

IT Security: BITS' Perspective and Initiatives

Catherine A. Allen
CEO, BITS

2002 OTS Interagency
IT Security Conference
Grapevine, Texas
October 15, 2002

BITS Proprietary and Confidential © BITS 2002.



Agenda

- **Background on BITS**
- **Customer Concerns**
- **Security Related Initiatives**
- **IT Service Provider Issues**
- **Crisis Management**

BITS Proprietary and Confidential © BITS 2002.

2



Background on BITS

BITS Proprietary and Confidential © BITS 2002.



Perspective on BITS' Initiatives

“Our goal is to establish the framework for safe, sound, private and secure financial services — whether online or in traditional settings. BITS fosters collaboration among financial institutions nationwide to leverage the intellectual capital and best practices in technology for the benefit of our key constituencies — customers, shareholders, employees and the communities we serve.”

James E. Rohr, Chairman and CEO
The PNC Financial Services Group
Chairman, BITS Board of Directors

BITS Proprietary and Confidential © BITS 2002.

4



A Bit About BITS

- CEO-created and CEO-driven Technology and Business Strategy Group
- Sister organization to The Financial Services Roundtable
- Founded in 1996 to address areas in which there is need for collaborative industry action
- Focuses on emerging technologies, payments and e-commerce
- Two membership categories:
 - BITS Members
 - BITS Affiliates



The Financial Services Roundtable

- Is a Washington DC-based trade association, and the advocate for integrated financial services providers
- Represents 100 of the largest integrated financial services companies providing banking, insurance and investment products and services
- Member companies participate through the CEO and other senior executives
- Uses grassroots power, knowledge and experience to help shape public policy
- Provides a forum at twice yearly meetings for members to discuss industry trends and public policy issues



Market Forces that Drive FIs

- **Concerns about terrorism-related impacts on the Nation — including public confidence, the economy, continuity of the industry's business operations and employee well being.**
- **Concerns about increased scrutiny of financial institutions with regard to operational and technology risk management.**
- **Gramm-Leach-Bliley legislation, Basel II and other regulatory guidelines in response to concerns related to privacy, security and operational risk.**



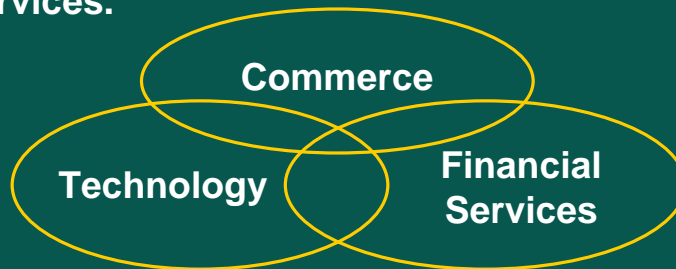
Market Forces, cont.

- **Rapid development/deployment of new technologies.**
- **Globalization of markets, competition and issues.**
- **Security, privacy and business continuity practices of outsourcers, service providers and aggregators.**
- **Urgency to migrate legacy payment systems and the impact on revenues and costs.**
- **Increased threats to the current and new payments systems.**
- **Ambiguity and confusion concerning definition of business method patents and challenges associated with the quality of the patent process.**

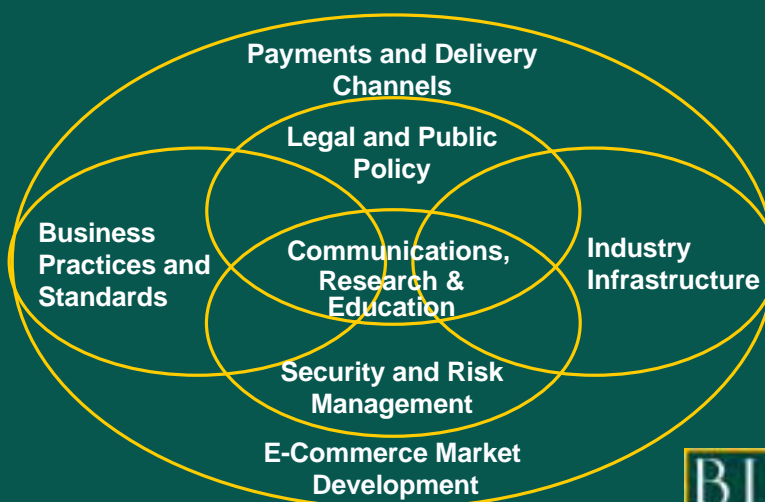


BITS Mission Statement

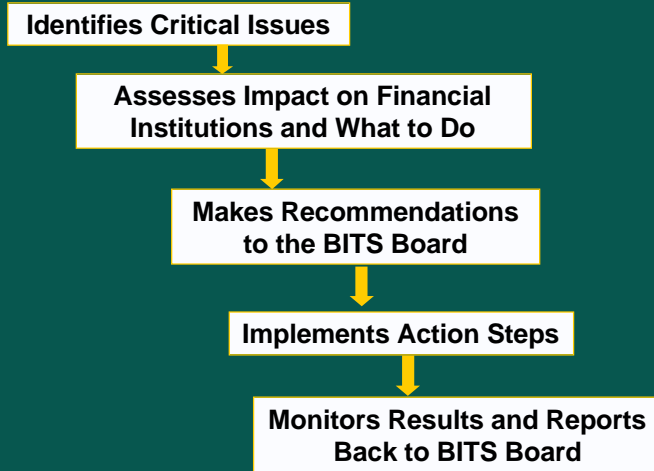
- The BITS Mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services.



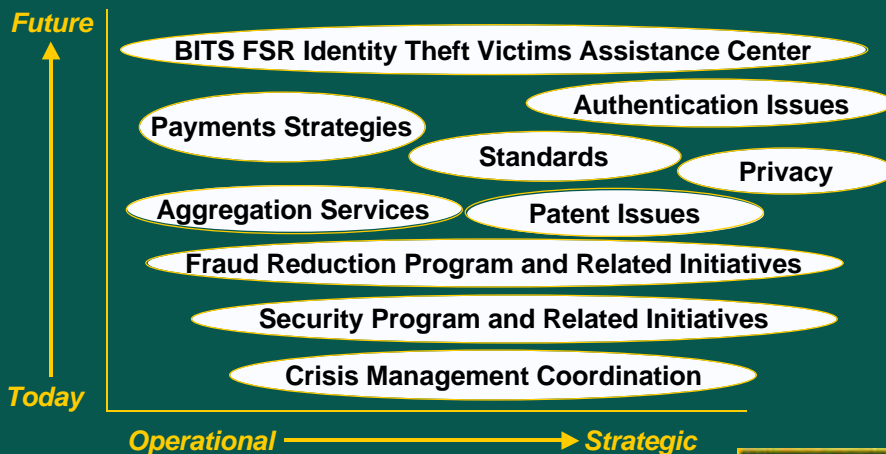
Imperative for Collaborative Action Exists in a Number of Areas



How BITS Works



BITS Initiatives 2002



BITS Priority Initiatives for 2002

- **Authentication**
- **Crisis Management Coordination**
 - Telecommunications
- **Fraud Reduction**
- **Payments Strategies**
- **Security and Risk Assessment**
 - IT Service Providers
 - Operational Risk
 - Product Certification Program
- **BITS FSR Identity Theft Victims Assistance Center**



BITS Initiatives to Monitor and Provide Information Sharing

- **Aggregation**
- **Business Methods Patents**
- **Privacy**
- **Standards**



Examples of BITS Deliverables

- BITS FSR Crisis Communicator
- BITS FSR Crisis Management Process: *Members' Manual of Procedures*
- *BITS Voluntary Guidelines for Aggregation Services*
- *BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships*
- *BITS Guidelines for Mobile Financial Services*
- *Business Method Patents White Paper*
- *Consumer Privacy Research and Business Implications*
- *EA/ECP Business Model and Tool (Updated 2002)*
- *E-Insurance Technology Risk Transfer Gap Analysis Tool*
- *Fraud Prevention Technologies in a Truncation Environment White Paper*
- Security Profiles and Testing Process for E-Commerce Products

BITS Proprietary and Confidential © BITS 2002.

15



Customers Concerns

BITS Proprietary and Confidential © BITS 2002.



Privacy, Security and Use of Information for Financial Services: What's Driving Consumer Behaviors

BITS Proprietary and Confidential © BITS 2002.



The Context

- Results of this second year of BITS' consumer research should be interpreted within the context of three major events:
 - The privacy notices required for mailing to consumers under the -Leach-Bliley Act;
 - September 11, 2001; and
 - The stock market downturn and recession at the time of the interviews in December 2001.

BITS Proprietary and Confidential © BITS 2002.

18



High Level Results

- Consumers are increasingly proactive about protecting the privacy and security of their information.
- The events of September 11 heightened concerns about privacy and security for many consumers.
- Concerns about threats, such as identity theft, continue to grow — in part out of myth, in part out of experience.



High Level Results, cont.

- Internet usage has grown from 59% one year ago to 70% by the end of 2001.
- The average number of hours online has decreased with more mainstream users getting online.
- There is a growth in online commerce, including financial services.



High Level Results, cont.

- While financial transactions on the Internet have increased, low-tech methods like speaking personally with a customer representative have also increased.
- The most active online users are very active transactors—more than 90% actually conduct business of some kind online, rather than simply seeking information.
- There is a growth in online banking since last year, from 29% to 35% of the Internet users interviewed by phone.



High Level Results, cont.

- There is a slight slippage in consumer trust of institutions overall, although the financial services industry—and especially banks and credit unions—continues to enjoy the highest level of trust for conducting safe, sound and secure financial transactions online.



High Level Results, cont.

- **Obtrusive direct marketing practices continue to be unacceptable—in fact, all forms of unsolicited direct marketing are even less acceptable than one year ago, with unsolicited phone calls the least acceptable.**
- **Consumers in growing numbers report taking action to avoid receiving unwanted solicitations.**



High Level Results, cont.

- **The Gramm-Leach-Bliley notices succeeded to some extent in addressing consumer concerns—but they were perceived as unclear and may have contributed to some erosion of trust.**



High Level Results, cont.

- Although the majority are comfortable with their financial institution's privacy policies, there is a significant increase in the number of consumers who feel they are losing control of how their personal information is used and a significant decline among those who believe their information is used appropriately.



High Level Results, cont.

- There is a pervasive skepticism about the benefits to be derived from financial institutions using consumer information to personalize products and services.



High Level Results, cont.

- Given a choice as to whether or not such information is used, the acceptability grows dramatically among all consumer groups.
- Consumers are likely to feel empowered and in control if they have a choice regarding whether and how their personal information is used.



Business Implications

- While there is growth in Internet use and growth in online financial transactions, consumers still want access to services in a variety of ways. Multiple channels are not going away.
- Consumers are receptive to being educated about how to participate in protecting the privacy and security of their information. Providing such information—combined with successful, friendly, easy-to-use and reliable systems—will help foster adoption of new online services.



Business Implications, cont.

- **The benefits from information use have to be conveyed meaningfully, through personalized communications where the value is obvious.**
- **The legacy of trust remains strong. Financial institutions remain the most trusted providers of safe and secure financial services. That trust must be leveraged and safeguarded.**

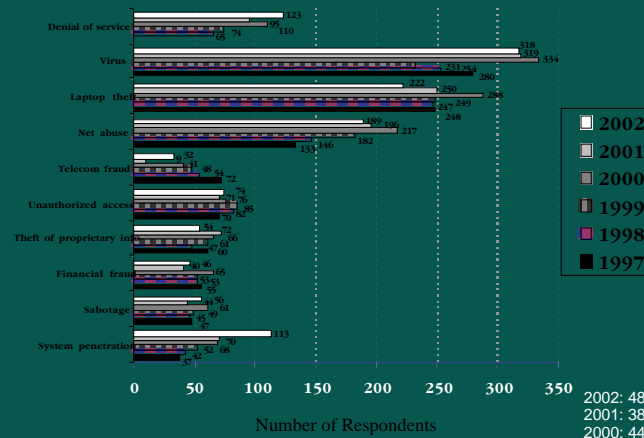


Computer Security Trends

- **In a survey of financial services companies, computer security firms, government agencies and medical institutions and universities, during 2001:**
 - **85% detected computer security breaches**
 - **64% suffered financial loss from system breaches**
 - **94% detected viruses**
 - **40% had their systems hacked into by someone outside their organization**
 - **38% detected denial-of-service attacks**



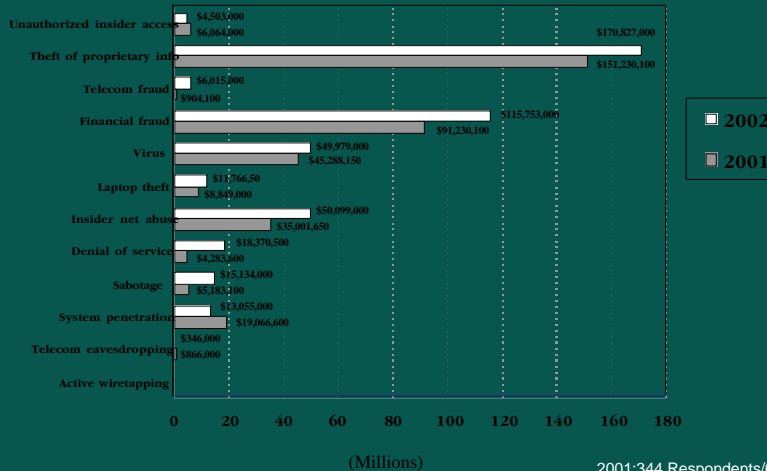
Financial Losses By Type of Attack or Misuse



2002: 481 Respondents/96%
 2001: 384 Respondents/72%
 2000: 443 Respondents/68%
 1999: 324 Respondents/62%
 1998: 279 Respondents/54%
 1997: 391 Respondents/69%
 1996: 174 Respondents/40%

CSI/FBI 2001 Computer Crime and Security Survey
 Source: Computer Security Institute

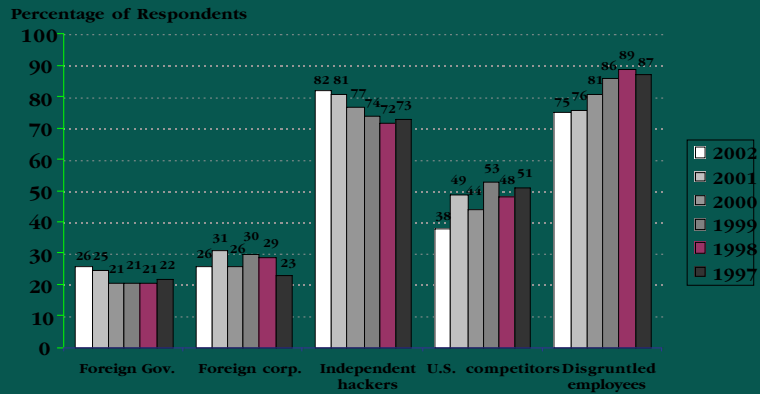
Dollar Amount of Losses By Type



2001:344 Respondents/64%
 2000: 477 Respondents/74%
 1999: 265 Respondents/51%
 1998: 376 Respondents/73%
 1997: 422 Respondents/75%

CSI/FBI 2001 Computer Crime and Security Survey
 Source: Computer Security Institute

Likely Sources of Attack



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/83%
1997: 503 Respondents/89%

BITS Proprietary and Confidential © BITS 2002.

33

Annual Cost of Fraud: More than \$37 Billion

- \$21 billion in insurance fraud (property and casualty)
- \$13 billion in check fraud
- \$3 billion in identity fraud
- \$600 million in credit card fraud



BITS Proprietary and Confidential © BITS 2002.

34

Fraud-related Trends

- **The growth of electronic payments is contributing to an increase in fraudulent activity, particularly identity theft.**
 - Electronic payments have grown from approximately 5 billion in 1979 to 30 billion annually.
 - Debit cards use is growing by 30% annually.
 - Internet use increased from 59% in 2000 to 70% in 2001
 - Online commerce, including online financial services, is increasing.
 - Consumers are increasingly proactive about protecting their information.
 - Public concern about fraud is increasing.



Identity Theft

- **Identity theft accounted for 42% of all consumer fraud complaints received by the Federal Trade Commission in 2001.**
- **According to Celent Communications, identity theft will more than triple by 2005, from 500,000 incidents in 2000 to 1.7 million in 2005.**
- **Ten percent of identity theft is thought to originate on the Internet.**
- **Identity theft—and other forms of fraud—are often the result of employee abuse of computer databases and misuse of sensitive information.**



Security Related Initiatives

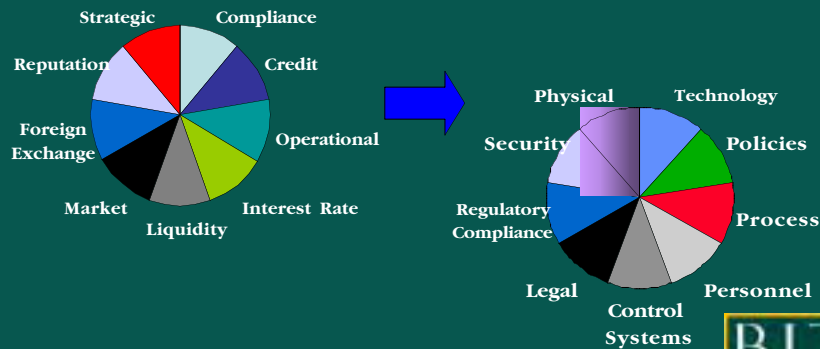


BITS Proprietary and Confidential © BITS 2002.

Categories of Risk

Risk Categories

Operational Risk



BITS Proprietary and Confidential © BITS 2002.

38



Operational Risk Defined

- **Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events.**
 - Transaction processing risk
 - Technology risk
 - Security risk (frauds, crime, theft)
 - Compliance risk
 - Legal/liability risk

Source: OCC Presentation to the BITS Advisory Group, March 7, 2002;
Based on Basel II.

BITS Proprietary and Confidential © BITS 2002.

39



Growing Concern and Attention to Operational Risk

- **Perceived increase in operational risk**
 - Growing service businesses
 - Reliance on technology
- **Reaction to major loss events that have occurred internally or to others.**
 - Accounting scandals
 - Rouge trading incidents
- **Regulatory attention**
 - New Basel Accord

BITS Proprietary and Confidential © BITS 2002.

40



Operational Risk Management

- **Key elements include:**
 - Establishing processes to assess risk in activities, products and systems and
 - Establishing policies, processes and procedures to control or mitigate risk.



BITS Role in Operational Risk Management

- **BITS' focus is information technology which represents a key component of operational risk.**
- **BITS frameworks, voluntary guidelines, information sharing and other tools are integrated into key operational risk management program activities.**



What Has BITS Done to Date?

- Held an industry forum in June, bringing together various perspectives about the issues to the membership.
- Conducted a member survey.
 - 80 institutions were surveyed - 40 institutions responded
- Conducted trade group interviews.
 - Interviewed seven financial and risk-oriented trade groups.
 - Examples:
 - American Bankers Association, International Institute of Finance, Consumer Bankers Association, Security Industries Association, Institute of Internal Auditors, Risk Management Association



Key Findings

- 31/40 survey respondents have or plan to appoint a Chief Operational Risk Officer.
- 22/40 survey respondents have established a Board level Operational Risk Committee.
- 35/40 survey respondents considered the following in their scope of operational risk:
 - Information Security, Business Continuity/Disaster Recovery, Information Technology, Physical Security, Third Party Service Provider Relationships, Fraud Reduction, Legal and Regulatory Risk, Compliance
- 35/40 respondents consider their effort to be “enterprise wide.”



Key Findings, cont.

- There is broad consensus on a role for BITS related to the information security component risk areas.
- There is agreement that we should help drive the regulatory response rather than react to it, providing proactive direction to the regulators as they set guidance and policy.
- There is considerable interest in education and awareness of enterprise-wide issues on operational risk management.



Direction for BITS

- Forming an Operational Risk Working Group with two tracks of activity.

“General Track”

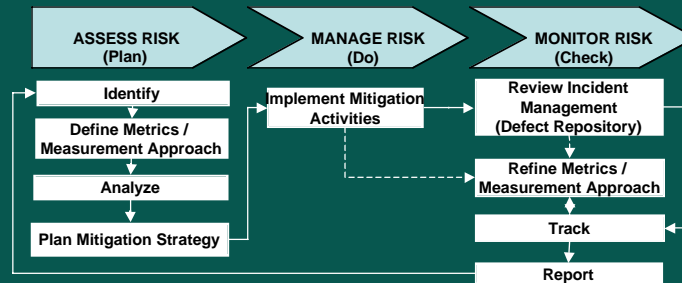
- Create a forum for the exchange and development of ideas around enterprise level operational risk challenges and for a dialogue with the regulatory agencies responsible for interpreting and implementing the new Basel Capital Accord.

“Specific Track”

- Look at the needs for managing the individual components of operational risk, starting with information security and working in conjunction with the Security & Risk Assessment Working Group’s members.



Risk Management Framework



Risk Management System Framework



Strategic Goals: Security and Risk Assessment

- Increase public and private sector confidence in the security of e-commerce.
- Provide leadership in addressing security issues for all financial services companies.
- Partner with government agencies and regulators in the assessment of needed legislation and regulation.
- Influence key technology providers on security aspects of product and service development.



Security and Risk Assessment (SRA) Executive Steering Committee

- Jeffrey Stempora, State Farm, Chair
- Sharon O'Bryan, ABN AMRO
- Eric Guerrino, The Bank of New York
- Mary Jane Bolling, Capital One
- Leigh Williams, Fidelity Investments
- Lari Sue Taylor, FleetBoston Financial Corporation
- Phil Venables, Goldman Sachs
- Gene Fredriksen, Raymond James Financial
- Fred Francis, Whitney National Bank



Security and Risk Assessment (SRA) Committee

- American Bankers Association (ABA)
- ABN AMRO North America, Inc.
- AEGON USA, Inc.
- Allfirst Financial, Inc.
- American General Financial Services
- AmSouth Bancorporation
- Aon Service Corporation
- Association for Payment Clearing Services (APACS)
- Bank of America Corporation
- Bank of New York Company, The
- BANK ONE CORPORATION
- BB&T Corporation
- Capital One Financial Corporation
- Chubb Corporation, The
- Citigroup, Inc.
- Citizens Financial Group
- City National Bank
- Comerica Incorporated
- Credit Suisse First Boston/ Pershing Company
- Edward Jones Investments
- Fidelity Investments
- Fifth Third Bancorp
- First Tennessee National Corporation
- First Virginia Banks, Inc.
- FleetBoston Financial Corporation
- Ford Financial
- Fortis, Inc./Assurant Group
- Goldman Sachs Group, Inc.
- Guaranty Financial Services
- Harris Bankcorp, Inc.
- Hartford Financial Services, The



Security and Risk Assessment (SRA) Committee

- Hibernia National Bank
- HSBC USA, Inc.
- Huntington Bancshares, Inc.
- IBJ Whitehall Financial Group
- Independent Community Bankers of America (ICBA)
- J.P. Morgan Chase & Co.
- KeyCorp
- MBNA Corporation
- M&T Bank Corporation
- Marshall & Ilsley Corporation
- Mellon Financial Corporation
- Mercantile Bankshares
- Nationwide Insurance Company
- Northern Trust Corporation
- PNC Financial Services Group, Inc., The
- Provident Financial Corporation
- Prudential Insurance Company of America
- Raymond James Financial, Inc.
- RBC Centura Banks, Inc.
- Regions Financial Corporation
- SouthTrust Bank
- Spectrum EBP, LLC
- State Farm Insurance
- SunTrust Banks, Inc.
- Synovus/Total System Services
- The St. Paul Company
- USAA
- US Bancorp
- Visa USA
- Wachovia Corporation
- Washington Mutual, Inc.
- Wells Fargo & Company
- Whitney National Bank



SRA 2002/2003 Focus Areas

- **Critical Infrastructure Assurance**
- **Regulatory/Compliance Issues**
- **Security Risk Management & Measurement Project**
- **Product Security**
 - BITS Product Certification Program (formerly the BITS Financial Services Security Lab)
- **Monitoring and input to BITS security related initiatives: Operational Risk, Crisis Management Coordination, IT Service Providers Aggregation, Authentication, etc, on an as-needed basis**



BITS Product Certification Program

The *BITS Tested Mark*



BITS Proprietary and Confidential © BITS 2002.



Product Certification Program Objectives

- Improve the baseline security of products that are used in the financial services industry.
- Provide an opportunity to leverage independent testing efforts including common criteria testing.
- Provide an outward facing seal to visibly recognize products that meet the criteria

Enhancing the Safety & Soundness of the Industry

BITS Proprietary and Confidential © BITS 2002.

54



Benefits to the Financial Services Industry

- Provides tangible evidence of implementing a best practice using industry criteria.
- Provides a vehicle to impose high internal security standards onto externally developed commercial products.
- Supports standard implementation processes used for managing operational risks and regulatory compliance.
- Achieves cost and time savings on individual institutions' product testing.



Industry Support

- Financial institutions have adopted the testing criteria as internal standards.
- Financial institutions are including language about the *BITS Tested Mark* in their procurement policies, RFPs and vendor contracts.
- Financial institutions will likely give favorable consideration to products with the *BITS Tested Mark* because of their known security features and the benefits listed.



BITS Tested Mark - Benefits to Technology Vendors

- **Product Visibility:** Recognition and product differentiation within the financial services industry.
- **Market Potential:** BITS members are committed to making the *BITS Tested Mark* a major part of their technology purchasing process.
- **Efficient Product Development:** The BITS certification provides guidance for future design and certainty that products meet industry-endorsed security standards.



BITS Product Security Criteria

- **A three year development effort involving the work of 32 BITS financial services member companies, 23 outside organizations and over 100 security individuals from technology vendors, government agencies and leading financial service firms.**
- **Criteria represent minimum baseline product security requirements for a set of security features including: identification, non-repudiation, authorization, confidentiality, data and system integrity, data disposal, audit, authentication, security administration, and guidance documentation.**



Security Criteria Status

•Profile - Product Class	•Product Examples
•Application Products	•Browsers, EBPP clients, personal finance managers, email and messaging clients, ERP clients, funds transfer applications, Web servers, EBPP servers, email servers, ERP servers
•Authentication Systems: Systems aimed at authenticating identity of users and systems.	•Smart cards, public-key infrastructure products, biometric devices, one-time passwords and tokens, authentication frameworks
•Access Control and Administration Systems: Products aimed at improving access control and authorization on systems as well as those products aimed at streamlining security administration.	•Single sign-on products, security administration tools, authorization systems, operating system access control products



Security Criteria Status, cont.

•Profile - Product Class	•Product Examples
•Application Security Products: Those products whose primary purpose is to improve security on an application. This class is exclusive of the authentication and access control systems, described above.	•Email security tools and Internet security products
•Monitoring and IDS Systems	•Network and host-based intrusion detection systems
•Network Security Products: Those products whose primary purpose is to improve security on a network. This class is exclusive of the authentication and access control systems described above.	•Firewalls, VPNs, link-layer encryption products



Harmonizing with Common Criteria

- With the help of SAIC, BITS recently completed a translation of the security criteria to “packages of requirements” using the language and schema of the internationally recognized Common Criteria certification program.
- A technology company wishing to obtain a BITS Tested Mark should include the functional security requirement package in the Security Target for the Target of Evaluation.
- If a product has already been through Common Criteria certification, the product can be submitted to a Common Criteria Testing Lab or to an authorized testing facility for testing of the criteria that are included in an applicable “BITS functional security requirement package,” but which were not present in the Common Criteria certification test.



Options for Third Party Testing

Third Party Testing Facility Authorized by BITS

- For smaller or niche-industry vendors seeking only BITS certification.
- Predictive Systems is the first testing facility.
- Additional facilities will follow within the year.

Common Criteria Testing Labs

- For technology providers seeking both CC and BITS certification.
- 6+ labs in U.S. accredited by National Institute of Science & Technology with more in progress.



Testing Process

- The technology provider will contract with a testing facility for testing services.
- The security criteria are used to perform a technical analysis of the product. Each product's features and capabilities are evaluated against the applicable security criteria, with a focus on the security functionality of the product.
- The product will be tested within an appropriately configured test environment, as specified by the technology provider.



Marketing Strategy: Focused Vendor List for Testing

- Symantec
 - Intruder Alert
 - Raptor Firewall
- RSA
 - SecurID
 - Keon
- CISCO
 - PIX Firewall
 - Intrusion Detection
- IBM Tivoli
- ISS RealSecure
- CA eTrust
 - Identity Manager
 - Access Control
- Checkpoint Firewall-1
- BMC
 - Patrol
 - Control SA
- Verisign Onsite
- Netegrity Siteminder
- Okena
 - StormWatch
 - StormFront



BITS Tested Mark

Hewlett-Packard is awarded first
BITS Tested Mark for VirtualVault 4.0



“The achievements in quality and performance signified by the *BITS Tested Mark* make a powerful statement about HP’s commitment to the financial community and the ability of HP VirtualVault 4.0 to contribute to the success of an organization’s overall security policy.”

Roberto Medrano, General Manager
HP Internet Security Solutions Division



IT Service Provider Issues



Financial Services Outsourcing Environment

- The number of financial institutions using outsourcing is expected to grow about 50% for most IT outsourcing types, and nearly double for data center and storage outsourcing between 2002 and 2003. Gartner
- 42% of financial services companies surveyed in late 2001 reported that they plan to reduce the number of IT vendors that provide them services. Gartner
- Over one-third of Fortune 500 companies perform at least some IT services work offshore and business process outsourcing is expected to explode to \$142 billion by 2008. PWC Consulting
- In a survey of 800 Indian companies across various industries, 78% of respondents said their organizations had not recently evaluated the controls portfolio in relation to the risks they face. KPMG



Environment, cont.

- Over one-third of Fortune 500 companies perform at least some IT services work offshore and business process outsourcing is expected to explode to \$142 billion by 2008. PWC Consulting
- In a survey of 800 Indian companies across various industries, 78% of respondents said their organizations had not recently evaluated the controls portfolio in relation to the risks they face. KPMG

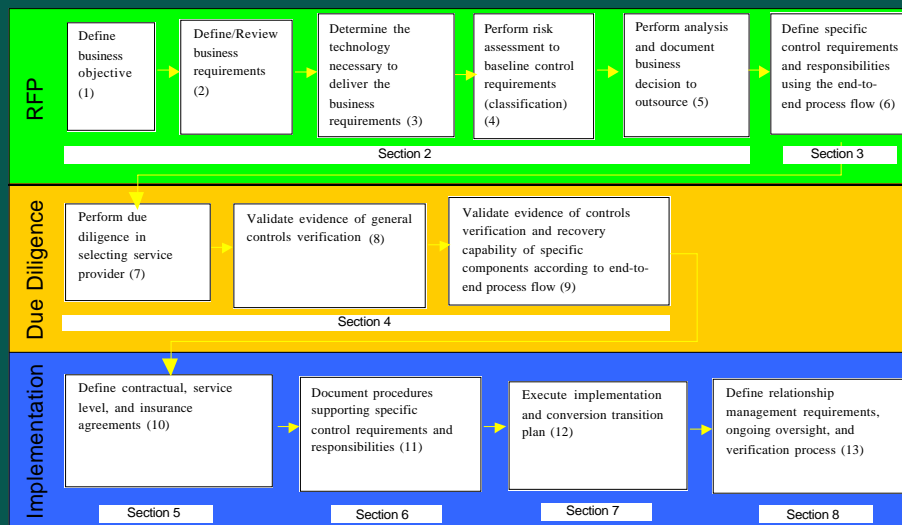


Financial Services Outsourcing Challenges

- Financial institutions must establish processes that evaluate risks, vulnerabilities and regulatory requirements at each stage of the service provider relationship.
- Disaster recovery/business continuity is a critical element in evaluating service provider relationships.
- In global relationships, political, country and infrastructure risks must also be considered.
- Tracking downstream outsourced relationships is important to understanding risk.



IT Guidelines Flow Chart



Phase II: Objectives and Subgroups

- **Education and Awareness:** Gain broad acceptance of the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* among key stakeholders.
- **Vendor Management:** Identify and share industry best practices and considerations for relationship and risk management of IT service provider relationships.
- **Crisis Management:** Update *BITS Framework* to include crisis management/business continuity issues for service providers.
- **Security Assessments:** Identify industry, regulatory and *Framework* requirements for third-party audits and assessments.
- **Cross-Border:** Identify industry issues and best practices related to cross-border outsourcing.



Security Assessments

- **Identify industry, regulatory and *Framework* requirements for third-party audits and assessments.**
 - The *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* set the stage for risk management strategies for outsourcing.
 - Create a high-level set of industry expectations for service provider operations.
 - Develop an RFI to communicate expectations and survey audit and assessment methodologies.
 - Review RFI responses to determine acceptable methodologies and best practices for audits and assessment documentation, validation, testing and reporting.



Crisis Management

BITS Proprietary and Confidential © BITS 2002.



Crisis Management Coordination: Objective and Assumptions

Objective

- To improve the industry's ability to recover from significant industry-wide disasters by focusing on enhanced preparation and communication.

Assumptions

- Crisis coordination is a senior management event.
- Crisis coordination is not a competitive issue.

BITS Proprietary and Confidential © BITS 2002.

74



September 11 – One Year Later

- Since September 11, the Financial Services Industry has significantly enhanced its ability to communicate, coordinate and recover in the event of another crisis.
- Areas of risk continue to exist and require additional attention



Communication Enhancements

- Crisis Communicator – High Speed Notification System
- “Virtual” crisis communications center available 24/7
- Forums on Operational Risk and Telecommunications
- Key messages to maintain public confidence



Coordination Enhancements

- **Crisis Management Process: *Members' Manual of Procedures***
- **Influenced the Formation of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)**



Recovery Enhancements

- **Identification, accumulation and distribution of best practices**
- **Scenarios building and event management based on scenarios**
- **Participation in the Federal Reserve's Payments Risk Committee**
- **GETS Card Policy for the Industry**



Areas of Risk

- The government's fragmented response capabilities and the absence of a financial services sector command center
- The threat of a major cybersecurity attack
- The financial services industry's dependence on other sectors – most notably telecommunications



Telecommunications in Crisis: The Situation

- Financial crisis in leading providers of voice services - \$2 trillion in losses
- The local telcos may be next
- Meltdown in service despite competition
- Little redundancy, diversity or security
- Lack of government policy to ensure reliability
- Regulators may shift the burden to financial services companies



Dependence on Telecommunications – An Industry in Crisis

- Addressing our industry’s dependence on telecommunications - develop a White Paper on critical issues and potential solutions to be used for discussions
- Schedule CEO to CEO discussions with key vendors
- Schedule CEO to Regulator discussions with key regulators
- Address issues through business practices and public policies
- Make issues known to the industry through business requirements

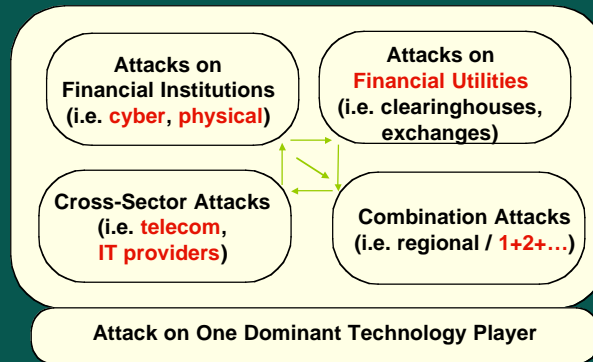


Comment Letter

- Responding to “Draft White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” Draft White Paper was released on August 30.
- BITS will draft a comment letter by the October 21 deadline.
- BITS will coordinate its response with other groups (e.g., the Financial Services Sector Coordinating Council).



Six Key Scenarios



Scenario Analysis – Cyber Attack

Scenario-Building		Event Management	
Risks	Potential Impacts	Preparation	Responses
<ul style="list-style-type: none"> • Could be dramatic catastrophic loss or gradual data corruption • Could target: internal networks, email, web servers, desktop, applications, customer desktop • Could target small to medium institutions with less elaborate security • Multiple or persistent attacks could overwhelm resources • Objective could be DOS or account takeover 	<ul style="list-style-type: none"> • Service interruption (web, ATMs) • Back office interruption (interrupted processing, unauthorized transactions) • Books and records compromised • Private data revealed (customer, corporate) • Theft of funds • Crisis management capability undermined • Public confidence undermined 	<p>Baseline preparation plus:</p> <ul style="list-style-type: none"> • ST: Establish communications channels with technology vendors • ST: Strengthen global early warning system • MT: Establish hardened backup for data transmission / crisis mgmt • MT: Consider the creation of a meta-ISAC • MT: Accelerate patch testing and installation • MT: Consider industry standards for backup, DR • MT: Build data valuation model for insur/risk mgmt 	<p>Baseline responses plus:</p> <ul style="list-style-type: none"> • Distribute alerts through FS/ISAC and BITS • Firms activate own cyber-protection plans • Facilitate info-sharing among BITS, FS/ISAC, vendors and authorities • Convene bridges to share detailed analysis of attack and impacts • Activate backup for data transmission/crisis mgmt



Crisis Management Coordination Member Participants

- ABN AMRO North America, Inc.
- AEGON USA North America, Inc.
- Allfirst Financial, Inc.
- AMCORE Bank
- American Bankers Association
- America's Community Bankers
- AmSouth Bancorporation
- Aon Risk Management Services
- Associated Banc-Corp
- Assurant Group
- BancorpSouth, Inc.
- Bank of America Corporation
- BANK ONE CORPORATION
- BB&T Corporation
- Capital One Financial Corp.
- Citigroup, Inc
- Citizens Financial Group
- City National Bank
- Comerica Incorporated
- Compass Bank
- Credit Suisse First Boston
- CUNA
- Edward Jones Investments
- Fidelity Investments
- First National Bank of Omaha
- First Tennessee National Corp.
- First Virginia Banks, Inc
- FleetBoston Financial Corp.
- Ford Financial
- Fortis, Inc.
- Frost Bank
- General Motors Acceptance Corp.
- Goldman Sachs Group Inc.
- Guaranty Financial Services
- Harris Bankcorp, Inc.
- Hibernia National Bank
- Household International, Inc.
- HSBC USA, Inc.
- Huntington Bancshares, Inc.



Crisis Management Coordination Member Participants, cont.

- IBJ Whitehall Financial Group
- ICBA
- J.P. Morgan Chase & Co.
- KeyBank, NA
- M&T Bank
- Marshall & Ilsley Corporation
- MBNA Americas
- Mellon Financial Corporation
- Mercantile Bankshares Corp.
- Metavante Corporation
- NACHA
- National City Corporation
- Nationwide Financial
- Northern Trust Corporation
- Old National Bancorp Svc.Co.
- PNC Financial Services Group
- Prudential Financial
- Raymond James Financial
- RBC Centura
- Regions Financial Corporation
- SouthTrust Bank
- Spectrum EBP, LLC
- State Farm Insurance
- SunTrust Banks, Inc.
- Synovus
- TCF Bank
- The Bank of New York Company
- The Chubb Corporation
- US Bancorp
- Union Planters Corporation
- USAA
- Visa USA
- Wachovia Corporation
- Washington Mutual Bank
- Wells Fargo & Co.
- Whitney Holding Corporation



Crisis Management Coordination Government Contacts

- Office of Homeland Security
- Office of Cyberspace Security
- Critical Infrastructure Assurance Office
- National Security Council
- National Infrastructure Protection Center
- National Infrastructure Simulation and Analysis Center
- National Institute for Standards and Technology
- Partnership for Critical Infrastructure Protection
- Government Services Administration
- Department of the Navy
- Institute for Defense Analysis
- Federal Bureau of Investigation
- Federal Emergency Management Agency
- Federal Reserve Board and Banks
- Federal Deposit Insurance Corporation
- U.S. Treasury
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- National Communications System
- U.S. Department of Justice



For More Information: BITS@fsround.org; Tel. (202) 289-4322 www.BITSinfo.org

BITS Staff Contacts

Catherine A. Allen, CEO cathy@fsround.org
Tanya Bailey, Senior Director Meetings tanya@fsround.org
Wattie Bennett, Executive Assistant wattie@fsround.org
Faith Boettger, Senior Consultant faith@fsround.org
John Burke, Outside Counsel jburke@foleyhoag.com
John Carlson, Senior Director, john@fsround.org
Cheryl Charles, Senior Director cheryl@fsround.org
Elaine Clayton, Administrative Assistant elaine@fsround.org
Jennifer Miller Dickerson, Senior Director jennifer@fsround.org
Teresa Lindsey, Chief of Staff, Senior Director teresa@fsround.org
Laura Lundin, Senior Director laura@fsround.org
Leslie Mitchell, Director leslie@fsround.org
Carrie Neckorcuk, Manager of Human Resources carrie@fsround.org
Ann Patterson, Manager Member Relations ann@fsround.org
Gary Roboff, Senior Consultant gary@fsround.org
Iris Simpson, Administrative Assistant iris@fsround.org
Robin Stade, Director robin@fsround.org
Susanna Space, Communications Manager susanna@fsround.org
Ben Stafford, Project Manager ben@fsround.org
Keviar Warner, Project Manager keviar@fsround.org
Heather Wyson, Project Manager heather@fsround.org



Appendix



BITS Proprietary and Confidential © BITS 2002.

BITS Board of Directors

Chair: James E. Rohr	Chairman and CEO	The PNC Financial Services Group
Vice Chair: Charles K. Gifford	President and COO	FleetBoston Financial Corp.
James H. Blanchard	Chairman and CEO	Synovus
Timothy C. Coughlin	President	Riggs National Corporation
James Dimon	Chairman and CEO	BANK ONE Corporation
Richard D. Fairbank	Chairman and CEO	Capital One Financial Corp.
Jerry A. Grundhofer	President and CEO	U.S. Bancorp
David Hayes	President and CEO	Security Bank (ICBA)
Thomas E. Hoaglin	President and CEO	Huntington Bancshares Incorporated
Richard M. Kovacevich	Chairman and CEO	Wells Fargo & Company
Donald H. Layton	Vice Chairman	J.P.Morgan Chase & Co.
Kenneth D. Lewis	Chairman, President and CEO	Bank of America Corporation
Martin G. McGuinn	Chairman and CEO	Mellon Financial Corporation



BITS Proprietary and Confidential © BITS 2002.

BITS Board of Directors, cont.

Eugene A. Miller	Chairman, President and CEO	Comerica Incorporated
Dean O'Hare	Chairman and CEO	The Chubb Corporation
Page Ogden	President and CEO	Britton & Koontz First National Bank (ABA)
Thomas A. Renyi	Chairman, President and CEO	The Bank of New York
Edward B. Rust, Jr.	Chairman and CEO	State Farm Mutual Automobile Insurance Company
G. Kennedy Thompson	Chairman, President and CEO	Wachovia Corporation
David Weinstein	Chief of Administration	Fidelity Investments
Robert Willumstad	CEO, Consumer Group	Citigroup

Founding Board Members Emeritus

Spencer F. Eccles	Chairman	Wells Fargo Intermountain Banking Region
Terrence Murray	Chairman and CEO	FleetBoston Financial Corp.



BITS Members

- ABN-AMRO North America, Inc.
- AEGON USA, Inc.
- Allfirst Financial, Inc.
- Allied Capital Corporation
- AMCORE Financial, Inc.
- American General
- AmSouth Bancorporation
- Aon Corporation
- Associated Banc-Corp
- AXA Financial, Inc.
- BancorpSouth, Inc.
- BancWest Corporation
- Bank of America Corporation
- The Bank of New York Company, Inc.
- Bank of Tokyo-Mitsubishi Trust Company
- BANK ONE CORPORATION
- BB&T Corporation
- Capital One Financial Corporation
- The Charles Schwab Corporation
- Charter One Financial, Inc.
- Chubb Corporation, The
- Citigroup Inc.
- Citizens Financial Group, Inc.
- City National Corporation
- Comerica Incorporated
- Commerce Bancshares, Inc.



BITS Members

- Compass Bancshares, Inc.
- Countrywide Credit Industries, Inc.
- Credit Suisse First Boston
- Cullen/Frost Bankers, Inc.
- Edward Jones Investments
- F.N.B. Corporation
- FMR Corp. (Fidelity Investments)
- Fifth Third Bancorp
- First Commonwealth Financial Corporation
- First National of Nebraska, Inc.
- First Tennessee National Corporation
- First Virginia Banks, Inc.
- FleetBoston Financial Corporation
- Ford Financial
- Fortis, Inc./Assurant Group
- Fulton Financial Corporation
- General Motors Acceptance Corporation
- The Goldman Sachs Group, Inc.
- Guaranty Financial Services
- Harris Bankcorp, Inc.
- The Hartford Financial Services Group, Inc.
- Hibernia Corporation



BITS Members

- Household International, Inc.
- HSBC USA Inc.
- Hudson United Bancorp
- Huntington Bancshares Incorporated
- ING Americas
- Jefferson_Pilot Corporation
- J.P. Morgan Chase & Co.
- KeyCorp
- Legg Mason, Inc.
- M&T Bank Corporation
- Marshall & Ilsley Corporation
- MassMutual Financial Group
- MBNA Corporation
- Mellon Financial Corporation
- Mercantile Bankshares Corporation
- Merrill Lynch & Co., Inc.
- Minnesota Mutual
- National City Corporation
- National Commerce Financial Corporation
- Nationwide
- Northern Trust Corporation
- Old National Bancorp
- Pacific Century Financial Corporation
- The PNC Financial Services Group, Inc.



BITS Members

- Provident Bankshares Corporation
- Provident Financial Group, Inc.
- Provident Financial Corporation
- The Prudential Insurance Company of America
- Raymond James Financial, Inc.
- RBC Centura Banks, Inc.
- Regions Financial Corporation
- Riggs National Corporation
- Sky Financial Group, Inc.
- SouthTrust Corporation
- The St. Paul Companies, Inc.
- State Farm Insurance Companies
- State Street
- SunTrust Banks, Inc.
- Synovus
- UBS Warburg LLC
- Union Planters Corporation
- U.S. Bancorp
- United Bankshares, Inc.
- USAA
- Wachovia Corporation
- Waddell & Reed Financial, Inc.
- Washington Mutual, Inc.
- Wells Fargo & Company
- Whitney Holding Corporation
- Zions Bancorporation
- Zurich North America

BITS Proprietary and Confidential © BITS 2002.

95



BITS Affiliate Members

- American Bankers Association (ABA)
- America's Community Bankers (ACB)
- Association for Payment Clearing Services (APACS)
- Canadian Bankers Association (CBA)
- Canadian Payments Association (CPA)
- CUNA
- ECCHO
- Independent Community Bankers of America (ICBA)
- NACHA
- Spectrum EBP, L.L.C.
- VISA USA

BITS Proprietary and Confidential © BITS 2002.

96

