

Best Practices on Protecting Your Greatest Asset: Your Audience Data

Speaker: Rhonda Drake, Drake Direct

Introduction

- Rhonda Drake –President and CEO of Drake Direct, a quantitative consultancy supporting B to C and B to B marketers.
- Drake Direct was founded in 1996.
- Clients include BBC America, SiriusXM, Source Interlink, illy caffe NA, Highlights for Children, Lorillard, Time Inc.
- Adjunct Professor at NYU in the School of Continuing Professional Studies Master's Program in Integrated Marketing.

Data Security Point of View

- As a consultant, data security is always important.
- Business data is a corporate asset, and should be respected, and protected as such.
- When the business data includes personal customer information, information that can give away a customer's identity, an extra layer of security should be employed.
- A security breach that allows one company to understand another's corporate strategy impacts the company.
- A security breach that involves customer information and allows potential identity theft has more far reaching consequences.
- Best practices should be observed including not receiving sensitive data if it is not needed for the business purpose.

How can lists be protected when data flows to and from my database?

Maximize Data Security Secure Transmission

- Personally Identifiable Information (PII) refers to the following:
 - E-mail Address
 - Name
 - Address (Street, City, State, Zip)
 - Anything that helps “phishers” get at the identity of a customer
- This type of sensitive information should *only be transmitted if absolutely necessary*, including but not limited to:
 - Use for Direct Mail or e-mail campaigns
 - List Rentals
- **Always transmit data with PII using a secure, password-protected FTP site**
- **All files with PII should be encrypted with a key, such as a PGP key**

How can lists be protected when data flows to and from my database?

Maximize Data Security Secure Access

- Control access: Pre-determine the list of users who will have access to customer data
- Grant access: Create unique user names for each individual with access
- Require individual security: Set requirements for a *unique* and strong password
- Require updates: Require password changes on a regular (but not rigid) basis
- Do not allow users to store the password

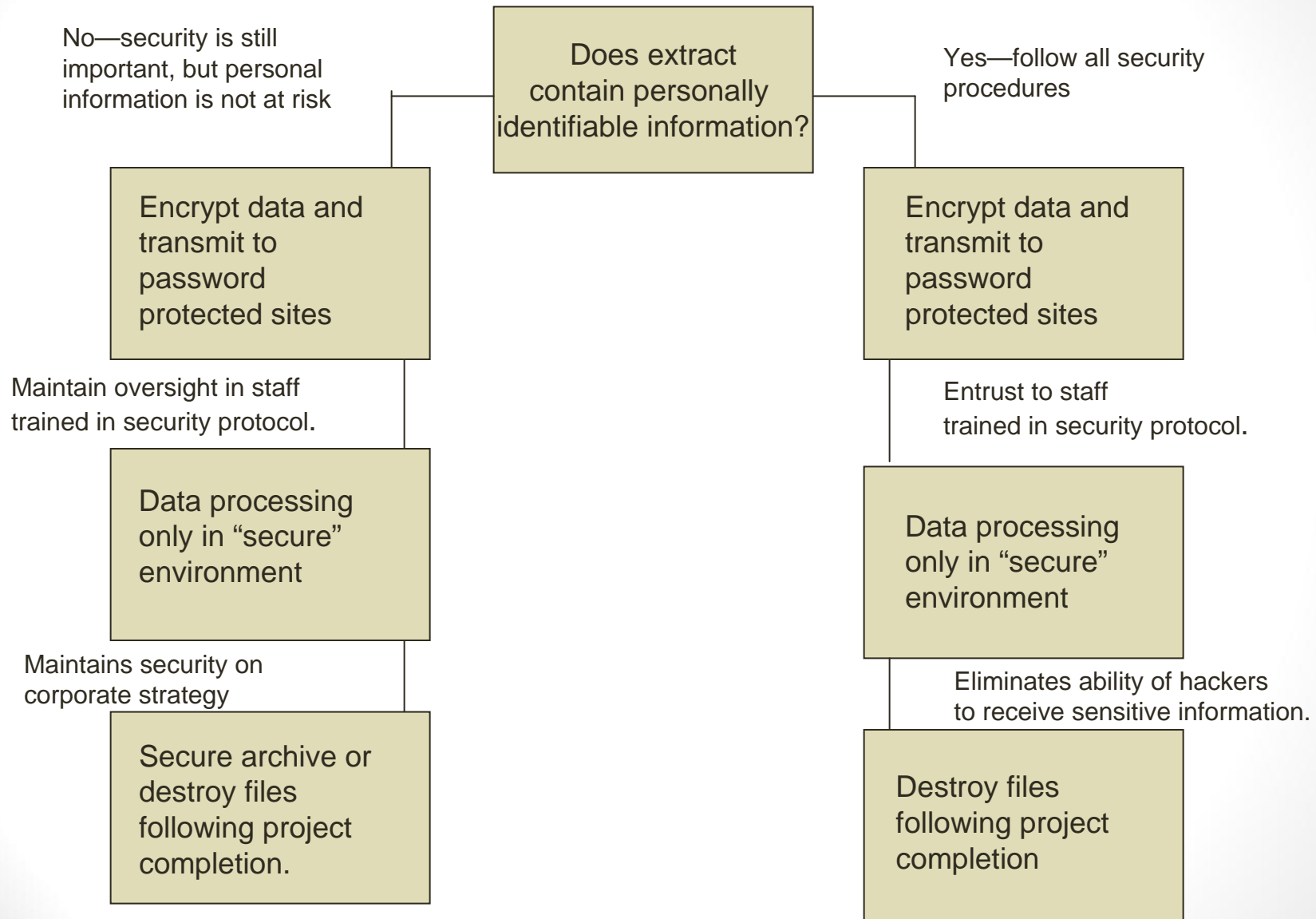
A unique password is one the user has never used before.

According to Microsoft*, a strong password consists of the following:

- 14+ characters
- Letters
- Varied letter case
- Numbers
- Symbols
- The more varied, the better

www.microsoft.com/security/online-privacy/passwords-create.aspx

Data Security



How can lists be protected when data flows to and from my database?

Check list

When transmitting and processing data with personally identifiable information:

- Dataset is encrypted
- Data is posted to secure ftp site or electronic drop box
- Unique passwords are used.
- Personnel accessing data are educated on data security practices
- Data analysis occurs only in secure environment
- Vendors receiving sensitive information have policies in place for handling data (including deletion upon project completion)

Privacy Practices that Earn Trust with your Audience

- For e-mail, set up a preference center
 - Opt-in marketing
 - CAN-SPAM compliant
 - Minimum two levels of opt in
 - Internal
 - Third Party
 - Possible additional levels, if there will be e.g. billing communications vs. promotional, or newsletters vs. promotional coming from internal sources

Privacy Practices that Earn Trust with your Audience

- **Breaches are unavoidable**
 - Key is to mitigate the impact by responding and addressing the issue as soon as possible
- Requirements:
 - Customer service communication back to consumer
 - Database setup that maintains:
 - Customer name
 - E-mail
 - Opt-in status (As this changes over time, it is advised to maintain each status change accompanied by the date)
 - Database “quick response” team equipped to research and manually change opt-in status

Financial impact of security breaches involving personal customer data

Direct costs

- Cost of communication of breach to customer.
- Provision of access to credit bureau reports to customers involved.
- Review of security policies/personnel following a breach.

Indirect costs

- Loss of future value of customers involved in the security breach.
- Unrealized revenue from consumers who hear about the breach and will never conduct business with your company.

Summary

- Data security is always important but extra controls should be in place if the data being transmitted to and from your database contains personally identifiers of your customers.
- Do not transmit such information unless it is imperative.
- Staff handling such data should be trained in best practices.
- Vendors receiving such data should have security policies in place
- A process for handling security breaches should be in place in the event that they occur.
- The financial impact of a breach is directly related to the number of customers impacted.
- Indirect costs cannot be measured as the impact is in the perception of safety by the consumer.