

THE **SANTA FE** GROUP

*Emerging Trends in Data Security:
What Senior Executives and Boards
Need to Know*

Catherine A. Allen, Chairman and CEO
The Santa Fe Group
9th Annual SSCL Strategies for Success Seminar
December 4-6, 2007 – Laguna Niguel

About The Santa Fe Group

- Strategic consulting firm based in Santa Fe, NM
- Strategic partner and preferred provider to BITS
- Trusted voice in the financial services industry
- A national network of thought leaders and innovators hand-picked for their deep knowledge, hands-on experience and objective approach

THE **SANTA FE** GROUP

2

The Santa Fe Group – What We Do

- Strategic Series: Board and C-level briefings
- The Santa Fe Group Vendor Council
- Industry projects:
 - Shared Assessments Program
 - Payments Partner Project
- Expert testimony
- Research and benchmarking
- Events
 - BITS/American Banker Outsourcing Conference – Nov 07
 - Operational Risk Summit – Oct 07
- The Santa Fe Group Innovation Institute

THE **SANTA FE** GROUP

3

Santa Fe Group Vendor Council

- Grew out of BITS financial institution/vendor interaction
- Member-driven: Microsoft, Metavante, Iron Mountain, others
- Bridges disconnect and builds thought leadership between technology providers and user community
- Dialogue among industry leaders and service provider community
- White papers: internal fraud, ACH fraud, e-discovery
- Critical insights into financial services technology strategy

THE SANTA FE GROUP

4

About BITS

- A division of The Financial Services Roundtable
- Works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions
- Provides intellectual capital, addresses emerging issues
- Participants include CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists
- Engages the vendor community in identifying problems and developing solutions

THE SANTA FE GROUP

5

BITS Core Initiatives – 2007-08

- Security: Strengthens financial services resiliency
 - Issues include wireless security, secure email, encryption key management and compliance with authentication regulations
- Fraud reduction: Reducing member fraud losses
 - Issues include rising fraud risks, ACH risk, debit card/ATM fraud, remote channel fraud, and mortgage fraud
- Vendors: Helps members manage risks, comply with regulatory requirements, and forestall additional regulatory requirements
- Regulation: Develop relationships with financial regulators and respond to proposed regulation

THE SANTA FE GROUP

6

Examples of BITS Deliverables

- BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information
- BITS Remote Deposit Image Capture: The Processes, Risks and Strategies Used to Mitigate Them
- BITS Key Considerations for Securing Data in Storage and Transport
- BITS Internal Fraud DataBase
- BITS Calculator: Key Risk Measurement Tool for Information Security Operational Risk
- BITS Consumer Confidence Toolkit: Data Security and Financial Services

THE **SANTA FE** GROUP

7

Examples of BITS Deliverables

- BITS/Roundtable Identity Theft Assistance Center (ITAC)
- BITS Guide to Business-Critical Telecommunications Services
- BITS Product Certification Program
- BITS Payments Roadmap
- Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy
- BITS Phishing Prevention and Investigation Network (hosted at the FS/ISAC)
- E-Scams White Paper Series

THE **SANTA FE** GROUP

8

Fraud and Security Today

- As many as one in five customers leaves an institution following a data security breach; another 40 percent consider cutting their ties
- In addition to targeting large financial institutions, online criminals are targeting smaller institutions, ISPs, government agencies, and educational institutions
- 9 out of 10 phishing sites are aimed at the financial services sector
- Technical sophistication of phishing attacks is increasing

THE **SANTA FE** GROUP

9

Identity Theft

	2003	2006
US Adult Victims of ID Fraud	10.1M	8.9M
Mean Fraud Cost Per Victim	\$53.2B	\$56.6B
Mean Resolution Time	33 hrs	40 hrs

Source: Javelin Strategy & Research

THE SANTA FE GROUP

10

Phishing

- Phishing continues to grow: Attacks increased 41% in 2006
- Number of distinct brands attacked grew 135%
- Most attacks target financial services; other sectors like retailers are becoming more common
- Attacks are moving from large banks to smaller banks and credit unions
- Expanding geographically to Europe and Asia

THE SANTA FE GROUP

11

Insider Fraud

- Organized criminals are infiltrating companies around the world, stealing money and data
- Insider fraud costs US financial institutions about \$2.3 billion annually
- 70% of insider theft is committed by employees who have been with the company for less than 30 days
- Just 8% of internal fraud perpetrators have prior convictions
- Nearly two-thirds of internal fraud in the US goes unsolved

THE SANTA FE GROUP

12

Data Security in Outsourcing Today

- 91% of senior executives from a variety of US industries reported being "somewhat" or "very concerned" about data theft or misuse in outsourced operations
- Information security is one of the top three most important factors for US companies in selecting an outsourcing partner
- Nearly 70% of executives surveyed in 2006 were reviewing their outsourcing strategy in response to recent high-profile cyber crime, customer data theft and network security incidents

Booz Allen Hamilton, 2006

THE SANTA FE GROUP

13

Market Forces that Drive Financial Institutions

- Impact of the mortgage "tsunami"
- Security breaches and related incidents that run the risk of eroding public confidence
- Rapid growth of ID theft and fraud, including international crime rings
- Concerns about terrorism, interdependencies of critical infrastructures and business continuity
- Growth of wireless technologies for banking and payments

THE SANTA FE GROUP

14

Market Forces that Drive Financial Institutions

- Changes due to electronification and intermediaries
- Increasing needs for regulatory efficiencies
- Concerns about security, privacy and business continuity practices of third party service providers
- Rapid development/deployment of new technologies
- Maintaining and transitioning legacy systems

THE SANTA FE GROUP

15

Top of Mind for CEOs – 2007-08

- Wireless security
- Costs of compliance
- Internal fraud
- Cross-channel payments risk
- Data breaches and public confidence
- New revenue streams

THE **SANTA FE** GROUP

16

Emerging Technologies to Have on Your Radar Screen

- The cell phone becomes everything
- Wireless technologies and applications
- Social networking systems
- Massive database search engines

THE **SANTA FE** GROUP

17

Focus on Two Issues

- Management of a data breach
- Management of third party providers

THE **SANTA FE** GROUP

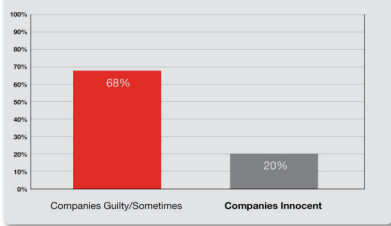
18

The Value Killers

■ Deloitte 2005 research:

- Almost 50% of global 1000 companies lost 20% or more in share price in less than a month during the past 10 years. Some never recovered.
- 80% of losses were due to interaction of multiple risks.
- Most major losses were the result of a series of high-impact but low-likelihood events.
- Almost all organizations put risk management in specialist silos.

Are Corporations Generally Guilty or Innocent?



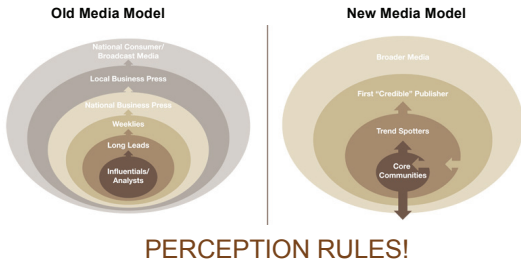
Source: Levick Strategic Communications

Triage

Assess	Control	Treat
Objective facts What's at stake?	Internal/external messages	Implement: proactive & reactive
Subjective considerations? Perception? Audience(s)?	Opposition?	Contribution/aggression?
Emotional considerations?	Media vulnerability Who/Where/How	Integration

Source: Levick Strategic Communications

A New Influential Model



Source: Waggener Edstrom Worldwide

THE SANTA FE GROUP

22

Impact of Events: What We Are Trying to Manage

- Impact on public trust / reputation risk
- Financial risk
- Litigation risk
- Regulatory actions
- Internal cost of response

THE SANTA FE GROUP

23

Elements of a Customer Response Program

- Developing an Incident Response Team
- Assessing the nature and scope of an incident
- Taking steps to contain and control the incident
- Notifying the institution's primary federal regulator
- Working with law enforcement
- Notifying customers and other stakeholders and providing assistance
- Corrective action to prevent re-occurrence

THE SANTA FE GROUP

24

Internal Response Team

- What resources need to be engaged?
 - Investigations
 - Fraud
 - Customer Service
 - Corporate Communications
 - Legal
 - Privacy
 - Information Security
- Develop an information breach response playbook with key players and refine it as events unfold

Internal Cost of Response

- Internal cost components:
 - Free or discounted services
 - Notification letters and phone calls
 - Legal and audit expenses
 - Call center expenses
 - Internal investigations
 - Public and investor relations
 - Loss of current and potential customers
- The average total cost of a data breach is \$182 per lost customer record (Ponemon)

Lessons Learned

- No two breaches are identical
- Immediate notification is critical to containment
- Type of law enforcement agencies needed depends on the type of breach
- Data storage methods can make gathering a complete customer profile can be difficult and time-consuming
- Expect federal guidance and state statutes on customer notification to create confusion and extra work
- Internal communication process is critical
- The number of letters to be sent will impact timing of and approach to mailing
- Engage relationship managers to retain high-value customers

Financial Institution Shared Assessments Program

- Created by BITS Members
 - IT Service Providers Expectations Matrix
 - Six members collaborated
- Formation of the Program
 - Proof of concept
 - Pilots
 - Operational recommendations



Why We Need Shared Assessments

- Risk: Financial institutions must ensure that third party providers are meeting the control environment specifications outlined in their outsourcing agreements
- Expense: Individual financial institutions use substantial resources to make these evaluations
- Inefficiency: Service providers must respond to inconsistent and costly questionnaires and information/audit requests



Program Benefits

- Raises the bar on security
- Reduces costs
- Increases efficiency
- A forum for industry collaboration
- A common sense approach
- Evolves to remain relevant



Controls

- Risk Management
- Information Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance



Standardized Information Gathering Questionnaire

- Replaces institution questionnaires
- Complete picture of provider operations and controls
- Once completed by service providers, can be distributed to all clients

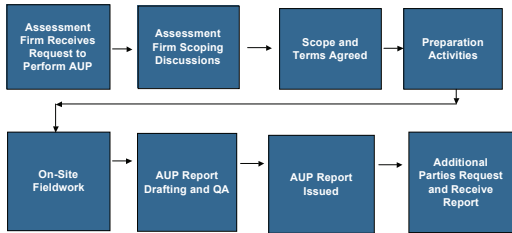


Agreed Upon Procedures

- Objectively test a control and report results
- Test and validate service provider information security controls
- Institutions view results in the context of their risk management requirements



The AUP Assessment Process



Working Group

- Open to all stakeholders
- Participation in ongoing program development
- Candid discussion with member financial institutions, service providers and consulting firms
- Be part of a solution that raises the bar on security



Membership Today: Financial Institutions

- Bank of America Corp.
- The Bank of New York Mellon
- Citi
- Goldman Sachs
- JPMorgan Chase
- Merrill Lynch
- Morgan Stanley
- M&T Bank
- Regions Financial
- Target Corporation
- US Bancorp
- Wachovia Corp.
- Wells Fargo & Company
- Wilmington Trust Co.



Membership Today: Service Providers

- Acxiom
- American Education Services
- Convergys
- The Depository Trust & Clearing Corporation
- Digital Insight
- Early Warning Services
- Equifax
- Experian
- First Data
- IBM
- Infosys Technologies Ltd.
- Iron Mountain
- Metavante Corporation
- SEI
- SunGard
- TSYS
- USi
- VeriSign
- Wipro
- Yodlee
- Zoot Enterprises



Membership Today: Assessment Firms

- Trustwave Holdings, Inc.
- BSI Management Systems America, Inc.
- Cybertrust, Inc.
- Deloitte & Touche*
- Ernst & Young*
- FishNet Security
- KPMG*
- NET2S
- PricewaterhouseCoopers*
- Relational Security



**Technical Advisers*

Licenseses

- Archer Technologies
- Avior Computing
- Control Path
- Cybertrust
- Modulo Security
- Relational Security Corporation



Expectations

- The top trends and issues in outsourcing today
- Managing data security risk
- Effective security evaluations vs. limited resources
- Getting the best value from your outsourcing program
- Knowledge transfer / retaining brand trust
- Human capital evolution and trends
- Customer data privacy
- Regulatory concerns



Thank You

Catherine A. Allen, Chairman and CEO
The Santa Fe Group
info@santa-fe-group.com / 505-466-6434
www.santa-fe-group.com

The Santa Fe Group

Catherine A. Allen, Chairman and CEO cathy@santa-fe-group.com
William J. Barr, Senior Consultant, bill@williambarr.com
Joyce Crawshaw, Client Relations Manager joyce@santa-fe-group.com
Michele Edson, SVP michele@santa-fe-group.com
Robert W. Jones, Senior Consultant bob@santa-fe-group.com
Janey Place, Senior Consultant janey.place@earthlink.net
Gary Roboff, Senior Consultant gary@santa-fe-group.com
Robin M. Slade, SVP and COO robin@santa-fe-group.com
Susanna Space, VP, Communications susanna@santa-fe-group.com
www.santa-fe-group.com / 505-466-6434
