July 2019

Security Awareness News

the security awareness newsletter for security aware people

DEFENDING DATA

Keeping It Classy

When Security Gets Personal

Defining Compliance

Keeping It Classy

Data classification is an essential process for managing the security of information. Without it, organizations would struggle to create effective policies for protecting sensitive data. By organizing data into distinct categories, we're able to implement controls, safeguards, and policies that map out the data's sensitivity and subsequent security requirements. Keep in mind that not all data is created equal. As such, not all data belongs on the same classification tiers.

The Data Classification Triad

Public

Public data is information that's available to everyone. This includes websites, business phone numbers and addresses, and social media accounts. Public info has no impact on data security.

Internal

Internal data could refer to NDAs (non-disclosure agreements), contracts, business relationships, and employee lists. Disclosure of this data can be damaging, but not necessarily debilitating, to operations.

Restricted

Often falling under compliance regulations, restricted or confidential data includes everything from personally identifiable information (such as health and financial data) to top-secret data that, if breached, could cost millions, lead to lawsuits, and devastate our organization's reputation.

Data Classification and You

While your day-to-day responsibilities may not include classifying data, they definitely include protecting data. Be sure to use extreme caution when handling sensitive info. Stay alert, think before you click, and remember that it's your job to know what our organization's data classification policies are and to always follow those policies. **If you need more information, please ask!**

WHEN SECURITY GETS PERSONAL

At the center of security efforts, we find personally identifiable information (PII)—the assets which organizations all over the world are entrusted to protect.

What is PII?

The most generic definition of **PII is any information that could be used to distinguish or trace an individual's identity**. Examples include: full names, date and place of birth, and Social Security or national ID numbers, as well as medical, educational, financial, and employment information.

Do all countries in the world recognize PII?

***Technically*, yes**. At least most of them do, but the term "PII" is specific to the United States. The EU, for example, refers to this type of sensitive info as "personal data". Both Australia and Japan simply call it "personal information". **Regardless of the term, the concept is the same: highly sensitive data that requires protection.**

What do cybercriminals do with stolen data?

You've likely heard the stories of major data breaches that expose the personal information of millions of people. Perhaps you've even been a victim of this. But what actually happens to exposed data? How do cybercriminals actually use the data?

They sell it on the dark web. Credit card numbers, national ID numbers, email addresses, and passwords all fetch certain prices on the underground economy.

They launch spear phishing campaigns. With enough information, cybercriminals increase their chances of successful phishing attacks because they're able to target specific individuals or organizations while sounding legitimate.

They pretend to be you. Identity theft is a top concern. If attackers gain access to your personal info, they can open accounts in your name, attempt to claim tax refunds, and file insurance claims, etc.

They attack even more accounts. In the case of stolen usernames and passwords, criminals use "credential stuffing," which is an automated attack using those same usernames and passwords to gain access to other accounts.

What's your role in protecting PII?

First and foremost, always follow our organization's policies, which were designed to protect sensitive data. Stay alert, treat all requests for sensitive data with skepticism, never allow someone to use your credentials (physical or digital) for any reason, and think before you click. If you see something or hear something, say something! Reporting incidents ASAP is a vital part of protecting data.

Defining Compliance

Compliance training comes in many forms, and most of us have encountered it at some point in our careers. Though tedious at times, it is critical not only to our jobs, but to our personal security, the security of our clients, and society in general. In its basic form, compliance training serves as a learning tool to inform individuals of the rules, guidelines, and laws that impact our organization.

Compliance (noun)

a: the act or process of complying to a desire, demand, proposal, or regimen; or to coercion

b: conformity in fulfilling official requirements

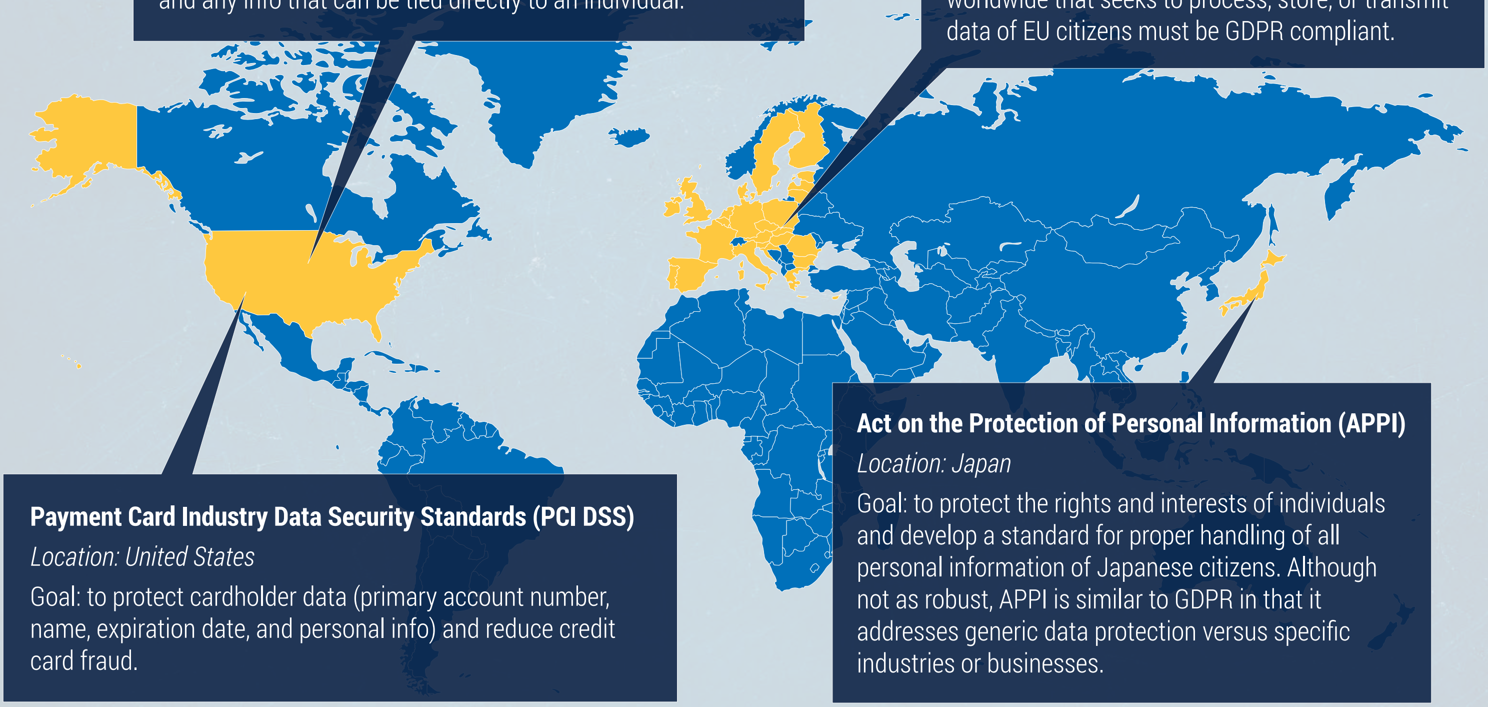
Comply (verb)

to conform, submit, or adapt (as to a regulation or to another's wishes) as required or requested

Sources: 1. https://www.merriam-webster.com/dictionary/compliance 2. https://www.merriam-webster.com/dictionary/comply

Examples of Compliance Regulations

Many countries around the world have regulations in place, aimed primarily at protecting our personal data. Here are a few examples:



Health Insurance Portability and Accountability Act (HIPAA)

Location: United States

Goal: to ensure the security and privacy of protected health information of individuals, such as Social Security numbers, medical records, account numbers, health insurance records, and any info that can be tied directly to an individual.

General Data Protection Regulation (GDPR)

Location: European Union

Goal: to protect the privacy of all European Union residents, regardless of where their private information gets used or accessed. Any entity worldwide that seeks to process, store, or transmit data of EU citizens must be GDPR compliant.

Payment Card Industry Data Security Standards (PCI DSS)

Location: United States

Goal: to protect cardholder data (primary account number, name, expiration date, and personal info) and reduce credit card fraud.

Act on the Protection of Personal Information (APPI)

Location: Japan

Goal: to protect the rights and interests of individuals and develop a standard for proper handling of all personal information of Japanese citizens. Although not as robust, APPI is similar to GDPR in that it addresses generic data protection versus specific industries or businesses.