ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY

Appropriate Disclosures and Assurances to Consumers

Security 3 Subgroup
Stewart Baker, Paula Bruening, Lance Hoffman, John Kamp, Larry Ponemon, Andrew Shen

February 18, 2000

1. Introduction

    1.1. Disclosure and Assurance Defined

    1.2. Relationship between Disclosure and Assurance

2. Disclosure
    2.1. Disclosure v. Standard-setting: Policy and Law
        2.1.1. Policy
            2.1.1.1. Advantages of Disclosure
                2.1.1.1.1. Disclosure allows websites flexibility in how it provides security.
                2.1.1.1.2. Disclosure provides information that allows consumer choice to drive security rather than government mandate
                2.1.1.1.3. It is easier for enforcers to check disclosure contents than to examine actual practices
                2.1.1.1.4. Disclosure serves a consumer education role about the limits of security, the tradeoffs between security and efficiency and the need for personal responsibility.
            2.1.1.2. Disadvantages of Disclosure
                2.1.1.2.1. Disclosure does not provide a security "floor" or minimum security standards.
                2.1.1.2.2. Complexities of security technologies raise the risk that disclosure statements may be inherently incoherent to the consumer
                2.1.1.2.3. Revealing the details of a security system may compromise that system to some degree.
        2.1.2. Law -- When the law requires security, is it enough to provide notice?
    2.2. Notices
        2.2.1. Methods for providing notice
            2.2.1.1. Website notice or link to disclosure statement
                2.2.1.1.1. Long, heavily detailed disclosure statement may not be useful to consumers

2.2.1.1.2. Layered-linked statement – first layer of the statement is relatively rudimentary, consumer can “click through” to obtain more information.

2.2.1.2. Disclosure statement with mandatory checkoff (like software licenses)

2.2.1.2.1. Provides security information and requires consumer to click "I understand" or "I agree" to proceed

2.2.1.2.2. Assures that consumers were at least aware that a disclosure statement existed before proceeding with a transaction

2.2.1.2.3. Mandatory checkoff could serve a disclaimer function for bad actors, arguably relieving them of liability

2.2.2. Standardized format for notice

2.2.2.1. Should format be standardized? By whom?

2.2.2.2. Plain English vs. Blather

2.2.2.2.1. Is there a precise and common security vocabulary?

2.2.2.3. Industry Efforts at notice and matching preferences

2.2.2.3.1. Technologies with preferential matching capabilities

2.2.2.3.2. Case Studies

2.2.2.3.2.1. P3P Case Study

2.2.2.3.2.2. Other Case Studies

2.2.2.3.3. The Promise of Standards like XML

2.2.2.4. Beyond simple matches: arbitrarily complex decision procedures and computer programs as agents

2.3. The Contents and Format of a Security Notice/Message

2.3.1. Up-front

2.3.1.1. Security steps taken

2.3.1.1.1. Executive summary of security steps taken

2.3.1.1.2. Details of security steps taken

2.3.1.1.2.1. Who is Taking What Security Steps at What Times?

2.3.1.1.2.2. In What Electronic Locations?

2.3.1.1.2.3. Why these steps are taken

2.3.1.1.2.4. Pointers to additional detail

2.3.1.1.2.4.1. Technical

2.3.1.1.2.4.2. Administrative

2.3.1.1.2.4.3. Legal

2.3.1.2. Reporting mechanisms for the consumer if he/she suspects there has been a security compromise

2.3.1.2.1. Reporting mechanisms provided by the website (e.g., phone, mail, fax, email or web form)

2.3.1.2.2. Appropriate organizations to contact (e.g., government, consumer organizations, the website.)

2.3.2. Post-incident

2.3.2.1. Additional notice in event of security breakdown

2.3.2.1.1. Is notice necessary or recommended?

2.3.2.1.1.1. Advantages of notice

2.3.2.1.1.1.1. Consumer may be able to cure effects of the security compromise

2.3.2.1.1.1.2. Consumer may be able to take legal action against dataholder

2.3.2.1.1.2. Disadvantages of notice

2.3.2.1.1.2.1. False positives – too many instances in which consumers are notified of even minor security compromises may produce either excessive concern or inure consumers

2.3.2.1.1.2.2. False negatives - many intrusions that are not detected and so not reported could lead to unwarranted consumer confidence

2.3.2.1.1.2.3. Difficulty locating the consumer to provide notice

2.3.2.1.1.2.3.1. Tools necessary to provide robust notice may raise their own privacy issues (e.g., maintaining a database of emails to provide notice.)

2.3.2.1.1.2.3.2. Notice on Website alone may be insufficient

2.3.2.1.1.2.3.3. Leading indicators or threshold levels of security violations – Or, setting the proverbial "bar" for making mandatory contact to consumers about security violations. When the extent of security violations (in a given timeframe) fall below the bar, companies are not obligated to disclose. When violations exceed to bar, companies must notify in a pre-specified form and time period to all consumers (in the breach area). Indicators can be based on objective criteria, including frequency, materiality or complexity.

2.3.2.1.2. If provided, what should notice say?

2.3.2.1.2.1. When did breakdown occur?

2.3.2.1.2.2. How long was security compromised?

2.3.2.1.2.3. What personal information was revealed?

2.3.2.1.2.4. If compromise gives rise to legal rights, should notice of rights be included in message?

2.3.2.2. What legal responsibilities may website bear for compromises of security?

What compensation should be made to the consumer? What damages may they expect?

3. Assurance

3.1. Introduction to Assurance

3.1.1. Benefits for the consumer

3.1.2. Benefits for Business

3.1.3. Self-regulation vs. government oversight

3.2. Assurance on Security Disclosures
    3.2.1. Assurance on existence --Does a security framework or process exist?
    3.2.2. Assurance on coverage – Does the security framework or process cover major risk areas in the organization?
    3.2.3. Assurance on effectiveness – Does the security framework or process mitigate the risk that consumers will be harmed by the misuse of personally identifiable information?
3.3. Assurance Standards to Test Assertions on Security Disclosure
    3.3.1. Essential ethical principles
    3.3.2. Generally accepted audit procedures
    3.3.3. Methods of verification
    3.3.4. Timing and frequency of verification
    3.3.5. Objectivity and independence
    3.3.6. Reporting