property to take photos • Recording individuals behind their property fence
Behavior and action	This is an extension of a person's privacy. It is focused on thoughts and emotions before they are expressed to somebody, activities in public and private, and targeted monitoring.	• Sexual preferences • Political views • Religious beliefs and activities • Use of traffic signal cameras to catch those who commit traffic violations • Use of police body cameras

Source: L. Wlosinski. Reprinted with permission.

Figure 2—Data Privacy Concerns and Risk

Concern	Area of Risk	Description/Questions
Laws and regulatory landscape	Compliance, penalties, fines, public embarrassment, and loss of business and revenue	• Each country has its own version of what privacy means and has laws for the types of privacy data. The PO should be familiar with the laws, directives, standards, guidelines and policies that can be developed by the government, professional associations and the organization itself.
Type of data	Exposure of personal information; exposure of business sensitive, confidential or classified information trade secrets; inability to control or manage data securely	There are many questions associated with data type: • Are the data considered PII? • Are the personal data medical in nature (e.g., person's current health, medical history, DNA information)? • Are the data personal financial data, such as salary, loans, amount of debt or credit history? • Are the data about records of personal activity or history (e.g., level of clearance, citizenship, arrest record, association membership, web activity)? • What is the information medium (e.g., text, audio, video, email, screen captures, photo or paper format)?
Amount of data	Not knowing where the data exist and, consequently, not being able to control the data	• How many systems have privacy data? • How many records are in the system? • How many devices store and process the data? • How many data are accumulated daily, weekly and monthly? • How long does the government and/or the business require the data to be stored and protected?
Location of data	Unauthorized access, use or disclosure of data; unable to investigate or litigate if offshore offender; unable to protect data	• How many locations are affected (e.g., primary facility, mirrored facility, off-site backup files, cloud service providers, contractor-managed facilities)? • Are the data on social media or on a website (by accident or by malicious intent)? • Do the data reside in retired systems and data stores?
Source of data	Not acquiring accurate information; obtaining the data illegally	• How is the information gathered? • Do the data exist in an internal system or in hard copy? • Do the data come from an external business partner? • Are the data from a major application or a general support system (GSS) in the organization? • Were the data obtained by internal and/or external surveillance devices (e.g., cameras, drones)? • Are cookies used by company web applications?

Enjoying this article?

- Read ***A Privacy Principles and Program Management Guide.*** *www.isaca.org/privacy-principles*
- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

Figure 2—Data Privacy Concerns and Risk *(cont.)*

Concern	Area of Risk	Description/Questions
Availability of data	Production; not having the data when needed; other party involvement	• Are the data available publicly via the Internet, internally on the intranet or remotely via a virtual private network (VPN) connection? • Will the data be available via a new system? • Are production data of a private nature and used by the developers when testing the system? • Are the data shared with other organizations/partners? • Has the organization employed data minimization techniques for privacy-related data? • Who has access to the data? • Are the data accessible by mobile devices (e.g., smartphones, tablets, laptops)? • How will the data be shared/exchanged?
Protective measures	Poor or inadequate device configuration protection	• Does the organization employ technical protective measures such as account authentication (e.g., account with a password), user access cards, multifactor authentication, data encryption in transit and at rest, network protective devices and software, software updates and patches? • What data integrity controls are in place, and are they effective? • Are the system access control lists checked on a regular basis for leftover accounts (that could be used as backdoors into the system)? • Are physical access controls in place?
Internal policy, processes and procedures	Accidental or malicious activity; possibility of insider threat; not adhering to government laws or company requirements; exposure of personal data of employees and hiring candidates	• What kind of record keeping is required? • Are the operational hard-copy data protected at work and in the field? • Are the soft-copy and/or hard-copy data saved and protected for extended periods when required for investigations? • How is the information controlled? • Are administrative safeguards sufficient? • Are there privacy procedures for email and texting? • Are the data sanitized and destroyed in compliance with government regulations? • Are the processes and procedures periodically audited for suitability and confidentiality? • What are everyone's privacy roles and responsibilities?

Source: L. Wlosinski. Reprinted with permission.

- Performing impact assessments/audits. A privacy impact assessment (PIA) questionnaire should be used to inform the PO of possible concerns and potential problems when a computer system is developed or changed. The PIA should identify the types of data, the scope of people affected, the type of information, any new information obtained and the other concerns described previously.

Privacy audits can measure effectiveness, demonstrate compliance, increase awareness, reveal gaps, and provide a basis for remediation and improvement plans. PIAs can be at all levels, e.g., department, system and process.

- Establishing a continuous monitoring program. Does the PO receive system monitoring and network access tracking information? Is the PO informed of the results of independent and/or internal systems assessments? Does the assessment cover all of the necessary privacy controls (which are mentioned in the following section)? Have all remedial actions been performed to limit the possibility of a privacy incident? Noncompliance reports should answer the questions what, where, when, why, who and how.

> **"There are four types of privacy controls: management, computer operations, business operations and technical."**

- Instituting metrics. Metrics should be specific/simple, manageable, actionable, relevant/results-oriented and timely (SMART). Examples of privacy metrics include number of privacy data systems, percentage of data lost, number of privacy incidents, number of systems affected, average time between incidents and average time to recover. Privacy events may not always be large or computer-oriented in nature, but might occur on a small scale, e.g., identity theft.
- Implementing a privacy incident response plan (PIRP). To quickly respond to data breaches, the PO must be informed of all breaches and have information about the data and systems compromised. The breach plan should include a questionnaire/form, roles and responsibilities, points of contact information (e.g., security, management, legal, public relations, governing organizations), and communication procedures.
- Providing an information privacy awareness and training program. This could include developing awareness brochures and flyers for internal staff and contractors. All employees, business partners and contractors need to be trained on the privacy policy and procedures.
- Developing a public privacy website to explain the program and display whom to contact with questions. It could also include frequently asked questions.
- Ensure that the contingency and disaster recovery plans can recover the data.

Privacy Controls

There are four types of privacy controls: management, computer operations, business operations and technical. Implementing the controls is critical to a successful privacy program. If time permits, they should be implemented in the following order: identify areas of concern, implement protective measures, install detection mechanisms and employ response management techniques.

The four types of privacy controls are described as follows.[6]

1. Management controls

- **Identification**—Responsibilities include documenting legal authority, scrutinizing the new uses of PII, and having an inventory of PII programs and systems.
- **Protective measures**—Management must monitor laws for changes; appoint the PO; provide funding; update procedures and tools; explain the privacy program; assign roles and responsibilities; define privacy statements on contracts, acquisition documents and websites; issue privacy notices, policies and procedures; develop a strategic privacy plan; identify and explain why PII is collected; limit the collection and retention of PII; design systems to support privacy (e.g., data minimization); issue data integrity guidance; have

external sharing agreements; and appoint a data integrity board and retain PII.

- **Detection**—This activity includes conducting PIAs, assessing risk and tracking incidents.
- **Response management**—This activity includes reporting incidents to management and governing bodies according to the law.

> **“A privacy plan must include information for management, data handling operations (e.g., the data center or service provider), business operations and technical controls.”**

2. Computer operations controls

- **Identification**—Identify systems and files affected.
- **Protective measures**—Responsibilities include implementing and maintaining data protection and spillage prevention systems; protect PII in testing, training and research; developing and maintaining a PIRP; and training and monitoring staff.
- **Detection**—Operations needs to write incident and activity reports for management.
- **Response management**—Responsibilities include training for and providing forensic support; issuing spillage and data breach alerts; and using approved methods to delete or destroy PII as prescribed by management.

3. Business operations controls

- **Identification**—Identify what business operations are affected.
- **Protective measures**—Measures include approving website content, explaining the consent and information usage program, and obtaining consent of the affected party when applicable.
- **Detection**—This activity includes monitoring business practices for fraud, identity theft and data misuse.
- **Response management**—This area covers data spillage-handling activities, tracking and retaining records of disclosure, notifying those affected, supplying information to requestors, correcting erroneous PII, explaining individual rights, managing complaints, and responding to privacy spillage incidents.

4. Technical controls

- **Identification**—This activity includes reviewing and assessing security tools and determining if other tools need to be acquired and implemented.
- **Protective measures**—Measures include account authentication (e.g., account with a password); providing user access cards; using multifactor authentication, automatic time-out and external/remote access controls; data encryption in transit and at rest, network protective devices and software; software updates and patches; data integrity controls; technical control testing; and sanitizing and destroying data in compliance with government regulations.
- **Detection**—This category includes the use of data mining software and cyberdetection techniques. It could also include the use of surveillance software in the systems infrastructure and devices in the building, as well as system and application transaction audit controls.

- **Response management**—Computer forensic analysis techniques and software are needed.

Privacy Plan

A privacy plan must include information for management, data handling operations (e.g., the data center or service provider), business operations and technical controls. The plan content should include the following:

- **List of authorities**—This list identifies who is dictating the compliance and reporting requirements and could also include the source of guidance and standards.
- **Definitions**—The types of privacy data must be defined to support the information contained in the plan.
- **Scope and purpose**—The plan should state who is affected by the plan, a general description of the plan and why it was written.
- **Roles and responsibilities**—The roles of various enterprise areas, including the PO, the office of information security, legal department, human resources, public relations, marketing, business development, finance and customer care need to be listed in the privacy plan. It is important for each area to know what needs to be communicated and what needs to be done, in what order and in what time frame. This should be supplemented by training and periodic tabletop exercises.
- **Privacy controls**—The plan should describe the requirements of the four categories of controls (previously described) and how the controls are to be implemented.
- **Other considerations**—This part of the plan would address areas of the governance strategy not covered and could be oriented to the industry or area of personal concern (e.g., financial, medical). A list of acronyms may also be needed.

Conclusion

The PO must identify the data, understand the business use of the data, protect the data, detect when the data are in jeopardy or have been exposed, and know how and what to do about it. Joining privacy associations, subscribing to privacy-related journals, following best practices from privacy organizations and having a comprehensive privacy plan will help to protect the data and everyone involved.

Endnotes

[1] Gemalto, *2016 It's All About Identity Theft*, 2016, *www6.gemalto.com/breach-level-index-report-1H-2016-press-release*

[2] Verizon, *2016 Data Breach Investigations Report*, 2016, *www.verizonenterprise.com/verizon-insights-lab/dbir/2016*

[3] Verizon, *Verizon Data Breach Digest: Perspective Is Reality*, 2017, *www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf*

[4] ISACA®, "The Seven Categories of Privacy That Every Enterprise Must Address," *www.isaca.org/knowledge-center/research/researchdeliverables/pages/isaca-privacy-principles-and-program-management-guide.aspx*

[5] International Association of Privacy Professionals (IAPP), *Privacy Program Management: Tools for Managing Privacy Within Your Organization*, USA, 2013

[6] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication (SP) 800-53 Rev. 4, USA, 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*