

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

**For Immediate Release**  
**April 27, 2004**

**Contact: Susanna Space**  
**BITS**  
**susanna@fsround.org**  
**505-466-6434**

***Software Providers Should Accept Responsibility for Their Role in Supporting US Financial Institutions and Critical Infrastructure***

**BITS AND THE FINANCIAL SERVICES ROUNDTABLE ADOPT SOFTWARE SECURITY POLICY**

**WASHINGTON, DC, April 27, 2004** – Two of the nation’s most influential financial services industry associations announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers (see attached). Software providers should accept responsibility for their role in supporting financial institutions and other critical infrastructure companies, according to the policy statement, which was recently approved at a CEO level meeting. BITS and The Financial Services Roundtable share a membership made up of 100 of the largest financial institutions in the US.

BITS’ and the Roundtable’s efforts have three overarching objectives. The associations want software and hardware vendors to: 1) provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; 2) ensure products comply with security guidelines before releasing products; and 3) make the patch-management process more secure and efficient for organizations. These objectives are outlined in greater detail in the attached policy statement and “Business Requirements for Software Security and Patch Management.”

The BITS and Roundtable policy statement calls on software vendors to be more accountable for the quality of their products. BITS and the Roundtable will support incentives (e.g., tax

incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. BITS and the Roundtable also will seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for software and hardware that they purchase. The associations will encourage regulatory agencies to explore supervisory tools to ensure that critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry. BITS and the Roundtable will work with other associations to adopt similar statements and to collaborate and coordinate with other critical infrastructure sectors and government agencies.

The policy statement is one in a series of steps by members of BITS and the Roundtable to address mounting concerns and skyrocketing costs related to software vulnerabilities and management of software patches. In a 2004 survey, the associations found that dealing with software vulnerabilities and “patching” systems costs BITS and Roundtable members close to \$400 million annually. Projecting this cost to the entire financial services industry, the cost is approaching \$1 billion annually.

“BITS and the Roundtable have already taken major strides in addressing software security,” said Thomas A. Renyi, Chairman and Chief Executive Officer of The Bank of New York Company, Inc. and Chairman of the BITS Board of Directors. “This policy is another critical step in advancing our industry’s interests to address the security of software products for the safety and soundness of our customers and the nation.”

“The future of our industry is integrally linked to the quality of the products that financial institutions buy from software vendors. As a result, the software industry must work with its clients to do more to meet the high security needs of financial institutions,” said Don Shepard, Chairman of the Executive Board and CEO of AEGON N.V. and Chairman of The Financial Services Roundtable.

“Financial institutions are ultimately responsible for ensuring the safety and soundness of financial services, but this is a shared responsibility,” said BITS CEO Catherine A. Allen. “BITS is working closely with key vendors and stakeholders in other critical infrastructure sectors to see that the products offered to our members are safe and reliable, and will not burden companies with applying costly fixes. Meeting the financial services industry’s business requirements will go a long way to achieve this goal.”

Financial Services Roundtable President and CEO Steve Bartlett said, “In the post 9/11 environment, it’s important that software providers step up their game and produce products that meet the needs of financial institutions and other critical infrastructure companies. Any steps software providers can take to reduce the impact of viruses, worms and hacking will reduce risks and enhance security in cyberspace.”

In February, BITS and FSR held an invitation-only event to facilitate dialogue among key leaders about software security and patch management issues. The agenda featured panel discussions and question-and-answer sessions on risk management costs, cross-sector approaches, public policy options, and legal and regulatory issues. Participants continue to work together to discuss the issues and implement solutions.

BITS has been addressing software security since its founding in 1996. In 1999, its Security and Risk Assessment (SRA) Working Group developed security criteria for products used in the financial services industry. That project resulted in the BITS Product Certification Program, used today to test the security of products offered to financial services companies. The BITS Product Certification Program is a venue for testing products used in the financial industry against industry-established security criteria. The *BITS Tested Mark* is awarded to products that meet those criteria.

### **About BITS**

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to [www.bitsinfo.org](http://www.bitsinfo.org).

### **About The Financial Services Roundtable**

The Financial Services Roundtable ([www.fsround.org](http://www.fsround.org)) represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine accounting directly for \$10.2 trillion in managed assets, \$888 billion in revenue, and 2.0 million jobs.

### **Contact**

Susanna Space, 505-466-6434 or [susanna@fsround.org](mailto:susanna@fsround.org)

# BITS

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

---

## SOFTWARE SECURITY

---

Security is a fundamental building block for all financial services. It is also a regulatory requirement. The financial services industry relies upon software to operate complex systems and provide services, as well as to protect customer information.

Financial services companies comply with a host of legal and regulatory requirements to ensure the privacy and security of customer information. Recently, the prevalence of security risks, threats and viruses, combined with a lack of accountability for software vulnerabilities, has saddled financial institutions with significant risks and skyrocketing costs.

In early 2004, BITS surveyed its members to estimate the costs to financial institutions of addressing software security and patch-management problems. Based on the survey, BITS and Financial Services Roundtable members pay an estimated \$400 million annually to deal with software security and patch management. Extrapolated to the entire financial services industry, these costs are approaching \$1 billion annually.

The members of BITS and The Financial Services Roundtable believe:

- Because the financial services industry plays a central role in the nation's critical infrastructure and is dependent on the products and services of software providers, such providers of mission critical software to the financial services industry need to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure and should exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.
- Software vendors should ensure their products are designed to include security as part of the development process using security-trained and security-certified developers on product development and lifecycle teams.
- Software vendors should ensure through testing that their products meet quality standards and that financial services security requirements are met before products are sold.
- Software providers should develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
- Software vendors should continue patch support for older, but still viable, versions of software.
- Collaboration and coordination among other critical infrastructure sectors and government agencies are essential to mitigate software security risks.

The members of BITS and The Financial Services Roundtable:

- Support measures that make producers of software more accountable for the quality of their products.
- Support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.
- Seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for software and hardware that they purchase.
- Encourage regulatory agencies to explore supervisory tools to ensure that critical third-party service providers and software vendors deliver safe and sound products to the financial services industry.
- Support and incorporate, where possible, the BITS Product Security Criteria into security policies, and encourage technology vendors to test products to meet these criteria.
- Apply a risk-management approach to software security by assessing risks and applying appropriate tools and best practices to ensure the most secure deployment and application of software possible across the entire enterprise.
- Participate in and support efforts to strengthen the Financial Services Information Sharing and Analysis Center (FS/ISAC) in order to share vulnerability information on the products deployed by financial institutions.
- Educate policy makers on the significance of the risks posed to the financial services sector and other critical infrastructure industries and the need to take action to mitigate these risks.

**BUSINESS REQUIREMENTS  
FOR  
SOFTWARE SECURITY AND PATCH MANAGEMENT**

Members of BITS and The Financial Services Roundtable believe software vendors should take responsibility for the quality of their products. Especially when selling products to companies that are within critical infrastructure industries, certain minimum requirements should be met. Following are recommended critical infrastructure sector Business Requirements.

**Provide a higher “duty of care” when selling to critical infrastructure industry companies.**

To meet this higher duty of care, vendors should:

- Make security a fundamental component of software design.
- Support older versions of software (e.g., NT), particularly if existing programs are functional and not past the end of their estimated life cycle.
- Make upgrading easier, less cumbersome and less costly, and offer more support.
  - Products should be less prone to failure and have an automated back-out feature.
  - Components (including embedded components used in other products) should be clearly defined in order for the customer to assess the cascading effect of the upgrade or installation.
- Publish metrics on security of new and existing products.
- Expand coordination and establish better communication with individual clients and industry groups.
  - Vendors should give customers an aggressive “patch playbook” which would provide clear guidance and explicit instructions for risk mitigation throughout the patch management process and especially in times of crisis.
  - Vendors should offer critical infrastructure customers access to one-on-one, private, early vulnerability notice prior to notifying the general public, possibly by establishing “preferred” customer levels. (Some vendors offer financial institutions advanced notification if they agree to serve as a “beta” site, however, this is not practical as an industry-wide solution.)
- Provide better security-trained and security-certified developers on product teams.
- Establish Regional Centers of Excellence to service major financial institutions in their area. Centers would keep IT profiles for each institution in order to:
  - Inform institutions of the likely effects of a new vulnerability on their specific IT environment.
  - Continually advise institutions on how to best apply patches.
  - Expedite patch installation by visiting the financial institution site.
  - Make on site or remote consultation available when patches affect other applications.

**Comply with security requirements before releasing software products.**

Vendors should:

- Meet minimum security criteria, such as BITS software security criteria and/or the Common Criteria.
- Thoroughly test software products, taking into consideration that:
  - Testing needs to address both quality assurance as well as functionality against known and unknown threats.
- Conduct code reviews.
  - Whether conducted internally or outsourced, code reviews should involve tools or processes, such as code profilers and threat models, to ensure code integrity.

**Improve the patch-management process to make it more secure and efficient and less costly to organizations.**

Vendors should:

- Issue patch alerts as early as possible.
- Continue patch support for older software.
  - Vendors should be clear about the level of support provided for each software version.
  - Vendors are strongly encouraged to provide support for up to two versions of older software, i.e., the N-2 level.
- Provide automatic, user-controlled patch-management systems, such as uniform, reliable, and, possibly, industry-standard installers.
- Ensure all patches come with an automated back-out function and do not require reboots.
- Support clients who purchase third-party installer tools (until a standard is established).
- Thoroughly test patches before release.
  - Testing should include patch-to-patch testing to identify any cascade effects and in-depth compatibility testing for effects on networks and applications.
- Issue better patch and vulnerability technical publications. Publications should include more thorough analyses of the impact of vulnerabilities on unpatched systems as well as data on the environments and applications for which the patches were tested. Impact on other patches should also be addressed.
- Conduct independent security audits of the patch-development and deployment processes.
- Distribute a communication and mitigation plan, including how vulnerability/patch information will be relayed to the customer, for use in times of crisis.