Implications of Data Integrity & Security Standards for Managing Web Survey Fieldwork

Carl Ramirez

U.S. Government Accountability Office

The views and statements expressed are the author's own and do not necessarily reflect official policies of the U.S. Government Accountability Office.

Overview

How authentication & access control practices interact with self-administered web survey fieldwork practices

1) Applicable information system security standards
2) Integrity of survey data: range of IS & survey practices
3) Balancing data integrity and fieldwork needs
4) Need to continuously re-examine evolving IS security and survey data collection practices

Relevance of Authentication & Access Control

Respondent	Researcher	Info System
• Confidentiality: Protection from disclosure and unauthorized access • Confidence in integrity of research	• Integrity: Protection from ineligible unit and cases • Control over reporter, authenticity of final submission	• Security: Attack prevention • System integrity, appropriate role-based access

IS Security Standards & Practices

- Objectives: confidentiality, integrity, and availability
- FISMA of 2002, implemented by:
  - Definitions in FIPS (“Federal Information Processing Standards”) 199 & 200
  - Controls in NIST Special Publication 800-53 (“Security and Privacy Controls for Federal Information Systems and Organizations”)

IS security standards & practices

- Approach: baselines for security controls for low-, moderate-, and high-impact information systems
- Selected access-related controls:
  - Account management
  - Access enforcement
  - Access control decisions
  - Permitted actions wo/ ID
  - Least Privilege
  - Bad logon attempts
  - Previous logon attempts
  - Session lock, termination

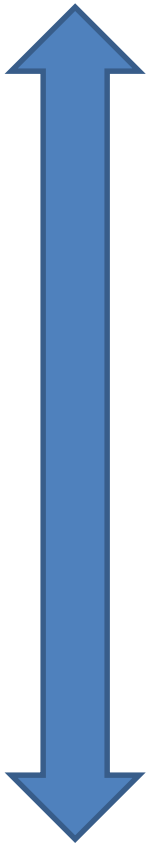
Example: Economic Census Industry Classification Report

- Mandatory, confidential, brief, no operating data - to determine NAICS code of company
- Respondent creates/signs in to account on Respondent Portal to access “my surveys”
- 12 digit Authentication Code to link respondent to one specific survey
  - One time use, for one reporter
  - Can’t always determine who used Code

Example: Economic Census Industry Classification Report

- Process for “sharing survey access” or delegation: request sendout of invitation email, recipient creates Portal account (no Authentication Code necessary)
  - Or: print and distribute questionnaire, facilitate aggregate data entry
  - Or (limited): spreadsheet download/upload (EDI)
- Mailed User ID and Password access for some not yet migrated to Authentication Code

Range of Web Survey Authentication & Access Control



- Open access to one URL
- Unique access code embedded in link to URL
- Static UserID and Password
- One-Time Password (e.g., additional PIN)
- Multi-Factor Identification (e.g., token)
- Digital certificate
- Identification device (card reader, biometrics)

Additional, Compensating Authentication & Access Controls

- Password strength and expiration options
- Security questions
- Identification/authorization of respondent device
- Challenge-and-response to prevent automated access attempts (e.g., “CAPTCHA”)

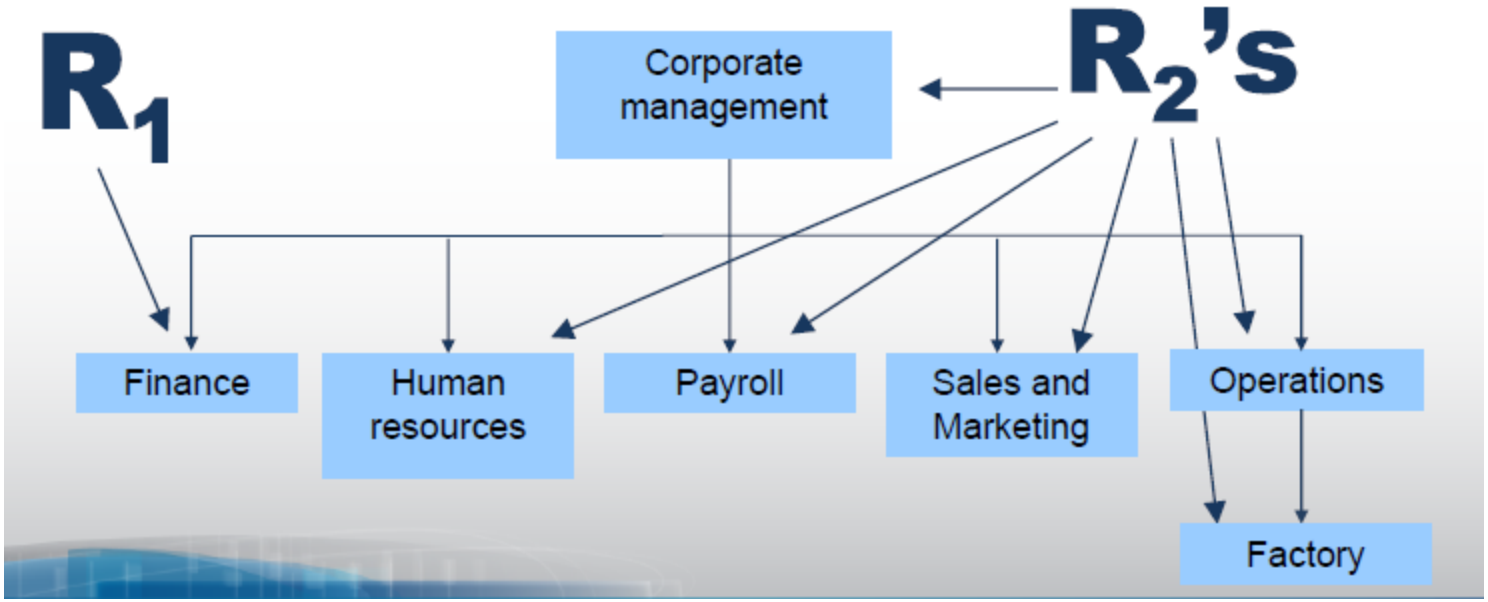
Web Survey Design for Integrity

(To Complement Authentication & Access Control)

- Instruct reporters on good access practices
- Reporter self-identification to determine role eligibility and enable validation follow-ups
- Review, certification and release by a specified authority
- Paradata, and response checks: legitimate respondent behavior?
- Time limitations decrease risk: response-related transactions, fieldwork period

Authentication & Access Control and Specific Fieldwork Activities

- High rate of substitute/multiple reporters in establishment (and some household) surveys



(Tuttle, 2016)

Authentication & Access Control and Specific Fieldwork Activities

- Limited workarounds in distributed response settings (e.g., enable facilitator/aggregator role with preview forms)
- Often impossible to identify, contact, and authorize only one eligible reporter for a unit
- Need “appropriate access” for help desk, case manager, and other research team agents interacting with reporters

Challenge of balancing security and response quality

- Human-computer interaction, usability, and cognitive research on survey burden:
  - Login effort may decrease participation and quality (Sedivi, Nichols, Kanarek, 2000)
  - But, manual login may not degrade response rate or quality over automated access (Heerwegh & Loosveldt, 2002)
- Working conclusion: burden matters, but security from disclosure or misrepresentation is increasingly important to respondents

Continuously Examine Authentication & Access Practices

- Adapt to new fieldwork methods, and enable good survey practices, while maintaining integrity aspect of information security
- But: “Do not remove security controls for operational convenience. Tailoring decisions regarding security controls should be defensible based on mission/business needs and accompanied by explicit risk-based determinations.” (NIST Special Pub 800-53)