Understanding Personally Identifiable Information (PII)

Inga Goddijn, CIPP/US
Executive Vice President, Managing Director of Insurance Services
Office: 855-RBS-RISK
inga@riskbasedsecurity.com
www.riskbasedsecurity.com

Table of Contents

About Risk Based Security 3
- Company History 3
- Solutions 3

Understanding Personally Identifiable Information (PII) 4
So where to begin? 5
Beyond Notification 6
But is that enough? 7
Conclusion 8
Contact Us 9
- Cyber Risk Analytics 10
- YourCISO 10

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established in early 2011 to better support the many users and initiatives of the Open Security Foundation - including the OSVDB and DataLossDB projects. RBS was created to transform this wealth of security data into actionable information by enhancing the research available, and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss.

VulnDB - Vulnerability intelligence, alerting, and third party library monitoring and tracking based on the largest and most comprehensive vulnerability database available today. Ability to integrate with products and services via an API or custom export.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Security Development Lifecycle (SDL) - Consulting, auditing, analysis, and independent verification specifically specialized in breaking code, which in turn greatly increases the security of software products.

Security Program Assessment Services / ISO/IEC 27001:2005 - Customized training, security assessments, security program audits, and gap analysis as well as pre-certification consulting services to both protect organizations with best practice security controls and to prepare for a smooth ISO/IEC 27001:2005 certification audit.

Understanding Personally Identifiable Information (PII)

Making the case that as data owners, we should develop a proprietary definition of PII that is sensitive to customers' expectations, considers the regulatory environment and is flexible enough to accommodate evolving privacy standards.

Since the passage of California's SB1386[1] and the rise of data breach notification laws, the term Personally Identifiable Information or PII has become a part of the modern lexicon. In fact, the phrase has become so ubiquitous in certain circles that an actual definition is no longer used, instead relying on a more commonly understood "I know it when I see it" standard. In reality, there are many legitimate definitions of PII. Furthermore, multiple definitions can be simultaneously valid depending on the context in which the information is collected, how it's used and where the person in question is located.

The lack of a uniform definition can be problematic. Regardless of the industry, size of the organization or clients served, every enterprise that collects, uses, processes or stores personal information faces a variety of privacy obligations and regulatory compliance issues.

What's more, there is little doubt the financial implications of a compromise of PII can be immense. Should a breach occur, the initial crisis response alone - establishing that a breach has taken place, understanding how it happened and containing the incident - can be a costly drain of time and resources. Factor in legal advice, notification expenses, identity protection services and a possible lawsuit or regulatory investigation, and the ultimate impact could be catastrophic.

With the stakes so high, it's critical for every organization to understand what type of data constitutes Personally Identifiable Information and establish a working definition of the term. Clearly identifying the type and scope of personal information that flows through the organization is a critical first step toward protecting this data and the cornerstone for creating well informed data handling practices.

[1] California's Senate Bill 1386 was the first privacy breach notification law enacted in the US, taking effect in July 2003. The law introduced the concept of notifying individuals when their personal information is lost, stolen or compromised. The statute allows for substitute notification in certain circumstances, including notifying statewide media of the breach. In this way, the statute deserves credit for bringing attention to the prevalence of data breach incidents. It has been modified and expanded several times since its inception.

So where to begin?

There is a wide variety of data privacy regulations at both the state and federal level that define personal information. Since California enacted the first data breach notification law in 2002, the notification regulations have become some of the most recognized privacy protection laws in existence. Because notification compliance can be an expensive proposition, the "personal information" definitions in these laws receive significant attention and provide a good foundation for what constitutes PII.

Although "personal information" definitions vary from one state to the next, the same data elements are frequently repeated. Also common is the concept that two or more data elements must be lost in tandem in order to trigger the notification requirement. Usually, this means the loss of a person's name or identifier along with one other piece of protected information constitutes a breach.

Because these laws were enacted for the protection of the state's residents, the notification rule will extend well beyond state lines. Regardless of where the organization is located if a breach involves residents across multiple states, each state's notification rule applies, and by extension, each state's definition of PII also applies. So when considering what data should be labeled personal, it is beneficial to look at some the broadest - or at least most populous - state definitions.

Illinois[2] and Florida[3] are two good examples to review. The Illinois definition includes:
An individual's first name or first initial and last name in combination with the individual's:

- social security number,
- drivers license or state identification card number, or
- account number or credit or debit card number **or** any account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- when any one of the above data elements is not encrypted or redacted.

The definition goes on to state that personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local governmental records.

[2] Illinois 815 ILCS 530 Personal Information Protection Act:
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%C2%A0ILCS%C2%A0530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act
[3] Fla. Stat. §817.5681:
http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.5681.html

Florida's definition is nearly identical to Illinois, but also includes a person's middle name and the exemption for publicly available information extends to "widely distributed media". Curiously, a small difference in the account number reference could have a sizable impact.

The Florida statute states:
an account number, credit card number, or debit card number, **in combination with** any required security code, access code, or password that would permit access to an individual's financial account.

Unlike Illinois, which considers a breach to have occurred when a name and account number are lost, the Florida statute implies the person's name, account number AND access code must be compromised in order for a breach to have occurred.

Beyond Notification

Less widely adopted, yet in many cases more far-reaching, are the data disposal laws. 29 states have enacted statutes regarding the destruction or disposal of records containing personal information. Like the notification laws, these statutes often contain unique definitions of personal information. However, unlike their notification counterparts, these newer definitions are often much broader in scope, including many additional data elements.

California provides an excellent example of these differences. When it comes to notification, the personal information definition is similar to Illinois and Florida, with the addition of medical information such as an individual's medical history, medical treatment or diagnosis by a healthcare professional.

However, California uses a much broader definition of personal information when it comes to records disposal. Under California Civil Code[4] §1798.80 - 81 "Personal information" means any information that identifies, relates to, describes or is capable of being associated with a particular individual, including, but not limited to:

• name	• telephone number	• address
• signature	• passport number	• medical information
• social security number	• insurance policy number	• bank account number
• physical characteristics or description	• driver's license or state identification card number	• credit card number, debit card number, or any other financial information
• employment or employment history	• education	• health insurance information

[4] California Civil Code §1798.80 – 81 can be found here:
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

But is that enough?

As helpful as statutes can be in defining the scope of personal information, these definitions only go so far in today's changing society. Our conception of private information is in flux and the boundaries of what can - or should - be considered protected information continue to change. Breaches at sites such as LivingSocial, LinkedIn and Twitter highlight the value of non-traditional PII such as e-mail and password information. Sporadically covered by breach notification or other privacy protection laws, this type of data has become increasingly valuable to hackers. Data thieves know passwords are reused and recycled on a regular basis, so the same log-in credentials that work for a lower value site might also work at a more valuable target such as a banking or credit card site.

Another interesting example of evolving data privacy standards is found in the fast growing field of behavioral advertising. We now have an unprecedented ability to collect, store and mine tremendous amounts of consumer data. While there is a long tradition of aggregating and analyzing customer spending patterns, the ability to combine that data with other, potentially personal information such as geo-location data from cell phones, is something entirely new. How much information and the type of personal information we're willing to share for the sake of better-targeted advertising are questions we're just beginning to ask. Less commonly discussed - but potentially much more damaging - are the implications of unauthorized access or use of this data.

Recognizing the need for transparent data collection practices and meaningful disclosure of the type of information being collected, the Network Advertising Initiative (NAI) updated their voluntary code of conduct for the collection and use of data for targeted advertising. The new standard, released in May of 2013, expands the definition of sensitive data to include information such as family medical histories, potential future health conditions, genetic information and sexual orientation. While not carrying the same force as law, the standard clearly recognizes society's evolving view of the type of data that should be considered "personal".

Conclusion

With so many different definitions of PII in existence, it is nearly impossible to track them all much less create processes to meet the regulatory demands tied to each. The only practical solution is to develop a proprietary definition that is sensitive to customers' expectations, gives consideration to the overall regulatory environment and is flexible enough to accommodate evolving standards of privacy.

Once established, a working definition is a beneficial tool that can be used to inform many data handling practices. It can help bring focus to questions such as who should have access to information and whether it is appropriate to share such data with third parties.

Furthermore, by clearly establishing what information should be treated as personal, organizations can begin to identify where the data resides in their system and how it flows through various business processes. Resources can then be focused on protecting the data where it is most vulnerable, thereby reducing the likelihood of a breach.

Contact Us:

www.riskbasedsecurity.com
sales@riskbasedsecurity.com
855-RBS-RISK

Cyber Risk Analytics

This web-based portal offers a full set of data breach analytics, threat reports and a user friendly dashboard that provide exceptional insight into a variety of security risks across a wide range of industries. Four service options are available, quarterly security intelligence reports, customized research reports, subscription access to the portal or database exports for special use purposes.

http://cyberriskanalytics.com/

YourCISO

YourCISO is a revolutionary, proactive risk management solution designed to improve your policyholders security posture and enhance the value of your policy to your customers. YourCISO is our proprietary web based portal that provides your Insureds with access to high quality information security resources at an affordable price.

http://yourciso.com/