

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Results of BITS Research and Development (R&D) PRIORITIES SURVEY July, 2005

BITS surveyed members of the BITS Security and Risk Assessment Working Group in late June/early July 2005 on the research and development (R&D) cyber security priorities of the financial services industry. The results of this survey will be used in discussions of the Financial Services Sector Coordinating Council for Critical Infrastructure and Homeland Security (FSSCC) and in advising the Federal Government (Congress, Treasury, Homeland Security) on R&D cyber security projects. In general, BITS members support the following statement on the R&D needs of the financial services industry:

The financial services industry is looking for R&D that provides genuine protection against real threats. The most productive and beneficial R&D closes the gap between what exists today with regard to security and protection methodologies and where the industry wants or needs to be in the future in light of existing yet unresolved threats and evolving threats. Financial institutions invest in security because it is central to maintaining customer trust, managing risks, complying with regulatory requirements, and driving strategic business opportunities.

The following is a list of the top cyber security-related R&D issues in order of priority, based on responses from 13 member companies.

High Priority:

1. Assess authentication methods that are acceptable/convenient to customers.
2. Assess the impact of ID theft and e-scams on e-commerce, individuals and society.
3. Identify the gaps in security between financial institutions, merchants, consumers, etc.
4. Quantify the impact of “safe practices” on reducing exposure.
5. Assess the risks associated with the growing dependence on the Internet.
6. Evaluate risks, returns, reliability and restoration issues with the use of encryption.
7. Identify the key elements of secure software code/products.

Medium Priority:

8. Evaluate the impact of regulation/supervision on security practices.
9. Identify the “shared responsibilities” of key players and quantify who benefits from good and bad security practices.
10. Evaluate the role of ISPs in facilitating e-scams, spam, malware.
11. Assess how the actions of ISPs (or lack thereof) affect organizations and individuals.
12. Evaluate the effectiveness of software certification and testing programs (e.g., Common Criteria).
13. Identify public policy incentives that lead to better security.
14. Quantify the costs/benefits of stronger security from Sarbanes-Oxley and Gramm-Leach-Bliley Act.

Other Priorities:

15. Identify the “tipping point” when security transitions from being “a cost of doing business” to a business driver/enabler and strategic business opportunity.”
16. Identify steps the government can take to address these risks.
17. Assess the roles countries play in securing global business (e.g., technology, infrastructure, taxes, law enforcement).
18. Evaluate the effectiveness of open sourcing on software security
19. Evaluate the effectiveness of logging all READ and WRITE access to data, such as scope of logs maintained (network, OS, application, database), where and how are logs stored, storage size, data retention, and cost versus benefits.
20. Assess the operational impact of the PCI Data Security Standard on insurance, service providers and merchants.