Implement a data security plan

Bookmark this page

Each organization should develop, enforce and update a comprehensive data security plan. That plan should include an inventory of the different categories of data collected, stored, processed or communicated by the organization. Security policies and procedures for each category of data should be clearly defined and expressed.

Those policies and procedures should include the following topics:

- Definition of required security measures (including those designed to protect the security of the data and those intended to provide for the physical security of the computers and other devices that store or access the data);
- Identification of the parties who are authorized to access the data;
- Description of authorized uses of the data;
- Actions to be taken in the event of service failures and service outages involving communications and computer networks;
- Training programs for employees and other authorized data network users to foster compliance with the data security policies and procedures.

The data security plan should also specifically address actions to be taken in the event of an actual or potential security breach. Those actions should include:

- defensive measures to stop or prevent the breach;
- documentation of the breach for evidentiary and remedial purposes;
- notification procedures for law enforcement authorities, individuals affected by the breach, business stakeholders (e.g., investors), and business partners;
- remedial actions to be taken to repair damages caused by the breach and to prevent similar breaches from occurring in the future.

The data security plan should address responses to data requests and demands made by government authorities. The plan should identify a single individual within the organization who is responsible for responding to the government data demand. It is a good idea to have that individual be one of the organization's lawyers.

As a matter of course, organizations should ask the authorities to present all such data demands in the form of a court-issued warrant. Each demand should be reviewed carefully for accuracy and the organization should require that the government correct all inaccuracies prior to providing the data at issue. The organization should exercise all rights of review and appeal available to it when the data requested are particularly sensitive (e.g., proprietary or customer information).