Westat®

An Employee-Owned
Research Corporation

Security Considerations in Blaise Environments: Options and Solutions

Mike Rhoads and Ray Snowden, Westat

Importance of IT Security

- Sample headlines

  Virginia (8/27/2010) — Virginia's IT operations arm has repaired the cause of a statewide IT system failure that affected online services and network operations of more than 20 of its agencies, including the Department of Motor Vehicles (DMV).

  Washington (5/22/2006) — America's veterans were sent scrambling for their credit reports Monday, as the Veterans Administration announced nearly all of them — and some of their family members — were at heightened risk for identity theft.

- Vulnerabilities and risks for survey data collection

  Platform-specific (laptops, Internet, etc.)

  PII and other highly sensitive information

  Professional and legal ramifications

Topics for This Talk

Quick, high-level overview of:

- Basic elements of an IT security framework
- Aspects of Blaise relating to IT security
- Platform-specific security considerations

Basic IT Security Framework

Based on “FISMA”

- Federal Information Security Management Act of 2002
  - Foundation for IT security of U.S. Government information systems
- Concepts similar in ISO/IEC 27001 (leading private and international standard)

Three Central Objectives of FISMA

- Confidentiality
- Integrity
- Availability

(just remember C-I-A)

Risk Management Framework

- Two dimensions of risk for possible threats:
  - Magnitude and prevalence of a threat
  - Amount of harm resulting from the threat
- Risk Management Framework (RMF) – approach to security planning developed by NIST
  - **Categorize** system – low, moderate, high
  - **Select** initial set of baseline **security controls**
  - **Implement** the controls and document their deployment
  - **Assess** the controls
  - **Authorize** system operation (ATO)
  - **Monitor** / assess controls on an ongoing basis

Examples of Security Controls

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency]* thereafter.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Security Control Categories

- Security policies – establishes organizational commitment and approach
- Human controls – security training, access agreements, screening
- Physical controls – fire prevention, secure access, locked cabinets
- Technical controls – encryption, anti-virus, complex passwords
- Systems management – development standards, change management
- Auditing and monitoring – record failed logins, web site monitors
- Systems continuity – data backups, recovery platforms, alternate site

Aspects of Blaise Relating to Security

Role of Blaise in Project Security Framework

- Blaise application just one of multiple layers of security
- Provides some built-in security features
- Must integrate into overall security framework
  - FDCC / USGCB
  - Version control packages
  - Testing
- Mature product – successful and secure operation on many data collection efforts over the years

Solving a Common Confidentiality Problem

- CAPI interview with some particularly sensitive items
- Want to make this section self-administered
- Don’t want interviewer to be able to get back to the answers

Blaise Code to the Rescue!

```
RULES
    ThankYou.KEEP
    RespondentIntro
    NEWPAGE
    IF ThankYou = EMPTY THEN
        Ticket
        SmallOffence
        MajorOffence
    ELSE
        Ticket.KEEP
        SmallOffence.KEEP
        MajorOffence.KEEP
    ENDIF
    ThankYou
```

Using Relational Databases for Data Storage

- Blaise Datalink – uses Microsoft OLE DB to allow Blaise to store data in non-native formats (e.g., Oracle, SQL Server)
- Take advantage of organization's established security practices
  - Access control
  - Special security zones

Platform-Specific Security Considerations

Web Surveys

- “Public” Internet is just that – need wide range of safeguards
- Data storage format – advantages of using relational database through Datalink
- User authentication and authorization
  - Nice write-up of technical aspects in Blaise documentation
  - Secure communication of credentials to respondents
- Communications encryption – Secure Sockets Layer (SSL)

CAPI Surveys

- Environment – portable devices, need to synchronize data and software with home office
- Encryption (on the laptop, during transmission, safeguarding keys)
- User authentication (password policies, other access protections, user training, resets)
- Platform controls (disable unneeded services/devices, firewalls, anti-virus etc.)
- Configuration management (need to implement, test, and log updates)


8

Conclusion

- Importance of an overall framework for IT security management (such as FISMA)
  - Use broad set of **security controls**
  - to reduce **risks**
  - to **confidentiality**, **integrity**, and **availability** of applications and data
- Different survey platforms share some common issues, but also present unique problems
- You’re in good hands with Blaise!

Questions?