Security Considerations in Blaise Environments: Options and Solutions

Mike Rhoads and Ray Snowden, Westat

1. Introduction

IT Security has become an increasingly important and costly component of survey research operations. This trend will continue for the foreseeable future due to the following general factors:

- The number and variety of applications and devices that are used to support survey data collection is continuously increasing as vendors develop new tools and technologies, such as smart phones, iPads, and faster and more reliable wireless communications, which can significantly improve the efficiency or reduce the cost of data collection. Each new technology exposes additional potential security risks, which must be understood and properly mitigated.

- The Internet has become the standard mechanism for business data communication and, given its open accessibility to the public, exposes confidential data and valuable IT assets to a wide variety of continuously evolving threats.

- The U.S. government, other regulatory bodies, and clients have become increasingly aware of the importance of IT security and have promulgated a steady flow of new security related regulations, guidelines, and best practices. The passage and implementation of the Federal Information Security Management Act of 2002 (FISMA) has created significant new compliance and reporting requirements for Federal systems.

Although the technologies, risks, and regulations continue to change, many of the scenarios that make security an important business concern remain very familiar. The following are just a sample of the common concerns that these regulations and controls are intended to address:

- A field system with personally identifiable information (PII) is lost or stolen

- Unprotected systems are exploited by a new virus

- Hackers exploit a web site and delete or deface valuable data

- An interviewer copies PII data to a flash drive which he loses

- A new OS security patch is installed and brings down 400 laptops for a week

- Employees are using work systems for Internet gambling

- An interviewer is at a respondent's house at 8:00pm and forgets her password

- Authority to Operate (ATO) is denied for an important project due to missing security controls

Given the scope of IT security, the variety of threats to be guarded against, and the number and complexity of the various regulatory requirements, IT security can seem to be an overwhelming undertaking, particularly if one assumes that the objective is the achievement of a perfectly secure system

and the elimination of all risk. Although the requirements and guidelines often appear to be unnecessarily burdensome and operationally inefficient, they are intended to reinforce a systematic and comprehensive approach to the planning, implementation, and monitoring of security controls to reduce the risks to an acceptable level, to detect incidents quickly when they occur, and to minimize the associated harm.

Blaise is an important component of a survey system and, as such, must provide security-related features, support secure development and operation, and be installed and operated in a secure environment. The next two sections of this paper summarize FISMA and the Federal Desktop Core Configuration (FDCC). Next, we look at some aspects of Blaise that specifically relate to IT security. We conclude by discussing security considerations for Blaise surveys on specific platforms. Although the specific details of FISMA and FDCC will be primarily relevant to U.S. Government agencies and contractors, the former in particular spells out a number of general principles that may well be useful for planning purposes even outside the United States.

2. FISMA as a Security Framework

2.1 Overview

Although numerous security regulations and frameworks have been developed and may impose specific requirements, FISMA has created a broad framework for IT security definition and implementation used by the Federal Government. Through the work of the National Institute of Standards and Technology (NIST), specific concepts, procedures, and guidelines have been developed and are experiencing widespread use. Given the broad scope of FISMA, these concepts and practices are relevant and applicable to many IT systems, even those not under governmental oversight, and will be used in this paper as a representative approach to IT security.

FISMA is the Federal Information Security Management Act of 2002. It was passed as Title III of the E-Government Act (Public Law 107-347) in December 2002. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. These agency programs are required to include the following types of activities:

- Develop an inventory of all information systems used by the agency, complete a risk assessment, and classify systems in terms of the harm resulting from accidental or malicious modification, damage, or loss in the data or supporting systems.

- Implement managerial and operational procedures and technical security controls that reduce the risks to an acceptable level in a cost-effective manner while satisfying any mandated security requirements.

- Provide training to staff and contractors about the importance of security, the risks to data and systems associated with their activities, and the policies and procedures that are to be followed.

- Perform periodic monitoring and testing, no less than annually, to ensure that policies and procedures have been implemented and are executed properly.

- Implement procedures to continuously review and evaluate security practices and identify and remediate deficiencies.

- Implement policies and procedures for detecting, reporting, and responding to security incidents.

- Implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

2.2 Security as Defined by FISMA

FISMA defines the term "information security" as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide the following general safeguards:

- **Confidentiality** – restricting access to information to authorized users only. This is a central security concern in survey research projects where respondent data often includes highly confidential personal information and PII. Unauthorized disclosure of confidential data is everybody's top concern.

- **Integrity** - guarding against the unauthorized modification or destruction of information due to either accidental or malicious actions. This is another important aspect of security in survey research projects where survey data is generally time-consuming and expensive to collect and the credibility of analytic findings depends on a high degree of confidence in the quality of the underlying survey data.

- **Availability** - ensuring timely and reliable access to and use of applications and information. Consistent and reliable access to survey systems in CAI projects can be particularly critical since response rates are extremely important. Once a respondent is contacted and ready to provide information, the CAI systems must work.

Confidentiality, integrity, and availability of information and systems are the three central objectives of FISMA and these are also critical issues for any survey research project.

2.3 NIST Activities in Support of FISMA

The FISMA regulation also directs the National Institute of Standards and Technology (NIST) to develop standards, guidelines, and security requirements to be used in the development and implementation of agency security plans. The work of NIST to support FISMA has been organized as the NIST FISMA Implementation Project.

In support of FISMA, NIST has developed an integrated Risk Management Framework which brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies. The name Risk Management Framework is used because the key organizing principle of FISMA and the focus of the framework is to identify and understand risk as a function of two related considerations: 1) the magnitude and prevalence of the threats to confidentiality, integrity, and availability that the IT system will be exposed to; and 2) the harm resulting from a loss of confidentiality, integrity, and availability to the IT system.

The RMF consists of the following 6 steps:

1. Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis. **NIST Publication FIPS 199** provides guidance around the categorization of information systems using an approach that assigns a security level to each system of low, moderate, or high.

2. Select an initial set of baseline security controls based on the information system's security categorization, tailoring and supplementing the baseline based on organizational assessment of risk and local conditions. **NIST Publication SP 800-53** provides a detailed list of management, operational, and technical controls that are considered requirements for systems for each of the 3 security levels.

3. Implement the security controls and document how the controls are deployed within the information system and environment of operation. The documentation that is developed in this process and generated as the system is operated are key artifacts for the remaining steps in the RMF.

4. Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This is often completed by a 3rd party security organization and involves examination of records, interviews with staff, server scans, etc.

5. Authorize information system operation based upon a determination of the risk resulting from the operation of the information system and the decision that this risk is acceptable. A security authorization package consisting of various documents including the system security plan (SSP), the results of the security assessment, and a plan of action and milestones (POAM) is submitted to a designated individual at the agency. An Authority to Operate (ATO) is the official designation by the agency that the risks of operating the system are understood and acceptable and that the system may be placed into production.

6. Monitor and assess selected security controls in the information system on an ongoing basis, which includes documenting changes to the system or environment, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.

NIST Publication SP 800-53 provides a catalog of several hundred management, operational, and technical security controls and indicates the applicability of each to the 3 security levels (low, moderate, and high). Although selecting, implementing, and documenting these controls seems at first to be a very daunting process, SP 800-53 does provide a structure and degree of comprehensiveness that can be very helpful in the development of a security plan, which is often characterized by the troublesome combination of a very broad scope and numerous complex details.

The security controls that are defined in SP 800-53 are organized into 17 security-related areas. These controls can be classified into the following broad groups:

- **Security policies** – formal statements published by an organization which establish the framework in which security controls are defined, implemented, and enforced. Security policies are established by the organization's management and should reflect the importance to the organization of sound security practices.

- **Human controls** – policies and procedures which describe required, acceptable, and unacceptable behavior in the secure use of systems and data. This is typically reinforced through formal training and documentation. Also included are personnel security controls, covering position categorization, screening, transfer, access agreements, and termination.

- **Physical controls** – steps that are taken to secure and protect information assets and the physical environment within which sensitive data and systems are installed and operated, including locked cabinets, secure rooms with controlled access, fire suppression, etc.

- **Technical controls** – technical features and practices that are employed to protect data and applications such as user authentication, platform policy settings, encryption technology, backups, etc. These controls usually employ features of the network, OS, application systems, and specialized COTS products.

- **Systems management** – procedures to manage the acquisition, development, deployment, and operation of new systems, and to manage changes to these systems over time using security standards and principles.

- **Auditing and monitoring** – procedures and practices employed to actively check for and log security vulnerabilities and incidents and to verify that required security controls are in effect and functioning properly.

- **Systems continuity** – procedures and resources that are defined and implemented in order to ensure that the necessary availability of critical systems and data will be maintained in the event of technical, platform, or facility failure.

3. The Federal Desktop Core Configuration (FDCC)

As part of its overall IT security policies, the U.S. Office of Management and Budget (OMB) mandated the Federal Desktop Core Configuration (FDCC), which is a security configuration designed to standardize the configuration of desktop computers used by U.S. Government agencies. The FDCC was initially announced in a memorandum (M-07-11) issued by OMB on March 22, 2007, with agencies directed to comply by February 2008. On February 28, 2008, Part 39 of the Federal Acquisition Regulation (FAR) was modified to require that information technology acquired by the government comply with relevant security configurations. A subsequent OMB memorandum issued in August of 2008 (M-08-22) provided additional information about procedures that IT providers need to follow in order to certify that their products comply with the FDCC requirements.

On May 7, 2010, the U.S. government's CIO Council announced the United States Government Configuration Baseline (USGCB). Under this initiative, security configuration baselines were released (Major Version 1.0.x.0) on September 24, 2010 for Windows 7, Windows 7 Firewall, and Internet Explorer 8. USGCB appears to be carrying out the same types of activities as were previously performed under FDCC, which it officially replaces. However, FDCC settings and requirements for Windows XP and Windows Vista will remain in effect unless and until USGCB issues its own settings for these platforms.

Since the Blaise development environment runs on Windows desktop computers, it is required to meet these guidelines. Federal agency staff needing to run the development environment on a desktop may be required to provide assurance of FDCC compliance either as part of the procurement process, or when they request government IT staff to actually install the software.

Westat, in its role as the licensor of Blaise software in North and South America, arranged with a third-party provider of assessment and certification services to perform the necessary validation testing for Blaise 4 under Windows XP and Windows Vista. This testing confirmed that Blaise complies with all FDCC requirements. Specifically:

- The desktop components of Blaise software are fully functional and operate correctly as intended on systems using the FDCC under Windows XP and Windows Vista.

- The standard installation, operation, maintenance, update, and/or patching of the Blaise desktop components does not alter the configuration settings from the approved FDCC configuration. Blaise uses the Windows Installer Service for installation to the default "program files" directory and is able to silently install and uninstall.

- Blaise applications designed for typical end users are able to run in the standard user context without elevated system administration privileges.

More information regarding Blaise compliance is available at http://www.westat.com/westat/statistical_software/blaise/fdcc_compliance.cfm.

4. Aspects of Blaise Relating to Security

Effective IT security measures take advantage of multiple layers of security, such as platforms and infrastructure, physical facilities, and organizational policies and procedures. A Blaise application is one of these layers. The existence of these other layers means that Blaise itself does not have to provide for every aspect of security – as we shall see, many important security practices and techniques are relatively independent of the specific software application involved. However, application software must be able to be gracefully integrated within the overall project security framework.

Fortunately, Blaise is a mature and well-designed data collection product that is highly suitable for operation in a secure environment. Numerous Blaise surveys for U.S. Government clients have successfully undergone certification and accreditation (C&A) and have been authorized for operational use. As noted in the prior section, Blaise also complies with all FDCC requirements.

Blaise also fits well into the set of security controls that relates to systems management, including development practices and change management. Tools such as Microsoft Visual SourceSafe can be effectively used for version control of Blaise code files. Software testing is also a critical component of sound development practices, and this topic has been addressed in many IBUC presentations.

4.1 A Blaise Coding Technique to Maintain Confidentiality

Although most aspects of security and confidentiality for Blaise surveys are typically implemented in security layers beyond the Blaise instrument itself, there is one relatively common situation involving confidentiality that can be effectively addressed within the rules of the Blaise data model. This occurs in CAPI instruments where some sections may elicit particularly sensitive information, such as participation in antisocial or even illegal activities. Since respondents may be reluctant to admit such behavior directly to an interviewer, a commonly-used technique in such situations is to have those sections of the interview be self-administered, with the laptop turned away from the interviewer but facing the respondent. This allows the respondent to operate the laptop and then turn it back to the interviewer after finishing the sensitive set of questions.

When this method is employed, it is important for the interviewer to be able to truthfully assure the respondent that the interviewer will not be able to look at the answers that the respondent has recorded. The Blaise developer can accomplish this by inserting a “wall” into the data model, which will prevent

the interviewer from going back and seeing the respondent's answers. The Blaise Online Assistant uses the following code snippet to illustrate this method.

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

  ELSE
    Ticket.KEEP
    SmallOffence.KEEP
    MajorOffence.KEEP

  ENDIF
  ThankYou
```

This code ensures that once the "Thank You" item has been presented to the respondent after having answered a sequence of private or sensitive questions, those questions and the populated answers can no longer be viewed. It works as follows:

This code uses the field (ThankYou) immediately following the sensitive questions to control the flow. The first time through, when the respondent is using the laptop, this field is empty, so the sensitive questions are asked. After responding to the ThankYou item, the laptop is returned to the interviewer. If the interviewer attempts to move backwards in the instrument, the rules branch around the sensitive questions, since the ThankYou item has already been completed. The KEEP method is used with ThankYou so that the rules can access the value that has been entered, and also in the Else branch of the If-Then-Else so that the values of the sensitive fields will be stored in the final Blaise data even if the interview backs up through the instrument.

For a complete code example illustrating this technique, see the keepdemo.bla sample file, which is in the Blaise sample library under \Datamodel\Basics.

4.2 Ability to Use Relational Databases for Data Storage

One important security feature in recent versions of Blaise is Blaise Datalink, which allows Blaise to utilize Microsoft's OLE DB technology to store its data in relational databases such as Oracle and Microsoft SQL Server. Most enterprises have a variety of established security practices for database security, such as locating the database servers in special security zones. Using Datalink to store Blaise survey data takes advantage of these existing security procedures.

5. Security Considerations for Web-based Blaise Surveys

Applications that run on the Internet can be especially vulnerable from a security standpoint. There are many network and platform features that must be implemented to securely operate a web site accessible over the public Internet. This includes an appropriate network configuration with adequate firewall protection, Windows servers that have been hardened for use as web servers, timely software patching,

virus protection, etc. This section discusses some of the important security considerations for web-based surveys.

1. One of the most basic yet important decisions to be made is the format to use for storing the incoming survey data (as well as any necessary preloaded data). The ability of Blaise to store its data directly into an RDBMS is especially important in a web environment, since enterprises are likely to locate their database servers in special security zones that are not directly connected to the public Internet. Using Datalink to store the Blaise Internet survey data in an enterprise database takes advantage of all of the security procedures that have already been established for the database servers, thus avoiding the need to implement customized methods to protect native Blaise data files.

2. User authentication and authorization is another important aspect of security for Blaise Internet surveys. Authentication is particularly complex due to the number of possible techniques and tradeoffs. The Blaise Online Assistant provides an extensive discussion of security considerations for web surveys, including several possible methods of implementing user authentication.

   A difficult issue for web-based surveys specifically can be the communication of authentication credentials to the end users. In some cases, where the sample for the survey is open, users may be asked to create their own login and password at a self-registration page of the site before taking the survey. In many cases however, the sample population is restricted and identified in advance. In order to implement an authentication mechanism that is secure and maintains a strong password, it is necessary to securely communicate an account and password to each user, and have the user change their password at their first login.

   Following the standard security principle of least privilege, users and applications should be authorized, through application, database, or OS permissions, to have access only to the specific resources required to complete the survey. This will help reduce the scope of damage that may be caused due to the activities of a malicious user or malfunctioning application.

3. Web-based surveys programmed in Blaise can be accessed over an encrypted connection using Secure Sockets Layer. SSL is implemented by acquiring, installing, and configuring a server-side encryption certificate under IIS and accessing the web site from the browser using the HTTPS protocol. Once this is done, IIS and the browser establish an encrypted connection over which all data is communicated. This technique protects the confidentiality of the data between the end-user computer and the web server.

   When setting up SSL it is important to ensure that all potentially sensitive data is encrypted including user credentials, case management data, and the survey itself. SSL should be configured as the required protocol to eliminate the possibility that an end user can mistakenly access the site without SSL in effect. Also, the SSL encryption mechanism chosen should be FIPS 140-2 compliant.

6. Security Considerations for CAPI Blaise Surveys

CAPI surveys also present a number of unique security considerations, due to the characteristics of the CAPI environment such as the use of single-user systems, disconnected and connected operations, and the need to synchronize data and software with central systems.

The following are some key security considerations and controls when using Blaise in a CAPI study:

1. **Encryption** – encryption plays a larger role in a CAPI study than for the Internet, due to the fact that sensitive survey data are stored on the field device and must be communicated back to the central system in a secure fashion. There are three different areas where encryption technology should be considered:

   - **Full disk encryption** – in 2006 the OMB mandated that sensitive data stored on mobile devices must be encrypted. The use of a full disk encryption mechanism ensures that all data stored on a device are encrypted before being written to the hard drive. The data are only decrypted when an authorized user enters valid user credentials and logs into the device. This protects instances where a laptop is lost or stolen by eliminating the possibility that the hard drive cannot be removed from the device and simply connected to another computer.

   - **File encryption** – data files sent between the central system and field devices can also be individually encrypted before being sent. This provides another level of protection beyond the encryption of the connection itself and can further protect the data as it is stored on the field device or at the central system. Often the vendor that provides the full disk encryption technology can also provide an API that can be used to programmatically encrypt and decrypt data files.

   - **Encrypted connection** – as noted earlier, when connecting to the central system to synchronize data, SSL or some other encryption mechanism can be used to encrypt all data sent between the central office and the field device. If wireless connections will be used, make sure that adequate protections are in place to protect the data during wireless transmission.

   When using full disk encryption or file-based encryption, it is very important to ensure that the encryption keys are safeguarded, as they represent the only mechanism to access the encrypted data. Often the encryption package will provide master encryption keys which can be used to recover data if the primary keys are lost. When choosing encryption solutions for any of these areas, compliance with FIPS 140-2 should be a consideration.

2. **User authentication** – as with web-based surveys, user authentication in a CAPI environment is a critical security control and presents some unique issues.

   Providing an account and password to log into the field device is one of the primary mechanisms for protecting the applications and data on the device. The entry of a valid account and password "unlocks" the full disk encryption, if it is used, and also provides access to the case management program, instrument data, and other field applications and data (e.g., e-mail) which may be installed on the device. It is essential that the user credentials and login process are configured and managed securely including:

   - The use of a strong password or pass phrase. This includes a minimum length, minimum complexity, an expiration period, and limits on password reuse.
   - Obscuring the password on the screen when it is entered.
   - Disabling the account after a certain number of failed attempts to login.
   - Displaying a password-protected screen saver after a period of inactivity.
   - Logging all failed login attempts.

One of the most important security controls with respect to authentication is user training. Users must be taught the importance of security and the need to keep the password secret. This means not writing it down where it can be easily found, not revealing it to friends or family members, not allowing respondents to see it being typed, etc.

Another issue for CAPI projects is having a procedure by which field staff can quickly have accounts and passwords reset by the home office in the event of a forgotten password. This may include connecting to a help site or the configuration of a single-use emergency account. Security should be configured to provide necessary protections without substantively interfering with the productivity of the field staff.

3. **Platform controls** – a laptop connected to the Internet for data synchronization to the home office is exposed to Internet threats from two sources: 1) other Internet users or devices that may attempt to connect to and access or damage data; and 2) web sites that field staff may voluntarily connect to that include malicious code. For this reason it is important to approach the configuration of the field device as one would approach the configuration of a web server. The following are the types of controls that should be considered:

   - Disable any services under Windows that are not absolutely necessary to running the survey applications. This is another interpretation of least privilege and will eliminate potential security vulnerabilities that are not needed.

   - Adopt the use of one of the standard Windows security templates that are available from NIST and other security organizations. These templates include default definitions for numerous obscure system settings for which the default setting is unacceptable. It is important to test the full operation of the survey software with the template to make sure that all required services and features function properly.

   - Install and configure a firewall on the field device to limit the ports over which outbound requests can be made and to block any unauthorized attempts to connect to the field device. If possible, limit the external web sites to which a field device user can connect.

   - Install and use anti-virus, anti-spyware, anti-malware tools.

   - Disable USB ports or any other external data devices that are not required by field operations.

   The list of the specific controls and protections which may be required continues to develop as new devices and new threats emerge. Suites of security tools are available from various companies that can provide a full range of protections that are controlled and monitored through a single integrated administrative and reporting interface.

4. **Configuration management** – another unique challenge for CAPI projects is the requirement to manage numerous, sometimes hundreds or thousands, disconnected devices in the field. Given the very dynamic nature of security threats and the survey project operation it is essential that tools are in place to manage and monitor the configuration of the field platform over time.

   The following types of configuration changes are common:

   - OS patches – new security threats are identified every day and many of them are the result of some vulnerability in the built-in OS controls. Security patches to the OS are

generated periodically or as needed by the OS vendor. Patches which correct serious errors should be evaluated for immediate dissemination to the field.

- Security application signature files - anti-virus software, intrusion detection software, and other anti-malware applications use signature files and other configuration information to detect and protect against threats. Updates to configuration files for this type of software should be updated at each connection.

- Corrections or updates to survey instruments and case management applications are sometimes necessary to correct a programming error or add some critical new functionality.

- Updates to the platform configuration or other security controls may be required either to protect against a newly discovered vulnerability or to allow a function that had initially been restricted.

Introducing change to devices already active in the field is itself a source of additional risk to the confidentially, integrity, and availability of the field devices and data. A mistake in a system update can expose unintended vulnerabilities, damage data or introduce new bugs, or render the devices inoperable. Changes of these types must be designed carefully and tested thoroughly to ensure that they work properly, fail gracefully, and roll back appropriately. It is also very important to keep a log of which systems have received updates to make sure that all systems are maintained at the current configuration and to help troubleshoot problems when they might arise.

7. Other Security Considerations

As we have seen, web-based and CAPI surveys involve some unique areas of vulnerability, based largely on their physical exposure in the former case and electronic exposure over the Internet in the latter. Traditional, centralized CATI surveys do not involve either of these vulnerabilities. Of course, this does not mean that security is not a concern for such studies, but only that these particular risks are not an issue.

As with other platforms, however, evolving technologies and capabilities bring additional risks into the picture. With CATI, the most significant recent development has been the increasing use of home-based interviewers. This brings back the issue of remote access, as well as raising new risks due to the less-controlled physical environment.

A number of strategies can be employed to mitigate these risks. In contrast to CAPI, there exists the option of storing all data centrally, due to the existence of a persistent Internet connection for the duration of each interview. Measures such as background checks, interviewer training, and interview monitoring to reduce the risks of inappropriate interviewer behavior can be employed. If Blaise Internet is chosen as the data collection platform, similar techniques can be adopted as for other web-based surveys. Alternatively, you can use appropriately-secured platforms such as Citrix.

An integrity consideration for even centralized CATI surveys (and CAPI surveys as well) is making sure that only one interviewer “owns” a case at any given time. The possible risks here range from respondent annoyance (if she is called a second time after already completing an interview) to data loss (if completed data are overwritten by blank data from an interviewer who was incorrectly assigned the same case).

Nor does data collection always operate on a single platform: multimode survey efforts are becoming increasingly common. As Hart and others discuss in their 2004 paper (Hart et al., 2004), such efforts involve a number of challenges for IT security, as well as for other aspects of the project.

Finally, the need for IT security does not end once an interview has been completed and transmitted to the home office. As long as survey data are being stored, processed, and analyzed, they need to be protected by a variety of human, technical, and physical controls. Encryption may be employed or even required for data storage on the home office network (Mamer, Hart, and Rozen, 2007). Nor can you assume that you are done with security once the data are no longer stored online; you may want to consider encrypting your backup media, and you certainly need to pay attention to retention periods and destruction dates.

8. Conclusion

IT Security in survey projects addresses a very broad set of concerns intended to reduce the risks to the confidentiality and integrity of survey data and the availability of survey support systems. In addition to the many actual vulnerabilities and threats that must be identified and addressed, there may also be a significant amount of supporting documentation and related activities necessary to meet the evolving regulatory requirements.

FISMA and the supporting NIST guidelines and publications are examples of a comprehensive and robust approach to IT Security management. Although FISMA is intended to regulate U.S. Government systems development, the concepts and processes address common security issues and can be used in a variety of situations.

The different survey modes and platforms share many common security issues but also present unique problems reflecting the specific configuration of devices, users, and data. Various security controls and techniques can be configured and combined to address these unique issues.

Blaise is a central IT component to many survey operations. Blaise is a mature and proven product that provides a number of security-related features and can be integrated and operated as part of a secure end-to-end solution.

9. References

Hart, Leonard, Amanda Foster-Sardenberg, and Yuki Okada. “System Implementation for a Blaise Multimode Web, CATI and Paper Survey.” *Proceedings of the 9th International Blaise Users Conference.* September 2004.
< http://www.blaiseusers.org/2004/papers/25.pdf> (August 31, 2010)

Mamer, John, Leonard Hart, and Josh Rozen. “Encrypting Blaise Data on Network Servers.” *Proceedings of the 11th International Blaise Users Conference.* September 2007.
< http://www.blaiseusers.org/2007/papers/A1%20-%20Blaise%20Encryption.pdf> (August 31, 2010)