

THE FINANCIAL SERVICES ROUNDTABLE



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

SOFTWARE SECURITY TOOLKIT

FEBRUARY 2004

TABLE OF CONTENTS

Introduction to Toolkit.....	1
Talking Points for Communications with Software Executives	2
Business Requirements for Software Security and Patch Management.....	4
Sample Email Cover for Business Requirements.....	6
Sample Procurement Language for Financial Institutions.....	7
Member Survey of Estimated Costs	8
Talking Points for Communications with Media	9
Press Release Issued February 4, 2004	11

BITS

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

SOFTWARE SECURITY AND PATCH MANAGEMENT INTRODUCTION TO TOOLKIT

Senior leadership from our industry, software providers, other business sectors and government are in agreement that the issues around software security and patch management are critical and require urgent attention.

This is an issue that one institution can't address alone. We need to launch CEO to CEO dialogue, backed up by specifics, in order to achieve the level of software security that meets our needs in the financial services industry. The attached documents have been developed to serve as tools for use in communications.

CEO Talking Points with Vendors

Points which can be used in communications with software vendor CEOs, CIOs and other senior executives in the software industry.

Business Requirements

Outlines detailed financial services industry requirements for software vendors:

- Higher “duty of care” by software vendors that sell to critical infrastructure industry companies.
- Compliance with security requirements before software products are released.
- A patch-management process that is more secure and efficient, and less costly to organizations.

Sample Email Cover

Draft language for a cover email that can be used to transmit the Business Requirements.

Sample Procurement Language

Recommended language to incorporate into software procurement specifications issued by financial institutions to potential vendors.

Cost Dimension Survey Overview

Results of a 2003 survey of BITS members on the estimated costs to financial institutions when addressing software security and patch management problems.

Media Talking Points

Talking points which can be used in communications with the media about BITS’ software security and patch management initiative.



SOFTWARE SECURITY AND PATCH MANAGEMENT TALKING POINTS FOR COMMUNICATIONS WITH SOFTWARE EXECUTIVES

BITS recommends the following language for use by BITS and Roundtable member CEOs and CIOs when communicating with software vendor CEOs, CIOs and other senior executives in the software industry.

Company X is among our most valued partners when it comes to software products. You do excellent work. That's why we buy your products.

Software security and patch management issues are top-of-mind for me and my fellow financial service CEOs/CIOs/executives.

The current level of risk is unacceptable. Software vulnerabilities are out of control. Damage from the SoBig and Slammer viruses in 2003 alone cost companies in North America billions of dollars.

Security experts are predicting 2004 to be our most challenging year yet for cybersecurity. MyDoom's release in January—the fastest spreading worm to date—is an example. I don't need to tell you that hackers and fraudsters are growing savvier. They're coming up with new ways all the time to exploit vulnerabilities and trick unsuspecting customers of financial services. All of this creates a climate of unacceptable risk with enormous potential to impact consumer confidence.

Patching is burdensome and outrageously expensive. In 2003, we had to patch more than 40 "critical" or "important" flaws from one major software provider alone. BITS conducted a survey of BITS and Roundtable member institutions to get an estimate of what it costs us to address software security risks, including patch management. We estimate that it is costing our members—who hold about 50% of the nation's financial assets—close to \$400 million, and can extrapolate the cost to the entire financial services industry to be approaching \$1 billion. This is money we'd far rather be spending in other ways.

Financial institutions are a target. We were a target on September 11, 2001 and the financial services industry is still a target now. If we're vulnerable, the country is vulnerable. Our reputations, our customers, and our nation rely on the strength of our systems. We are one of the nation's critical infrastructure sectors. It is essential that our software is safe, sound, secure and resistant to all the attacks that come our way.

We need your commitment to serve the business requirements of the financial services sector and other critical infrastructure sectors. We need to have:

- A higher “duty of care” when you sell to critical infrastructure industry companies, like ours.
- Compliance with security requirements before software products are released.
- A more effective and secure patch-management process that is less cumbersome and less costly.

BITS members have come up with a detailed set of business requirements. I invite you to take a look at them. Can I send them to you?

If we can’t solve these problems cooperatively in a cross-industry setting like this, we’re likely to see action from legislators and regulators.

My colleagues and I are in discussion with a number of top software companies. I encourage you to spread the word about these issues of concern within your institutions and among your peers, and stress the importance of meeting the critical infrastructure sector Business Requirements.

I urge you to take action now.

BITS

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

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.

BITS

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

SOFTWARE SECURITY AND PATCH MANAGEMENT PROJECT SAMPLE EMAIL COVER FOR BUSINESS REQUIREMENTS

To: Software Provider CEO
From: Financial Institution CEO/CIO/CISO
Subject: Financial Services Industry Software Security Business Requirements

Software security and patch management are major concerns for the financial services industry and other critical infrastructures. Based on a survey of member companies, BITS estimates the impact to the financial services industry from software vulnerabilities and patch management is approaching \$1 billion on an annual basis.

In response to these issues, BITS has embarked on a major initiative to strengthen software security and the patch-management process. We would like to work with your company to achieve three goals outlined in more detail in the attached Business Requirements document:

- Meet a higher duty of care when selling products to critical infrastructure companies such as financial services companies.
- Comply with security requirements **before** software products are released.
- Make the patch management process more secure, more efficient and less costly.

The financial services industry cannot achieve these objectives without your help. We are committed to working with you and would like to schedule a meeting to discuss these business requirements with you.

Sincerely,



**SAMPLE PROCUREMENT LANGUAGE FOR FINANCIAL INSTITUTIONS
BITS PRODUCT CERTIFICATION PROGRAM
AND SOFTWARE SECURITY INITIATIVE**

The following is sample language. It is recommended for incorporation within software procurement specifications issued by financial institutions to potential vendors.

Financial institution X prefers products that meet or exceed the baseline security features established under the BITS Product Certification Program (BPCP). BPCP criteria are posted at www.bitsinfo.org.

Please describe, for products to be provided under this agreement, the status of your efforts to bring the product into compliance with the BITS criteria and your plans to have these products tested and certified under the BPCP.

If your product is selected and has not been awarded the *BITS Tested Mark*, please indicate your plans to initiate testing and certification within three months of your acceptance of this agreement. If testing criteria does not currently exist for your product type, indicate your plans to initiate testing when criteria become available.

For products provided under this agreement that have not attained the *BITS Tested Mark* and for which there is no current plan to test, specify how you will demonstrate validation of your compliance with BITS' baseline security requirements.

It is financial institution X's intent to use third-party products that have been awarded the *BITS Tested Mark*. In the event financial institution X selects a product that has not been awarded the *BITS Tested Mark*, and for which the BITS Product Certification Program has applicable testing criteria (i.e., a security product profile or Common Criteria security package), the vendor will commence testing of the product using the BITS testing criteria within 90 days of contract award. Should the testing not result in a *BITS Tested Mark*, a summary of the test results, including passing and failing components, will be presented to financial institution X.

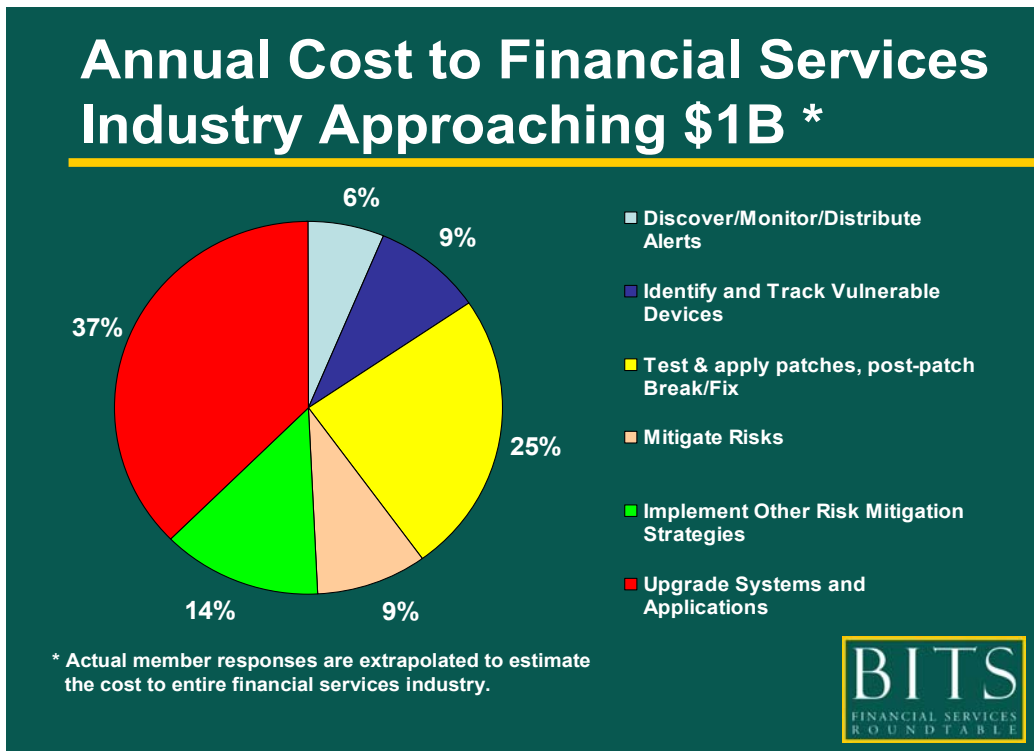
SOFTWARE SECURITY AND PATCH MANAGEMENT MEMBER SURVEY OF ESTIMATED COSTS

BITS surveyed its members in late 2003 on the estimated costs to financial institutions when addressing software security and patch management problems. Results are kept confidential and were analyzed to determine the estimated total annual cost to BITS and Roundtable member institutions. These figures were then extrapolated to estimate the overall annual cost to the financial services industry.

High Level Results:

- Software vulnerabilities are approaching a cost of \$1 billion annually to the financial services industry.
- BITS and Roundtable member companies pay an estimated \$400 million annually to deal with software security and patch management issues.
- Just managing patches—which is only a fraction of what we do to deal with vulnerabilities—costs BITS and Roundtable members an estimated \$55 million annually and costs the industry an estimated \$110 million annually.
- Patch management and implementation alone can cost one financial institution millions of dollars annually.

Percentage Breakdown of Annual Costs:



BITS

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

SOFTWARE SECURITY AND PATCH MANAGEMENT TALKING POINTS FOR COMMUNICATIONS WITH MEDIA

BITS recommends members use the following talking points in communications with the media about BITS' software security and patch management initiative.

BITS and our member financial services companies are aggressively responding to increasing concerns about security risks resulting from software vulnerabilities. This is a critical, high-level issue across the financial services industry.

- Security is a fundamental building block for all financial services and a regulatory requirement.
- The prevalence of security risks combined with a lack of accountability for vulnerabilities has escalated both risks and costs to the financial services industry.
- Internet viruses and worms are becoming increasingly virulent and expensive.
- The Slammer worm was the fastest-spreading worm in history, prior to the recent Mydoom worm, which spread even faster.
- Damage from 2003's SoBig virus cost billions of dollars to repair, making it one of the costliest viruses yet.
- In 2003, the most commonly used software provider released patches for more than 40 "critical" or "important" flaws.
- To mitigate risk to customers and prevent damage to company systems, financial institutions must implement patches, which can cost a company millions of dollars annually.

The BITS Software Security and Patch Management Initiative has three primary goals.

- Encourage a higher "duty of care" by software vendors that sell to critical infrastructure industry companies.
- Promote compliance with security requirements before software products are released.
- Make the patch-management process more secure and efficient, and less costly to organizations.

BITS and Roundtable members are taking action.

- Developing best practices for managing software patches.
- Encouraging the software industry to notify companies of vulnerabilities as early as possible.
- Communicating clear industry business requirements for secure software products.
- Facilitating CEO-to-CEO dialogue between the software and financial services industries as well as other critical infrastructure sectors.
- Analyzing industry costs.
- Communicating to the federal government the importance of investing to protect critical infrastructure industries.
- Exploring potential legislative and regulatory remedies.

We have brought these issues to the attention of the major software providers.

- BITS' goal is to foster dialogue and produce solutions that are effective, equitable, and achievable in the near term.

The BITS Product Certification Program (BPCP) is a cornerstone of our efforts.

- The BPCP tests software against baseline security criteria established by the financial services industry to help ensure the security of application products and the supporting infrastructure used by financial institutions.
- With criteria aligned with the Common Criteria, the BPCP is one way BITS influences the vendor community to include security considerations in the development process.
- Created by BITS to improve the security of software products used in the financial services industry, the *BITS Tested Mark* indicates to financial services companies that a product has passed BITS Product Certification Program (BPCP) testing. Since its inception, BITS has announced that Archer Technologies' Archer SmartSuite Framework Version 3.0 and HP's VirtualVault have earned the *BITS Tested Mark*. With product security issues top of mind, software vendors and financial institutions are increasingly interested in meeting the criteria.

BITS (www.bitsinfo.org) 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 and FSR represent the 100 largest integrated financial services companies. BITS provides intellectual capital to address emerging issues where financial services, technology and commerce intersect. BITS' Board of Directors is made up of the Chairmen and CEOs of twenty of the largest U.S. financial services companies, as well as representatives of the American Bankers Association and the Independent Community Bankers of America.

The Financial Services Roundtable (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 \$12.4 trillion in managed assets, \$561 billion in revenue, and 1.8 million jobs.

For more information, contact John Carlson, senior director, john@fsround.org, Faith Boettger, senior consultant faith@fsround.org, or Ann Patterson, director, ann@fsround.org.

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

**For Immediate Release
February 4, 2004**

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

**NATION'S LARGEST FINANCIAL INSTITUTIONS
HOLD CYBERSECURITY SUMMIT
BITS and The Financial Services Roundtable
Advance Security Agenda, Urge Software Companies to Make Products Safer**

ARLINGTON, Va., February 4, 2004 – Leaders of the nation's largest financial institutions outlined steps to address software vulnerabilities and patch management issues affecting the industry at a joint BITS and Financial Services Roundtable Summit today. The BITS/FSR Software Security CEO Summit is one step in members' collective response to mounting concern about software vulnerabilities and management of patches that have been issued by software vendors to fix flawed code.

Speaking to the crowd of more than 80 executives representing financial services, other critical infrastructure industries, software companies, and government, James E. Rohr, Chairman and Chief Executive Officer of The PNC Financial Services Group, Inc. and Chairman of the BITS Board of Directors, laid out the software security landscape in his keynote address. Mr. Rohr said the financial services industry was not alone in being affected by software security issues and he emphasized the importance of collaborating with other critical infrastructure industries and government to identify solutions.

Outlining the cost impact to financial institutions, Mr. Rohr said addressing software vulnerabilities costs BITS and FSR members close to \$400 million annually, with the total cost to the industry approaching \$1 billion annually. BITS members, he said, hold about \$9 trillion of the nation's total assets of about \$18 trillion.

BITS' efforts have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-

management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them.

“BITS has already taken major strides in addressing software security,” said James E. Rohr, Chairman and Chief Executive Officer of The PNC Financial Services Group, Inc. and Chairman of the BITS Board of Directors. “This Summit 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.”

“Financial institutions are ultimately responsible for ensuring the safety and soundness of financial services,” said Ms. Allen. “We are working with vendors to see that the products offered to our members are safe and reliable, and will not burden companies with applying costly fixes.”

The invitation-only event was held primarily 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 shared their perspectives and worked together to identify solutions.

BITS has been addressing software security since 1999, when 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. BITS’ efforts are spearheaded by BITS’ Security and Risk Assessment group, whose members represent more than 70 of the nation’s largest banking, securities and insurance organizations. Since its inception in 1996, the SRA Executive Committee and Working Group have swiftly galvanized the industry to address challenges, coordinate industry response, and champion key causes.

The BITS Product Certification Program provides a cornerstone to these efforts. The 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.

The Summit followed The Financial Services Roundtable’s Mid-Winter Conference on February 2 and 3 at the Ritz Carlton Pentagon City in Arlington.

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, BITS Advisory Group and BITS Council. For more information, go to www.bitsinfo.org.

About The Financial Services Roundtable

The Financial Services Roundtable (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.

Contact

Susanna Space, 505-466-6434 or susanna@fsround.org

###